



Implementation

Domain 3 – 25%

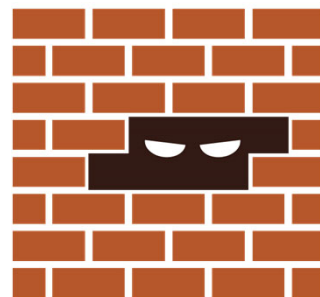


1

1

Network Devices

- Hub
- Switch
- Router
- Firewall
- Load Balancers
- Proxies
- Intrusion Detection Systems / Intrusion Protection Systems
- Unified Threat Management

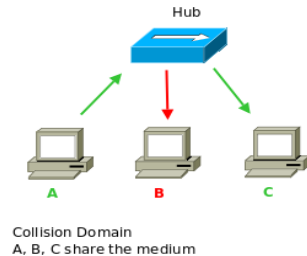


2

2

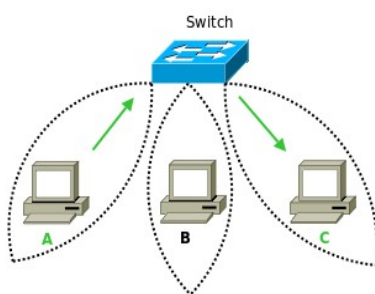
Hubs

- Collision Domain - A physical connection where only one device can send data at
- Collision - When data is transmitted at the same time on a network that does not properly separate network traffic
- A hub is a multi-port device that connects devices into a single collision domain
- Traffic on a hub is broadcast to all devices connected to the Hub
- Hubs operate at Layer 1, Physical Layer, of the OSI model



3

Switches

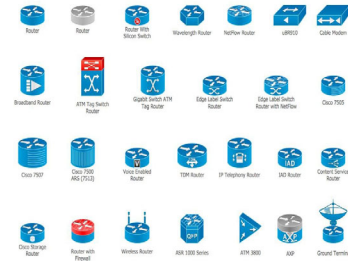


- Broadcast Domain – A logical network separation that allows nodes to communicate through broadcasts
- Each port on a switch contains an independent broadcast domain
- Media Access Control (MAC) – Unique network interface for each device on a network
- Switches operate Layer 2, Data Link Layer, of the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

4

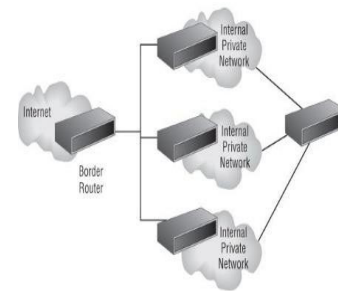
Routers

- Routers can be used to connect Local Area Networks (LANs) to Wide Area Networks (WANs)
- Routers operate a Layer 3, Network Layer, of the OSI model
- Routers can be configured to act as a packet filtering firewall through deployment of Access Control Lists (ACLs)



Routers Definitions

- Border Router – Connection of 100BaseT network to T1 network
- Zone – Using a router to segment a network into multiple network
- Access Control List (ACL) – Routers can be configured with ACLs to shape who and what has access to organizational resources



Routers Details

- Routers can be configured using either Simple Network Management Protocol (SNMP) or telnet connections which can create a security gap
 - ✓ Unencrypted Protocols - Telnet, SNMPv1, SNMPv2
 - ✓ Encrypted Protocols – SSH, SNMPv3
- Routers work by creating internal tables that specify routes and connections between networks
- Routers primarily use three different protocols:
 - ✓ Routing Information Protocol (RIP)
 - ✓ Border Gateway Protocol
 - ✓ Open Shortest Path First (OSPF)
- Routes inside of Routers are configured as either:
 - ✓ Static – Manual route configuration
 - ✓ Dynamic – Automated route configuration



7

7

Proxy

- A device that is an intermediary for another device
- A proxy should provide
 - ✓ Mechanisms to block malicious sites
 - ✓ Cache data
- Combination of Proxy and caching functions is referred to as “Web Security Gateway”
- A proxy works at Layer 7, Application Layer, of the OSI model

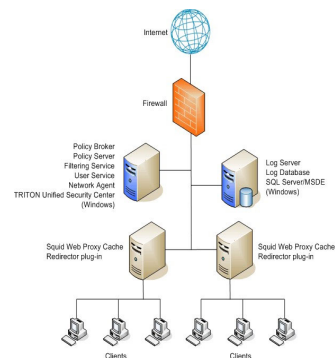


Image courtesy of: http://www.websense.com/content/support/library/deployctr/v76/dic_ws_int_squid.aspx

8

8

Proxy Types

- Forward Proxy (Anonymizing Proxy)
 - ✓ A proxy used to prevent identification of the requesting system (internet access)
- Caching Proxy
 - ✓ A proxy that stores data locally to reduce the amount of time needed to make future requests (i.e. Web Proxy)
- Content Filtering
 - ✓ A proxy that evaluates the content of network traffic to determine if meets specified criteria
- Reverse Proxy
 - ✓ A proxy that analyzes incoming, not outgoing, traffic to perform analytics and filtering
- Open Proxy
 - ✓ Circumvent existing security posturing
 - ✓ Third party



9

9

Load Balancer

- Redirection of traffic load to prevent overutilization of a resource
 - ✓ Server
 - ✓ HDD / SSD
 - ✓ CPU
- Load Balancers can be implemented as hardware or virtualized and associated with:
 - ✓ Router
 - ✓ Firewall
 - ✓ NAT appliance
- In order to determine if a host is operational a load balancer will send a health check request to all connected servers

Image courtesy of: http://xwebhosting.org/?page_id=9437

10

10

Network Address Translation

- Reduces the number of outward facing IP addresses
- NAT essentially proxies internal IP structure

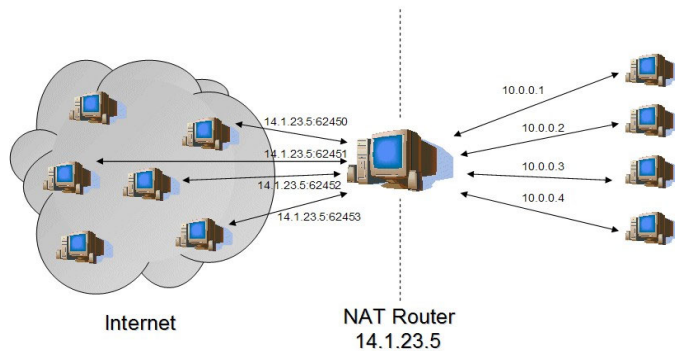


Image courtesy of: <http://windowsitpro.com/networking/what-types-network-address-translation-nat-exist> 11

11

Remote Access

- Remote Access Service (RAS)
 - ✓ Connection of remote systems
 - ✓ Example: Routing and Remote Access Services (RRAS), Windows
 - ✓ Runs over multiple protocols
 - Dial-Up (POTS)
 - Virtual Private Networks (VPN)
 - Integrated Services Digital Network (ISDN)
 - Digital Subscriber Line (DSL)
 - Cable Modem



