



Architecture and Design

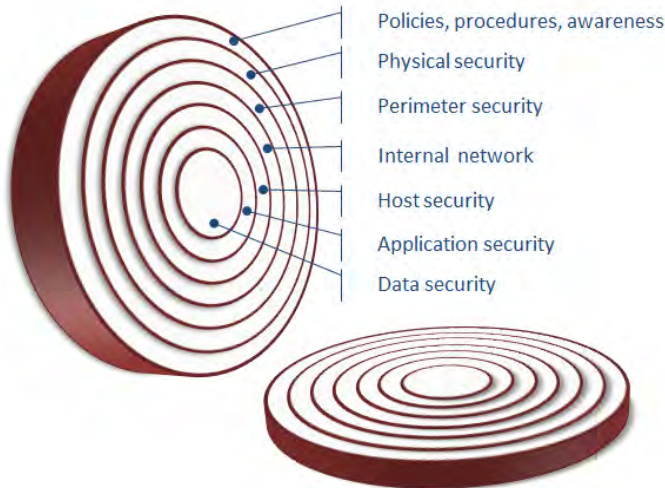
Domain 2 – 21%



1

1

Defense in Depth



When dealing with threats, the assumption should always be that any layer can be violated. Thus, protection must be provided by the sequential layers.

Image courtesy of: Theuns, M. Layering Information Security Controls. <http://www.content-loop.com/layering-information-security-controls/>



2

2

Security Controls

Administrative, technical, and physical controls should work in a synergistic manner to protect a company's assets



Administrative	Policies/procedures including onboarding, off boarding, and backup media
Technical	Hardware, software, firewall, active directory, authentication, and disk encryption
Physical	Doors, locks, fences, and cameras



3

3

Security and Risk Frameworks

COBIT

Created by Information Systems Audit and Control Association (ISACA) with IT Governance to assist businesses develop, organize and implement operating procedure. COBIT can be used at the highest level of IT governance, providing an overall control framework based on an IT process model including security, risk management and information governance

ISO 27000 Series

A family of international standards developed by International Organization for Standardization/International Electric Technical Commission for managing sensitive company information. It contains 133 detailed information security controls based upon 11 focus areas. The guidelines provide a roadmap to meet ISO certification. The 2014 published ISO/IEC 27001:2013 – Information technology – Security techniques – Information security management systems – Requirements, which helps manage cybersecurity.

NIST SP 800 Series

National Institute of Standards and Technology (NIST) series is a set of documents that provide the structure for policies, procedures, and guidelines for federal government assets. Each series covers a specific area concentration including NIST SP 800-30 focuses on Information System Risk Management, NIST SP 800-39 focuses on organizational risk management, and NIST SP 800-66 was written specifically for HIPPA.

RMF / CMMC / DFARS

The Risk Management Framework (RMF) associated with the NIST SP 800-37 guide for "Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," which has been available for Federal Information Security Management Act (FISMA) compliance since 2004.



4

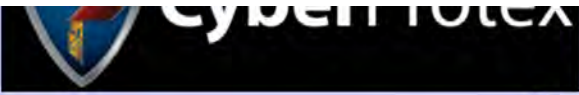
4

Frameworks

Framework	Description
Total Quality Management	A structured approach to improve the quality of goods and services through continuous improvement of internal practices
ISO	Code of practice for information security management
ITIL	Set of best practices for IT service management
COSO	Managing internal risks by identifying relevant vulnerabilities and determining impact

Frameworks

Framework	Description
COBIT	Sets control points are used by organizations meeting Sarbanes-Oxley Act
Six Sigma	A disciplined, statistical-based, data-driven approach for eliminating risks and establishing continuous improvement
CMMI	Capability Maturity Model Integration used to guide process improvement across a project - Initial, Managed, Defined, Quantitatively Managed, and Optimizing
Basel II	International business standard that requires financial institutions to maintain reserves to cover risks


hackme.cyberprotex.com

Production

Version: 2.6.42 Security Level: 0 (Hosed) Hints: Enabled (1 - 5cr1pt K1dd1e) Not Logged In

[Home](#) | [Login/Register](#) | [Toggle Hints](#) | [Show Popup Hints](#) | [Toggle Security](#) | [Enforce SSL](#) | [Reset DB](#) | [View Log](#) | [View Captured Data](#)

OWASP 2017

OWASP 2010

OWASP 2007


Web Services

HTML 5




Others

Documentation

Resources


Video Tutorials

Login

 [Back](#)
  [Help Me!](#)
 SQL = Structured Query Language
  SELECT *
UPDATE *
DELETE *


Hints and Videos


```

btnLogin_OnClickEvent(){
  txtUserName.value
  txtPassword.value

  SELECT * FROM Users
  WHERE
  Username = ' OR 1=1
  AND
  Password = txtPassword.value
        
```

Please sign-in

Username  txtUserName.value

Password  txtPassword.value

Dont have an account? [Please register here](#)

7

' or ('a' = 'a' and username='lacey') or '

8

8

Laws, Directives, and Regulations

- The Sarbanes-Oxley Act (SOX)
- The Health Insurance Portability and Accountability Act (HIPAA)
- The Gramm-Leach-Bliley Act of 1999 (GLBA)
- The Computer Fraud and Abuse Act
- The Federal Privacy Act of 1974
- Payment Card Industry Data Security Standards (PCI-DSS)
- The Computer Security Act of 1987
- The Economic Espionage Act of 1996



How it Fits Together

Industry	Regulation	Audit Framework	Best Practices
Publicly Traded Company (NYSE, NASDAQ)	Sarbanes Oxley (SOX, SARBOX)	COSO, SAS70, COBIT	GAAP, ISO, CIS
Hospital, Medical	Health Insurance Portability and Accountability Act (HIPAA)	COBIT, FISCAM	ISO, CMS, NIST
Credit Card Merchant, Broker, or Clearinghouse	Payment Card Industry (PCI)	COBIT	SANS, ISO, CIS



DUE CARE vs DUE DILIGENCE

DC = Do Correct

DD = Do Detect

11

Compliance

Legal and Regulatory
Issues

Privacy requirements



12

Build a Legal Wall



- Intellectual Property Laws
- Trade Secret
- Copyright law
- Trademark
- Patents

PRIVACY PROTECTION

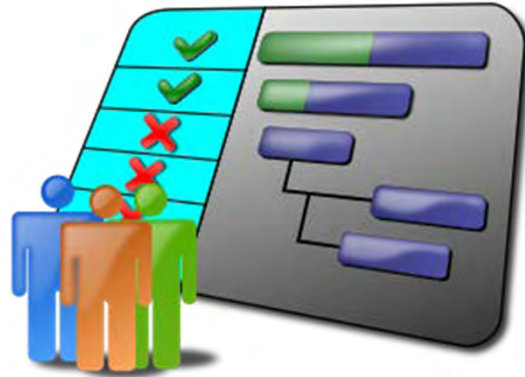
Methods vary and include:

- Individual users: Passwords, encryption, awareness
- Self-regulation: PCI DSS
- Laws on corporations: HIPAA, HITECH, GLBA, PIPEDA
- Laws on government: FPA, VA ISA, USA PATRIOT



Liability

- Personal Information
 - Legally recognized obligation
 - Failure to conform to the required standard
- Proximate causation and resulting injury or damage



Configuring a Network Security Topology

- Consider the following elements when wanting to secure a network:
 - ✓ Demilitarized Zones (DMZ)
 - ✓ Subnetting
 - ✓ Virtual Local Area Networks (VLANs)
 - ✓ Remote Access
 - ✓ Network Address Translation
 - ✓ Voice Communications
 - ✓ Network Access Control (NAC)

Network Hardening

➤ Network hardening activities:

- ✓ MAC Limiting & Filtering *
- ✓ 802.1X Security
- ✓ Disable Unused Ports (Physical)
- ✓ Disable Unused Services / Applications
- ✓ System Updates & Service Packs
- ✓ Identification of "Rogue" Systems
- ✓ Continuous Security Monitoring
- ✓ Remediation Policy (i.e. Audits)
- ✓ Incident Handling, Response, & Reporting
- ✓ Firewall (i.e. Port Blocking and Disabling)
- ✓ Account Disable vs. Deletion

➤ There are a number of excellent online guides to help harden systems and reduce the organizational surface area *

* <https://www.sans.org/score/checklists>



17

17

Demilitarized Zone

➤ A DMZ is an untrusted area where organizational assets can be more easily accessed from the internet

➤ The DMZ prevents into more sensitive organizational networks

➤ The DMZ has three interfaces that MUST be correctly configured to ensure security:

- ✓ Internal Network
- ✓ Internet
- ✓ DMZ

➤ Any time a host is placed outside of the DMZ, this is commonly referred to as a Bastion Host



