CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

CECS 303: Networks and Network Security

Final Review

Chris Samayoa

Week 16 – 2nd Lecture
5/5/2022

Course Information

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

- CECS 303
  - Networks and Network Security – 3.0 units
- Class meeting schedule
  - TuTH 5:00PM to 7:15PM
  - Lecture Room: VEC 402
  - Lab Room: ECS 413
- Class communication
  - chris.samayoa@csulb.edu
  - Cell: 562-706-2196
- Office hours
  - Thursdays 4pm-5pm (VEC-404)
  - Other times by appointment only

Network Layer

- Protocol functions
  - Translate network addresses into physical counterparts
  - Decide how to route data from sender to receiver
- Addressing
  - System for assigning unique identification numbers to network devices
- Types of addresses
  - Network addresses (logical or virtual addresses)
  - Physical addresses

Network Layer (cont'd)

- Common Network Layer Protocol
  - IP (Internet Protocol)
- Fragmentation
  - Subdividing Transport layer segments
  - Performed at the Network layer
- Segmentation preferred over fragmentation for greater network efficiency

Data Link Layer

- Protocol functions
  - Divide data received into distinct frames for transmission in Physical layer
- Frame
  - Structured package for moving data
  - Includes raw data (payload), sender's and receiver's network addresses, error checking and control information
- Communications Issues
  - Not all information received
  - Corrected by error checking

Data Link Layer (cont'd)

- Two Data Link layer sublayers
  - LLC (Logical Link Control) sublayer
  - MAC (Media Access Control) sublayer
- MAC sublayer
  - Manages access to the physical medium
  - Appends physical address of destination computer onto data frame
- Physical Address
  - Fixed number associated with each device's network interface

OSI Model - Summary

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

OSI model layer	Function
Application (Layer 7)	Provides interface between software applications and a network for interpreting applications' requests and requirements
Presentation (Layer 6)	Allows hosts and applications to use a common language; performs data formatting, encryption, and compression
Session (Layer 5)	Establishes, maintains, and terminates user connections
Transport (Layer 4)	Ensures accurate delivery of data through flow control, segmentation and reassembly, error correction, and acknowledgment
Network (Layer 3)	Establishes network connections; translates network addresses into their physical counterparts and determines routing
Data Link (Layer 2)	Packages data in frames appropriate to network transmission method
Physical (Layer 1)	Manages signaling to and from physical network connections

Image: Course Technology / Cengage learning

TCP/IP Model

- Four Layers
  - Application layer
  - Transport layer
  - Internet layer
  - Network access layer (or Link layer)

TCP/IP Model (cont'd)

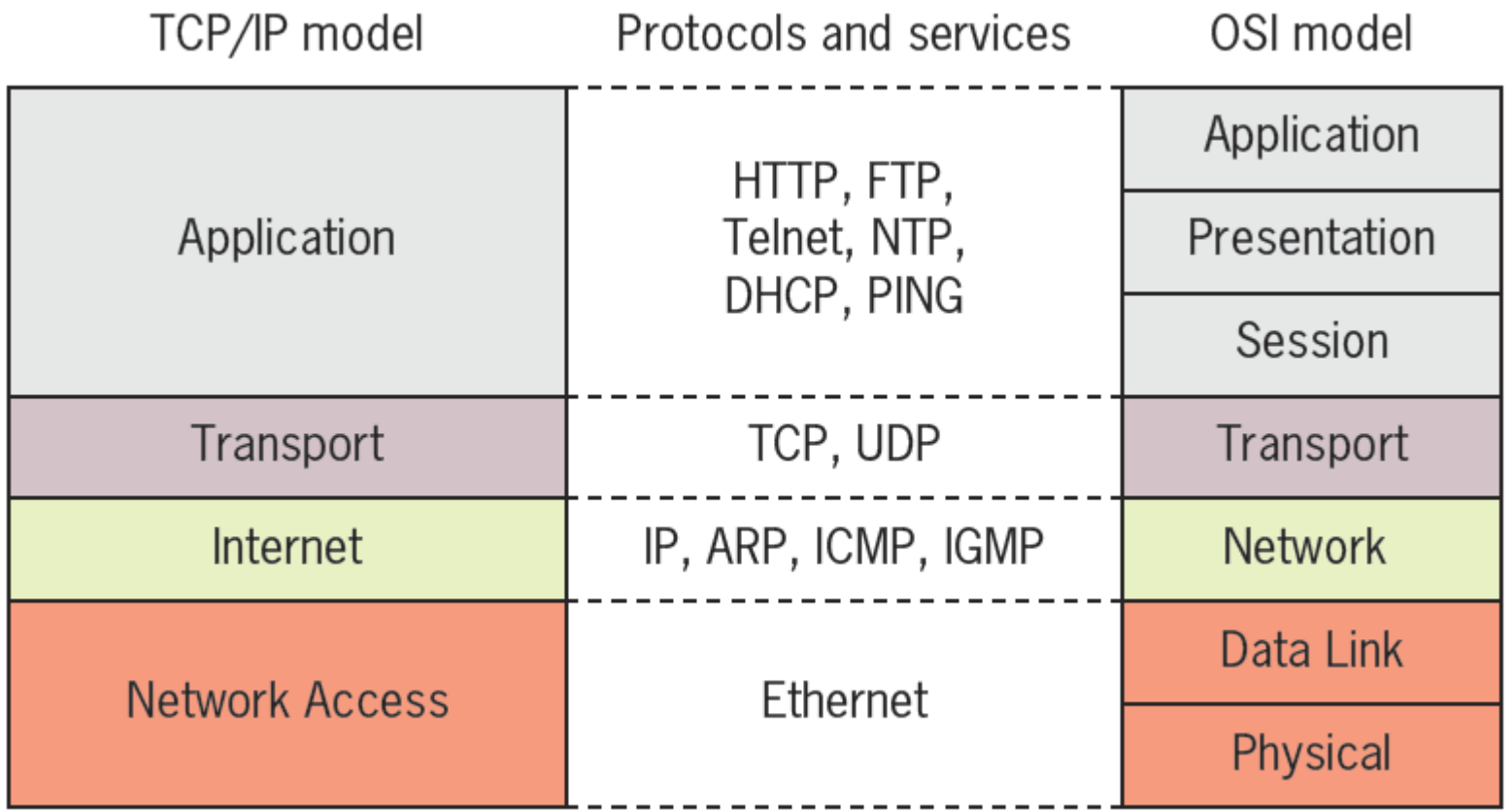


Image: Course Technology / Cengage learning

TCP/IP Overview

- TCP/IP = Transmission Control Protocol / Internet Protocol
- Protocol Suite
  - Commonly referred to as “IP” or “TCP/IP”
  - Subprotocols include TCP, IP, UDP, and ARP
  - Internet layer
  - Network access layer (or Link layer)
- Developed by US Department of Defense
  - Specifically DARPA (Defense Advanced Research Projects Agency)
  - ARPANET (developed in late 1960s) was precursor to TCP/IP protocol suite and internet as a whole

TCP/IP Core

- TCP/IP suite subprotocols
- Mainly operates in Transport or Network layers of OSI model
- Provide basic services to protocols in other layers
- Most significant protocols in TCP/IP suite
  - TCP
  - IP

TCP

- TCP = Transmission Control Protocol
  - Transport layer protocol
- Provides reliable data delivery services
  - Connection-oriented subprotocol
    - Establish connection before transmitting
- Uses sequencing and checksums
- Provides flow control
- TCP segment format
  - Encapsulated by IP packet in Network layer
    - Becomes IP packet's "data"

TCP 3-Way Handshake

- Three segments establish a connection
- Host A issues message to Host B
  - Sends segment with SYN bit set
    - SYN field: Random synchronize sequence number
- Host B receives message
  - Sends segment
    - ACK field: sequence number Host A sent plus 1
    - SYN field: Computer B random number
- Host A responds
  - Sends segment
    - ACK field: sequence number Host B sent plus 1
- FIN flag indicates transmission end

3-Way Handshake (cont'd)

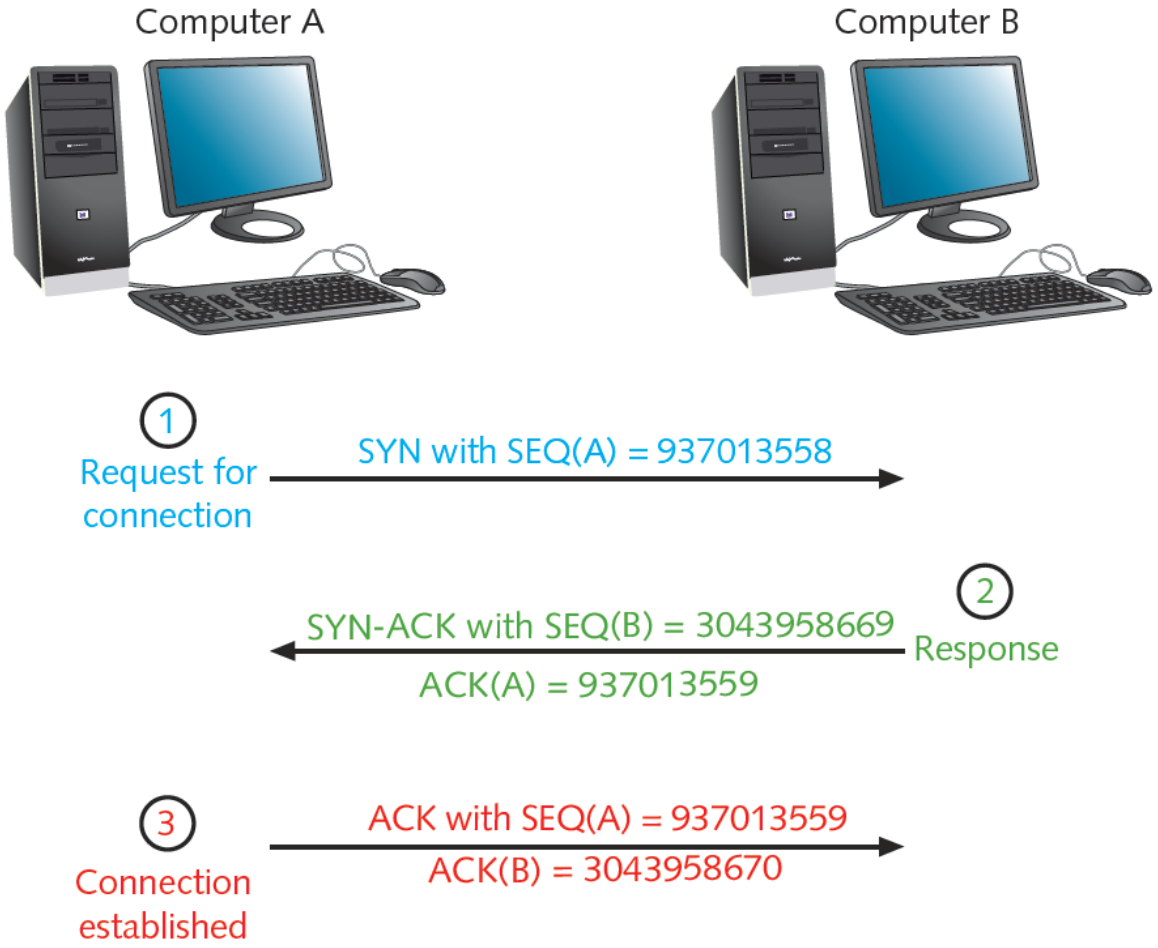


Image: Course Technology / Cengage learning

UDP

- UDP = User Datagram Protocol
  - Transport layer protocol
- Provides unreliable data delivery services
  - Connectionless transport service
  - No assurance packets received in correct sequence
  - No guarantee packets received at all
  - No error checking, sequencing
  - Lacks sophistication
    - More efficient than TCP
- Useful situations
  - Great volume of data transferred quickly

IP (Internet Protocol)

- Network layer protocol
  - How and where data delivered, including:
    - Data's source and destination addresses
- Enables TCP/IP to internetwork
  - Traverse more than one LAN segment
    - More than one network type through router
- Network layer data formed into packets
  - IP packet
    - Data envelope
    - Contains information for routers to transfer data between different LAN segments

IP (cont'd)

- Versions
  - IPv4: unreliable, connectionless protocol
  - IPv6: connectionless or connection-oriented
- "Newer" version of IP protocol
  - IP next generation
  - Released in 1998
- Advantages of IPv6
  - Provides trillions of additional IP addresses
  - Better security and prioritization provisions

ARP

- ARP = Address Resolution Protocol
- Network layer protocol
- Used with IPv4
- Obtains MAC (physical) address of host or node
- Creates database that maps MAC to host's IP address
- ARP table
  - Table of recognized MAC-to-IP address mappings
  - Saved on network device's local storage (host, network switch, etc.)
  - Increases efficiency
  - Contains dynamic and static entries

IPv4 Addressing

- Networks recognize two addresses
  - Logical (Network layer)
  - Physical (MAC / hardware) addresses
- IP Protocol handles logical addressing
- Specific Parameters
  - Unique 32-bit number
    - Divided into four octets (sets of eight bits) separated by periods
    - Example: 192.168.1.1
  - Network class determined from first octet

Common IPv4 Classes

Network class	Beginning octet	Number of networks	Maximum addressable hosts per network
A	1–126	126	16,777,214
B	128–191	> 16,000	65,534
C	192–223	> 2,000,000	254

Image: Course Technology / Cengage learning

IPv4 Addressing (cont'd)

- Class D, Class E rarely used (never assign)
  - Class D: value between 224 and 239
    - Multicasting
  - Class E: value between 240 and 254
    - Experimental use
- Eight bits have 256 combinations
  - Networks use 1 through 254
  - 0: reserved as placeholder
  - 255: reserved for broadcast transmission

IPv4 Addressing (cont'd)

- Class A devices
  - Share same first octet (bits 0-7)
    - Network ID
  - Host: second through fourth octets (bits 8-31)
- Class B devices
  - Share same first two octet (bits 0-15)
  - Host: second through fourth octets (bits 16-31)
- Class C devices
  - Share same first three octet (bits 0-23)
  - Host: second through fourth octets (bits 24-31)

IPv4 Classes

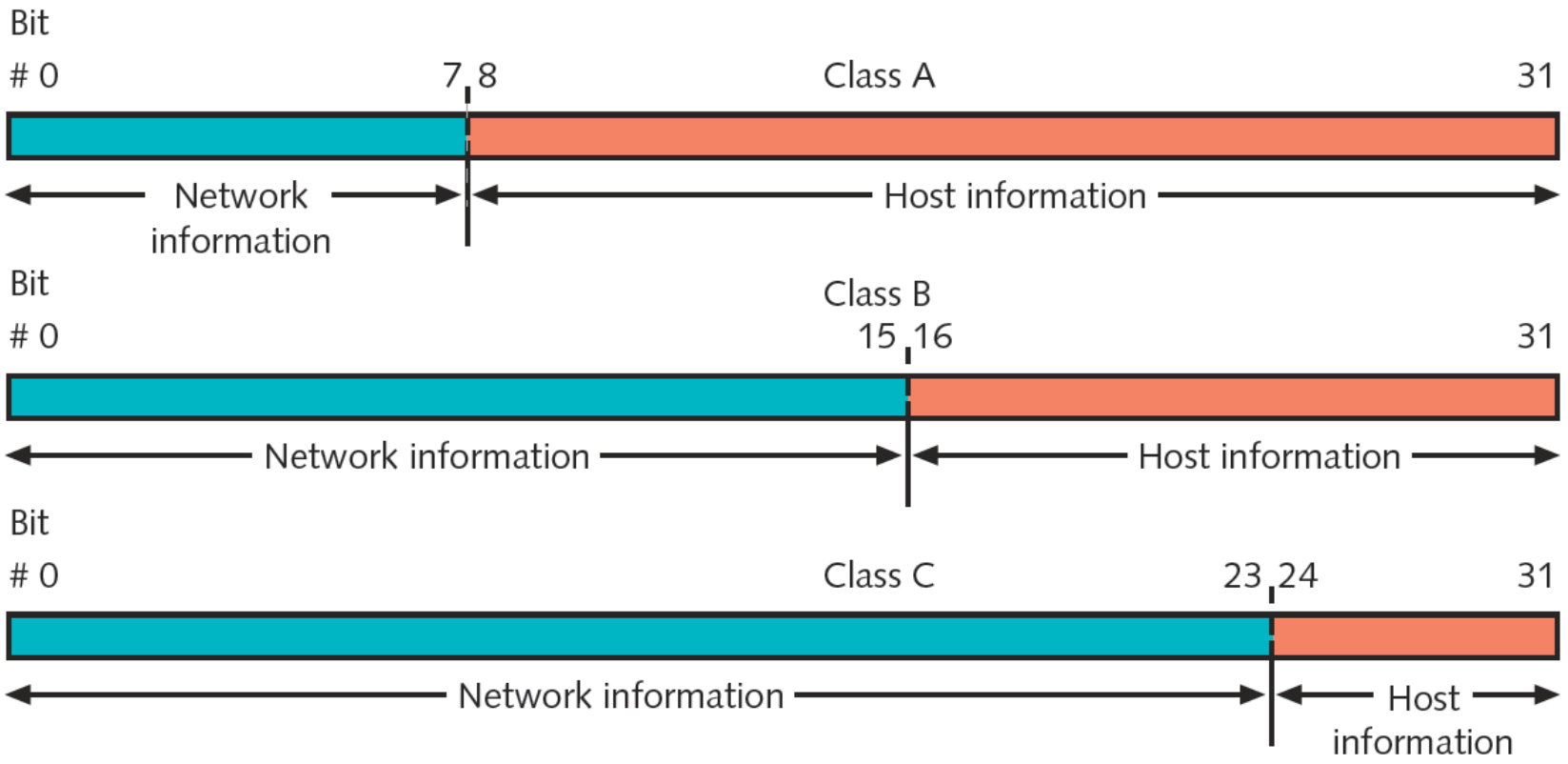


Image: Course Technology / Cengage learning

Subnet Mask

- 32-bit number identifying a device's subnet
- Combines with device IP address
- Informs network about logical subdivision of IPs
- Four octets (32 bits)
  - Expressed in binary or dotted decimal notation
- Assigned same way as IP addresses
  - Manually or automatically (via DHCP)