12

12

Unified Threat Management

- Unified Threat Management (UTM) are systems that consolidate security functions under one management resource
- UTM's can include integration of:
 - ✓ Firewalls
 - ✓ IDS / IPS
 - ✓ Anti-Virus
 - ✓ Virtual Private Network Access
 - ✓ Web Application Security
 - ✓ Email Security

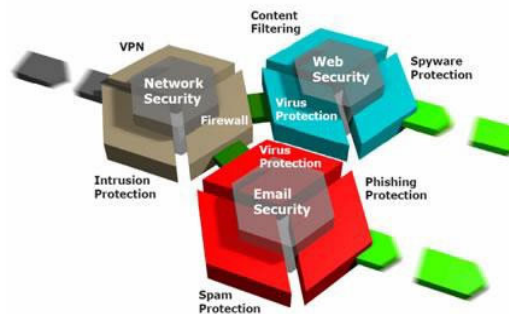


Image courtesy of: <http://www.jaringankita.com/blog/knowning-unified-threat-management-utm>

13

13

Firewalls



- Firewalls provide network isolation and protection and can be implemented in hardware, firmware, and / or software
- Firewalls can allow or limit internal or external network traffic
- Firewall mechanisms:
 - ✓ Application Layer Proxy
 - ✓ Stateful Packet Inspection
 - ✓ Network Address Translation (NAT)
 - ✓ Access Control List (ACL)
- Firewalls should apply the principle of least access to prevent as much traffic while allowing authorized traffic
- Network based firewalls filter at OSI layer 4
- Network based firewalls can be at layer 3 of the OSI Model



14

14

Stateless versus Stateful Firewalls

Stateless	Stateful
Monitor network traffic and restrict or block packets based on source and destination addresses or other static values	Monitor traffic streams from end to end
Not aware of traffic patterns	Can tell what state a session/TCP connection is in (open , open sent, synchronized, synchronization acknowledge, or established)
Simple rule-sets	Everything within a valid flow is allowed
Each packet is individually inspected	Faster and perform better under heavy loads



15

15

Firewall Ruleset

Strategy	Description
Block by Default	Explicitly allow only specific traffic to known services The last rule in an access control list Implicit Deny
Allow Specific Traffic	Based Principle of Least Privilege Specific rules at the top Limited scenario where an "ANY" is permitted
Access Control Lists	Source IP address (inbound to HTTPS), destination IP address, and port number Read top to bottom
Specify the Destination Port	Value corresponds to the service that needs to be accessed This should never have an ANY value Avoid using too wide a range of ports



16

16

Stateful Firewalls

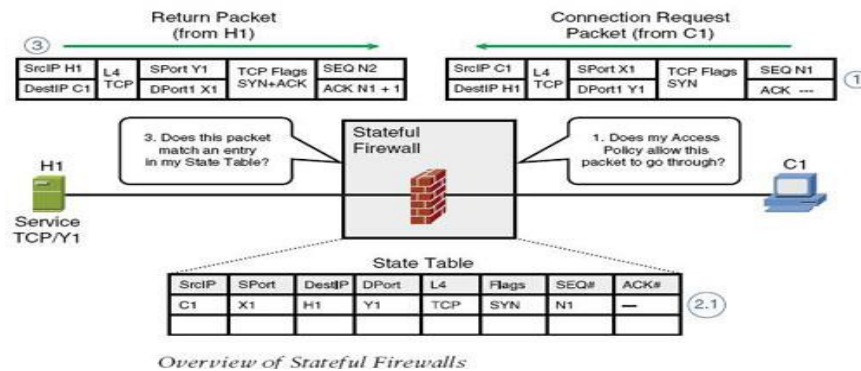


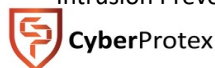
Image courtesy of: <http://rumyittips.com/what-is-stateful-packet-inspection-firewall/>

17

17

Intrusion Detection Systems (IDS) / Intrusion Protection System (IPS)

- An IDS is a system configured to detect misconfigurations or unauthorized access into a system
- Inline monitoring results from IDS/IPS sitting where all traffic must pass through it
- IDSs can be configured to identify specific:
 - ✓ Signature-Based (Static signature – perfect match with pattern matching)
 - ✓ Anomaly-Based (Build a baseline of acceptable behavior)
 - Training a system with data to establish baseline
 - Use the established profile on real data to flag deviations
 - ✓ Behavior-Based (Outside of Baseline – looking for evidence of a compromise by observing and reporting)
 - ✓ Heuristics-Based (Algorithms with artificial intelligence)
- If a detection is followed by active modification of network infrastructure, that is considered an Intrusion Prevention System (IPS)



18

18

IDS/IPS Definitions

- Activity
 - ✓ An activity is an element of a data source that is of interest to the operator
- Administrator
 - ✓ Personnel responsible for IDS administration
- Alert
 - ✓ An alert is a message from the analyzer indicating that an event of interest has Occurred
 - The alert contains information about the activity as well as specifics of the occurrence
- Event
 - ✓ Occurrence in a data source that indicates that a suspicious activity has occurred



19

19

IDS/IPS Types

- Passive
 - ✓ Logging
 - ✓ Notification
 - ✓ Shunning (Ignoring)
- Active
 - ✓ Process Termination
 - ✓ Network Configuration Change
 - ✓ Deception



20

20

IDS/IPS Responses



- Out of band response – With detection, IPS send TCP RST frames
 - ✓ limited UDP response
- In band response – Traffic is dropped at IDP/IPS
- False positives
 - ✓ Time consuming to resolve
 - ✓ Updated signatures is the major countermeasure
- False negatives
 - ✓ No indication of malicious traffic
 - ✓ Most dangerous
 - ✓ Anti-virus may help

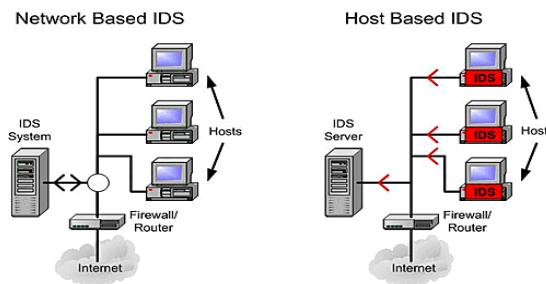


Host versus Network IDS

➤ Host-Based IDS – An IDS that resides on and only evaluates activities related to that host

- ✓ Integrity Checkers

➤ Network-Based IDS – An IDS that is distributed throughout a network and collects inbound and outbound traffic to identify misconfigurations and unauthorized network access



Virtual Private Network (VPN)