18

18

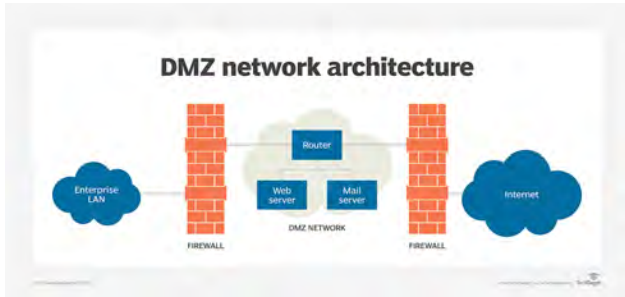


Image courtesy of: <https://searchsecurity.techtarget.com/definition/DMZ>

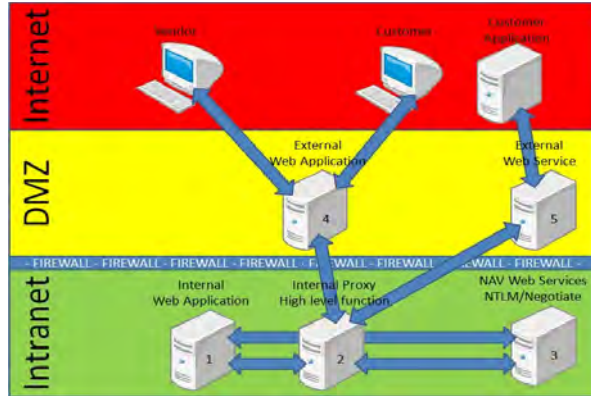
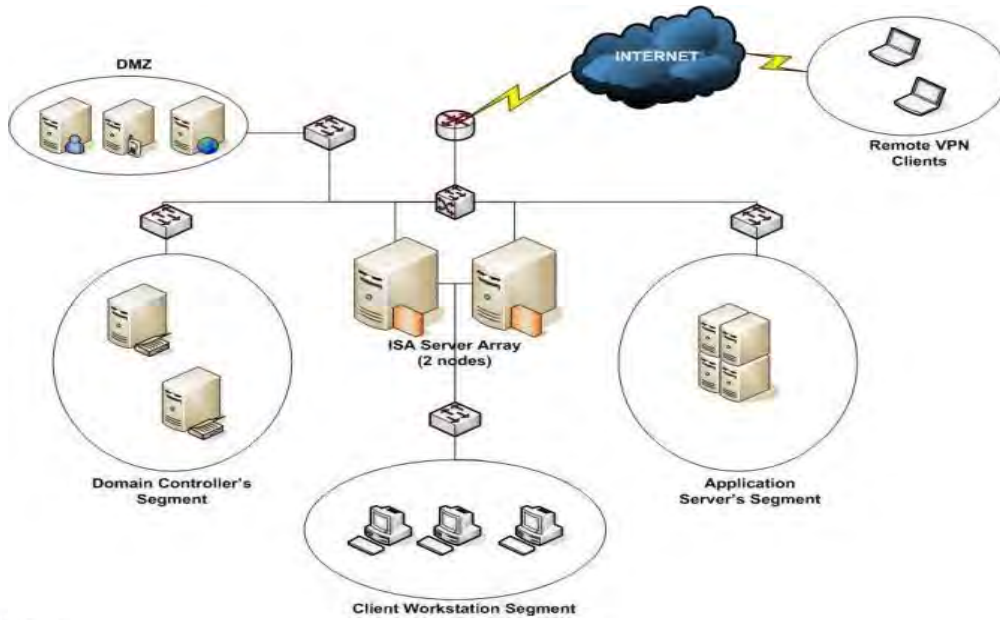


Image courtesy of: <https://blogs.msdn.microsoft.com/freddyk/2010/01/30/web-services-infrastructure-and-how-to-create-an-internal-proxy/>



Network Hardening - Addressing

➤ In order to obtain information about network parameters on a system, there are some easy to use command-line tools

- Windows
 - ✓ ipconfig
 - ✓ ipconfig /all
- Linux
 - ✓ ifconfig
 - ✓ ifconfig -a

```
eth0    Link encap:Ethernet  HWaddr 00:00:27:0F:00:00
        inet6 addr: fe80:a0:27ff:fe0f:8a74 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:6 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:0 (0.0 b)  TX bytes:468 (468.0 b)
        Interrupt:19 Base address:0x0020

lo      Link encap:Local Loopback
        inet addr:127.0.0.1  Mask:255.0.0.0
        inet6 addr: ::1/128 Scope:Host
        UP LOOPBACK RUNNING  MTU:16436  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
        RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

virbr0  Link encap:Ethernet  HWaddr 52:54:00:75:C2:9B
        inet addr:192.168.122.1  Bcast:192.168.122.255  Mask:255.255.255.0
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:0 errors:0 dropped:0 overruns:0 frame:0
        TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0
```



Network Hardening – Remote Access

➤ When considering how to harden a system or network, it is important to identify any necessary remote access protocols and tools such as:

- ✓ Remote Procedure Call (RPC) - Graphical
- ✓ Virtual Network Computing (VNC) - Graphical
- ✓ Secure Shell (SSH) - Shell
- ✓ Secure Copy (SCP) – Shell and Graphical



Tools Supporting Network Security

	Firewall	Intrusion Detection System(IDS)	Intrusion Prevention System (IPS)
Definition	Filters traffic based on IP address and port numbers – first line of defense	Monitors traffic for malicious activity or policy violations	Inspects real time traffic, classifies, and then proactively stops malicious traffic from attack
Placement	Placed at the perimeter	Placed after the firewall - Inline or as end host (via span) for monitoring and detection	Placed after the firewall - Normally at layer 2 inline mode
Action	Blocks traffic by port and protocol rules	Alerts or alarms with a detection of anomaly	Alerts and reacts to detection of anomaly
Types	Stateful packet filtering	Anomaly based detection Signature detection Zero day attacks Monitoring Alarm	Anomaly based detection Signature detection Zero day attacks Blocking the attack



23

23

Detection vs. Prevention

- Detection – Emplacing systems throughout your hosts and / or network to identify specific types of activity
- Prevention – Active measures that make specific modifications to system and network settings to prevent an activity from occurring
- Detection and Prevention Systems
 - ✓ Authentication Systems
 - Windows (Kerberos)
 - Linux (/var/log/secure /var/log/auth.log, /var/log/faillog)
 - ✓ Host-based Intrusion Detection System (HIDS)
 - ✓ Host-based Intrusion Prevention System (HIPS)
 - ✓ Network-based Intrusion Detection System (NIDS)
 - ✓ Network-based Intrusion Prevention System (NIPS)
 - ✓ Honeypot (Purposely made to appear to be insecure)



24

24

Honeypot - Legal

➤ Although honeypots are effectively utilized across many organizations there are some legal issues to consider

- ✓ Enticement – luring someone toward certain evidence after that individual has already committed the crime
- ✓ Entrapment – encouraging someone to commit a crime that the individual may have had no intention to commit



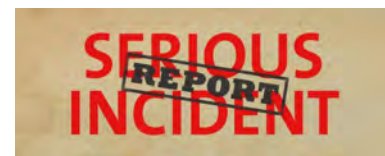
25

25

Network Hardening – Reporting

➤ Some important terms to consider when reporting incidents

- ✓ Alarms – Indication of an ongoing current problem
- ✓ Alert – System issues, but not as important as an alarm
- ✓ Trends – The current threat trajectory



26

26

System Hardening

- What does it mean to harden an organizations resources?
- System Services
- Peripheral Systems
- Network Shares
- Software



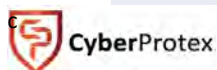
27

27

System Settings

Most security guidelines stress the need to remove unneeded services. A server or system should be dedicated to a particular function. In addition to increasing the speed of the system and helping to debug third party applications, removing or disabling unneeded services has multiple security advantages.