Subnet Mask (cont'd)

Network class		Default subnet mask
A	1–126	255.0.0.0
B	128–191	255.255.0.0
C	192–223	255.255.255.0

Image: Course Technology / Cengage learning

Assigning IP Addresses

- Government-sponsored organizations
  - Distribute IP addresses
  - IANA, ICANN, RIRs (Regional Internet Registries)
    - ARIN (American Registry for Internet Numbers) responsible for serving the United States (and Antarctica, Canada, and various islands)
- Companies and individuals obtain IP addresses from ISPs (typically)
- Every network node must have a unique IP address
  - Otherwise network errors occur
  - Only one can exist in a router or switch's ARP table

Assigning IP Addresses (cont'd)

- Static IP address
  - Manually assigned
  - To change -> modify client workstation TCP/IP properties
  - Human error causes duplicates
- Dynamic IP address
  - Assigned automatically
  - Most common method
    - Dynamic Host Configuration Protocol (DHCP)

DHCP

- Automatically assigns device a unique IP address
- Application layer protocol
  - Uses lower layers, but functions as a service
  - Still some debate over whether it is an application or network layer protocol
- Reasons for implementing
  - Reduce time and planning for IP address management
  - Reduce potential for error in assigning IP addresses
  - Enable users to move workstations and printers
  - Make IP addressing transparent for mobile users

DHCP (cont'd)

- DHCP leasing process
  - Device borrows (leases) an IP address while attached to network
- Lease time
  - Determined when client obtains IP address at log on
  - User may force lease termination
- DHCP service configuration
  - Specify leased address range
  - Configure lease duration
  - Many additional options are configurable
- Several steps to negotiate client's first lease
  - DHCPDISCOVER
  - DHCPOFFER
  - DHCPREQUEST
  - DHCPACK

DHCP Leasing Process

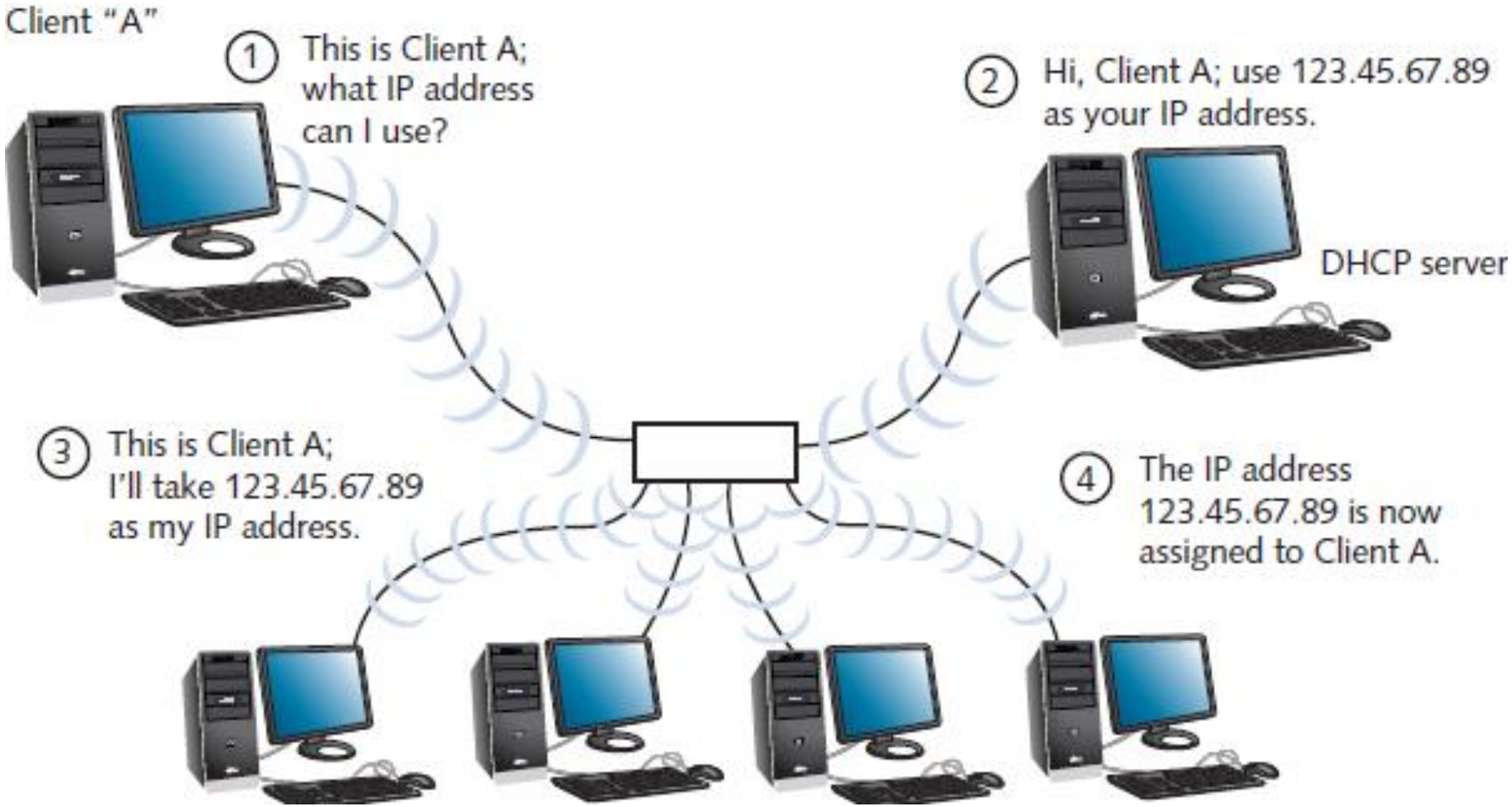


Image: Course Technology / Cengage learning

DHCP (cont'd)

- Terminating a DHCP Lease
  - Expire based on period established in server configuration
  - Manually terminated at any time
    - Client's TCP/IP configuration
    - Server's DHCP configuration
- Circumstances requiring lease termination
  - DHCP server fails and replaced
- DHCP services run on several server types
  - Installation and configurations vary

Private and Link-Local Addresses

- Private addresses
  - Allow hosts in organization to communicate across internal network
  - Cannot be routed on public network
- Specific IPv4 address ranges reserved for private addresses
  - Class A: 10.0.0.0 to 10.255.255.255
  - Class B: 172.16.0.0 to 172.31.255.255
  - Class C: 192.168.0.0 to 192.168.255.255
- Link-local address
  - Provisional address
  - Capable of data transfer only on local network segment

Sockets and Ports

- Processes assigned unique port numbers
- Process's socket
  - Port number plus host machine's IP address
- Port numbers
  - Simplify TCP/IP communications
  - Ensures data transmitted correctly
- Example
  - Telnet port number: 23
  - IPv4 host address: 192.168.1.28
  - Socket address: 192.168.1.28:23

Common Port Numbers

Port number	Process name	Protocol used	Description
20	FTP-DATA	TCP	File transfer—data
21	FTP	TCP	File transfer—control
22	SSH	TCP	Secure Shell
23	TELNET	TCP	Telnet
25	SMTP	TCP	Simple Mail Transfer Protocol
53	DNS	TCP and UDP	Domain Name System
67 (client to server) and 68 (server to client)	DHCPv4	UDP	Dynamic Host Configuration Protocol version 4
69	TFTP	UDP	Trivial File Transfer Protocol
80	HTTP	TCP and UDP	Hypertext Transfer Protocol
110	POP3	TCP	Post Office Protocol 3
123	NTP	TCP	Network Time Protocol
143	IMAP	TCP	Internet Message Access Protocol
443	HTTPS	TCP	Secure implementation of HTTP
546 (client to server) and 547 (server to client)	DHCPv6	UDP	Dynamic Host Configuration Protocol version 6
3389	RDP	TCP	Remote Desktop Protocol

Image: Course Technology / Cengage learning

DNS

- DNS = Domain Name Service
- Hierarchical
- Associate domain names with IP addresses
- DNS refers to:
  - Application layer service accomplishing association
  - Organized system of computers, databases making association possible
- DNS redundancy
  - Many computers across globe related in hierarchical manner
  - Root servers
    - 13 computers (ultimate authorities)

DNS (cont'd)

- Three components
  - Resolvers
    - Any hosts on Internet needing to look up domain name information
  - Name servers (DNS servers)
    - Databases of associated names and IP addresses
    - Provide information to resolvers on request
  - Namespace
    - Abstract database of Internet IP addresses and associated names
    - Describes how name servers of the world share DNS information

Domain Name Resolution

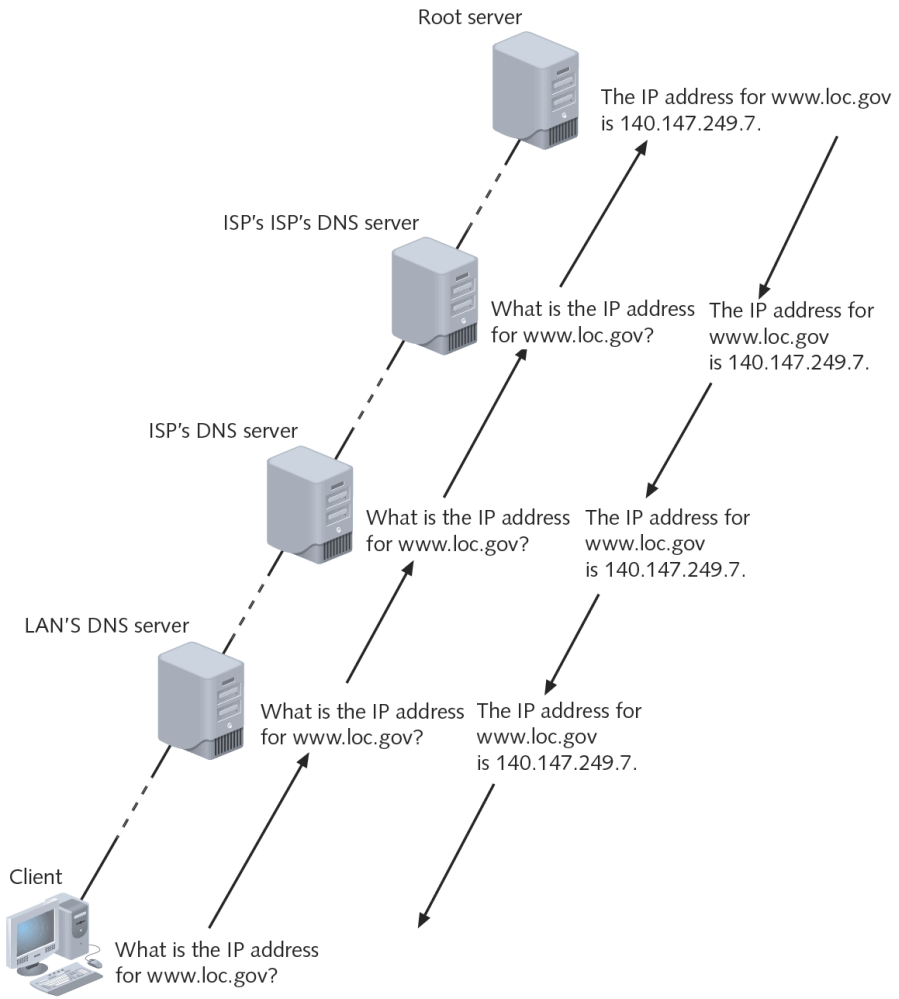


Image: Course Technology / Cengage learning

DNS (cont'd)

- Resource record
  - Describes one piece of DNS database information
  - Many different types
    - Dependent on function

Type	Name	Description
A	Address record	A host's IPv4 address
AAAA	Address record	A host's IPv6 address
CNAME	Canonical name record	Another name for the host
MX	Mail exchange record	Identifies a mail server
PTR	Pointer record	Points to a canonical name

Three Aspects of Security

- Confidentiality
  - Keep data private
- Integrity
  - Keep data from being modified by unauthorized individuals/processes
- Availability
  - Keep the system running and reachable

Policy vs. Mechanism

- A **security policy** defines what is and is not allowed on a network or system
  - Needed for organizations of all sizes
- **Security mechanism** is a method or tool for enforcing security policy
  - Prevention
  - Detection
  - Response
- Types of mechanisms:
  - Identification
  - Authentication
  - Audit
  - Containment

Attacker Type: Published Attack Tools

- Attacker has specific tools
  - Casts the tool widely to see what can be caught.
  - Sometimes described as script-kiddies
    - Gets them into systems with specific vulnerabilities
    - Gets them account access to susceptible employees
  - They gather what they find, exfiltrate or modify, and stop there
- Strong security posture is effective
  - Sound security practices
  - Systems up to date
  - Least privilege

Attacker Type: Opportunistic

- Looks for a weak link
  - Uses tools to scan for vulnerabilities
  - Once in, repeats the process
    - This time starting with elevated access because of the system or user ID already compromised.
  - They gather what they find, exfiltrate or modify, and stop there
- Good containment architecture can be effective
  - Administrators need to be aware of what paths might be used to reach sensitive data

Attacker Type: Goal Oriented and Top Down

- Researches your organization and system
  - Goal is to compromise some component of your system or access specific data.
  - Learns precursor activities that must be achieved to meet that goal.
  - Often applies APT – Advanced Persistent Threat tactics
  - Will wait for threat vector to propagate
- Defense requires comprehensive strategy:
  - Strong security posture
  - Training of privileged employees
  - Containment Architecture
  - Strong defenses to subversion

Monetary Motivations

- Botnets
  - Controlled machines for sale
- “Protection” or “recovery” for sale
- Attack software for sale
- Stolen data for sale
- Intermediaries used to convert online balances to cash
  - These are the pawns and the ones that are most easily caught

Terminology

- Vulnerability
  - A weakness in a system, program, procedure, or configuration that could allow an adversary to violate the intended policies of a system
- Threat
  - Tools or knowledge (capabilities) that are capable of exploiting a vulnerability to violate the intended policies of a system
- Attack
  - An attempt to exploit a vulnerability to violate the intended policies of a system
- Compromise
  - The successful actions that violate the intended polices of a system

Terminology (cont'd)

- Penetration
  - A successful attack (intrusion) that exploits a vulnerability in the code base of a system or its configuration. The result will often be to install a subversion
- Denial of Service
  - An attack that prevents authorized access to a resource, by destroying a target or overwhelming it with undesired requests
- Subversion
  - An intentional change to the code base or configuration of a system that alters the proper enforcement of policy. This includes the installation of backdoors and other control channels in violation of the policy relevant to the system
- Subversion vectors
  - The methods by which subversions are introduced into a system. Often the vectors take the form of malicious code

Terminology (cont'd)

- Secure
  - A system is secure if it correctly enforces a correctly stated policy for a system. A system can only be secure with respect to a particular set of policies and under a set of stated assumptions. There is no system that is absolutely secure.
- Attack Surface
  - The accumulation of all parts of a system that are exposed to an adversary against which the adversary can try to find and exploit a vulnerability that will render the system insecure (i.e. violate the security policies of the system).