- A Virtual Private Network (VPN) establishes a secure connection with organizational resources over an unsecure network
- Can be configured with a VPN appliance or software solutions
- VPN can connect LAN-to-LAN networks
- Common protocols used by VPNs:
 - ✓ Point-To-Point Tunneling Protocol (PTPP)
 - ✓ Layer 2 Tunneling Protocol (L2T)
 - ✓ IPSec
- VPN Concentrator – Hardware appliance that creates remote access VPNs
 - ✓ Creates encrypted tunnel session between hosts
 - ✓ Cisco – Scalable Encryption Processing



23

23

Full vs Split VPN Tunnel



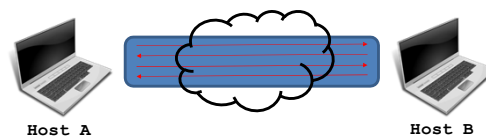
Image courtesy of: <http://blog.soundtraining.net/2013/03/how-to-configure-split-tunneling-on.html>

24

24

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 of the OSI model; Network Layer



Tunneling Protocols

- Point-to-Point Tunneling Protocol (PPTP)
 - ✓ Encapsulates and encrypts PPP packets
 - ✓ Unencrypted
 - ✓ PPTP – TCP Port 1723
- Layer 2 Forwarding (L2F)
 - ✓ Cisco proprietary
 - ✓ Creates tunnels for dial-up connections
 - ✓ Authentication
 - ✓ Unencrypted
 - ✓ L2F – TCP Port 1701
- Layer 2 Tunneling Protocol (L2TP)
 - ✓ Microsoft / Cisco Collaboration
 - ✓ Combination of PPTP and L2F
 - ✓ Works over numerous protocols including Internetwork Packet Exchange (IPX), Systems Network Architecture (SNA) (i.e. IBM), and Internet Protocol (IP)
 - ✓ Unencrypted
 - ✓ L2TP – UDP Port 1701

Tunneling Protocols

- Secure Shell (SSH)
 - ✓ Secure connection between endpoints
 - ✓ Can be used as a tunnel for other unencrypted protocols
 - ✓ SSH – TCP Port 22

- IP Security (IPSec)
 - ✓ Unlike previous examples, IPSec is not a tunneling protocol
 - ✓ Used for both dial-up and LAN-to-LAN configurations
 - ✓ IPSec provides
 - Authentication Headers (AH)
 - Encapsulating Security Payload (ESP)



27

27

IP Security (IPSec)

- A set of protocols developed for secure network communication through cryptography
 - Authentication Header (AH) provides authentication and integrity
 - Encapsulating Security Payload (ESP) provides data encryption (confidentiality) and integrity
- Three key services
 - Data verification
 - Protection from data tampering
 - Private transactions
- Modes
 - Tunnel – entire IP packet is protected (Headers and Payload)
 - Transport – only the payload or data is protected



28

IPSec Modes

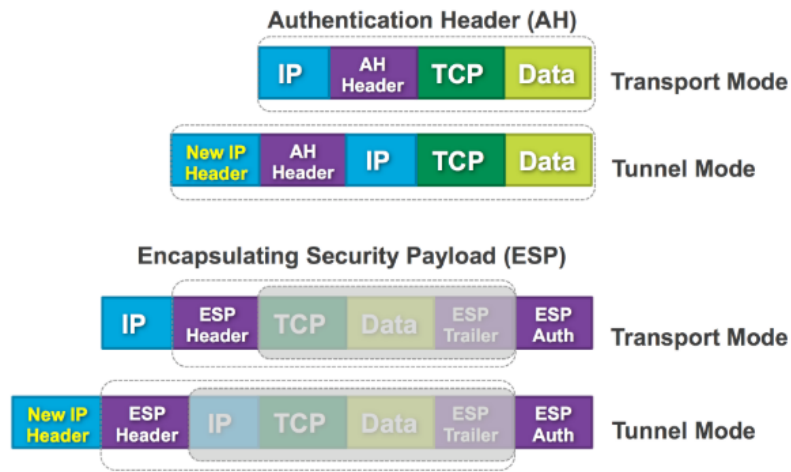


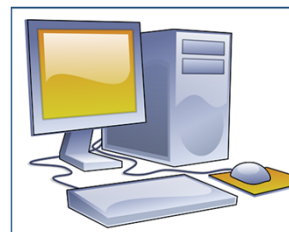
Image courtesy of: <https://community.cisco.com/t5/security-documents/crypto-map-based-ipsec-vpn-fundamentals-negotiation-and/ta-p/3153502>

29

29

Mail Gateway

- An email security gateway is a service that is designed to prevent the transmission of emails that break company policy, send malware or transfer information with malicious intent.
- Spam
 - ✓ Spam is undesired messaging transmitted to users through a wide variety of technologies including:
 - ✓ Email
 - ✓ Text Messages
 - ✓ Messaging Applications
 - ✓ Numerous techniques have been deployed to prevent spam from proliferating including:
 - Domain Blacklists / Whitelists
 - DNS Lookup
 - Content Filters
 - Static or Rule-Based
 - Statistical
 - Delay-Based Filtering
 - SMTP connection delay
 - Spam generators send spam immediately
 - Callback Verification
 - Outbound or Egress Filtering



30

30

Web Application Firewall

- A web application firewall (WAF) is either a software or appliance that conducts content filtering of HTTP / HTTPS network traffic
- WAFs can filter out critical data and prevent transmission of that data outside of organizational boundaries
- WAFs provide flexibility by being able to block or allow similar content on the same resource
- A key function of WAFs is to decrypt SSL enabled traffic prior to being transmitted within an internal network allowing for proper filtering and analysis
- Bridges the gap between the network firewall, network-based intrusion detection system (IDS) and the web application.



31

31

Web Application Firewall

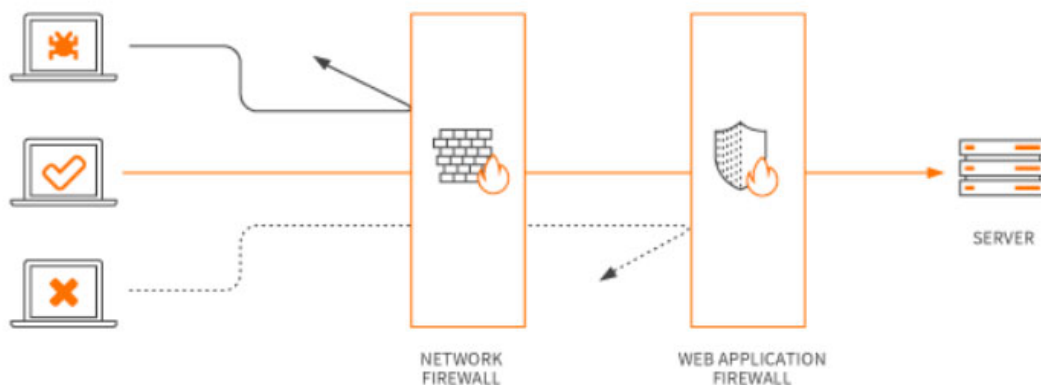
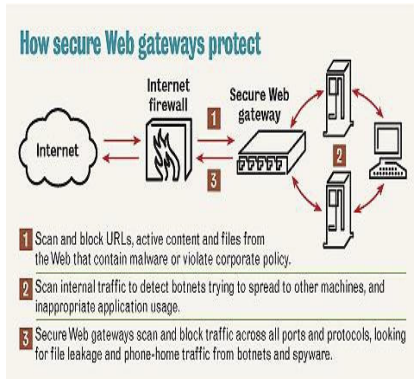