- Every service adds a risk to the security posturing.
- Removing/disabling unneeded services lessen the probability of incompatibility
- Limiting the number of services creates a cleaner configuration and aids in management
- Limiting the number of services reduces patch management
- Customizing the number of services promotes a functionality delineation among the servers and supports public facing versus private



28

28

Filesystems

➤ The following filesystems are used across different operating systems:

- ✓ File Allocation Table (Windows – Legacy)
- ✓ New Technology Filesystem (Windows – Current)
- ✓ ext2, ext3, ext4 (Linux)
- ✓ XFS (Linux)
- ✓ Hierarchical File System (Mac)
- ✓ Hierarchical Extended File System (Mac)



29

29

Default Accounts and Passwords

Action	Description
Change default passwords	Default passwords must be changed before deployment
Use unique default passwords	Vendors should design systems using unique default passwords which could be based on the customer or system type
Use alternative authentication mechanisms	Use alternative authentication mechanisms like Kerberos or multifactor authentication should be implemented
Force default password changes	Force a reset at first use of the account
Restrict network access	Restrict both ingress and egress access
Identify product which might have default passwords	Include software, systems, and services



30

30

Programming Languages

Scripting Languages	Programming Languages
Bash (Bourne Again shell) Csh (C shell) JavaScript Ksh (Korn shell) MS-DOS batch files Perl Python Ruby Sh (Bourne shell) Tcl	Assembler BASIC C C++ C# FORTRAN ADA Forth Java LISP Modula-2,/Modula-3 Oberon Pascal

Compiled		Interpreted/Runtime	
Ready to run	Not cross-platform	Cross-platform	Interpreter needed
Usually faster	Inflexible	Simple to test	Usually slower
Source code is private	Extra steps to compile	Easier to Debug	Source code is public



31

31

Programming Vulnerabilities

Category	Exploit	Countermeasures
Input Validation	Buffer overflow, cross scripting, SQL injections, and canonicalization (normalizing of data)	All strings are truncated with set length and range of possible values
Authentication	Network sniffing, brute force/dictionary attacks, session hijacking and credential theft	Deny telnet, rsh, and other clear text authentication methods
Configuration Management	Unauthorized access Lack of nonrepudiation	Establish clear permissions based on least functionality
Sensitive data	Data access	Establish clear permissions with sensitive data not stored on publicly accessible systems



32

32

Programming Vulnerabilities

Category	Exploit	Countermeasures
Cryptography	Poor key generation Exploited ciphers	Enforce 1024 byte encryption with the removal of broken ciphers
Parameter Manipulation	Manipulation of a query string, form field, cookie, and HTTP header	Set removal of temporary variables, all variables explicitly defined
Exception Management	Information disclosure and denial of service	Define exception handlers with a default of termination of process
Auditing and Logging	Altering of logs	Central log server to house secondary copy of all logs



33

33

Web Applications

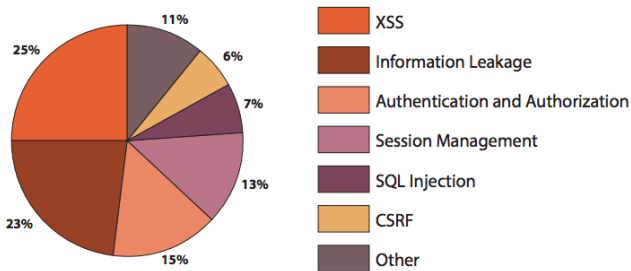


Image Courtesy of: Kumar, C. 12 Online Free Tools to Scan Website Security Vulnerabilities & Malware. <https://geekflare.com/online-scan-website-security-vulnerabilities/>



34

34

Web Applications

Type	Description	Countermeasure
Injection Flaws	Caused by a failure to filter to untrusted input Hacker injects command into the input to steal credentials or take control of session via a buffer overflow	Filter input Whitelist/blacklist sources
Weak Authentication and Session Management	Improper handling or configuration of authentication leads to the following risks: <ul style="list-style-type: none"> • URL containing a session ID to be leaked in a referrer header • Passwords not encrypted for data at rest or data in transit • Session ids are predictable • Fixation of session is possible • Session hijacking from not terminating sessions or failure to implement SSL 	Implement strict guidelines on system and web application guidelines. Use a secure framework to generate code



35

35

Web Applications

Type	Description	Countermeasure
Cross Site Scripting (XSS)	Attacker submits javascript tags as input, which is implemented when a user loads the page	Do not allow hypertext markup language (HTML) tags to be returned to the client Sanitize input to strip away HTML tags using regular expressions on < and >
Insecure Direct Object References	Internal object (file or database key) is visible to the user When authorization is not enforced or broken, the hacker can gain access or modify the form	Implement user authorization and validate input



36

36

Web Applications

Type	Description	Countermeasure
Security Misconfiguration	<ul style="list-style-type: none"> • Debug enabled in protection • Directory listing enabled • Outdated software • Least functionality not implemented • Default passwords enabled • Error handling information is public accessible 	Implement As-Built with secured settings
Sensitive Data Exposure	Data at rest (DAR) and Data in Transit (DIT) are not encrypted	DAR: 1025 byte encrypted DIT: HTTPS with a proper certificate
No Function Level Access Control	Authorization access is not enforced at a function level	Deploy authorization



37

37

Web Applications

Type	Description	Countermeasure
Cross Site Request Forgery (CSRF)	Attack website fools the victim's browser to request information using vetted credentials stored on the victim's computer Typically the script is embedded into a known visited site	Store secret tokens in a hidden form field protected from unauthorized parties
Using or Continued Use of Known Vulnerable Components	Using code without MD5 checks or from open sites as github	Patch Only download from trusted sites
Invalidated Redirects and Forwards	Input filtering issue	Block redirects If supporting redirects, only implement static links Validate user-defined inputs



38

38

Peripherals

Initial Configuration	Change the administrator password Patch the Device Disable unused Functionality Configure Access Control Private network
Continuous Monitoring (at least yearly)	Software level Configuration Regular patching Regular scanning
Disposal/Retirement	Sanitization Repurpose Destruction

Input devices – mouse and keyboard

Storage devices – hard drive and flash drive

Output devices – monitor and printer



39

39

Embedded Systems

Supervisory Control and Data Acquisition (SCADA) / Industrial Control Systems (ICS)

An embedded system is a dedicated computer system (hardware and software elements) designed for one or two specific functions.

Actions:

Control: monitoring, limited, telemetry, and remote/local

Data acquisition: access and acquire information, sends it to a other sites, analog/digital

Vulnerability:

Legacy systems with no outside access for patch management

Examples

Energy	Food and beverage
Manufacturing	Oil and gas
Power	Recycling
Transportation	Water and waste water



40

40

Internet of Things (IoT)

Wirelessly connected sensors can be found embedded in multiple items including refrigerators, auto part, dog collars, and microwaves. Together, these items can provide a coordinated, secure and transparent tracking of transactions and activities for the owner. Unfortunately, these is no requirement for patch management, hardening of the systems, or even directions on how to disable the feature. Thus, the weakest link within the landscape are the unmanaged IoTs.

In October of 2016, the Internet of things (IoT) became the medium for a Trojan horse and facilitated a DDoS throughout the internet. The botnot of infected IoT devices hosting the Mirai Trojan horse is still in existence waiting for the puppet master's signal. Although XiongMai Technologies, the Chinese company responsible for many of the insecure IoT devices, has issued a recall for millions of devices. Unfortunately, the Mirai code has been leaked and is now open source

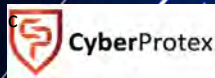
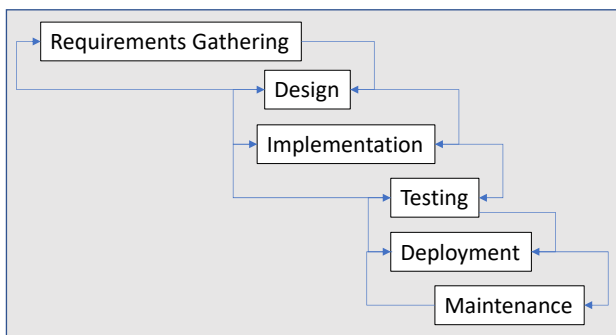


Image courtesy of: <https://martechtoday.com/wp-content/uploads/cld-assets/Internet-of-Things-147x96.png>

41

41

Secure Application Development



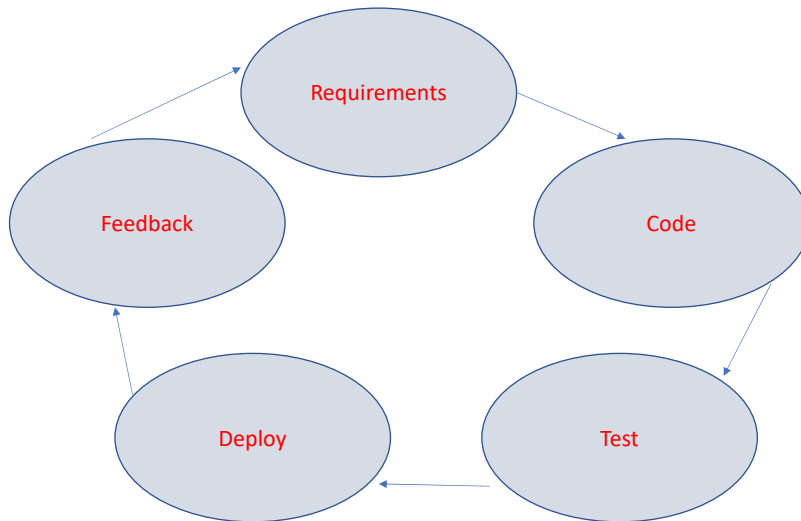
Waterfall Chart is a linear, plan-driven approach is most useful in the aspect of software engineering where the plan and specifications have been defined