General Security Concerns

- Buggy code
- Protocol design failures
- Weak crypto
- Social engineering
- Insider threats
- Poor configuration
- Incorrect policy specification
- Stolen keys or identities
- Denial of service

Security Mechanisms

- Encryption
- Checksums
- Key management
- Authentication
- Authorization
- Audit logs
- Firewalls
- Virtual Private Nets (VPNs)
- Intrusion detection
- Intrusion response
- Development tools
- Virus Scanners
- Policy managers
- Trusted hardware

Identification vs Authentication

- Identification
  - Associating an identify with an individual, process, or request
- Authentication
  - Verification of a claimed identity
  - Ideally
    - Who you are
  - Practically
    - Something you know
    - Something you have
    - Something you are
- Often used in combination
  - e.g. Diffie-Hellman in TLS to exchange AES cipher

Something You Know

- Password or Algorithm
  - e.g. Encryption key derived from password
- Issues
  - How to keep it secret?
    - Find it, sniff it, social engineer it
  - You need to remember it
  - How is it stored and checked?
- Potential attacks
  - Brute force
  - Dictionary
  - Pre-computed Dictionary
  - Guessing
  - Finding elsewhere

Something You Have

- Cards
  - Mag stripe
  - Smart Card
  - USB Key
  - Time varying password
- Issues
  - How to validate?
    - Verifier can be compromised
  - Need special infrastructure
  - e.g. RSA SecureID (https://www.wired.com/2011/06/rsa-replaces-securid-tokens/)

Something You Are

- Biometrics
  - Iris scan
  - Fingerprint
  - Picture
  - Voice
- Issues
  - Need to prevent spoofing

Router Access Lists

- Control traffic through routers
- Router's main functions
  - Examine packets
  - Determine destination
    - Based on Network layer addressing information
- ACL (access control list)
  - aka. access list
  - Routers can decline to forward certain packets
- Stateless
  - Access lists look at packets independent of what traffic has come before

Firewalls

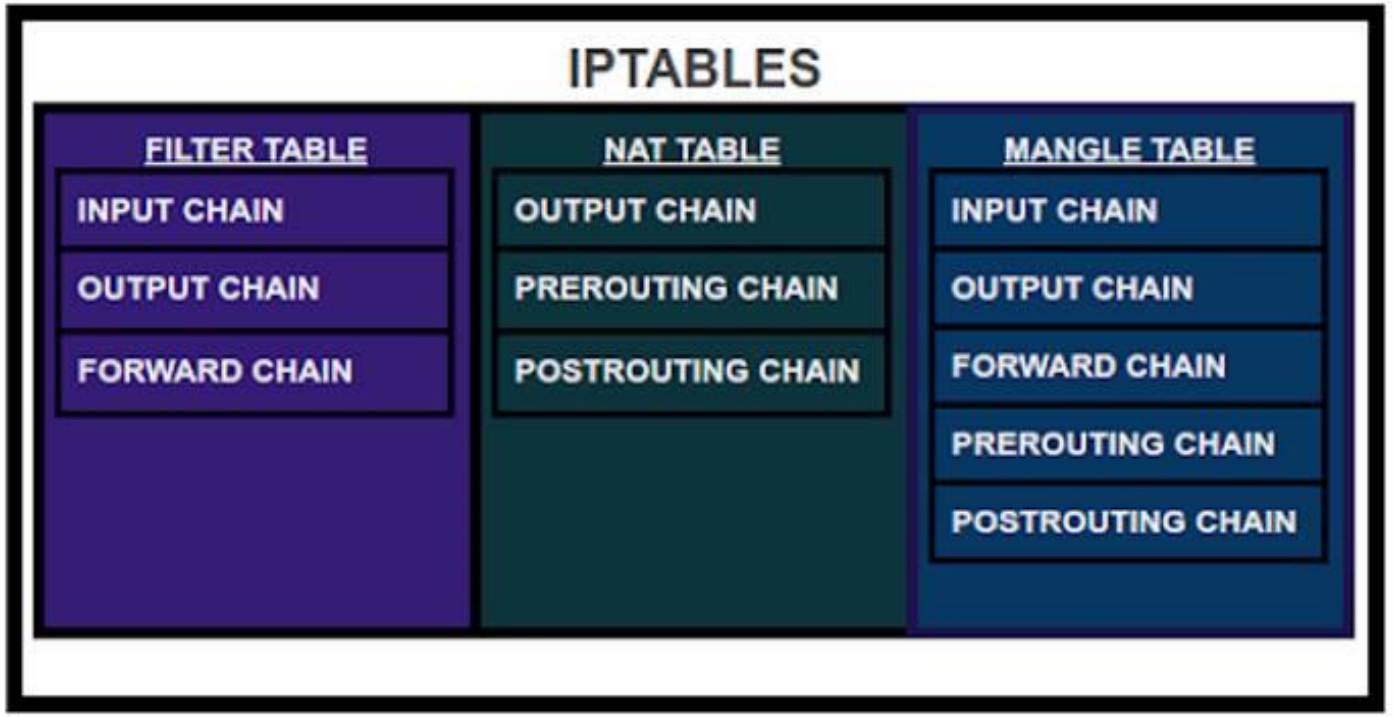
- Specialized device or computer installed with specialized software
  - Selectively filters and blocks traffic between networks
  - Involves hardware and software combination
  - Stateful
    - Decisions can be made based on previous traffic
    - e.g. Allowing return traffic from a web server
- Firewall locations
  - Between two interconnected private networks
  - Between private network and public network (network-based firewall)
  - Between two hosts (host based firewall)

iptables

- What is iptables
  - Firewall utility built for Linux operating systems
  - Stateful
    - But can be configured in a stateless manner
  - Uses policy chains to allow or block traffic
    - List based
- Types of chains
  - Input: used to control behavior for incoming connections
  - Forward: used for rerouting of traffic or NAT
  - Output: used to control behavior for outgoing connections
    - Need to consider return data as well

Iptables (cont'd)

- Filter table
  - Control flow of packets to and from the system
- NAT table
  - Redirect connections to other interfaces on network
- Mangle table
  - Modify packet headers



Source: linode.com

iptables (cont'd)

- Policy chain default behavior
  - What should iptables do if the connection doesn't match any existing rules?
    - ACCEPT
    - DROP (deny)
    - REJECT (deny)

```
user1@cecshost1:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
user1@cecshost1:~$
```

Address Translation

- Private Network
  - Access typically restricted
    - ➢ Clients and machines have proper authentication mechanisms
  - Hiding IP addresses
    - ➢ Provides more flexibility in assigning addresses
- NAT (Network Address Translation)
  - Gateway replaces client's private IP address with public (internet-recognized) IP address
    - ➢ Occurs in packet header
  - Separates private / public transmissions on TCP/IP network
- Reasons for using address translation
  - Overcome IPv4 address availability limitations
  - Add small level of security to private networks that need connectivity to public networks

CVE

- CVE = Common Vulnerabilities and Exposures
- List of publicly disclosed computer security flaws
  - Uses unique ID numbers to track separate vulnerabilities
- Overseen by MITRE corporation
  - Not-for-profit organization
  - Center for research for government and private instititutions
  - Received funding by CISA (Cybersecurity and infrastructure Security Agency) for maintaining CVE program
- Maintains list of vulnerabilities, but does not find them
  - Vulnerabilities are found by various organizations and individuals
- CVSS (Common Vulnerability Scoring System)
  - Open standard for assigning a value to a given vulnerability (0.0 – 10)
  - Higher numbers indicate a higher level of severity

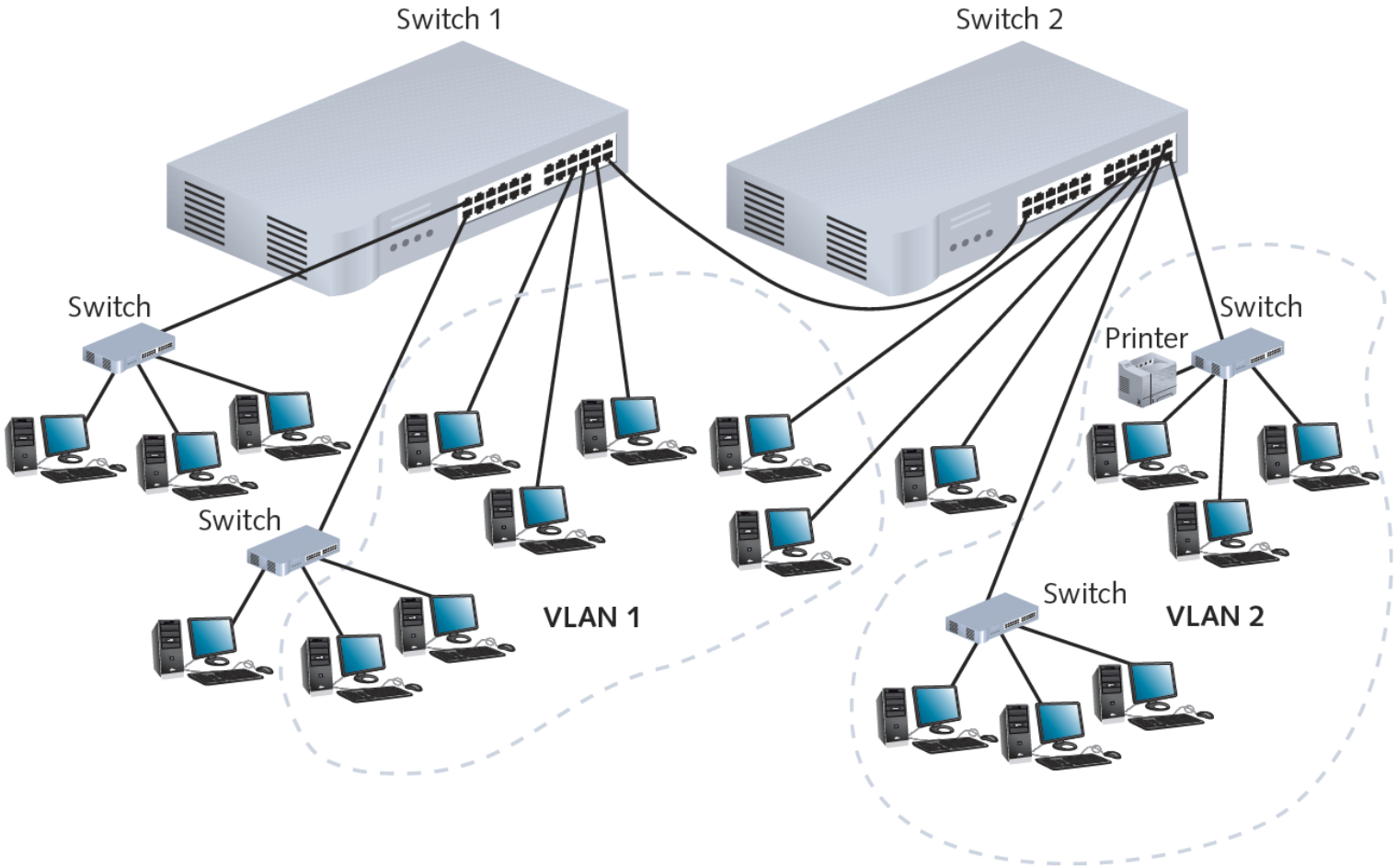
Switches

- Connectivity devices that subdivide a network
  - Segments
- Traditional switches
  - Operate at Data Link OSI model layer
- Modern switches
  - Can operate at Layer 3 or Layer 4
- Switches interpret MAC address information
- Common switch components
  - Internal processor, operating system, memory, ports

VLANs

- VLANs (virtual local area networks)
  - Logically separate networks within networks
    - Groups ports (physical) into broadcast domain
- Broadcast domain
  - Port combination making a Layer 2 segment
  - Ports rely on Layer 2 device to forward broadcast frames
- Collision domain
  - Ports in same broadcast domain could have collisions
  - Switches take care of this issue – each port is a separate collision domain

VLAN Example



Source: Course Technology / Cengage Learning

VLANs (cont'd)

- Advantages of VLANs
  - Flexible
    - Ports from multiple switches or segments
    - Use any end node type
  - Reasons for using VLANs
    - Separating user groups
    - Isolating connections
    - Identifying priority device groups
    - Grouping legacy protocol devices
    - Separating large network into smaller subnets

VLANs and Trunking

- Potential problem
  - Group of nodes getting cut off from rest of network
    - Fix by using a router or Layer 3 switch
- Trunking
  - Switch's interface carries traffic of multiple VLANs
  - Typically used to interconnect multiple switches
- Trunk
  - Single physical connection between switches
- VLAN data separation
  - Frame contains VLAN identifier in header

Attack Vectors

- Trojan Horse
  - Extra code added manually to web page, program, plugin, etc.
- Viruses
  - Self-propagating (on execution)
  - Contains a malicious payload
- Worms
  - Self-propagating through process exploit.
  - Contains a malicious payload
- Penetration Tools (remote or local)
  - Exploits vulnerabilities to violate policy
  - Injection, Overrun, Logic, other
- Impersonation / Insider

General Actions - Payloads

- Modification of data
- Spying - exfiltration
- Stepping off point for further attacks
- Advertising – and tracking interests
- Self Preservation - Rootkits
- Subversion

Defenses to Malicious Code

- Detection
  - Virus scanning
  - Intrusion Detection
- Least Privilege
  - Don’t run as root
  - Separate users ID’s
- Isolation
  - Mandatory controls on information flow
- Sandboxing
  - Limit what the program can do
- Backup
  - Keep something stable to recover

Categorizing Malicious Code

- How does it propogate??
- Trojan Horses
  - Embedded in useful program that others will want to run.
  - Covert secondary effect
- Viruses
  - Tries to propagate itself when the program is started
- Worms
  - Exploits vulnerabilities (bugs) to infect running programs
  - Infection is immediate

Trojan Horses

- People use programs because of a desired and documented effect
- Malicious payload
  - An “undocumented” activity that might be counter to the interests of the user
- Examples: Some viruses; much spyware
- Issues: How do you get a user to run your program?
  - Software that doesn’t come from a reputable source may embed trojans
  - Program with same name as one commonly used can be inserted in search path
  - Depending on settings, visiting a web site or reading an email may cause a program to execute

Zombies / Bots

- Machines controlled remotely
  - Infected by virus, worm, or trojan
  - Can be contacted by master / control server
  - May make calls out so control is possible even through firewall
  - Often uses IRC for control

Spyware

- Infected machines collect data
  - Keystroke monitoring
  - Screen scraping
  - History of URL's visited
  - Scans disk for credit cards and passwords
  - Allows remote access to data
  - Sends data to third party
- Spyware can be local
  - Targeted ads
  - Revenue for referring victim to merchant
  - Might rewrite URL's to steal commissions

Malicious Code - Defenses

- Detection
  - Signature-based
  - Activity-based
- Prevention
  - Prevent certain actions in an environment
  - Take action based on detection
- Sandbox
  - Limits access of running program
  - Program doesn’t have full access or even user-level access
- Detect Modifications
  - Signed executables
  - Tripwire or similar

Root Kits - Subversion

- Hide traces of infection or control
  - Intercept systems calls
  - Return false information that hides the malicious code
  - Return false information to hide effect of malicious code.
  - Some root kits have countermeasures to attempts to detect the root kits
  - “Blue Pill”

Types of Hackers

- White Hat
  - Ethical hacker
  - Trained penetration testers
- Black Hat
  - Malicious attacker
  - “Script Kiddies”?
- Grey Hat
  - Violates laws and ethical standards, but no malicious intent

White Hat

- Permission to engage by organization or customer
  - Always discloses found vulnerabilities
- Techniques
  - Penetration Testing
  - Email Phishing
  - Denial-of-service (DoS) Attack
  - Social Engineering
  - Security Scanning
    - Vulnerability scanners (Nessus)
    - Web Application Vulnerability Scanners (Acunetix / Netsparker)
    - Nikto
    - Metasploit

Black Hat

- Has malicious intent
  - Does not request permission to find vulnerabilities
  - Does not disclose vulnerabilities when found
- Can be skilled hackers or “script kiddies”
  - Title has more to do with intent than ability
  - Traditionally Black Hat hackers referred to skilled malicious actors
- Use same techniques as White Hat hackers
- Often develop specialties
  - Command and control of remote assets
  - (spear)Phishing campains
  - Malicious software development

Black Hat - Organized

- Types of organizations
  - Criminal
  - Nation-state
- Resources
  - Training
  - Sales (partners / resellers / vendors)
  - Call centers
  - International
- Goals:
  - Data exfiltration
  - Extortion
  - Botnets (crypto-mining or DoS for hire)

Grey Hat

- Intent is “typically” not malicious
  - Does not request permission to find vulnerabilities
  - Sometimes discloses vulnerabilities when found
- Can be skilled hackers or “script kiddies”
- Use same techniques as White / Black Hat hackers
- Differences
  - Sometimes violates ethical standards, but without malicious intent
  - Could be attempting to collect a fee for patching vulnerabilities
    - Businesses can decide to seek prosecution
  - Exploitation of vulnerability could be for a “good” cause

Why Pen Test?

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

- Compliance
  - Some industries have specific frameworks that they must adhere to legally
    - Payment card industry (PCI DSS)
    - North American utility companies (NERC CIP)
    - Medical Industry (HIPAA)
    - Department of Defense (CMMS [Cybersecurity Maturity Model Certification])
  - Other organizations may have a self imposed compliance requirement
    - Good publicity
    - ISO 27001
    - NIST-CSF
- Risk Management
  - Cybersecurity insurance will often require penetration testing
  - Acceptable risks can be calculated if needed
- Baselines
  - Regular penetration tests can serve as baselines for needed remediations
  - Set future architecture roadmaps
- Stay informed!