Image Courtesy of: Ndegwa, A. What is a Web Application Firewall? <https://www.maxcdn.com/one/visual-glossary/web-application-firewall/>

32

32

Web Security Gateways



- Provide protective mechanisms for organizations by combining network proxy and content filtering functions in one appliance
- Benefits of using web security gateways
 - ✓ Real-Time Traffic Analysis
 - ✓ Packet Content Inspection
 - ✓ Web Utilization
 - ✓ Data Exfiltration Detection

Image Courtesy of : <http://www.networkworld.com/article/2286101/tech-primers/secure-web-gateways--slamming-the-door-on-malware.html>



33

33

All About the Data

Data Execution Prevent (DEP)

- Help prevents damage to your computer from viruses and other threats
- Monitors the programs for system memory user
- No-execute
 - ✓ Intel – XD bit (eXecute Disable)
 - ✓ AMD – Enhanced Virus Protection

Data Loss Prevention (DLP)

- Tools and process used to ensure that sensitive data is not lost, misused, or accessed by unauthorized
- Monitor and control endpoints activities and filters data streams



Image courtesy of: <https://blog.hostpoint.ch/en/2015/12/protect-your-personal-data-with-domain-privacy/>

34

34

Protocols Risks

Clear Text Protocols and Encrypted Replacements

Clear Text Protocol	Encrypted Replacements
FTP	SFTP/SCP
HTTP	HTTPS
Telnet	SSH
RSH	SSH
SNMPv1 and v2	SNMPv3
IMAP	IMAP with SSL/TLS port 993
POP3	POP3 with SSL/TLS port 995
SMTP	SMTP with SSL/TLS port 465
MIME	S/MIME

Protocols Risks

Core Protocols and Encrypted Replacements

Clear Text Protocol	Encrypted Replacements
IP	IPSec
DNS	DNSEC
BGP	SBGP

Protocol Analyzers

- A protocol analyzer is a tool that can be used to evaluate the function of protocols over a network
- Protocol analyzers are also known as:
 - ✓ Network Analyzer
 - ✓ Packet Sniffer
 - ✓ Sniffer
- In order to work effectively, protocol analyzers must have access to a switch that allows:
 - ✓ Port Mirroring
 - ✓ Switched Port Analyzer (SPAN) Port
- When used correctly, protocol analyzers can be used to:
 - ✓ Collect network traffic for future analysis
 - ✓ Collect evidence for incident response activities
- Network interface cards (NICs) have 2 modes of operation:
 - ✓ Non-Promiscuous Mode
 - ✓ Promiscuous Mode



37

37

Network Commands

Command	Operating System	Description
arp/rarp	Linux/Windows	Change and view arp table (mapping between IP and MAC/MAC to IP)
ifconfig/ipconfig	Linux/Windows	Display network configuration for system
netcat	Linux/Windows	Swiss army knife – send or receive information
netstat	Linux/Windows	Identifies all TCP connections and UDP open
nmap/zenmap	Linux/Windows	Father of general network scanners - status of hosts and/or ports
dig/nslookup	Linux/Windows	Resolution of hostname to IP
ping	Linux/Windows	Sends ICMP packets to target IP to confirm network connectivity



38

38

Network Commands

Commnad	Operating System	Description
tcpdump	Linux/Windows	Advanced command used to inspect traffic from different interfaces of a machine so you can get the exchanged packages.
tracert/traceroute	Linux/Windows	Number of hops to destination
vnstat	Linux	Monitor network traffic from console
whois	Linux/Windows	Query data domains

Banner Grabbing

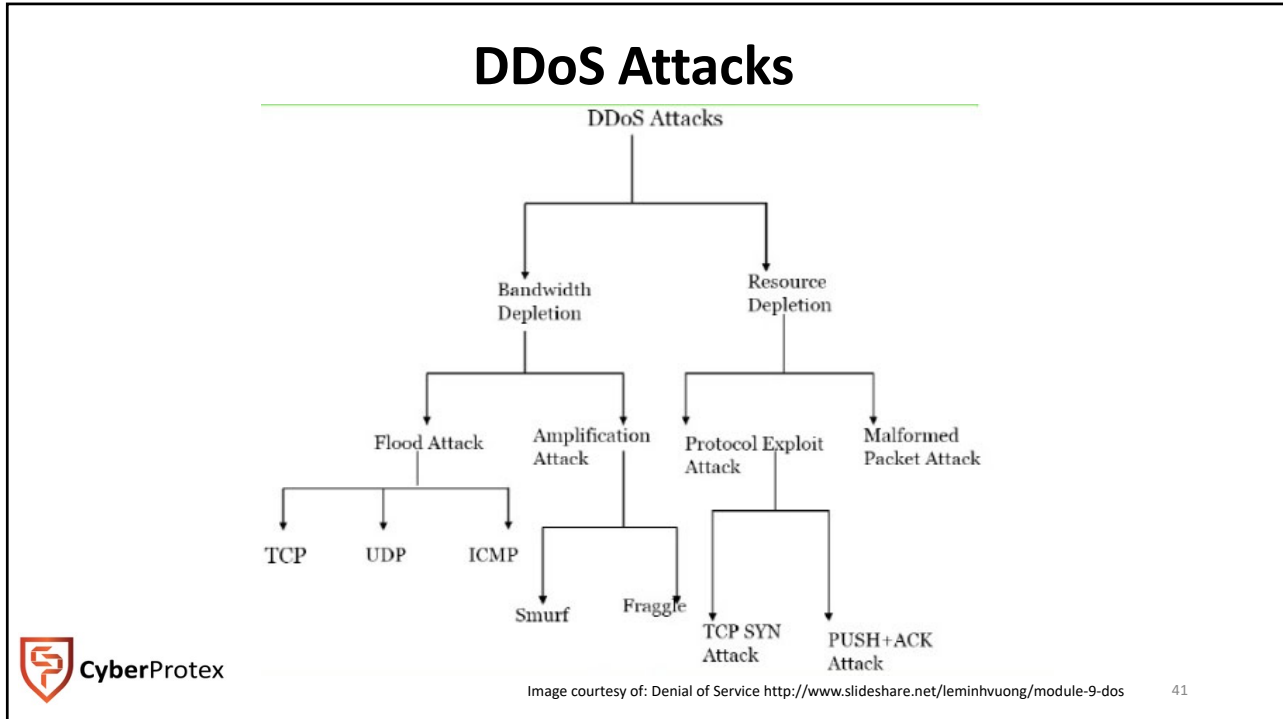
Banner is a text message received from a probed hosts.
 Banner grabbing collects data concerning the network and services on open ports.
 Administrator: catalog assets
 Intruder: determine attack vector