42

42

Secure Application Development



Agile stresses rapid changes from end-users and delivers feedbacks of software at the end of each lifecycle through continuous integration and continuous delivery



43

43

Code Quality and Testing

Goal: Find the bugs before the bad guys do

- Static code analyzers
 - ✓ Static Application Security Testing (SAST)
 - ✓ Automation helps, but is not 100%
 - ✓ False positives are an issue
- Dynamic analysis (fuzzing)
 - ✓ Random input
 - ✓ Fuzz Generator
- Stress testing
 - ✓ Overloading (1000 instead of 1)
 - ✓ Inadvertent results in overload
 - ✓ Automation is key
- Sandboxing
 - ✓ Compartmentalize
- Model verification
 - ✓ Verification (does the software work)
 - ✓ Validation (does it meet requirements)

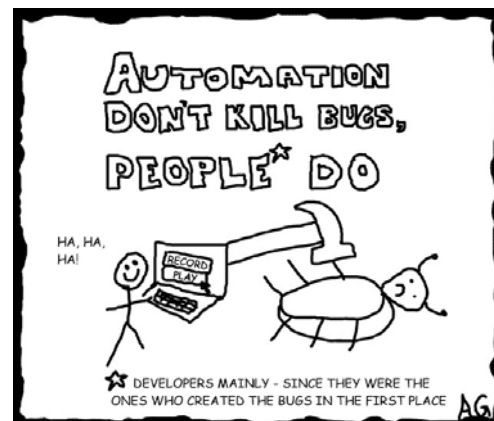


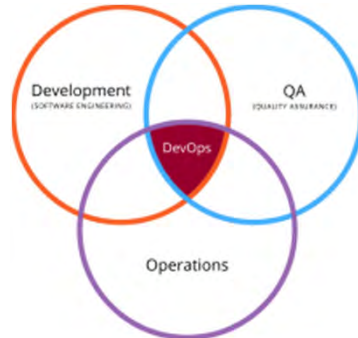
Image courtesy of: <https://i.pinimg.com/736x/f9/4c/5d/f94c5da26dffe616a26e9cf484f19e9c--software-testing-assurance.jpg>



44

44

Secure Application Development



DevOps combines software development with information technology operations. DevOps supports providing features, fixes, and updates frequently in close alignment with business objectives and shortens the systems development life cycle.

Goal: speed, availability, and security



Image courtesy of: <https://en.wikipedia.org/wiki/DevOps>

45

45

What is Cloud Computing?

National Institute Standards and Technology (NIST)

“A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (i.e., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction”

The cloud is just a metaphor for the Internet (from the old days of flowcharts when server farms were drawn similar to fluffy clouds with connections representing inputs/outputs)

Cloud computing is the storing and accessing data and programs over the internet instead of your local computer or network. Within the cloud are multiple systems. Some servers specialize in storage and others are used for computing power.



46

46

Defining Characteristics

<u>Characteristics</u>	<u>Definition</u>
Shared / Pooled Resources	Resources are drawn from a common pool Common resources builds consistency across programs for budgets Common infrastructure
Broad Network Access	Open standards Configurable (IP, HTTP, and other protocols) Simple access with a an internet connection
On-demand Self Service	Automated Users not tied implementation details Near real-time delivery Web interface to access services
Scalable and Elastic	Additionally resources added or released as project demands evolve
Metered by Use	Services are a pay as use May cancel service or suspend at any time



47

47

Defining Functionality

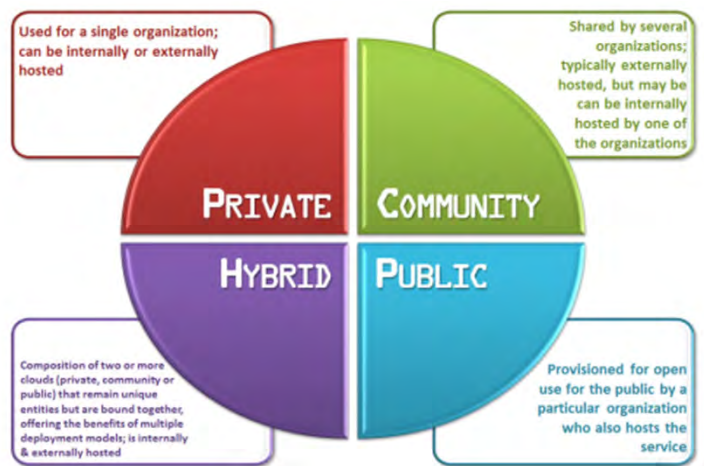
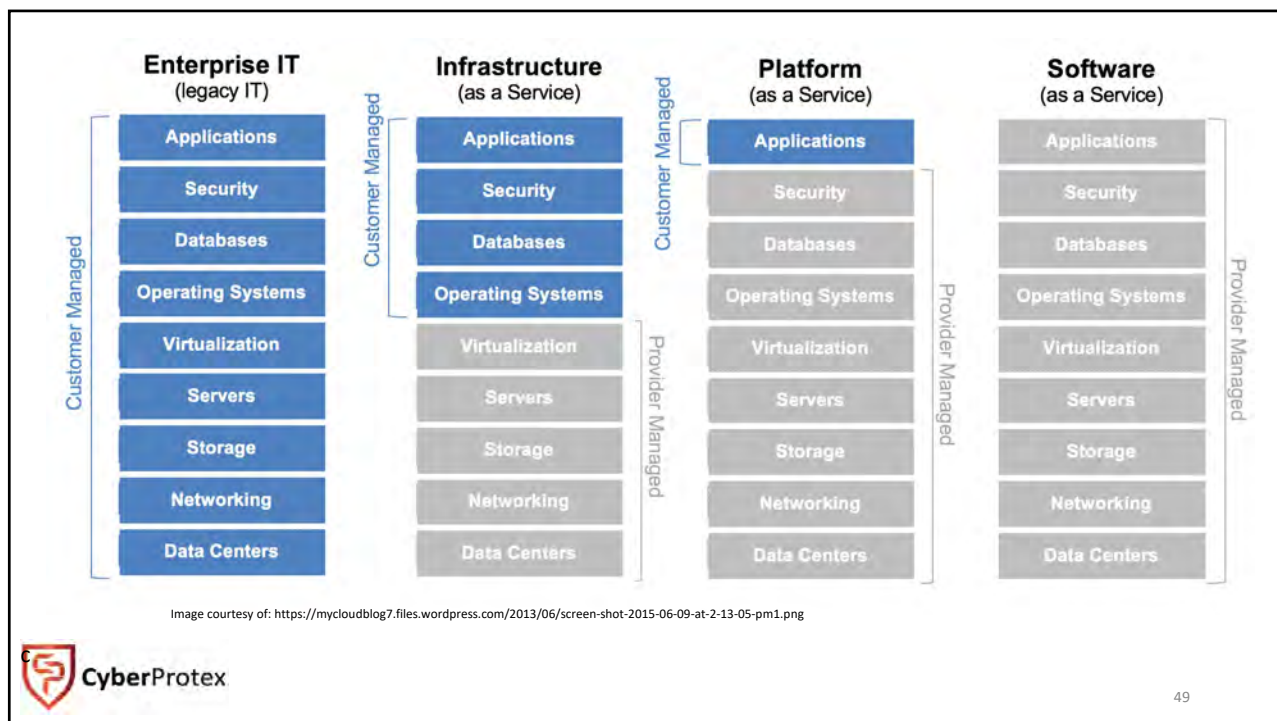


Image courtesy of <https://blog.econom.com/en/blog/why-companies-are-adopting-hybrid-cloud/>