Penetration Testing Types

- White Box
  - Internal structure of network environment is known
  - Tester can view source code and have access to applications and systems
  - Test from developer's / administrators point of view
- Black Box
  - Internal structure is unknown for network environment
  - Little to no information provided to testers
  - Can most closely resemble external actors
    - Time restraints are different
- Grey Box
  - Combination of white box and black box
  - Tester can partially "see" inner working of a network environment
    - Allows for more of the network to be tested within a given time frame
    - Tester granted some permissions or internal access on the network
  - Typically where most penetration tests land

Penetration Testing Stages

- Planning (scoping)
- Reconnaissance
- Gaining Access (exploitation) – Lateral Movement
- Maintaining Access / Escalation
- Analysis / Reporting
- Remediation

Reconnaissance

- Goals
  - Discover attack surfaces (physical and network)
  - Discover overall cybersecurity environment
  - Gain information to assist with vulnerability exploitation
- Publicly available information
  - Company employee directories
  - Whois information
  - DNS information
  - ARIN
- Physical visits
  - What can be learned about the facilities?
  - Lobby officers?
  - Server room locations?
  - Access control?

Reconnaissance (cont'd)

- Social engineering
  - Tailgating
  - Phishing
  - Discover overall cybersecurity environment
  - Gain information to assist with vulnerability exploitation
- Social media or other employee profiles
  - Potential usernames
  - Potential passwords
  - Vacations
  - Insider information
  - Many of this information can help to impersonate individuals

Exploitation

- Can begin while reconnaissance is still ongoing
  - More reconnaissance is needed after successful exploitation
  - Time constraints are always of concern
- Opportunistic approach
  - Chase whatever leads become available
  - Prioritize based on sensitivity and criticality
- Human-hacking
  - Use information gained from reconnaissance to guess passwords or used exposed ones
  - Use known personal information to fool an employee or one of their relations
- Find lateral avenues to continue testing

Exploitation (cont'd)

- General Exploitation Techniques
  - Buffer Overflows
  - Physical Access
  - PC Access
  - WiFi Attacks
    - Rogue access points
    - Crack passcodes
    - Exploit protocol vulnerabilities

Masscan

- Two types of port scanners
  - Synchronous (connection-oriented)
    - Send request to target port and waits for response or time-out
    - Slower
    - More accurate
  - Asynchronous (connectionless
    - Does not wait for response prior to sending out next port probe
    - Less accurate – can't detect dropped packets
- Masscan is incredibly fast (asynchronous scanner)
  - Can facilitate DoS attacks
  - Said to be able to scan the entire internet in 6 minutes
    - 10 million packets per second

POST-MIDTERM

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

Exploitation

- Can begin while reconnaissance is still ongoing
  - More reconnaissance is needed after successful exploitation
  - Time constraints are always of concern
- Opportunistic approach
  - Chase whatever leads become available
  - Prioritize based on sensitivity and criticality
- Human-hacking
  - Use information gained from reconnaissance to guess passwords or used exposed ones
  - Use known personal information to fool an employee or one of their relations
- Find lateral avenues to continue testing

Exploitation (cont'd)

- Evasion (avoiding detection)
  - Anti-Virus
    - Avoid known attack signatures and other known TTPs
  - Encoding
    - Obfuscate actual data/information by rearranging
  - Encrypting
    - Attempt to bypass security checks with encryption. Goal is to decrypt in memory after security mechanisms have performed their checks
  - Process Injection
    - Hide malicious activity within another, legitimate, process
  - Purely Memory Resident
    - Ability to detect when writing to disk is typically greater
    - Attacker can find a way to only live in running memory

Exploitation (cont'd)

- Zero-Day Angle
  - Fuzzing
    - Automated process used to uncover software security bugs using crafted inputs into a program that analyzes the results; often looking for system crashes that can be exploited
    - Can be used with software, firmware, networks, and hardware
    - Can function with or without access to source code
  - Source Code Analysis

Exploitation (cont'd)

- General Exploitation Techniques
  - Buffer Overflows
  - Physical Access
  - PC Access
  - WiFi Attacks
    - Rogue access points
    - Crack passcodes
    - Exploit protocol vulnerabilities

Escalation

- Privilege escalation
  - e.g. Dirty Pipe
  - Allows for additional lateral or local movement
- Continually search for new opportunities
  - Access to new devices or credentials offer potential pathways
  - Different VLANs, IP addresses, or devices have access to different network resources
- Establish persistent access
  - Reverse shells
  - VNC servers
  - Firewall rule changes
  - “Malicious” software

Defense in Depth

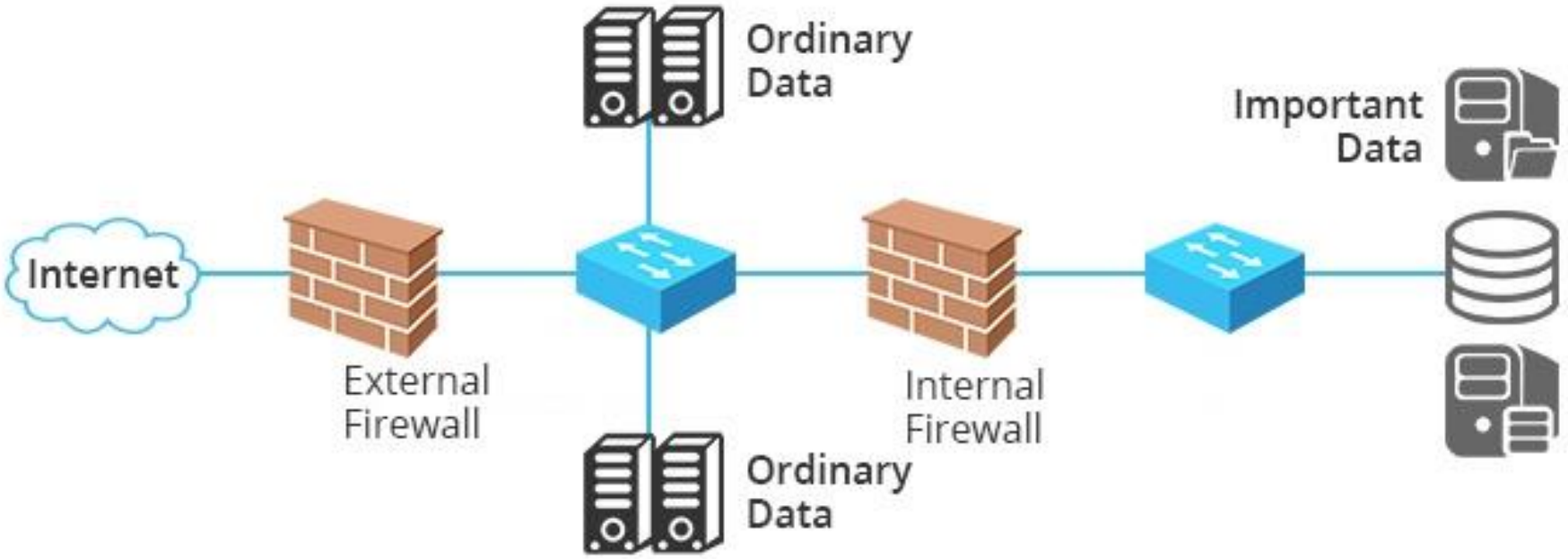
- Refers to a layered approach to network security where defenses are placed at different locations in the environment to enhance an organizations overall security posture
  - Mechanisms may be redundant
  - Overall approach depends on what is being protected
- Major categories
  - Administrative (e.g. policies, procedures, and directives)
  - Physical (e.g. guns, guards, and gates)
  - Technical Controls

Technical Controls

- Commonly used controls
  - Firewalls
    - DMZ
    - Segmentation
  - VPNs
  - Antivirus Software
  - Encryption / Hashing
  - Authentication / Multi-factor Authentication
  - Vulnerability Scanners
  - Sandboxing
  - Intrusion Detection System (IDS)
  - Packet Filters / Deep Packet Inspection (DPI)
  - Logging / Auditing

Firewall Placement

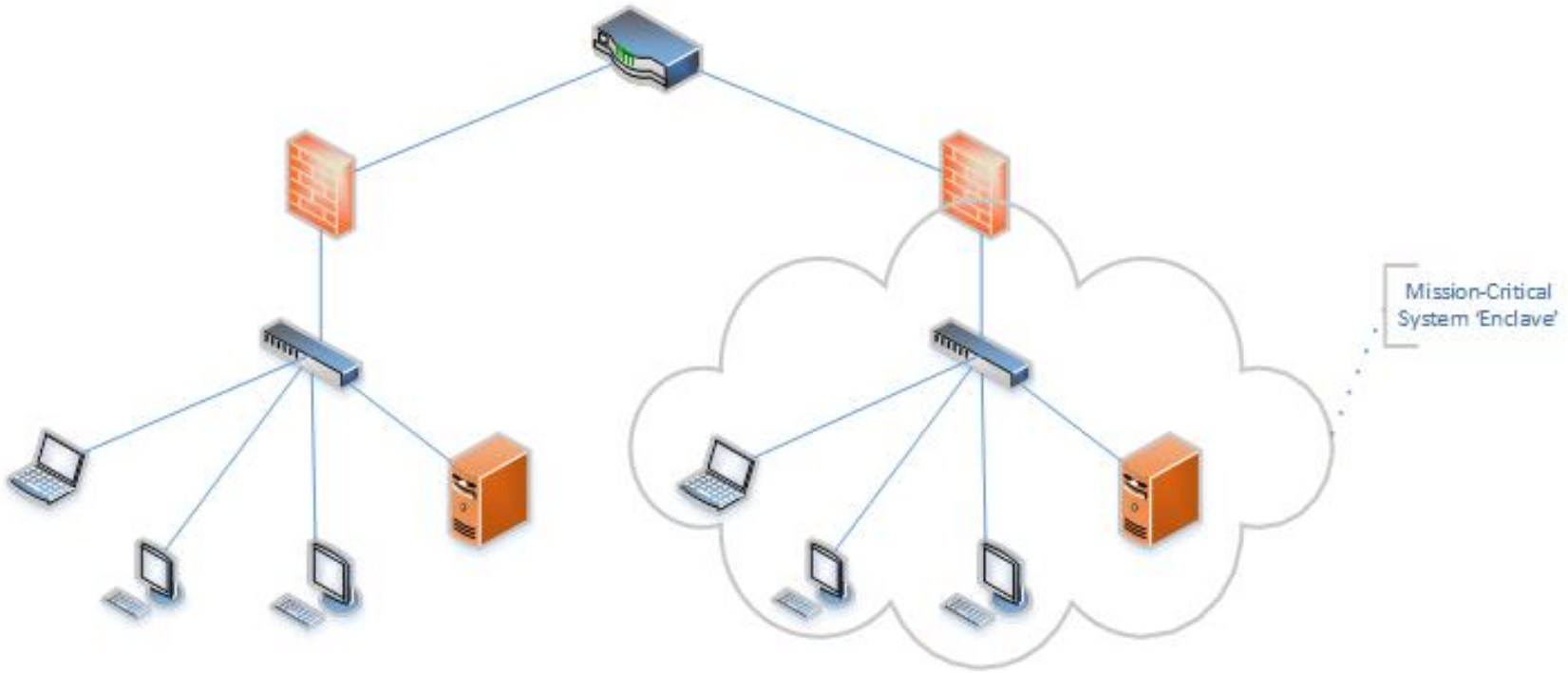
CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering



Source: https://community.fs.com/blog/network-switch-router-firewall-why-need-all-three.html

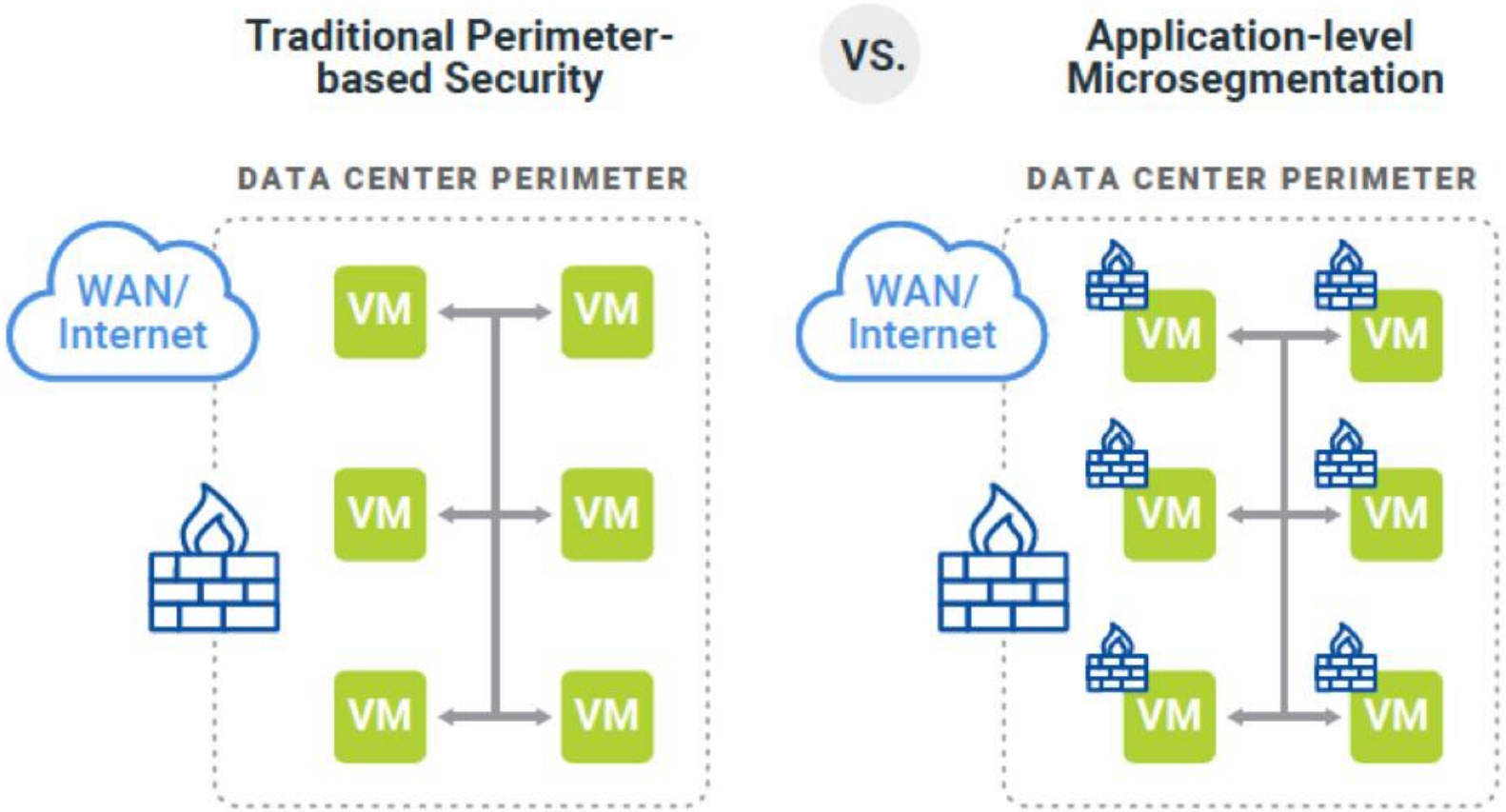
Firewall Segmentation

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering



Source: https://insights.sei.cmu.edu/blog/network-segmentation-concepts-and-practices/

Micro-Segmentation



Source: https://medium.com/@me_isbella/microsegmentation-for-a-better-iot-cdeb25e51941

Sandboxing

- The practice of creating an isolated environment for observing behavior of potentially malicious code or threat actors
  - Important to keep separate from normal / production environments to avoid compromise
- Benefits
  - Mitigation of risk to network devices (e.g. host operating systems)
  - Evaluate potentially malicious software for threats
  - Quality assurance (QA) usage
    - Test before introducing code to production
  - Quarantine threats (including zero-day attacks)

Sandboxing (cont'd)

- Implementation
  - Cloud-based
  - On-premise appliance
  - Software
  - Web browser extensions
- Potential Evasion
  - Malware can be programmed to terminate if sandbox environment is detected
  - Intrusion detection capabilities can be circumvented
    - Encrypted files
    - Large formats
    - Benign file extensions
  - Malware can be "context-aware" in order to wait for triggers that typically indicate end user activity

NMAP

- Main objectives
  - Identify information regarding the scanned target
- What can be found?
  - Existence of network device
    - Ping scans
  - Running services (http, https, smtp, etc)
    - Determined by finding open ports and gathering data
  - Host information
    - Hardware manufacturer
    - Operating system
    - Firewall detection

NMAP (cont'd)

- Linux installation commands:
  - sudo apt update
  - sudo apt install nmap -y
- Common commands
  - Regular Scan
    - nmap [host URL or IP address]
  - Quick Scan
    - nmap -T4 -F [host URL or IP address]
  - Intense Scan
    - nmap -T4 -A –v [host URL or IP address]
  - Intense Scan – All TCP Ports
    - nmap –p 1-65535 -T4 -A –v [host URL or IP address]
  - Intense Scan – With UDP Ports
    - nmap –sS –sU -T4 -A –v [host URL or IP address]