NMAP

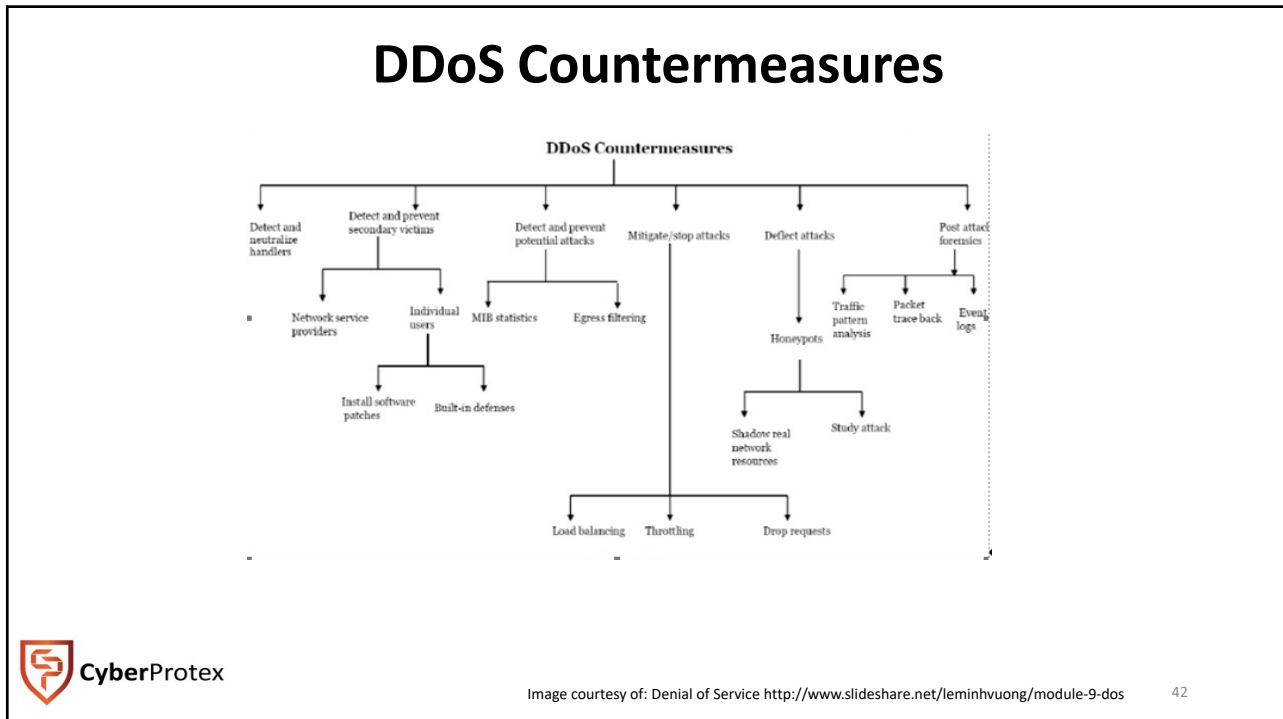
```
nmap -sV --script=banner
nmap -Pn -p 80 -sV --script=banner
```

NETCAT

```
nc -v 192.168.1.106 22
```



41



42

Password Cracking

Tool	Description
Brutus	Online based
	Open source
	Resume and load options to allow pauses in an attack Windows based only
RainbowCrack	Hash cracker uses large amount of memory to speed breaking of the password
	Time-memory process used
	<ul style="list-style-type: none"> • Plain text and hash pairs are calculated using preselected hash algorithms • Results are stored in structure identified as a rainbow table • Rainbow tables used to crack passwords • Rainbow tables available for download
Wfuzz	Web based application
	Brute force
	Locates hidden resource files



43

43

Password Cracking


Tool	Description
Cain and Abel	Multi-tasking tool - Windows based
	Password cracking based upon dictionary attack, sniffed VoIP conversations, brute force, cryptanalysis attack, revealing password boxes, cached passwords, decoding scrambled passwords, and analyzing routing protocols
John the Ripper	Open Source
	Multiple platforms (Linux, Unix, and Mac OS)
THC Hydra	Network password cracker
	Multiple platforms (Windows, Linux, Free BSD, Solaris, and Mac OS)
	Multiple protocols
Medusa	Network password cracker
	Command line tool
	Efficiency depends upon connectivity
	Supports parallel attacks




44

44

Password Cracking




Tool	Description
OphCrack	Free rainbow table based tool Windows based
LOphtCrack	Windows based Alternative to OphCrack Works with hashes
Aircrack-NG	WiFi password cracking tool Works with WEP and WPA Works with Linux and Windows




45

45

Tools for Testing and Attacking



Tool	Description
Wireshark	Network protocol analyzer Multi-platform sniffer that captures data packets on a wired LAN or a Wireless network
Dsniff	Suite of programs that can be used in auditing and penetration testing
Ettercap	Man in the middle attacks
Kismet	Wireless network detector, sniffer, and intrusion detection system (IDS)
NetStumbler	Windows based - detect Wireless Local Area Networks



46

46

Tools for Testing and Attacking

Tool	Description
AirSnort	Wireless LAN (WLAN) tool which recovers encryption keys Operates by passively monitoring transmissions
Cain & Abel	Windows based password recovery tool
EtherApe	Graphical network monitor for Unix modeled after Etherman
Netcat	A simple Unix utility which reads and writes data across network connections
PSTools	Command line utilities that allow you to manage local and remote systems

Log Analysis

- Log analysis can provide significant information about organizational network activity
- Internal system access can be evaluated using a number of system logs including:
 - ✓ Firewall
 - ✓ Router
 - ✓ IDS
- Log analysis can also be aided with the use of protocol analyzers to identify potential ongoing malicious activity
- Central logger

Security Information and Event Management (SIEM)

- Asset management with real time monitoring
 - ✓ Triggers:
 - Email, text, and even call
 - Change Requests Tickets

- Logs from multiple sources (Event forwarding for windows, syslog for Linux)
 - ✓ Write-Once-Read-Many(WORM)

- Record retention supported

- Time synchronization a mandatory requirement (ntp automated updates)



➤ File Integrity for the hosts can be configured as an element

Mobile Device Connection

Connection Type	Description
WiFi	Local network access Vulnerable to man-in-the-middle, denial-of-service
Satellite communications	Remote locations Low earth orbit or geostationary orbit
Near Field Communications (NFC)	Two way communications Used in payment systems like Google wallet and Apple Pay
ANT/ANT+	Wireless sensor network protocol Not 802.11 or Bluetooth
Infrared (IR)	Smartphones, tablets, and smartwatches
Universal Serial Bus (USB)	Physical connectivity to mobile device Physical access is a must Need to auto-lock



CyberProtex

Mobile Device Management (MDM)