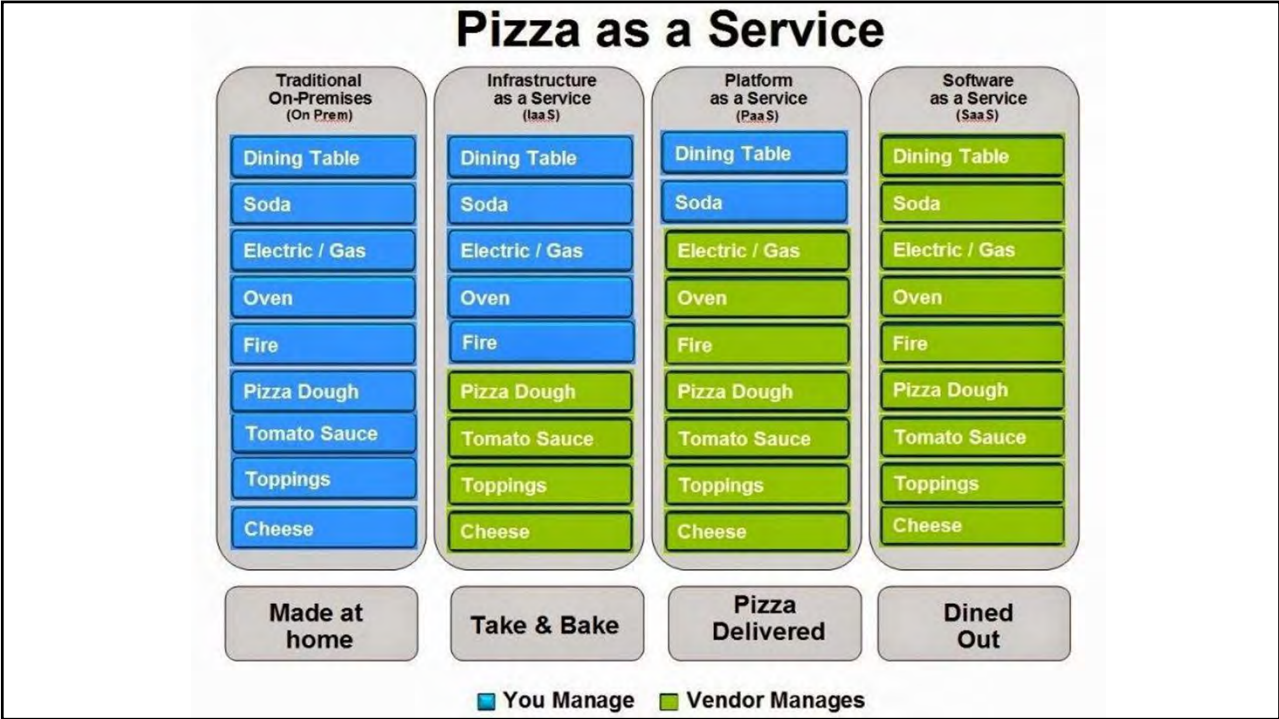
48

48



Examples in the Wild

Model	Examples
PaaS (Platform as a Service)	Google App Engine, and Red Hat's OpenShift
SaaS (Software as a Service)	Email and collaboration, customer relationship management, and healthcare-related applications
IaaS (Infrastructure as a Service)	Amazon Web Services (AWS), Microsoft Azure, Google Compute Engine (GCE), Joyent
SECaaS (Security as a Service)	Palerra (Cloud Access Security Broker CASB), Okta (Single Sign On (SSO)), Proofpoint (Email Security), White Hat Security (Website and App Security)



51

Physical Security Controls

Without physical security, all other forms of security become difficult if not impossible. It encompasses the protection of the building site and all assets (hardware and software) from theft, vandalism, natural disaster, and manmade catastrophes. Things to consider include building construction, suitable emergency preparedness, reliable power supplies, adequate climate control, and appropriate protection from intruders.

Image courtesy of: <https://www.getkisi.com/blog/physical-security-assessment-problems-it-can-uncover>



52

52

Physical Security Response

Action	Definition	Examples
Deter	Discourage unauthorized individuals	Fences, walls, guards, guard post, sign in, barbed wire/razor wire, alarms, standing military
Delay	Slow down the access attempt to allow a security response	Walls, gates, road blocks, bollards, badge/pin biometrics
Detect	Discover unauthorized access expediently	Camera, motion detection, sensors, guards, random checks, random patrols, audits
Assess	Determine damage and implement effective and efficient countermeasures	Investigation, internal security, external security, drills, simulations
Recovery	Restore operations	Camera, law enforcement, tracker, serial numbers, asset number



53

53



Cryptography Concepts

Summarize the basics of cryptographic concepts.



54

Cryptography

- Cryptographic life cycle
- Cryptographic types
- Public Key Infrastructure (PKI)
- Key management practices
- Digital signatures
- Digital rights management
- Non-repudiation
- Integrity
- Methods of cryptanalytic attacks



55

Cryptography - Terms

- Derived from the Greek work *krypto* which means to hide
- Cryptography means secret writing
- Cryptanalysis is the breaking of an encryption(a mathematically flawed cipher is a weak cipher)
- Steganography is the art of covered messages
- Cryptology is the science of hiding and includes cryptography, cryptanalysis, and steganography



56

STEGANOGRAPHY

- Greek word *steganos* (covered or protected) and *graphein* (writing)
- Hiding one piece of data within another

Since everyone can read, encoding text in neutral sentences is doubtfully effective

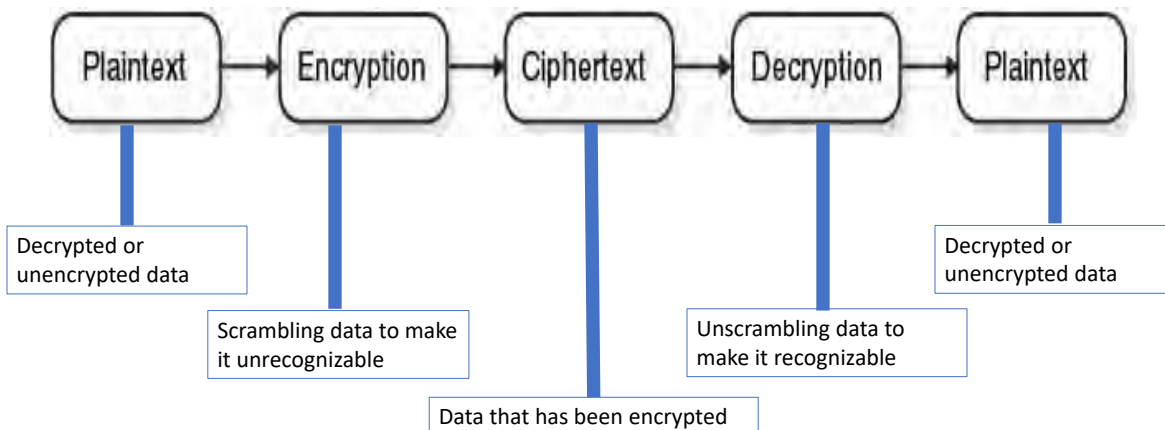
Since Everyone Can Read, Encoding Text In Neutral Sentences Is Doubtfully Effective

Secret Inside



57

Cryptography – Security through Secrecy



Key: A complex sequence of alpha-numeric characters generated by the algorithm that supports the scrambling and unscrambling (larger/random the key = stronger the encryption)

Cipher: Algorithm

58

Classical Encryption Techniques

Substitution Cipher	Transposition Cipher
Each letter is replaced with a different letter or symbol	Letters are moved around according to a give rule (the key)

59

Cryptosystems Offers

- Confidentiality
- Integrity
- Authentication
- Authorization
- Nonrepudiation



60

Classical Encryption Techniques

The Caesar cipher is one of the earliest known and simplest ciphers. It is a type of substitution cipher in which each letter in the plaintext is 'shifted' a certain number of places down the alphabet.

The ROT13 cipher as a type a Caesar cipher.
It is a substitution cipher with a specific key where the letters of the alphabet are offset 13 places.

ROT13 cipher

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
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

ROT3 cipher

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
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

61

Classical Encryption Techniques

A transposition cipher hides information by reordering the symbols in a message based on a key. The goal of transposition is diffusion.

Columnar Transposition Cipher follows simple rules for creating the ciphertext.

1. Keyword determines row length use a padding character (x)
2. Write out the message to reflect row lengths
3. Reorder the columns alphabetically by keyword
4. Ciphertext is read off along the columns

Keyword: cyber Message: CyberProtex Rocks

<u>C</u>	<u>Y</u>	<u>B</u>	<u>E</u>	<u>R</u>
C	Y	B	E	R
P	R	O	T	E
X	R	O	C	K
S	X	X	X	X

<u>B</u>	<u>C</u>	<u>E</u>	<u>R</u>	<u>Y</u>
B	C	E	R	Y
O	P	T	E	R
O	X	C	K	R
X	S	X	X	X

BOOXCPXSETCXREKXYRRK

62

Modern Ciphers

Complexity deters brute force.

Substitution followed by a transposition makes a new much harder cipher much harder cipher



Substitution + Transposition

Bridge from classical to modern ciphers

XOR – mathematical operation



63

Exclusive OR (XOR)



Input (plaintext)	Input (key)	Output (ciphertext)
0	0	0
0	1	1
1	0	1
1	1	0

64

Stream vs Block Ciphers

- Stream ciphers convert one symbol of plaintext directly into a symbol of ciphertext.
- Block ciphers encrypt a group of plaintext symbols as one block.