Common Network Attacks

- Malware
  - Malicious software that is used to exploit devices at the expense of victim resources
- Distributed Denial of Service Attack (DDOS)
  - An attack where multiple (typically compromised) systems attack a target with the goal being to overwhelm the resource and make it unavailable for use
- SQL Injection Attacks
  - Attackers can construct a web request that provides unintended access to database resources
  - Can be used to create, modify, delete, or extract data from a database
- Cross-site Scripting (XSS) Attack
  - Attacker injects a malicious script into a trusted website
  - Injected script will then be delivered to a victim's web browser
  - Used to spread malware, steal credentials, or steal user sessions
- Man-in-the-Middle Attack
  - Attacker intercepts communications between two or more parties to intercept data
- DNS Tunneling
  - Command-and-control tactic that uses DNS queries to go undetected
- Email Attacks

Malware Types

- Virus / Worm
- Trojan Horse
  - Program that is downloaded and installed on a device that is believed to be trusted, but is actually malicious
  - e.g. Free program downloads or email attachments
- Spyware
  - Any malicious software that monitors a user's activity on a given device without their knowledge
  - e.g. Internet activity, credentials, and other sensitive information
  - Can perform reconnaissance for government agencies or criminal organizations
- Ransomware
  - Malicious software designed to encrypt a target's files and then demand a ransom to receive a decryption key
  - Often used in conjunction with extortion – Pay us or we leak your data online

DDOS

- Purpose
  - Compromise the availability of a target (e.g. server or website)
  - Can take the form of flooding with traffic or any other exploited vulnerability that crashes the system
- Prevalence
  - Attacks increased by 15% in first half of 2020 to 4.83 million (Help Net Security)
    - Largest attack in 1 hour was 1.12 TBPS (per their available data)
    - 92% of attacks were for less than an hour – 51% decrease in duration from 2019
- Costs
  - Vary by size of business
  - Ransom / extortion

SQL Injection

- Purpose
  - Craft calls to web server with the intention of having malicious instructions sent to a SQL server in the backend
  - Works on dynamic SQL statements
    - Statement is generated at run time using parameters from web form or other query
- Potential Impacts
  - Database corruption
  - Authentication bypass
  - Data tampering / modification (integrity issue)
  - Data theft / exfiltration (confidentiality issue)
  - Deletion of data
  - Arbitrary code execution
  - Complete compromise of system (root access)

SQL Injection - Methods

- Based on user input
  - Web application that uses a form to obtain a user's input
  - Inputs accepted without sanitizing properly
    - ➢ Leads to malicious SQL statements being injected
- Based on cookies
  - Modified cookies can "poison" database queries
  - Web application commonly load cookies from a user's browser
- Based on HTTP headers
  - Fake headers with arbitrary SQL commands can be used to inject code into a database
- Second-order SQL injection
  - Complex
  - Can lie dormant for long periods of time
    - ➢ User-supplied stat is stored by application and later incorporated into SQL queries

Source: https://brightsec.com/blog/sql-injection-attack/

XSS

- Overview
  - Use third-party web resources to run scripts in a victim's web browser
  - Attacker injects malicious payload into a website's database
    - Payload delivered to victim's browser when a webpage is requested
    - JavaScript is typically used by the attacker
  - Similar to SQL injection, but target is website's users (not the web application itself)
- Prevalence
  - According to OWASP.org these are the third most common vulnerability type in 2021
    - Now counted in combination with SQL injections
- Potential Impacts
  - Steal cookies
  - Log key strokes
  - Establish remote access
  - Use machine as botnet

Man-in-the-Middle (MitM)

- Overview
  - Any attack that seeks to intercept communication between two parties
    - Can be user-to-user or user-to-application
  - Goal can be to spy on communication or to impersonate one of the parties
- Prevalence
  - Malware likely used more often to collect personal information from large groups of victims
  - Still a potentially high risk type of attack that can be used to target more specific types of users
- Potential Impacts
  - Stolen personal information
    - e.g. Credentials or credit card information
  - Identify theft
  - Gather information to use for an APT
  - Financial gain

Common MitM Types

- SSL Stripping
  - Establish HTTPS connection between themselves and the server, but use an unencrypted HTTP connection to the client / victim
- Evil Twin
  - Imitates a legitimate Wi-Fi Access Point
  - Connection can be used to prompt user to access a malicious certificate file
  - Pineapple Attack
    - ➢ Device used to emulate a trusted Wi-Fi network / SSID

DNS Tunneling

CALIFORNIA STATE UNIVERSITY LONG BEACH College of Engineering

- Overview
  - Uses DNS protocol to establish persistent communication channel to send data out
    - Could be to command and control server or simply to extract data
  - DNS traffic is often not scanned – so attack can go undetected
- Prevalence
  - Common method to communicate outside of a network once initial compromise has been established
- Potential Impacts
  - Attack can establish persistent access (reverse shell)
  - Sensitive data can be stolen

Common Network Defenses

- Anti-virus
  - Signature-based and NGAV
- Firewalls
  - Host-based
  - Network based
    - Including NGFW(e.g. pfSense, OPNSense, NG Firewall)
    - Deep Packet Inspection (DPI)
- Intrusion Detection Systems
  - Can include network monitors
  - e.g. Snort
- Content Delivery Networks
  - Internet edge protection
  - e.g. Akamai (Kona DDoS Defender), Cloudflare

Common Network Defenses

- Large Cloud Providers
  - Amazon Web Services (AWS), Microsoft Azure, Google Cloud
- Network Security Focused Database Development
  - Parameterized database queries
  - Validate user-supplied data
- Software Development Best Practices
  - Dynamic Testing
  - Fuzzing
- Wireless Protection Best Practices
  - Strong passwords
  - VPNs
  - PKI

DPI

- What is it?
  - Process of analyzing network packets to detect and prevent potential threats and analyze user behavior
- Why is it useful?
  - Can look for signatures and patterns of malware and other types of attacks
    - Detection occurs at a network level
    - Can stop malicious activity before it reaches endpoint devices
  - Prevent data exfiltration
  - Can be used to enforce lawful interception of data by law enforcement
- What about SSL/TLS?
  - Agents can be deployed to individual workstations
  - Certificate signed by organization can be deployed to clients and installed via GPO
    - Often signed by Active Directory Domain's Certificate Authority (CA)

Application-Level Inspection

- What is it?
  - Uses information known about a particular application to determine what “normal” behavior is
  - Typically works in conjunction with DPI
- Why is it useful?
  - Can readily protect against certain attacks on common network protocols
    - e.g. HTTP, HTTPS, SMTP, or FTP
  - Acts as a proxy device between subject / user and application
    - Protections can be added at this layer if necessary
  - Additional rules can be added for custom / unknown applications as needed to be detected at a network level

IDS

- Overview
  - System that monitors network traffic for suspicious or anomalous activity and issues alerts to administrators
  - Should be configured to reflect network policy
    - Often generate false alarms
    - Required fine-tuning to be used effectively
  - Can be signature or anomaly based
  - Custom rules can be created
    - e.g. Snort rules

Source: https://www.geeksforgeeks.org/intrusion-detection-system-ids/

IDS (cont'd)

- Types of IDS
  - Network Intrusion Detection System (NIDS)
    - Monitors whole subnet(s) for known attacks or anomalous activity
  - Host Intrusion Detection System (HIDS)
    - Scans inbound/outbound traffic from single host
    - Can takes snapshots of existing system files and compare them with previous snapshots to detect unexpected changes
  - Protocol-based Intrusion Detection System (PIDS)
    - Can be used to monitor a specific protocol such as HTTPS on a server
    - Can scan traffic as its unencrypted, but before it is processed by the web application
  - Application Protocol-based Intrusion Detection System (APIDS)
    - Can monitor system used by a group of servers
    - e.g. Monitor SQL server middleware from web servers watching for database interactions
  - Hybrid Intrusion Detection System (e.g. NIDS + HID)

Source: https://www.geeksforgeeks.org/intrusion-detection-system-ids/

Content Delivery Networks

- Overview
  - Initially, a content delivery network (CDN) was used to speed up delivery of web content by caching web pages, images, video, etc.
    - Relieved web congestion by bringing content closer to providers
    - Focus is on distributing content of "origin" servers to local caches
  - Adds resiliency to web applications
    - Content is distributed geographically so that there is not a single point of failure
  - Often used to protect against DDOS attacks
    - Large availability of bandwidth and servers can typically withstand these attacks without affecting the web application
    - Avoids bringing down individual company networks (e.g. internet connections)
  - CDNs carried 56% of all internet traffic in 2017
    - Expected to carry 72% of internet traffic by 2022 according to Cisco

CDNs (cont'd)

- Overview of services
  - Increases performance in serving content by using caches
  - Protects against other common attacks
    - SQL injection
    - Cross-site scripting
  - Provides threat intelligence based on vast networks
    - Data can be used to protect customers from zero-day attacks
  - Attacker can still directly attack an organization's public IP addresses
  - Can be used as a proxy for filtering outbound user traffic for an organization

DB Development

- Overview
  - SQL injection attacks can largely be avoided by using best practice development, including the following:
    - Parameterized database queries (Prepared Statements)
      - Bound / typed parameters
    - Parameterized stored procedures in the database
  - Important to keep network security in mind during all stages of development
- Additional recommendations
  - Keep software components patched
    - e.g. libraries, frameworks, web server software, etc.
  - Use appropriate service accounts for transactions from web servers to databases
    - Consider principle of least privilege when creating accounts
    - Never use root / admin accounts for services
    - Use separate service accounts for different web applications
  - Validate user input for expected format
  - Ensure that database error messages are not sent to client web browser

DB Development (cont'd)

- Unsafe SQL query example:

```
String query = "SELECT account_balance FROM user_data WHERE user_name = "
            + request.getParameter("customerName");
try {
      Statement statement = connection.createStatement( ... );
      ResultSet results = statement.executeQuery( query );
}
...
```

* Unvalidated "customerName" parameter is appended to the query

Source: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

DB Development (cont'd)

- Prepared Statements
  - Definition: precompiled SQL statement
  - Includes the use of variable binding
    - Meaning that user-supplied inputs can only used as a variable and not separate commands
  - Developer must first define all SQL code
    - Each parameter is passed to SQL query later on
    - Allows database to distinguish between code and data
  - Allows database to distinguish between code and data
  - Attacker unable to change intent of query
    - Even when using SQL commands within user-supplied input
    - e.g. userID of ***tom' or '1' = '1*** would be interpreted literally as the name of a user

Source: https://owasp.org/www-community/attacks/SQL_Injection

DB Development (cont'd)

- Prepared statement example using Java:

```
// This should REALLY be validated too
String custname = request.getParameter("customerName");
// Perform input validation to detect attacks
String query = "SELECT account_balance FROM user_data WHERE user_name = ? ";
PreparedStatement pstmt = connection.prepareStatement( query );
pstmt.setString( 1, custname);
ResultSet results = pstmt.executeQuery( );
```

  - '?' is a placeholder for the variables
  - 'pstmt.setString' command passes the prepared statement the user-supplied input
  - SQL injection attack has now been avoided

Source: https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

DB Development (cont'd)

- Prepared statement example 2 using Java:

```
String firstname = req.getParameter("firstname");
String lastname = req.getParameter("lastname");
// FIXME: do your own validation to detect attacks
String query = "SELECT id, firstname, lastname FROM authors WHERE firstname = ? and lastname = ?";
PreparedStatement pstmt = connection.prepareStatement( query );
pstmt.setString( 1, firstname );
pstmt.setString( 2, lastname );
try
{
    ResultSet results = pstmt.execute( );
}
```

  - '?' is a placeholder for the variables
  - 'pstmt.setString' command passes the prepared statement the user-supplied input
    - Numbered from left to right for placeholder values
  - SQL injection attack has now been avoided

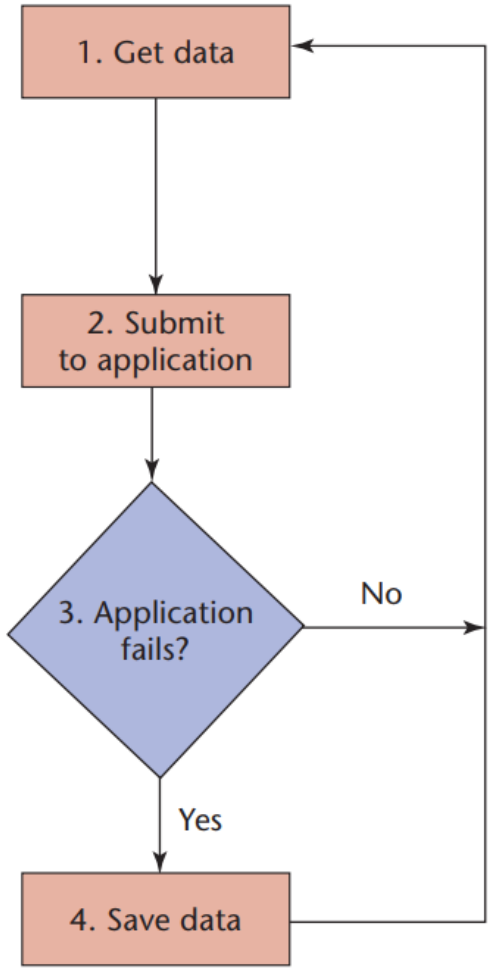
Dynamic Testing

- What is it?
  - Testing of software behavior with dynamic variables to find weak areas in software
    - Essentially software validation
    - Attempt to test in “real” environment
  - Code is executed
    - Hopefully with extremes of valid/invalid input
    - Altered timing – time of check to time of use (TOCTOU)
    - Stress tests
  - Typical of QA testing for a product
- Types of dynamic testing
  - White Box
    - Internal structure / design is known to tester
    - Typically performed by developers
    - Goal is to check system performance
  - Black Box
    - Internal structure / design is not known to the tester
    - Typically performed by third party or QA team
    - Goal is to ensure functionality of system and to test non-functional items as well such as security
      - e.g. verify that authentication / authorization is functioning properly

Source: https://www.guru99.com/dynamic-testing.html

Fuzzing

- What is it?
  - Highly automated testing technique that covers a multitude of boundary cases using invalid data as input in search of exploitable vulnerabilities
    - ➢ Attempt to ensure that a product does not do what it is not supposed to do
    - ➢ Behavior of application is observed for unexpected results / flaws
      - ○ e.g. crashes or memory leaks
  - Random testing
    - ➢ Use static / dynamic testing results as starting points
  - Tool / technique used by both testers and potential attackers
- Types of inputs typically used
  - Extreme limits / bounds (or beyond)
    - ➢ Value, size type, etc.
  - Test via different avenues
    - ➢ e.g. command line and GUI



File-based Fuzzing

- Mutate or generate inputs and run the target program with them
- Example for grammar-based file
  - Specified as regular expressions or CFGs (content free grammars)
    - ➢ e.g. Blab tool

```
% blab -e '(([wrstp][aeiouy]{1,2}){1,4} 32){5} 10'
soty wypisi tisyro to patu
```

Network-based Fuzzing

- Fuzzer acts as ½ of communicating pair
  - Potential inputs could come from replaying previous interaction mutating inputs or by using generational inputs
- Functions as “man-in-the-middle” for purposes of testing
  - Fuzzer can mutate inputs as they are exchanged by two other parties
- Applications
  - SPIKE
  - BURP Intruder

Fuzzing (cont'd)

- Limits
  - Random sample of behavior
  - Usually only finds simple flaws
  - Often a rough measure of software quality
  - Not a proof that software is correct
    - Bugs found are not a comprehensive list
- Goals
  - Find root causes of issues found
    - Commonalities among inputs that cause crashes or unexpected behavior can point towards the same bug
  - Determine whether the unexpected behavior is an exploitable vulnerability
    - e.g. buffer overrun

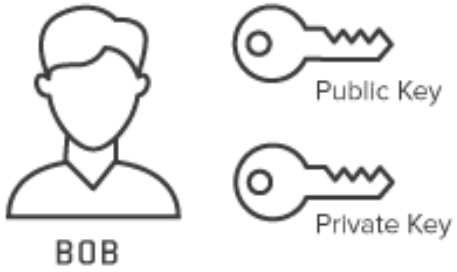
PKI

- Public Key Infrastructure (PKI)
  - Framework for encrypting communications between two nodes
    - Server-to-server
    - Client-to-client
    - Server-to-client
  - Most common form uses private and public key combination (asymmetric)
    - Allows for encrypted messaging
    - Allows for digital signatures to verify authenticity
  - PKI Certificates verify the owner (authentication) of a private key to allow for a trusted relationship
- Why use PKI?
  - Authentication
    - Signatures
  - Encryption
  - Data integrity
    - e.g. signed applications

Asymmetric Encryption

- Public key can be used by anyone to encrypt data
- Private key can be used by specific entity to decrypt data
- Common uses?
  - SSH algorithms
  - SSL/TLS
  - S/MIME encrypted email
  - Code signing
  - Bitcoin/Blockchain
  - Signal private messenger
  - Digital signatures
  - Authenticating nodes connecting to a wireless network
  - Authenticating connections to your VPN
  - Smart card authentication
- Powers PKI

PKI (cont'd)