Mobility	allows users to access information beyond their desk and conduct business from anywhere without having a wire connectivity
Reachability	enables people to be stay connected and be reachable, regardless of the location they are operating from
Simplicity	deploys easy and fast
Maintainability	low cost and time to maintain the setup
Roaming Servers	provides service anywhere any time
New Services	provide various smart services like SMS and MMS

51

Mobile Device Management (MDM) Issues

Data Interception	Ad Hoc and Soft APs
Denial of Service	Misbehaving Clients
Rogue APs	Endpoint Attacks
Wireless Intruders	Evil Twin APs
Misconfigured APs	Wireless Phishing

52

Mobile Device Deployment Models

- **BYOD**
 - ✓ Bring Your Own Device
 - ✓ Most common method
 - ✓ Minimum requirements
- **COPE**
 - ✓ Corporate owned, personally enabled
 - ✓ Contains both sensitive and personal data
 - ✓ Policy to handle decommission
- **CYOD**
 - ✓ Choose Your Own Device
 - ✓ Corporation provides options
- **Corporate – owned**
 - ✓ Corporation purchased, own, and control content
 - ✓ High level of security
- **VID/VMI**
 - ✓ Virtual Desktop Infrastructure/Virtual Mobile Infrastructure
 - ✓ All data and applications are running on remote servers
 - ✓ Risk is minimized of lost device leading to data leakage



53

53

Access Control

Goal is to grant access to the right assets to the right users with the right content. A collection of process and technologies are used to control access to critical assets. A primary medium is through logical or technical controls aimed at systems/devices and/or facilities.

Access control provides two functions:

- Allowing authorized users in
- Keeping unauthorized users out



54

54

Identity and Access Management

A security process that provides identity, authentication, and authorization mechanisms for entities to work with organizational assets.

Identification: Claiming an identity

You can define attributes in an identity, such as purpose, function, clearance, etc.

- Attributes enable access systems to make decisions for authentication and authorization.
- Example: Employee role factors into identity, like department and managerial status.

IAM is crucial for bolstering overall IT security.



55

55

Authentication Authorization, Accounting

AAA - A security concept for a centralized platform that performs three separate identity-based tasks. Acts as gatekeeper that provides access to network systems.

- **Authentication:** Verifying an identity
- **Authorization:** Assigning rights and privileges
- **Accounting:** Tracking and recording system activities



56

56

Multifactor Authentication

Authentication can be accomplished with:

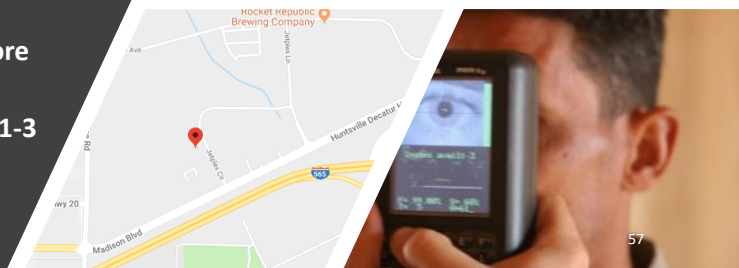
- Something you know (1)
- Something you have (2)
- Something you are (3)
- Somewhere you are
- Something you do

Multiple authentication uses two or more methods to verify an identity

Authentication mostly depended upon 1-3



Password123



57

Authentication Types

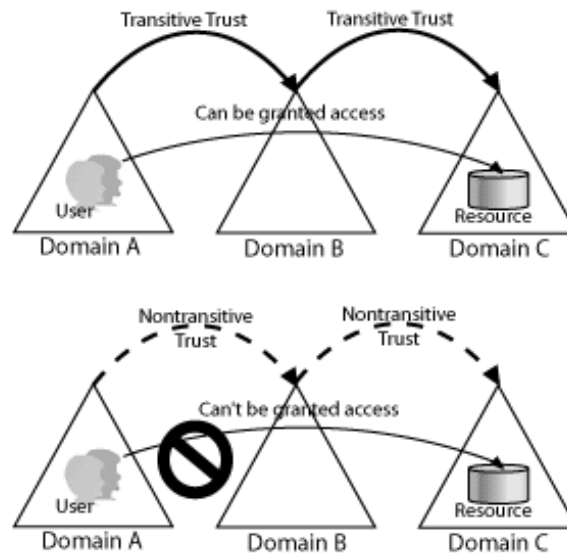
- **Single Factor Authentication**
 - ✓ Only 1 authentication method is used to verify an identity
 - ✓ Example: Username and Password
- **Mutual Authentication**
 - ✓ When multiple entities authenticate each other
- **Multifactor Authentication**
 - ✓ Multiple authentication methods are used to verify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



58

58

Transitive vs. Non-Transitive



59

Transitive Risks

➤ For all of the advances in authentication and access, there are a number of challenges that must be understood including:

- ✓ Transitive Access Attack – This attack occurs when trust is taken advantage of

Node A ↔ Node B ↔ Node C
A trusts B, B trusts C, therefore A trusts C

- ✓ Transitive access attacks can be mitigated with strong security controls including firewalls, strict transitive trust relationships, and encryption of the data

60

Single Sign-On (SSO)

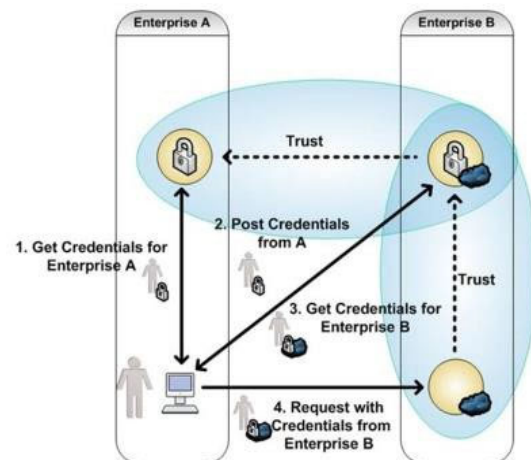
- Every account that exists in a system, network, application or other asset provides a point of failure for unauthorized access
- Single sign-on (SSO) is an authentication process that allows a user to access multiple applications with one set of login credentials
- A compromised user's credentials can give the keys to the kingdom to the bad guys
- Complex to setup with heterogeneous network, especially with legacy systems



61

Federations

- Networks that operate on a common set of standards and could include:
 - ✓ Security
 - ✓ Communication
 - ✓ Data Sharing
- Federated Identify – Utilizing a single identify across multiple systems



62

Remote Authentication Systems

- AAA – Authentication, Authorization, and Accounting
- RADIUS - Remote Authentication Dial-In User Service
- TACACS - Terminal Access Controller Access-Control System
- TACACS+ - Terminal Access Controller Access-Control System +
- XTACACS – Extended Terminal Access Controller Access-Control System