Encryption Standard	Advantages	Disadvantages
Stream	Speed of transformation and low error propagation	Low diffusion and susceptibility to insertions and modifications
Block	High diffusion and an immunity to tampering	Slowness of encryption and error propagation

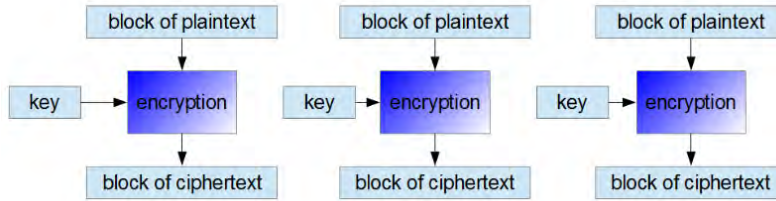
65

Block Ciphers Mode of Operations

Mode	Definition
Electronic Code Book (ECB)	Simplest mode Each block is encrypted with same key Identical plaintext blocks == identical ciphertext blocks
Cipher Block Chaining (CBC)	Easy to implement and popular mode Each plaintext block is XOR with the previous ciphertext block Uses an initialization vector (IV) for first block
Counter (CTR)	Acts like a stream cipher Encrypts successive values of a counter Variable plaintext size
Galois / Counter Model	Encryption with authentication Combines the counter mode with Galois authentication

66

Electronic Code Book (ECB)



Cipher Block Chaining (CBC)

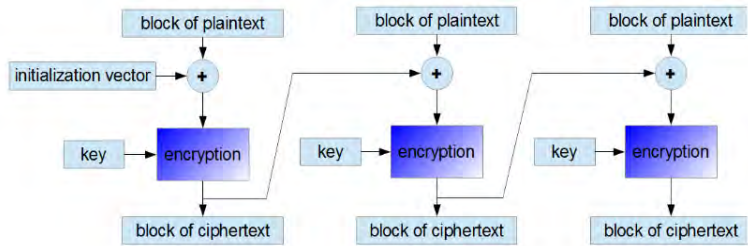
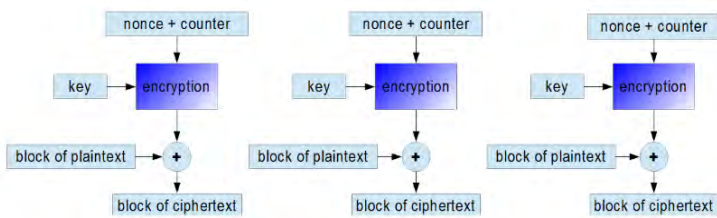


Image courtesy of: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

67

Counter (CTR)



Galois / Counter Model

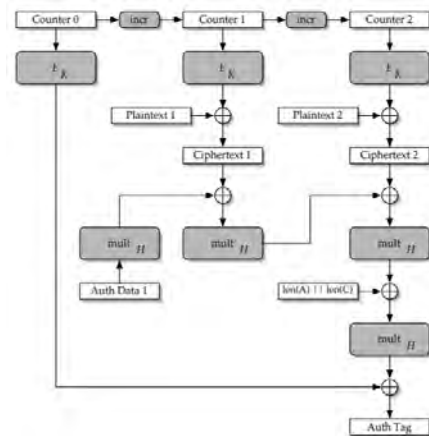
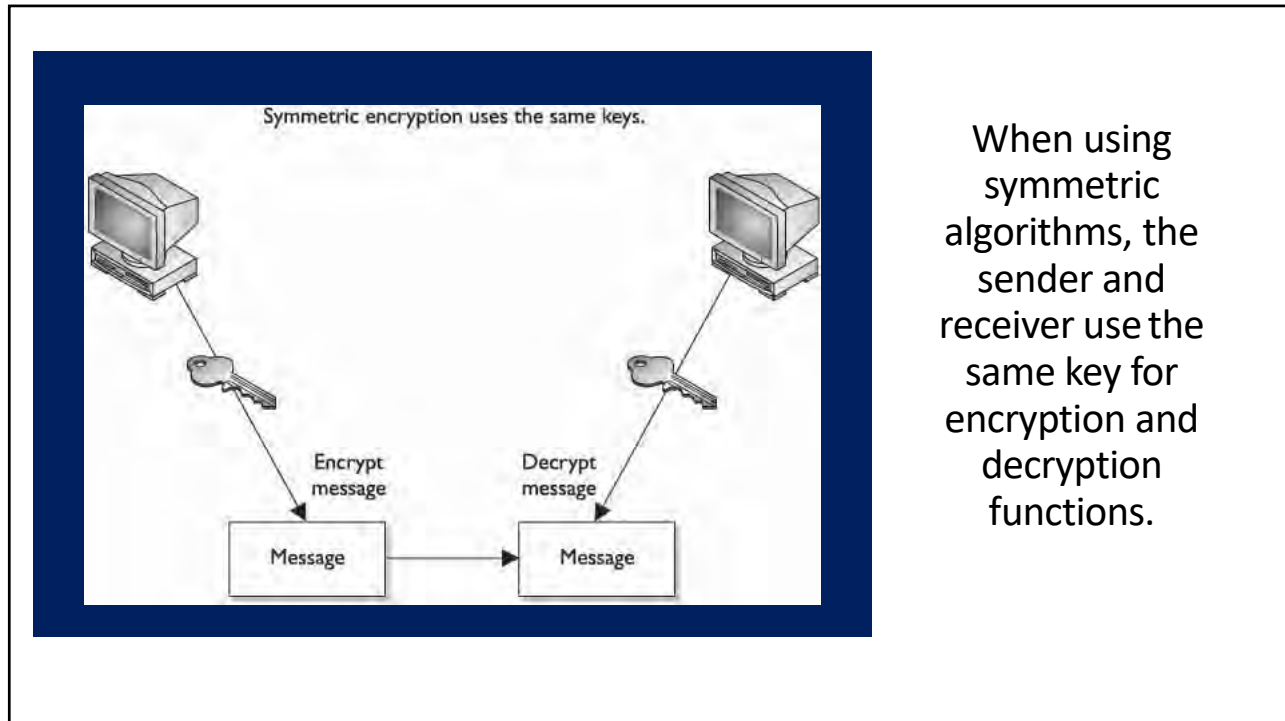


Image courtesy of: https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

68



69

US Government Blessed Algorithms

- *Data Encryption Standard (DES)*
- *Advanced Encryption Standard (AES)*

Most modern symmetric encryption algorithms are block ciphers.
Block sizes vary (64 bits for DES, 128 bits for AES)

Confusion: relationship between the key and the ciphertext must be obscured and is achieved by substitution
Diffusion: DES implements bit permutations a diffusion element, while AES uses MixColumn operation

70

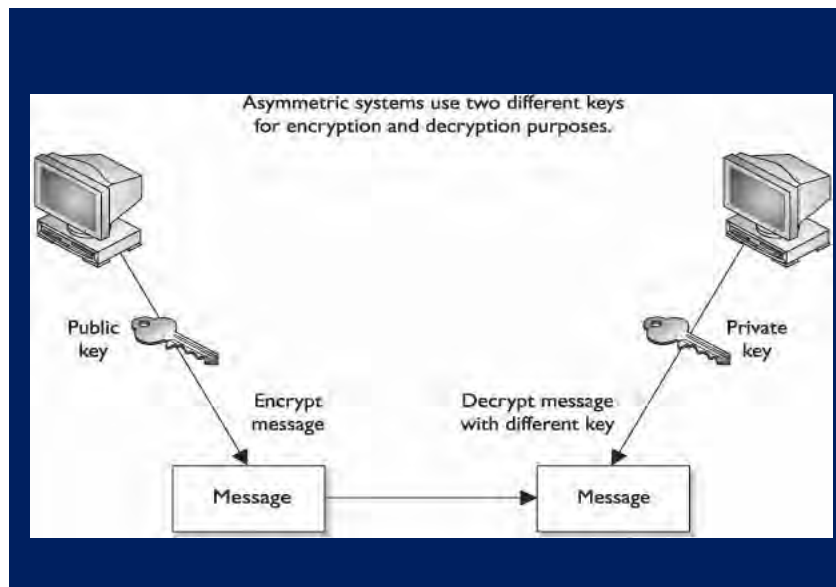


Modern Cryptography – Symmetric Algorithms

23 BRAIDS

Algorithm	Description
Twofish	Public domain Block cipher 128 bit blocks Finalist in the AES selection process
3DES	Extended the life of DES – key stretching Message is encrypted by using one key, encrypted by a second key, and then again encrypted by using either the first or third key
Blowfish	Public domain 64 bit Block Cipher with 16 rounds Variable key lengths up to 448 bits
RC4/5	A stream cipher (data is encrypted in real time) Uses a variable length key (128 bit is standard)
AES	Based on Rijindael Block Cipher – variable block and key lengths (128, 192, or 256 bits)
IDEA	International Data Encryption Algorithm Block cipher 64 bit blocks with key length of 128 bits 8 rounds on 16 bit sub-blocks using a 128 bit key
DES	56 bits + 8 parity bits = 64 bit block cipher Sbox rounds (16 rounds of transpositions and substitutions) Modes of operations: Electronic Code Book (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), and Output Feedback (OFB)
Safer	It is designed for use in software. The plaintext is directly changed by going through S-boxes, which are replaced by their inverses for decryption

71



When using asymmetric algorithms, the sender and receiver use key pairs (public key and private key) for encryption and decryption functions.