Decrypt: $D(K_{priv}C) = M$

Sign: $S = E(K_{priv}M)$

Encrypt: $C = E(K_{pub}M)$

Verify: $D(K_{pub}S) = M$

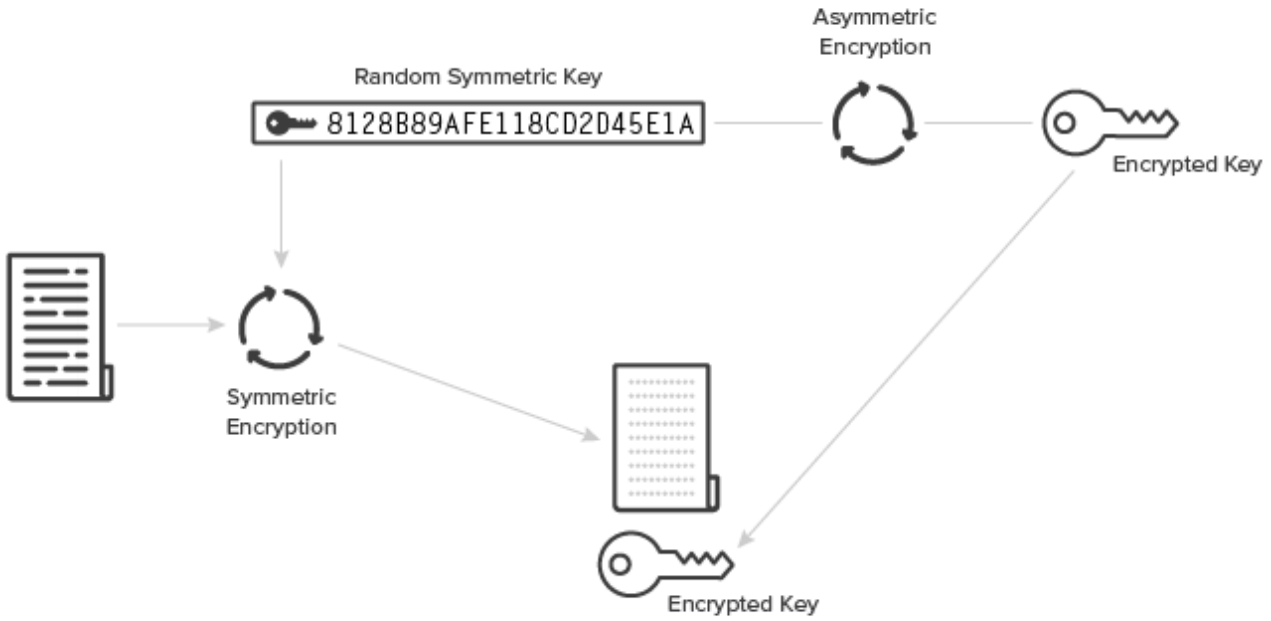
RSA, Diffie-Hellman, ECC

- SSH
- SSL / TLS
- S/MIME encrypted email
- Code Signing
- Bitcoin / Blockchain
- Signal Private Messenger
- Public Key Infrastructure

Source: https://www.keyfactor.com/resources/what-is-pki/

PKI (cont'd)

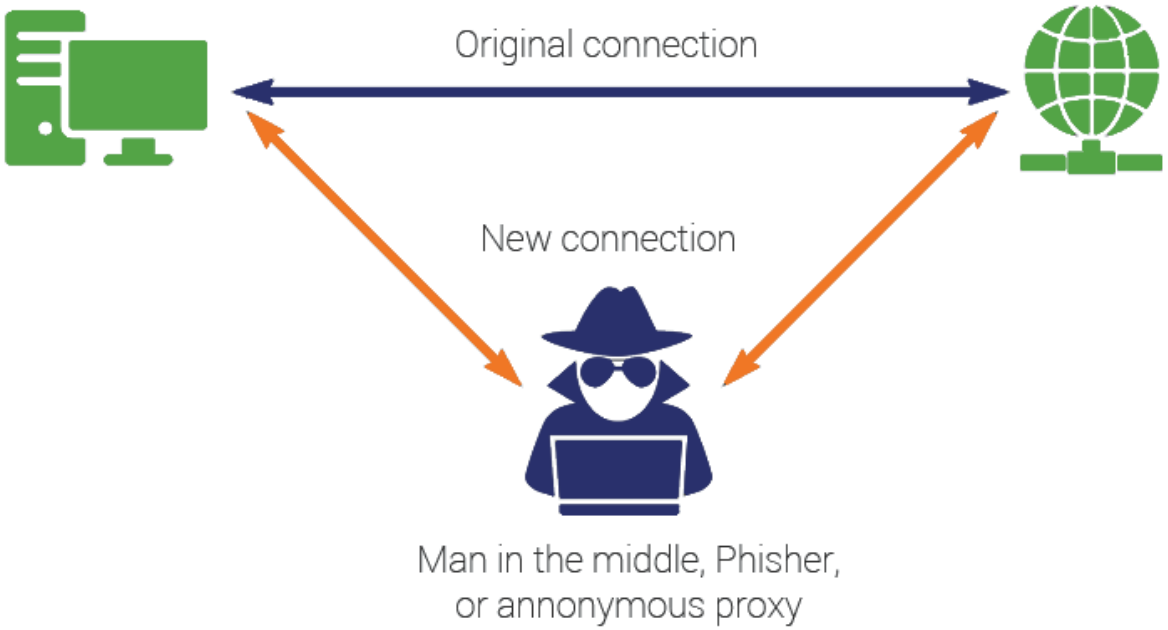
- Symmetric encryption is faster than asymmetric encryption
  - Asymmetric is often used just to send a symmetric key instead of a whole message



Source: https://www.keyfactor.com/resources/what-is-pki/

PKI Problem

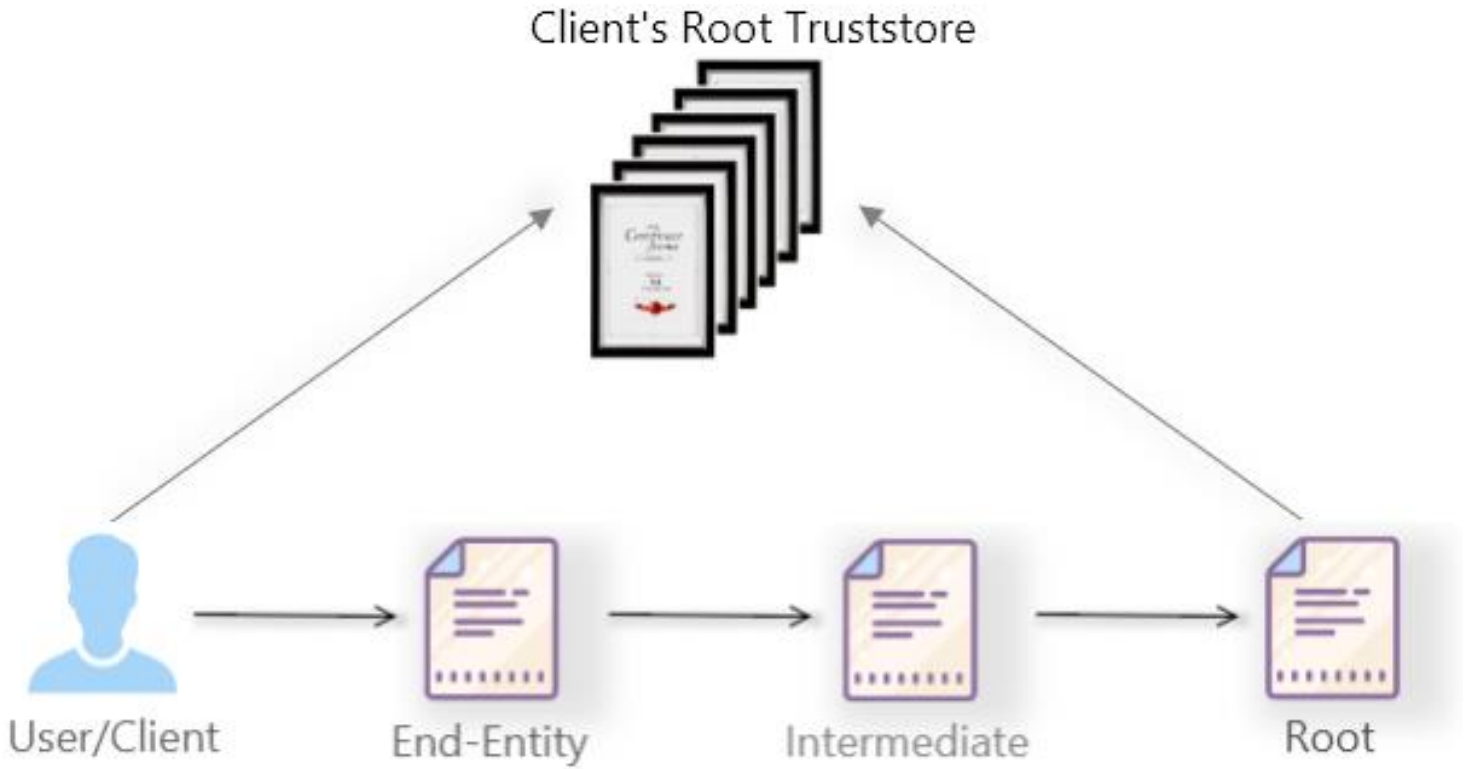
- How do you know that the public key you received comes from the entity you are trying to communicate with?
  - Major potential for MitM attack



Source: https://www.thesslstore.com/blog/man-in-the-middle-attack-2/

PKI Solution

- Trusted third party



Source: https://www.keyfactor.com/blog/certificate-chain-of-trust/

Digital Certificates

- Verify the identify of a device or user and enable encrypted connections
  - aka X.509 certificates or PKI certificates
    - IETF – RFC 5280
    - https://datatracker.ietf.org/doc/html/rfc5280
- Features
  - Mechanism for authentication
  - Hold information about a particular entity
  - Issued by trusted third party
  - Tamper-resistant
  - Authenticity of document can be proved
  - Trackable back to issuer
  - Set expiration date
  - Is presented for validation
  - Authenticating connections to your VPN
  - Smart card authentication

Digital Certificates (cont'd)

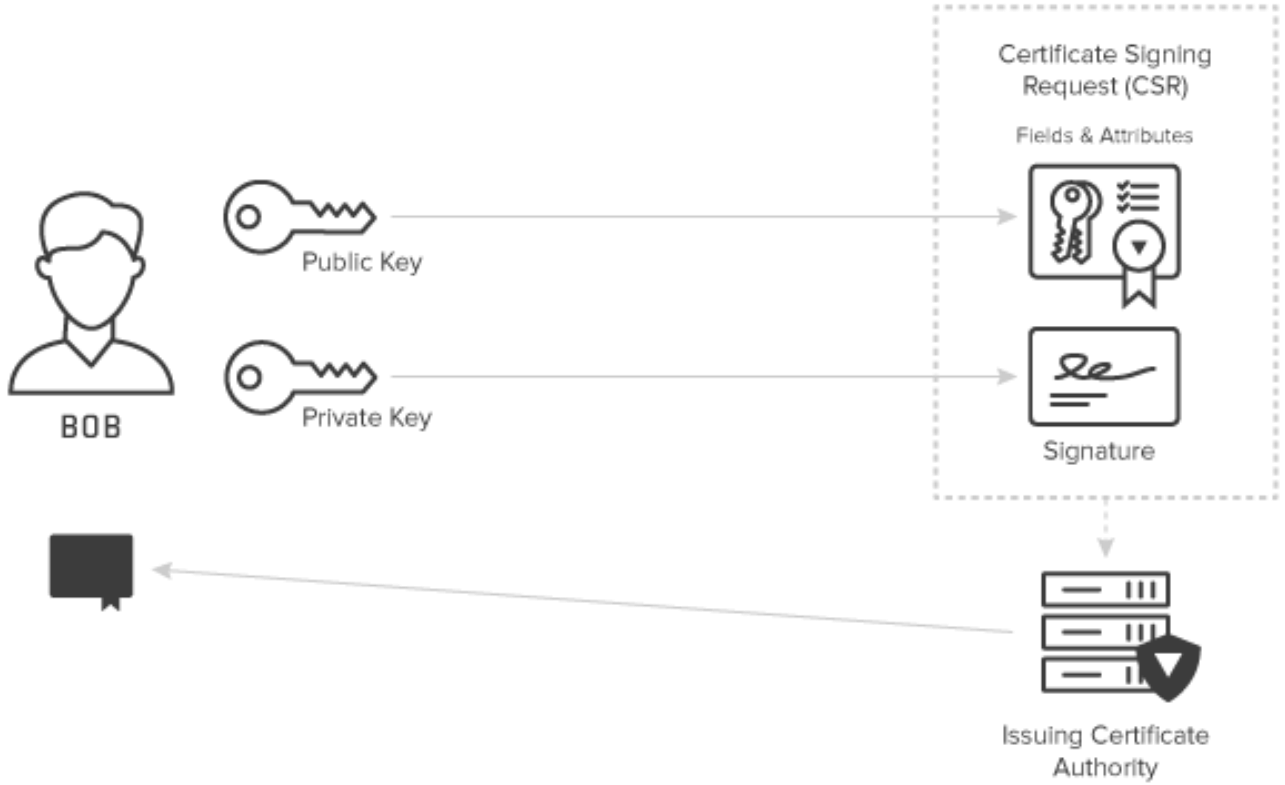
- Major Components
  - Digital Certificates
    - Electronic identification for websites and organizations
    - Can be self-created or obtained through a trusted third-party issuer
  - Certificate Authority (CA)
    - Vet organizations requesting certificates
    - Issue certificates
    - Establish "trusted" relationships
  - Certificate Revocation Lists (CRLs)
    - Mechanism to track revoked certificates

Certificate Authority

- Overview
  - Responsible for creating and issuing digital certificates, including
    - Vetting methods for certificate requestors
    - Scope of certificate(s)
    - Parameters specified within certificate(s)
- Certificate creation process
  - Private key generated and used to compute corresponding public key
  - CA requests identifying attributes of the private key owner and vets the information
  - Public key and vetted attributed are encoded into a Certificate Signing Request (CSR)
  - CSR is signed by key owner to prove possession of specific private key
  - Issuing CA validates the request and signs the certificate with the CA's own private key
    - Note that each CA also has its own public and private keys
    - Establishes need for CA hierarchies
- As long as CA is deemed trustworthy by end users, they can be used to verify the owner of a particular public key

Source: https://www.keyfactor.com/resources/what-is-pki/

Certificate Authority (cont'd)



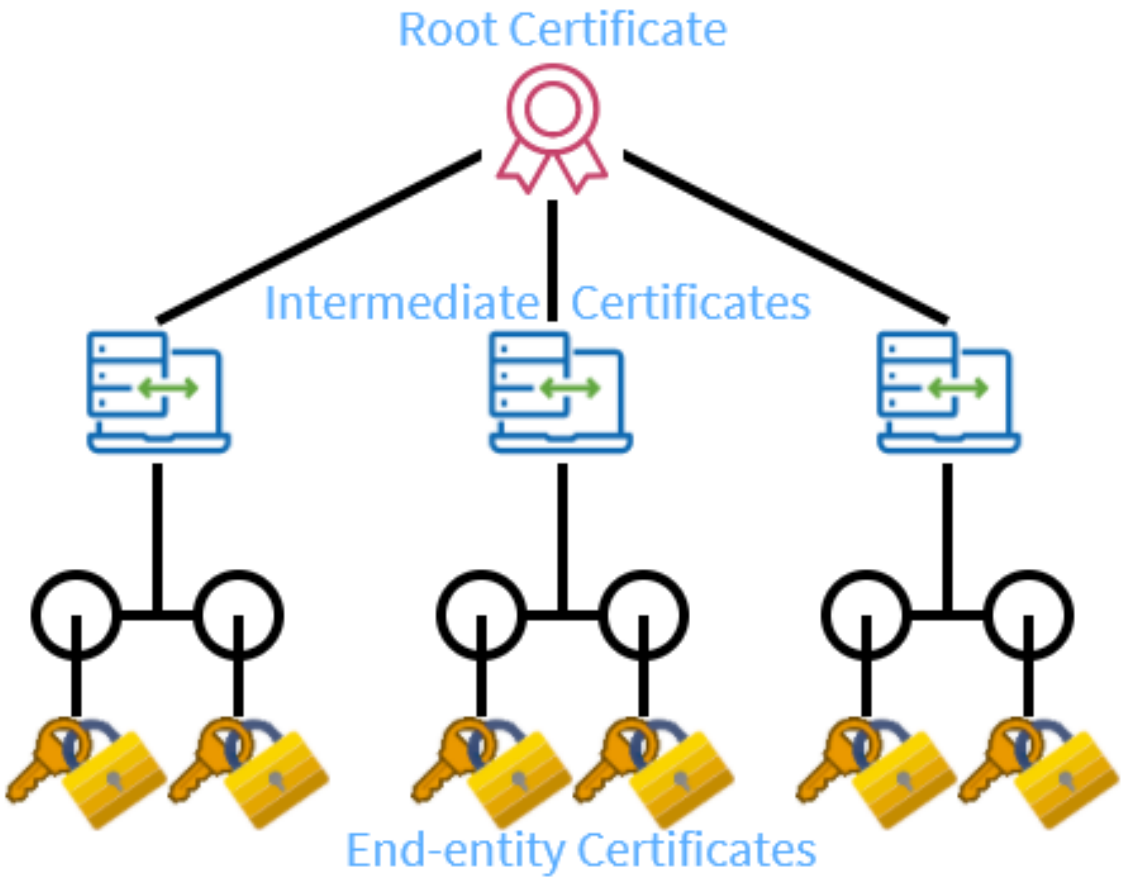
Source: https://www.keyfactor.com/resources/what-is-pki/