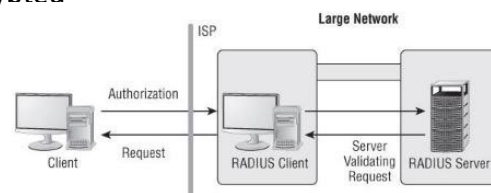


63

63

RADIUS

- Remote Authentication Dial-In User Service
- Networking protocol
- Centralized authentication, authorization, and accounting (AAA)
- Username: Cleartext, Password: Encrypted
- Operates over UDP



64

64

TACACS / XTACACS

- TACACS - Terminal Access Controller Access- Control System
- TACACS is a legacy protocol that is similar to RADIUS and is used to communicate with an authentication servers
- XTACACS – Extended Terminal Access Controller Access-Control System added on to TACACS by combining authentication and authorization with logging to enable auditing



65

65

TACACS+

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



66

66

TACACS+

A possible example includes using a Cisco ACS running TACACS+ authentication protocol. This system resides on the internal network. A firewall administrator authenticates via the AAA server when requesting access to the console

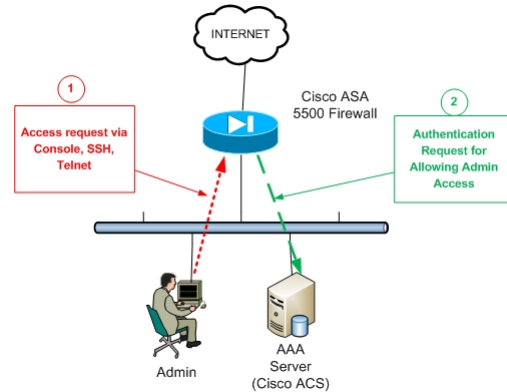


Image courtesy of: How to Configure AAA Authentication on Cisco ASA Firewall?
<http://ciscorouterswitch.over-blog.com/article-how-to-configure-aaa-authentication-on-cisco-asa-firewall-117804401.html>



RADIUS vs TACACS+

RADIUS	TACACS+
Combines authentication & authorization.	Separates all 3 elements of AAA, making it more flexible.
Encrypts only the password.	Encrypts the username and password.
Requires each network device to contain authorization configuration.	Central management for authorization configuration.
No command logging.	Full command logging.
Minimal vendor support for authorization.	Supported by most major vendors.
UDP- Connectionless UDP ports 1645/1646, 1812/1813	TCP- Connection oriented TCP port 49
Designed for subscriber AAA	Designed for administrator AAA

Table courtesy of: <http://www.tacacs.net/docs/TACACS+Advantages.pdf>



RADIUS vs TACACS+

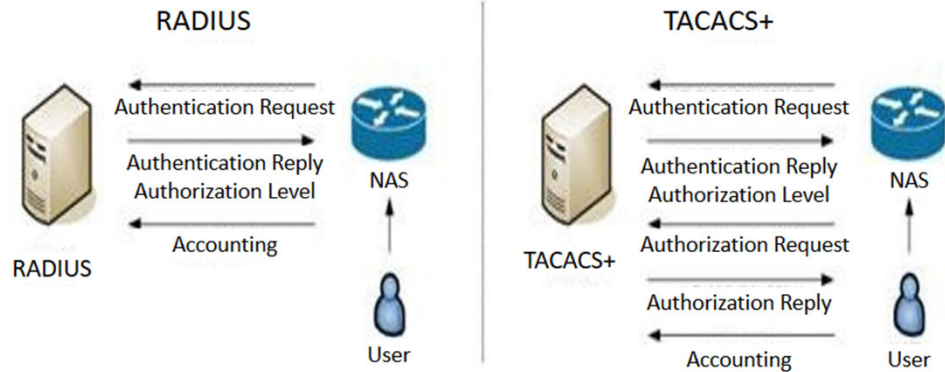


Image courtesy of: <http://rumyitips.com/what-is-the-difference-between-tacacs-and-radius/>

69

69

Kerberos

➤ A network authentication protocol used to provide strong authentication for client/server applications by using secret-key cryptography

- Standard Port: 88, TCP
- Components of Kerberos authentication
 - ✓ Key Distribution Center (KDC)
 - ✓ Ticket Granting Ticket (TGT)
 - ✓ Service Ticket

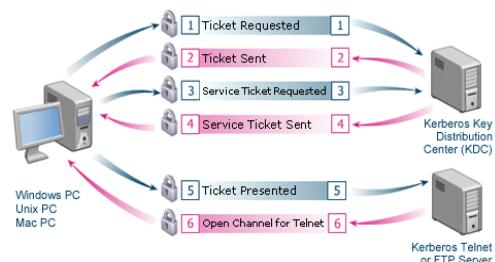


Image courtesy of: <http://www.ericom.com/kerberos.asp>

70

70

Microsoft NTLM

- Authenticating accounts between Microsoft Windows machines and servers
- Based on a challenge/response authentication protocol
- NTLM authentication is still supported and must be used for Windows authentication with systems configured as a member of a workgroup.
- Replaced LANMAN

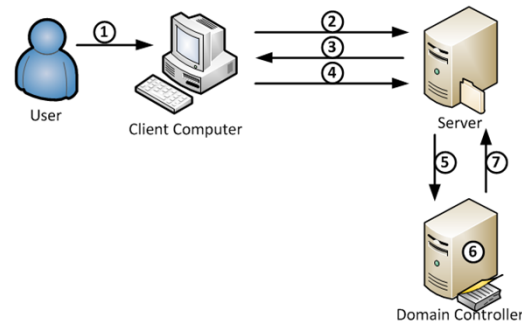


Image courtesy of: <https://blogs.technet.microsoft.com/isrpfelpl/2010/11/05/optimizing-ntlm-authentication-flow-in-multi-domain-environments/>

71

71

Lightweight Directory Access Protocol (LDAP)

- ✓ Software protocol that allows users to locate organizations, individual, and other resources such as files and devices in a network
- ✓ Standardized directory access protocol
- ✓ Hierarchical structure
- ✓ Based on X.500 standard – Directional Informational Tree
- ✓ Used in Windows Active Directory, Apple Open Directory, and Novell eDirectory

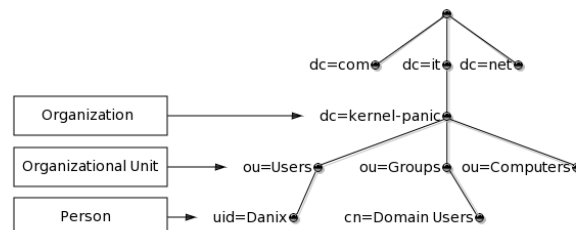


Image courtesy of: <http://www.kernel-panic.it/openbsd/pdc/pdc2.html>



72

72

WAN Technology



- Function at the lower three layers of the OSI model
- Point to point links
 - ✓ Single pre-established WAN (Public Switched Telephone Network) to a remote network
 - ✓ Point to Point Tunneling Protocol
 - ✓ Point to Point Protocol over Ethernet
 - ✓ Authenticate using PAP, CHAP, or MS-CHAP