72



Modern Cryptography – Asymmetric Algorithms DEREK

Algorithm	Description
Diffie-Hellman	Key exchange Based on discrete logarithms Vulnerable to Man-in-the-Middle attacks
ECC	Elliptic Curve Small key Faster than other asymmetric algorithms Wireless and smart cards
RSA	Based on factoring a number that is the product of two large prime numbers (typically 512 bits)
El Gamal	Unpatented and based on the discrete logarithms Extends the functionality of the Diffie-Hellman to include digital signatures
Knapsack	Based on fixed weights

73

Digital Signatures

- Asymmetric Crypto
- Provides authenticity (non-repudiation)
- Known sender
- Message not altered in transit
- Detects forgery and tampering
- Three acceptable algorithms: RSA Digital Signature Algorithm, the Digital Signature Algorithm (DSA – modified El Gamal algorithm) and the Elliptic Curve Digital Signature Algorithm (ECDSA)



74

Symmetric vs Asymmetric

Attribute	Symmetric	Asymmetric
Key	A single, shared key	Key pair
Key exchange	Out of band	Public key is encrypted with message and the key is distributed by inbound means
Speed	Faster because algorithm is less complex	Slower because the algorithm is more complex
Number of keys	$n*(n-1)/2$ So for 1000 users, there would be 499,500 keys (Scalability Issue)	N key pairs so for 1000 users, there would be 1000 key pairs

75

Key Sizes

Asymmetric Key Size (RSA and Diffie-Hellman) (Prime Number Factorization)	ECC (Curves)
1024	160
2048	224
3072	256
7680	384
15360	521

Benefits:

The small key sizes make ECC very appealing for devices with limited storage or processing power (IoT).

76



Key Management

- Key management is the most challenging part of cryptography and also the most crucial.
- It is one thing to develop a very complicated and complex algorithm and key method, but if the keys are not securely stored and transmitted, it does not really matter how strong the algorithm is.

77

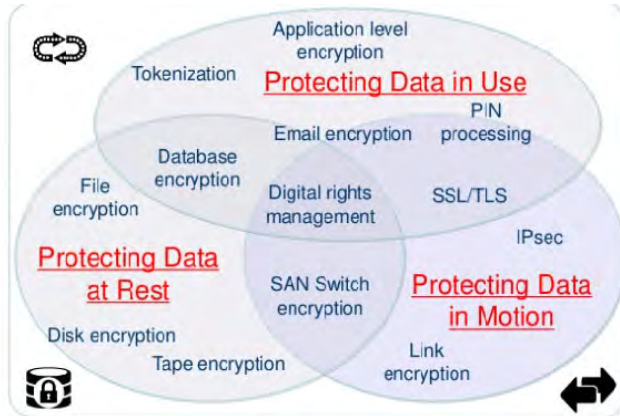
Hash - Really Not My SHH!T (RNM@SHH!T)



Algorithm	Description
RIPEMD	RACE Integrity Primitives Evaluation Message Digest Based on MD5 but performs as SHA-1 RIPEMD found to have a collusion and replaced with RIPEMD160
NTLM	Encrypts user authentication details in the Microsoft operating systems
MD5	Message Digest produces a 128 bit hash; suffers from collisions Used to store passwords and to check the integrity of files
SHA	Secure Hash Algorithm produces a 160 bit digest
HAVAL	Supports hashes of lengths - 128 bits, 160 bits, 192 bits, 224 bits, and 256 bits and supports a variable number of rounds of 3, 4, or 5
HMAC	Hashed Message Authentication Code (checksum) uses a keyed digest
TIGER	Designed for efficiency on 64-bit platforms. The default hash value is 192 bits

78

Cryptography is Fundamental Security Technology



Data at Rest (DaR)

Data is at rest when it is stored on a hard drive. Encrypting hard drives is one of the best ways to ensure the security of data at rest.

Data in Use (DIU)

Data in use is more vulnerable than data at rest because, by definition, it must be accessible to those who need it.

Data in Transit (DiT)

Data is at its most vulnerable when it is in transit. Protecting information in motion requires specialized capabilities including encryption.

Image courtesy of: Hubbard, T. IBM Guardian Data Encryption for IMS and DB2 Webinar.
http://www.slideshare.net/IBM_CICS/ibm-guardium-data-encryption-for-ims-and-db2-webinar

79

Wireless

Encryption Protocols	Description	Encryption/Key
Wired Equivalent Privacy (WEP)	First 802.11 security standard; easily hacked due to its 24 bit initialization vector (IV) and uses weak authentication	RC4 stream cipher and 64 or 128 bit keys Static master key must be manually entered into each device
Wi-Fi Protected Access (WPA)	Interim standard to address WEP. It is backward compatible and supports personal and enterprise modes	RC4 but adds longer IVs and 256 bit keys. Each client has new TKIP. Enterprise mode uses stronger authentication with 802.1x and EAP.
WPA2	Standard in the field today. Modern hardware supports the advanced encryption to prevent performance issues. Supports both personal and enterprise modes	Uses CCMP and AES algorithm for stronger encryption and authentication

80

Wireless and IEEE Standards

802.11 refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients.

IEEE Standard	Frequency	Max Data Rate	Max Range
802.11a	5 GHz	54 Mbps	400 feet
802.11b	2.4 GHz	11 Mbps	450 feet
802.11g	2.4 GHz	54 Mbps	450 feet
802.11n	2.4/5 GHz	600 Mbps	825 feet
802.11ac	5 GHz	1 Gbps	1000 feet

81

Encryption for Networking

Authentication Protocol	Definition
EAP	Extensible Authentication Protocol was developed to provide an authentication framework that can be used for both Point-Point connections as well as wireless networks. WPA and WPA2 use five EAP types as authentication
PEAP	Protected Extensible Authentication Protocol, created by Cisco, Microsoft, and RSA Security, provides a method to transport securely authentication data, including legacy password-based protocols, via 802.11 Wi-Fi networks. It encapsulates EAP in a TLS tunnel with one certificate on the server
LEAP	The LEAP (Lightweight Extensible Authentication Protocol) was originally created by Cisco Systems prior to the official ratification of the 802.11i standard. The LEAP protocol was first distributed to get the industry to adopt 802.1X as well as dynamic WEP adopted by industry. It has been compromised.

82

Encryption for Networking

Authentication Protocol	Definition
EAP-FAST	Flexible Authentication via Secure Tunneling was developed by Cisco, and it uses a mutual authentication is achieved by means of a Protected Access Credential which can be managed dynamically by the authentication server. Light weight and secure, it was proposed to replace LEAP.
EAP-TLS	EAP-TLS (Transport Layer Security) provides for certificate-based and mutual authentication of the client and the network. It relies on client-side and server-side certificates to perform authentication and can be used to dynamically generate user-based and session-based WEP keys to secure subsequent communications between the WLAN client and the access point.
EAP-TTLS	Tunneled Transport Layer Security was developed as an extension of EAP-TLS. This security method provides for certificate-based, mutual authentication of the client and network through an encrypted channel (or tunnel), as well as a means to derive dynamic, per-user, per-session WEP keys. It requires only server-side certificates.