Chain of Trust

- Types of entities
  - Root CA
    - Self-signed certificate -> “trust anchor”
    - Must be trusted for entire process to work
    - Very closely guarded – often kept “offline”
    - Expire every 15-20 years
  - Intermediate CA
    - Responsible for issuing certificates
      - To other intermediate CAs
      - To end-entity
    - Provides extra level of security between end-entity servers and root CA
  - End-entity Certificate
    - Does not guarantee that subject is trustworthy
    - Certificates are typically issued for organizations (not employees)
    - Parameters specified within certificate(s)

Source: https://www.keyfactor.com/blog/certificate-chain-of-trust/

Typical Trust Model



Source: https://www.keyfactor.com/blog/certificate-chain-of-trust/

Digital Certificate Risks

- What happens if private keys are compromised?
  - End-entity
    - Communication to that server can no longer be authenticated
    - Certificate needs to be revoked
    - New certificate needs to be issued
  - Intermediate CA
    - All end-entity certificates issued by the CA must be revoked and reissued
    - New asymmetric keys
    - New certificate must be issued by root CA (or other authority)
  - Root CA
    - All child CA certificates and end-entity certificates issued by those child CAs must be reissued
    - Root CA must be re-established

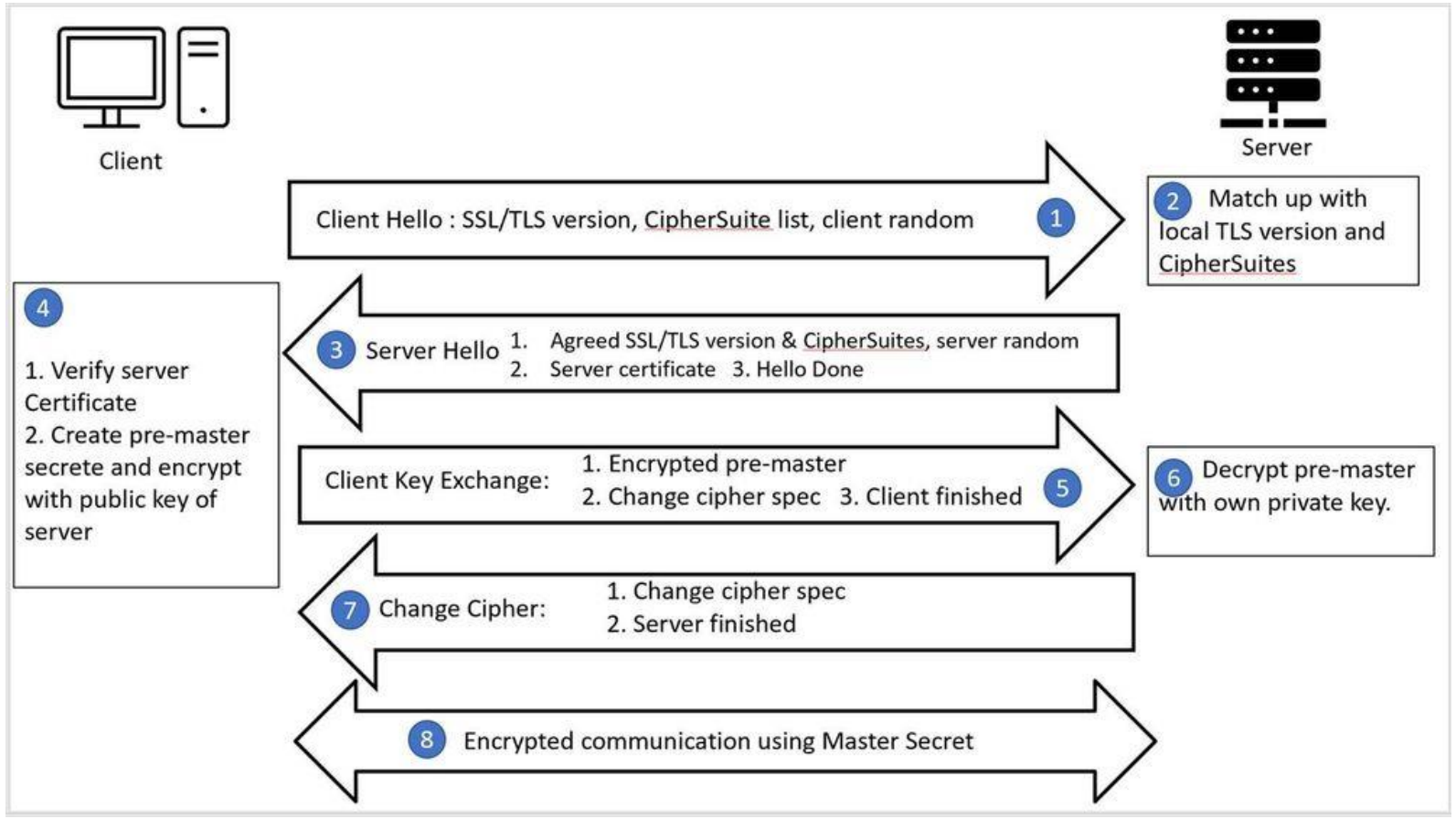
Certificate Revocation Lists

- Each CA must issue its own certificate revocation lists
  - Part of the standard for X.509 certificates
- Consumers must check CRLs for them to be effective
  - Slows down authentication process
    - Slower for each part of the hierarchy checked
- Were not commonly used before
- Have grown in usage by consumers
  - Due to internet security concerns

Check CRL

Source: https://www.thesslstore.com/blog/crl-explained-what-is-a-certificate-revocation-list/

TLS



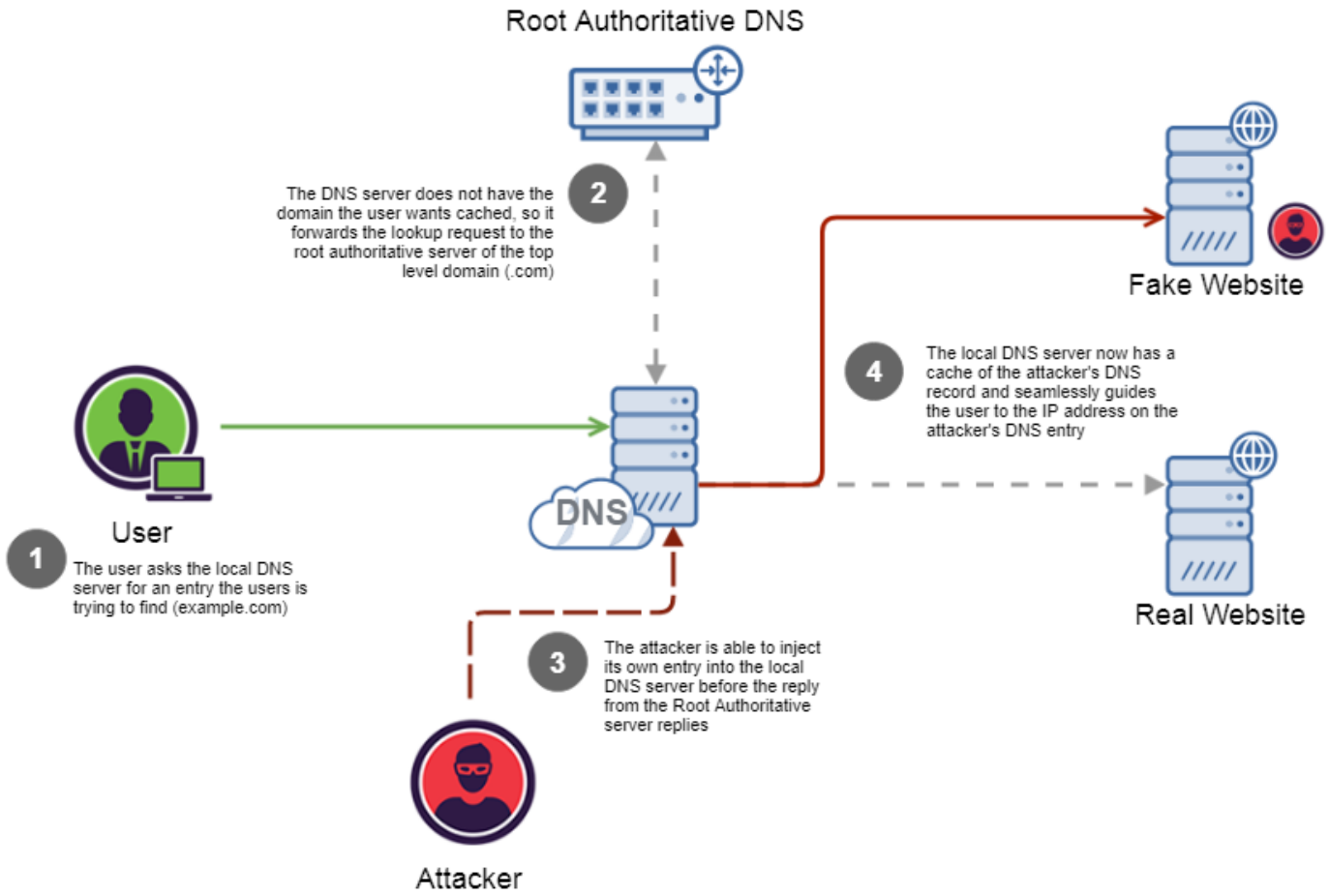
Source: Microsoft

DNSSEC

- Background
  - Security not a primary design consideration for DNS initially
    - No authentication for DNS query responses
    - Source IP of expected DNS server can be spoofed
  - IETF RFC 3757, 4033, 4034, 4035, 4509, 4641, 5155
  - DNS Cache Poisoning
    - If recursive resolver accepts false DNS response, then any devices querying for the data will be sent the incorrect address
- DNS Security Extensions (DNSSEC)
  - Suite of extensions meant to strengthen DNS security
  - Strengthens DNS authentication using digital signatures
    - Based on PKI
  - DNS data itself is signed by owner of data
  - Each DNS zone has public/private key pair
    - Each zone owner signs DNS data within the zone using the private key
    - Public key can be used by any resolver to validate the authenticity of DNS data received
  - Failure to authenticate signature results in discarded data and an error
- Two most important features added
  - Data origin authentication – verify that the data received came from the expected zone
  - Data integrity protection – resolver can ensure that they data received has not been modified in transit

Source: ICANN

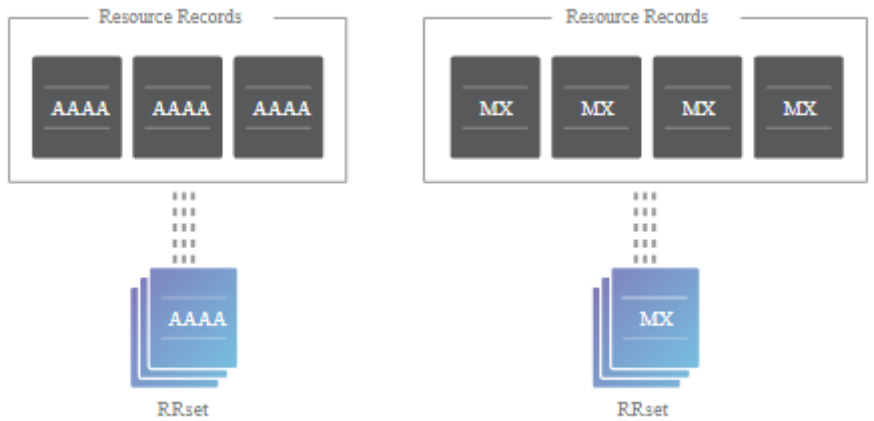
DNS Cache Poisoning



Source: https://medium.com/iocscan/dns-cache-poisoning-bea939b5afaf

Zone-Signing Keys

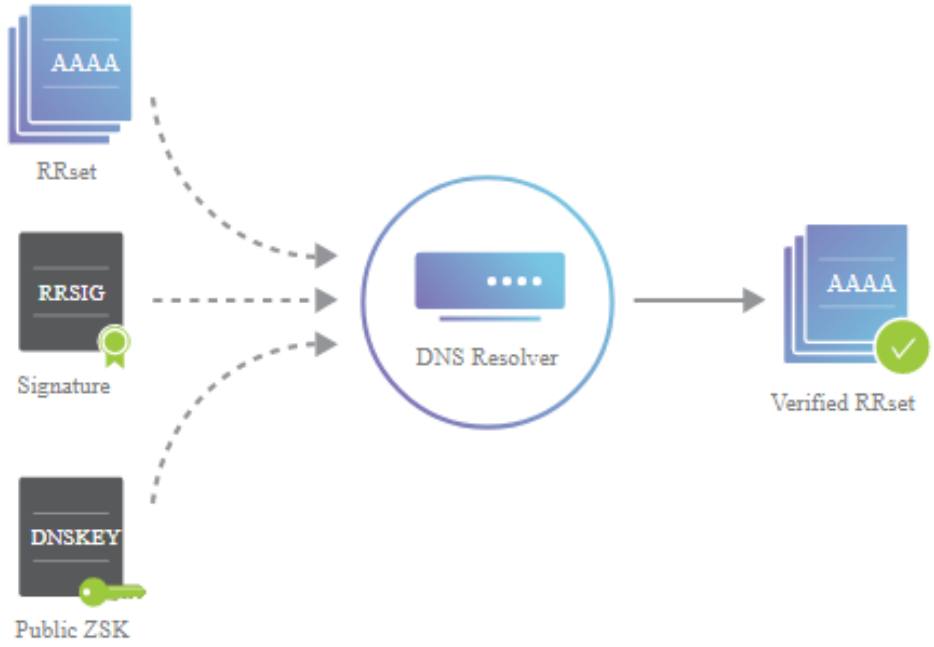
- Each zone has a Zone-Signing Key (ZSK) pair
  - Used to sign data in a zone routinely
  - Can be updated with no interaction outside of the zone it serves
  - Private portion signs each RRset
    - Public portion used to verify signature
    - Public key stored in zone operator's DNSKEY record
  - Signed RRset stored as RRSIG records
  - RRset
    - Grouping of same type of resource records within a zone



Source: https://www.cloudflare.com/dns/dnssec/how-dnssec-works/

ZSK (cont'd)

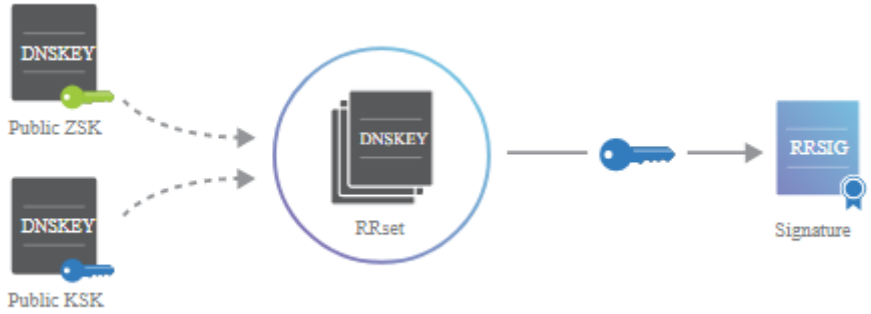
- How is public ZSK used by a DNSSEC resolver?
  - When a record type is requested (e.g. A record), the answer returns along with the appropriate RRSIG
    - ➢ Resolver can then request the zone's DNSKEY record (public ZSK) to validate the response received

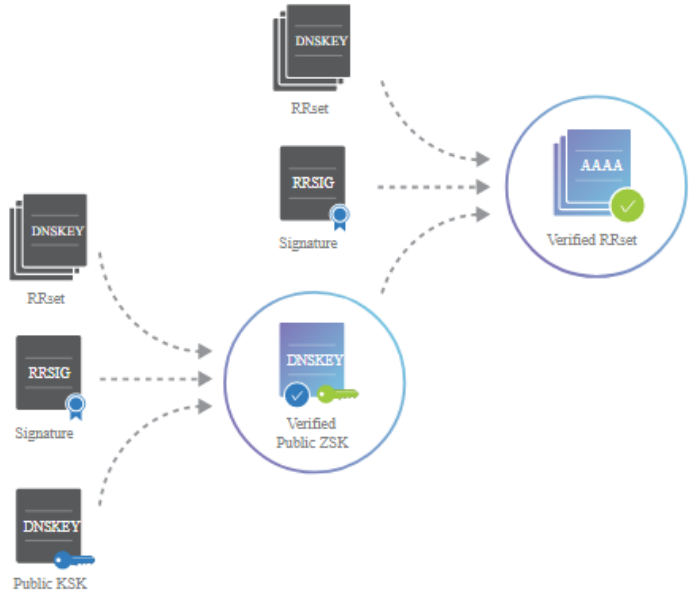


Source: https://www.imperva.com/learn/application-security/dnssec/

Key-Signing Keys

- Key-signing Key (KSK) is used to validate the DNSKEY record for the requested zone
  - Only used to sign DNSKEY RRsets
  - This key needs action outside of zone to be updated
  - Used to sign the public ZSK
    - Separate DNSKEY record
    - RRset exists for public ZSK and public KSK
- Validate process for DNSSEC record is as follows:
  - RRset requested
    - Returned with corresponding RRSIG record
  - Request DNSKEY with public ZSK and public KSK
    - Returned with RRSIG for DNSKEY Rrset
  - RRSIG of requested RRset verified with public ZSK
  - RRSIG of DNSKEY RRset verified with public KSK