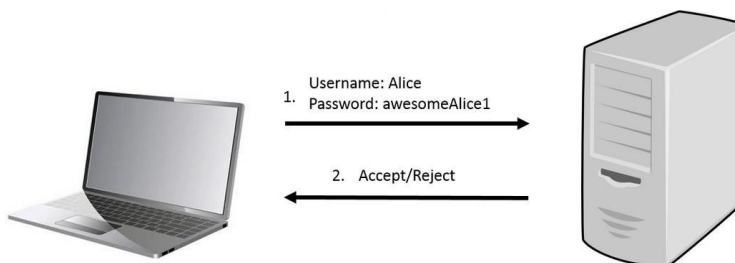


73

73

Authentication Protocols

- **Password Authentication Protocol (PAP)**
 - ✓ **Legacy authentication protocol**
 - ✓ **Cleartext username and password**



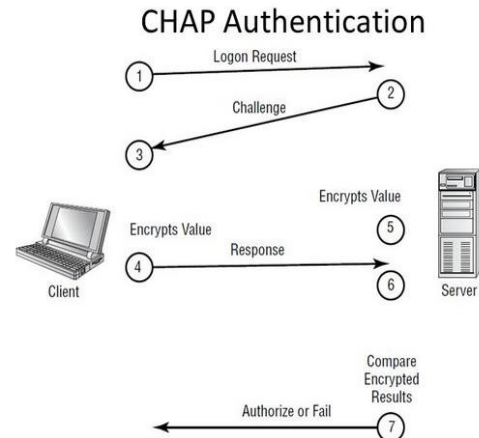
https://en.wikipedia.org/wiki/Authentication_protocol

74

74

Authentication Protocols

- Challenge Handshake Authentication Protocol (CHAP)
 - ✓ Designed to defeat MITM attacks



https://en.wikipedia.org/wiki/Authentication_protocol

75

75

Federated Identities/Authentication

- SAML – Security Assertion Markup Language
 - ✓ Open standard data format for exchanging authentication and authorization data
 - ✓ Open XML standard used for authentication and authorization data
 - ✓ XML-based standard that enables the secure communication of identities between organizations
- OAuth
 - ✓ Authorization Framework – determines what resources
 - ✓ Enables an application to obtain limited access to user accounts on a HTTP service (Facebook and GitHub)
 - ✓ OpenID Connect is designed for attribute release and authentication
- Server Based
 - ✓ Server manages overhead
 - ✓ Assigning session ID
 - ✓ Logs
 - ✓ Difficult with redundancy
- Shibboleth
 - ✓ Open source software package
 - ✓ Web single sign-on
 - ✓ Supports authorization decisions for individual access for protected online resources



76

76

Access Control Model	Description
Mandatory Access Control (MAC)	<ul style="list-style-type: none"> • Compares object's security designation with subject's clearance level. • Clearance level must meet or exceed designation to gain access. • Security labels usually changed by administrator only.
Discretionary Access Control (DAC)	<ul style="list-style-type: none"> • Access to object is controlled through ACLs. • Owner can place subject on ACL or not. • Object owners can usually modify object ACLs.
Role Based Access Control (RBAC)	<ul style="list-style-type: none"> • Subjects assigned predefined roles. • Subject must be in a certain role to access object. • Roles assigned to subjects based on policies.
Rule Based Access Control	<ul style="list-style-type: none"> • Based on operational rules or restrictions. • Restricting access based on time of day is an example. • Rule sets examined before subject is given access to objects.
Attribute Based Access Control (ABAC)	<ul style="list-style-type: none"> • Based on set of attributes the subject possesses. • Follows if x, then y procedure. • Example: If subject has all required attributes, then grant access. • Attributes are created ahead of time and assigned as needed.

Password Management

Password length	Password complexity	Password history	Password reuse	Password lockout
<ul style="list-style-type: none"> • Protects against brute force cracking. • Cracking time increases exponentially with every character. 	<ul style="list-style-type: none"> • Complex password may require special characters, numbers, and lower/uppercase letters. • amsnpcjnyk becomes 4mSn!cjnyk; attacker must use more characters for each round. 	<ul style="list-style-type: none"> • Users must change passwords every so often. • Creates a "moving target" for attackers. • Password remembering forces users not to choose the same passwords over and over. 	<ul style="list-style-type: none"> • Prevents person from using same password for multiple accounts. • If one account is compromised, the others are at risk. • Not fully enforceable on a technical level. 	<ul style="list-style-type: none"> • Account Lockout Duration • Account Lockout Threshold • Resetting Account Lockout Counter

Access Control Technologies

Proximity Card	Smart Card
Microchip has one function - provide identification number	Microchip and memory provides identification, authentication, and store information
Close range and connectionless	Contact or contactless
Commonly used for door access	Commonly used for credit cards and access
	Digital access - digital certificate



79

79

Biometrics

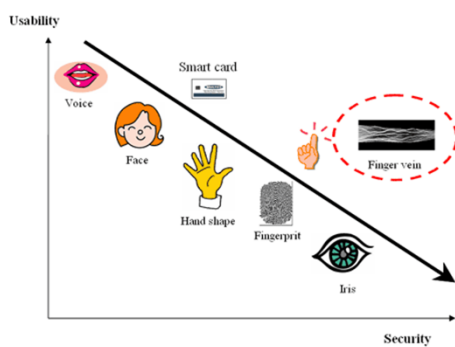


Image courtesy of: <https://security.stackexchange.com/questions/144428/how-secure-is-a-fingerprint-sensor-versus-a-standard-password>

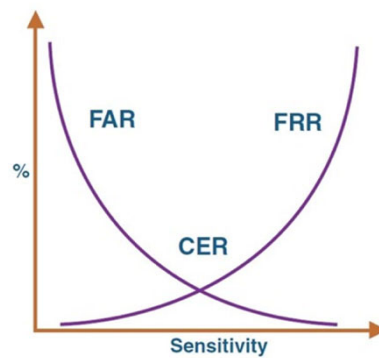


Image courtesy of: <https://pen-testing.sans.org/blog/2015/10/08/whats-the-deal-with-mobile-device-passcodes-biometrics-part-1-of-2>



80

80

Tokens

Pseudo random token generators serves an authentication factor

Physical	Soft
User set pin	Variety of platforms/operating systems
Token generated passcode	SMS based authentication
Must resync with server	Google Authenticator

Event-Based One-Time Password (HMAC-Based One-Time Password)	Time Based One-Time Password
HOTP	TOTP
Secret key and counter	Time
Counter on token and server	30 to 60 second time step
Uses counter as the seed	Short term OTP valid for time step



81

81

Access Control Best Practices

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



82

82

Types of Users



Type of Account	Description
User	General user with restricted privileges
Shared	Application based/group based Difficult to enforce nonrepudiation Shared password
Guest	Anonymous - no privileges
Service	Specific service - vulnerability scanning (tagging sudo)
Privileged	Administrator / root Need two factor authentication Strong password management



83