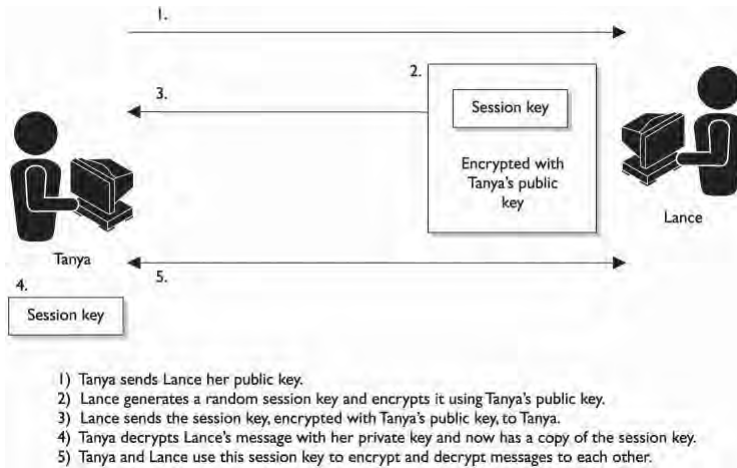
83

SSH is used for remote terminal-like functionality



84

Session Keys



A session key is generated so all messages can be encrypted during one particular session between users.

85



Perfect Forward Secrecy

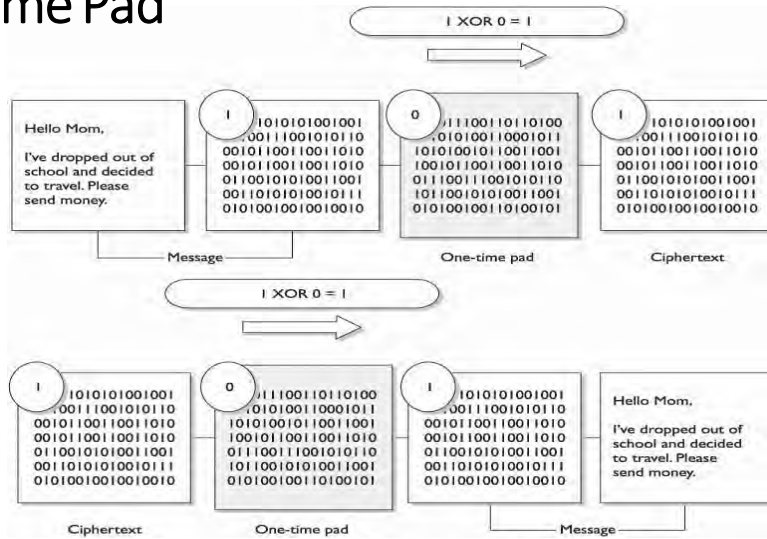
Perfect Forward Secrecy is a feature of specific key agreement protocols that gives assurances the session keys will not be compromised even if the private key of the server is compromised.

Two important things must occur for perfect forward secrecy:

1. Use Diffie-Hellman: The client and the server have to be capable of using a cipher suite that utilizes the Diffie-Hellman key exchange.
2. Ephemeral: The client and the server generates a new set of Diffie-Hellman parameters for each session.

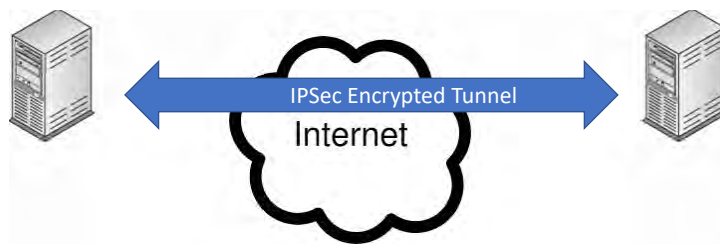
86

A One-Time Pad



87

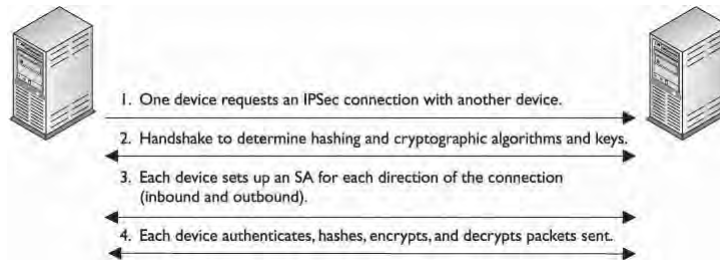
IP Security (IPSec)



- Can encrypt and authenticate network transmissions
- Function
 - ✓ Tunnel Mode – data or payload and message headers are encrypted
 - ✓ Transport Mode – payload is encrypted
- Two protocols
 - ✓ Authentication Header (AH) – authentication and integrity checking for data packets
 - ✓ Encapsulating Security Payload (ESP) – encryption services

88

IPSec



Steps that two computers follow when using IPSec

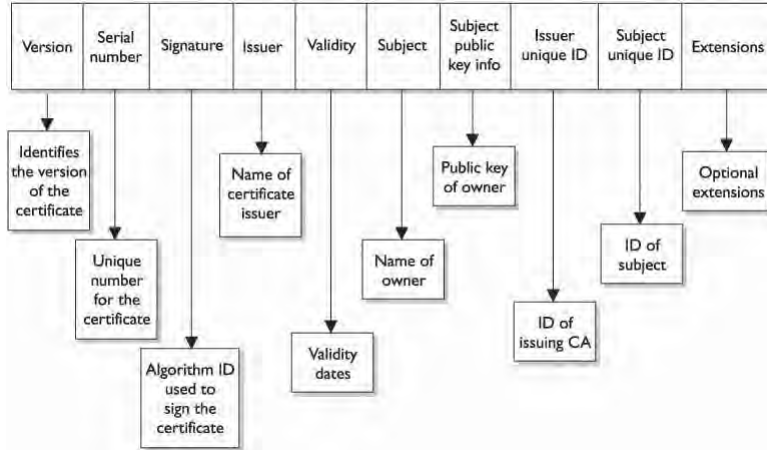
Public Key Infrastructure (PKI)

Trust models – “web of trust”

- Certificate Authority (CA) - Issues
 - ✓ Public key
 - ✓ Private keys
- Registration Authority (RA) - Maintains
 - ✓ Key escrow
 - ✓ Certificate Revocation List (CRL)
 - ✓ Online Certificate Status Protocol (OCSP)
 - ✓ Recovery agent

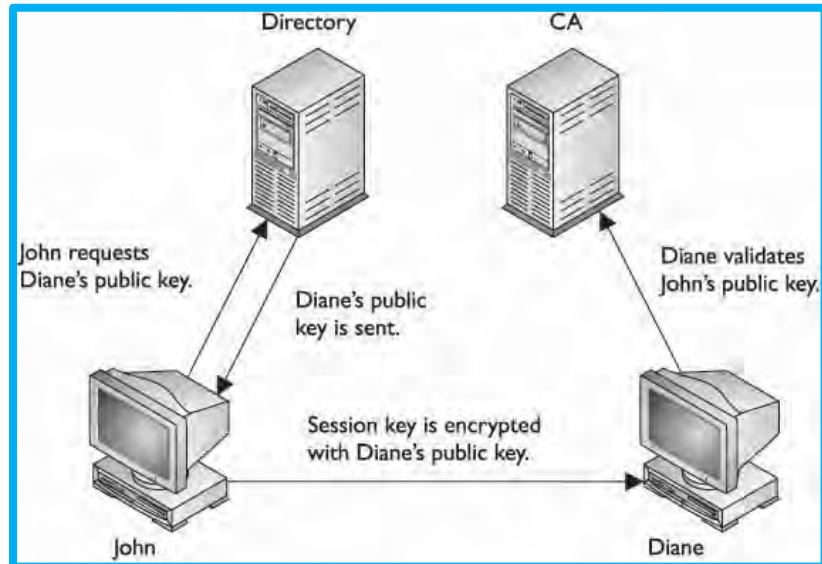
X.509

Each certificate has a structure with all the necessary identifying information in it.



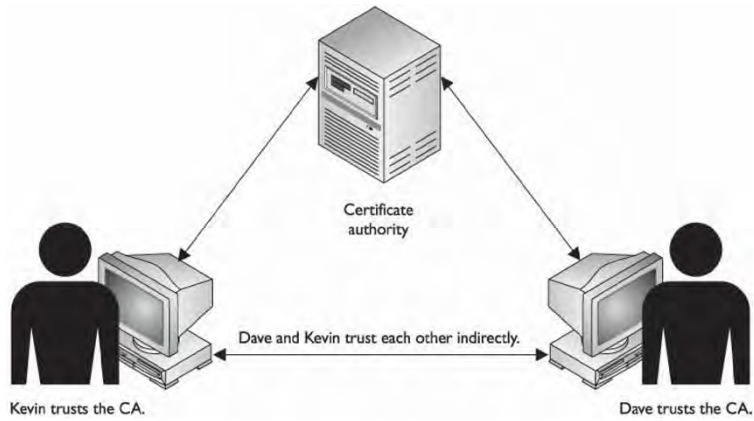
91

CA and User Relationships



92

CAs



93



Questions?

www.cyberprotex.com

training@cyberprotex.com



94

94