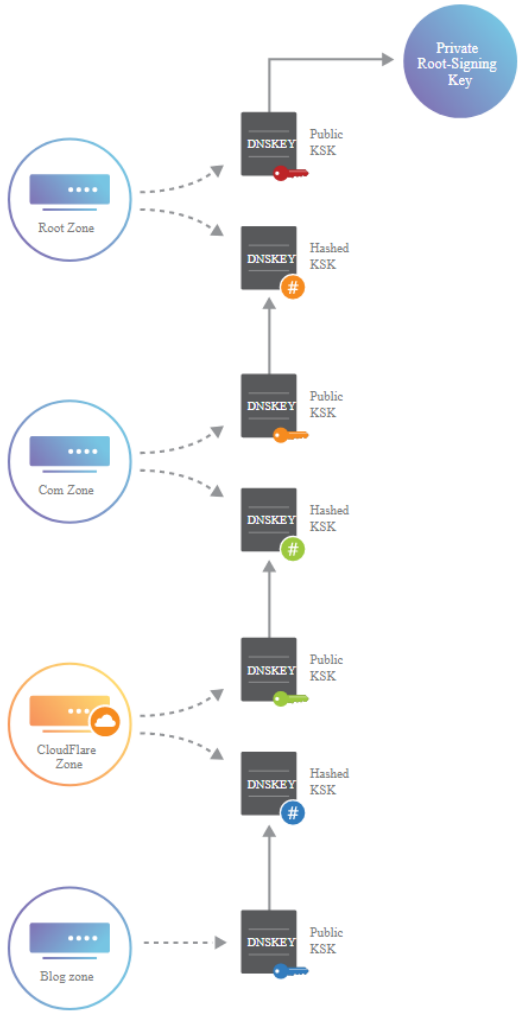




Source: https://www.cloudflare.com/dns/dnssec/how-dnssec-works/

DNSSEC Chain of Trust

- Similar to Chain of Trust used for SSL/TLS Certificate Authorities
  - Uses PKI
  - "Trust Anchor" necessary to establish chain of trust
    - ICANN maintains a trusted root server for DNSSEC
      - Public KSK often used as trusted root server (trust anchor)
    - DNSSEC enabled resolver must have at least one trust anchor's public key installed
      - Similar to trusted root CAs in web browsers
    - Root signed in public and highly auditable manner to produce RRSIG at that level
- DS records are also signed and have a corresponding RRSIG record
  - This allows for a repeatable process to validate signatures until the root is reached



Source: https://www.cloudflare.com/dns/dnssec/how-dnssec-works/

Let's Encrypt

CALIFORNIA STATE UNIVERSITY LONG BEACH College of Engineering

- Overview
  - Sponsorship allowed the creation of this nonprofit Certificate Authority (CA) for TLS certificates
    - Major sponsors: Mozilla, Cisco, Meta, AWS, and Chrome
  - Used by 260 million websites
  - API friendly for automated certificate renewals
    - 60 day renewal period recommended (90 day max)
  - Offers domain-validated certificates
    - Use web or DNS to validate ownership of domain using unique tokens
- Certbot
  - Popular Let's Encrypt client
    - Includes automated configurations for Apache and Nginx web services
  - Certificate creation: "sudo certbot --apache -d www.example.com"
  - Certificate renewal: "sudo certbot renew"
  - Easily use crontab to automate renewal process

NAC Overview

CALIFORNIA STATE UNIVERSITY LONG BEACH College of Engineering

- Network Access Control (NAC) definition
  - Establish fine controls over how endpoint devices connect to a network and what resources they have access to
    - Base authorization on security policy
  - Core aspect is authentication and authorization
    - Software can also include additional tools such as antivirus, firewall, and vulnerability scanners
  - Creates auditable record of authorized and unauthorized resource requests
- Types of NAC
  - Pre-admission
    - Performs checks prior to allowing user/device on the network
  - Post-admission
    - Re-authenticates and checks for authorization when lateral movement on the network is requested

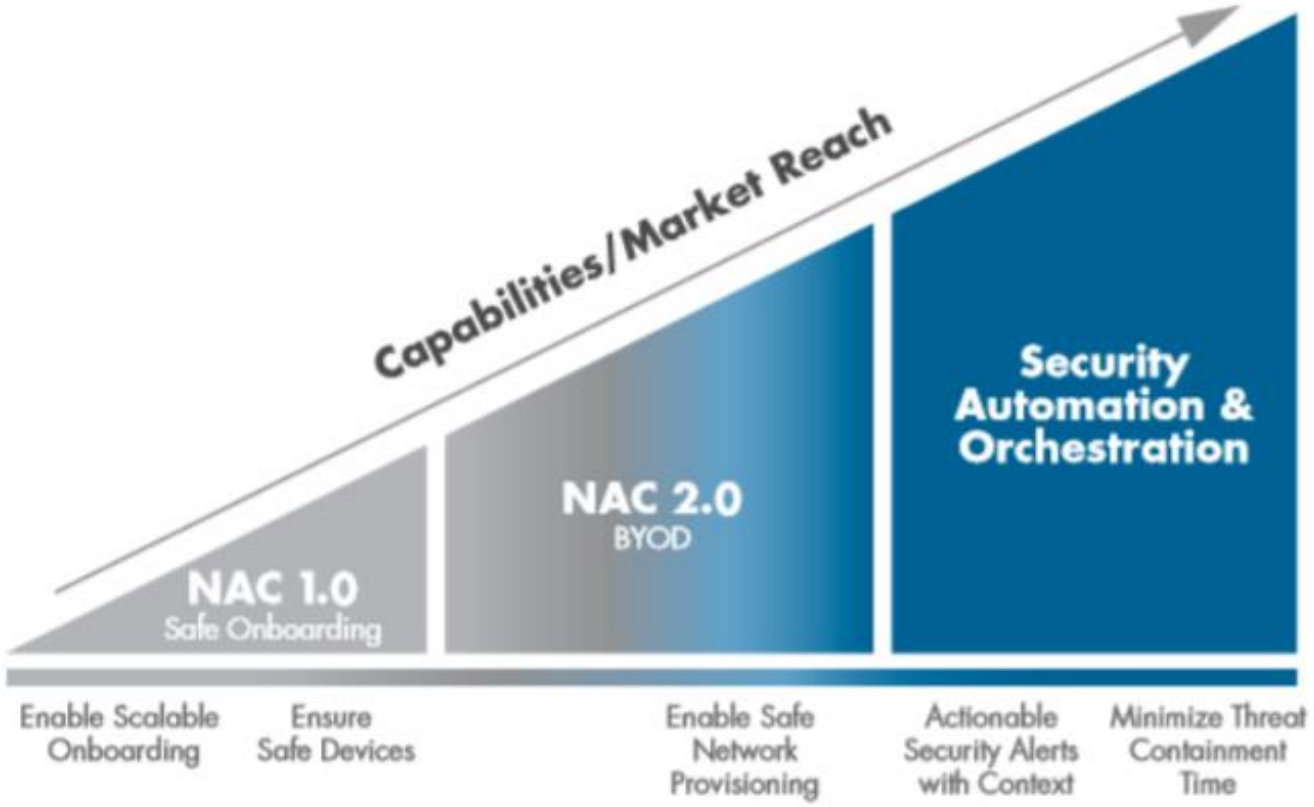
Source: https://www.techtarget.com/searchnetworking/definition/network-access-control

NAC Overview (cont'd)

- Network Access Server
  - Centralized authentication/authorization server that determines access to network resources
    - VPN
    - Network load balancing
    - Network resource management
- Common use cases
  - Bring your own device (BYOD)
  - Access for non-employees
  - IoT
  - Incident response
- Capabilities
  - Limit / prevent unauthorized access to data
  - Block network access from non-compliance devices / users
  - Manage policy for connected network devices
  - Recognize and block malicious activity
  - Integrate with central monitoring solutions

Source: https://www.techtarget.com/searchnetworking/definition/network-access-control

Evolution of NAC



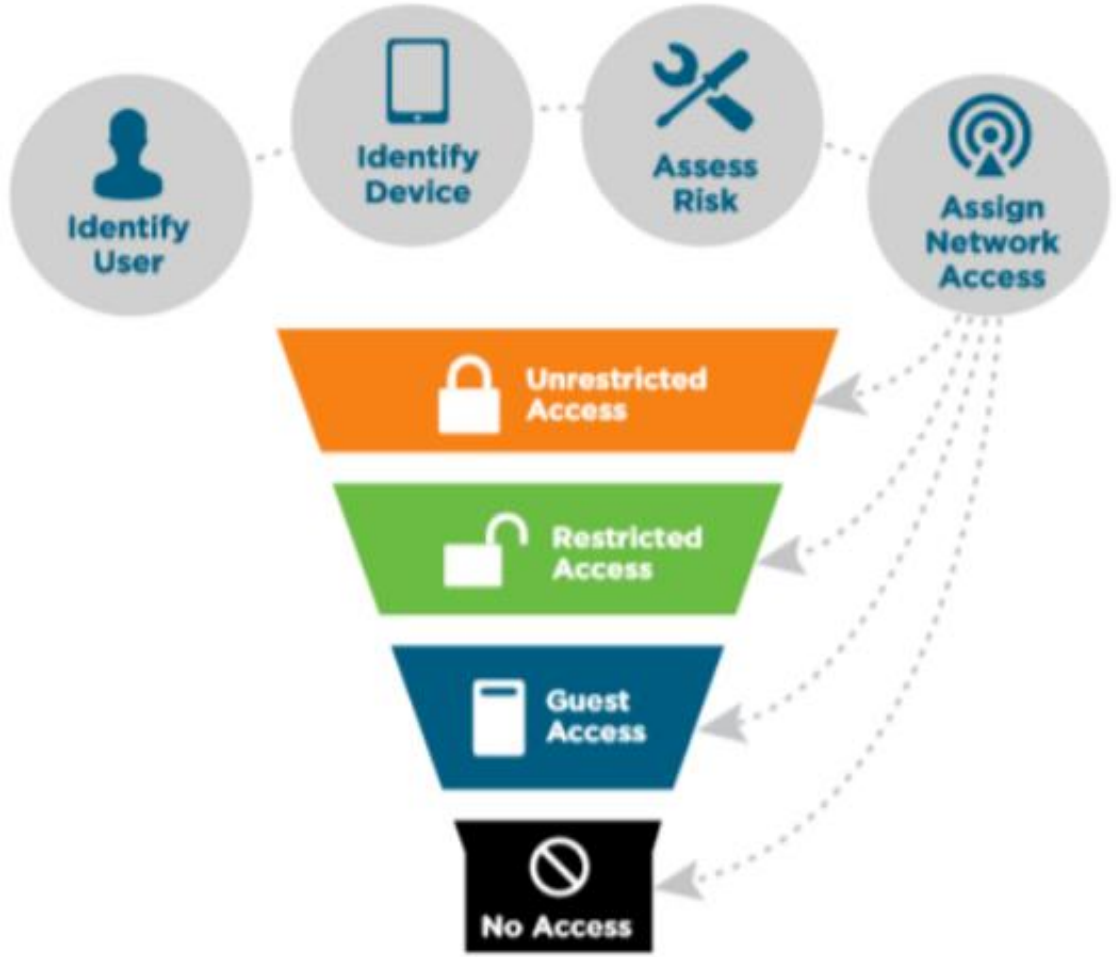
"Network access control is the act of keeping unauthorized users and devices out of a private network.“ - VMware

- Access Control
  - Local
  - External
- Compliance Enforcement
- Device / User Identification
- FAR Clause 52.204-21(b)(1)(i) - “Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).”
- Principle of Least Privilege

Source: The SANS Institute

Workstations

- "NAC 1.0"
- Company Owned
- Wired LAN Devices
- Easier to Manage
  - Complete administrative control



Source: The SANS Institute

Wireless / BYOD

CALIFORNIA STATE UNIVERSITY
LONG BEACH
College of Engineering

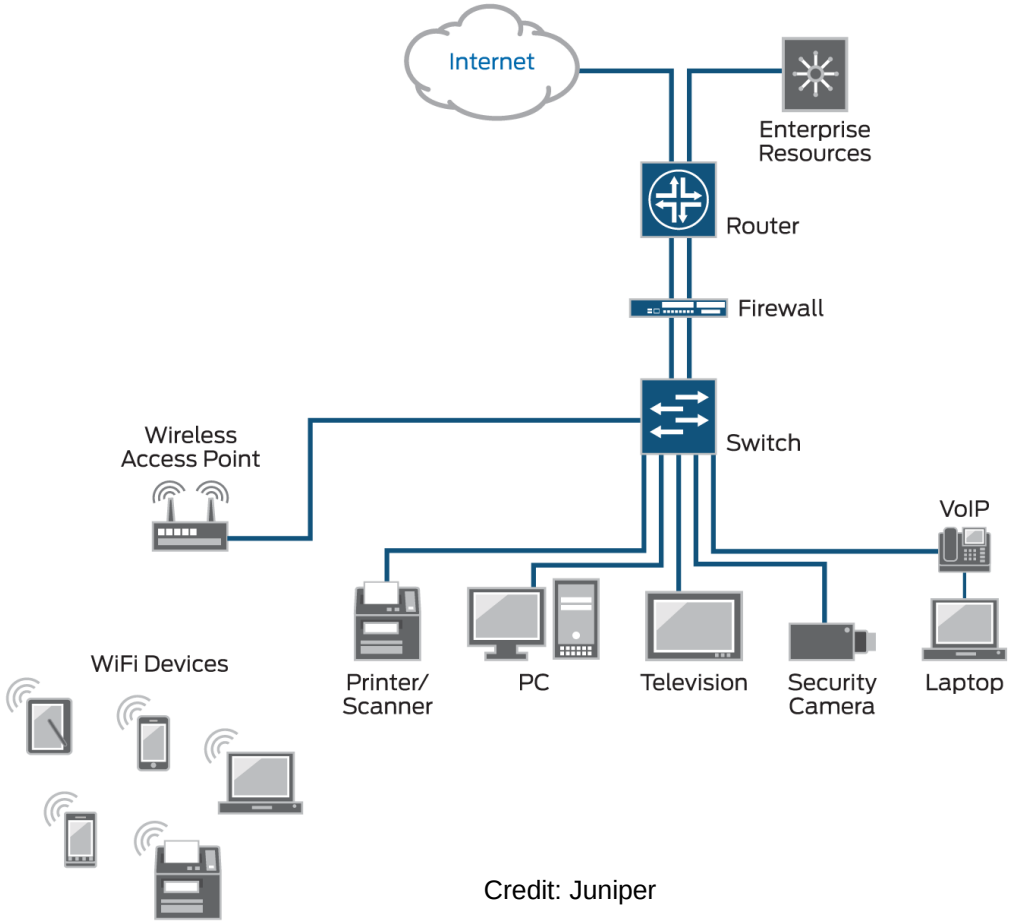
- “NAC 2.0”
- Laptops
- Cell Phones
- Remote Connections / VPN
- Enforce Compliance

CIS Control 1: Inventory and Control of Hardware Assets			Applicability	
Sub-Control	Control Title	Control Description	Included?	Justification
1.4	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all assets, whether connected to the organization's network or not.	•	This Sub-Control helps to ensure that IoT devices that are never intended to be connected to the enterprise network, or only connected to an internal network, are still properly tracked.
1.5	Maintain Asset Inventory Information	Ensure that the hardware asset inventory records the network address, hardware address, machine name, data asset owner, and department for each asset and whether the hardware asset has been approved to connect to the network.	•	This can present a variety of challenges for IoT devices, as the hardware asset information can drastically change from manufacturer to manufacturer. It can be difficult to standardize field formats as well. Broadly, it is best to collect whatever hardware asset information is available.
1.6	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.	•	Unknown IoT devices connected to enterprise networks and systems should be quickly investigated and removed.
1.7	Deploy Port Level Access Control	Utilize port level access control, following 802.1x standards, to control which devices can authenticate to the network. The authentication system shall be tied into the hardware asset inventory data to ensure only authorized devices can connect to the network.	•	It is unlikely that this will be possible for most IoT devices, but if the capability is available, it should be enabled. Note that 802.1x does not work on many IoT devices that do not support supplicant software. Network-level authentication can cause reliability issues if not strictly maintained.
1.8	Utilize Client Certificates to Authenticate Hardware Assets	Use client certificates to authenticate hardware assets connecting to the organization's trusted network.	•	It is unlikely that this will be possible for many IoT devices, but if the capability to store and utilize certificates within an authentication protocol is available, it should be enabled.

CIS Control 1

Internet of Things

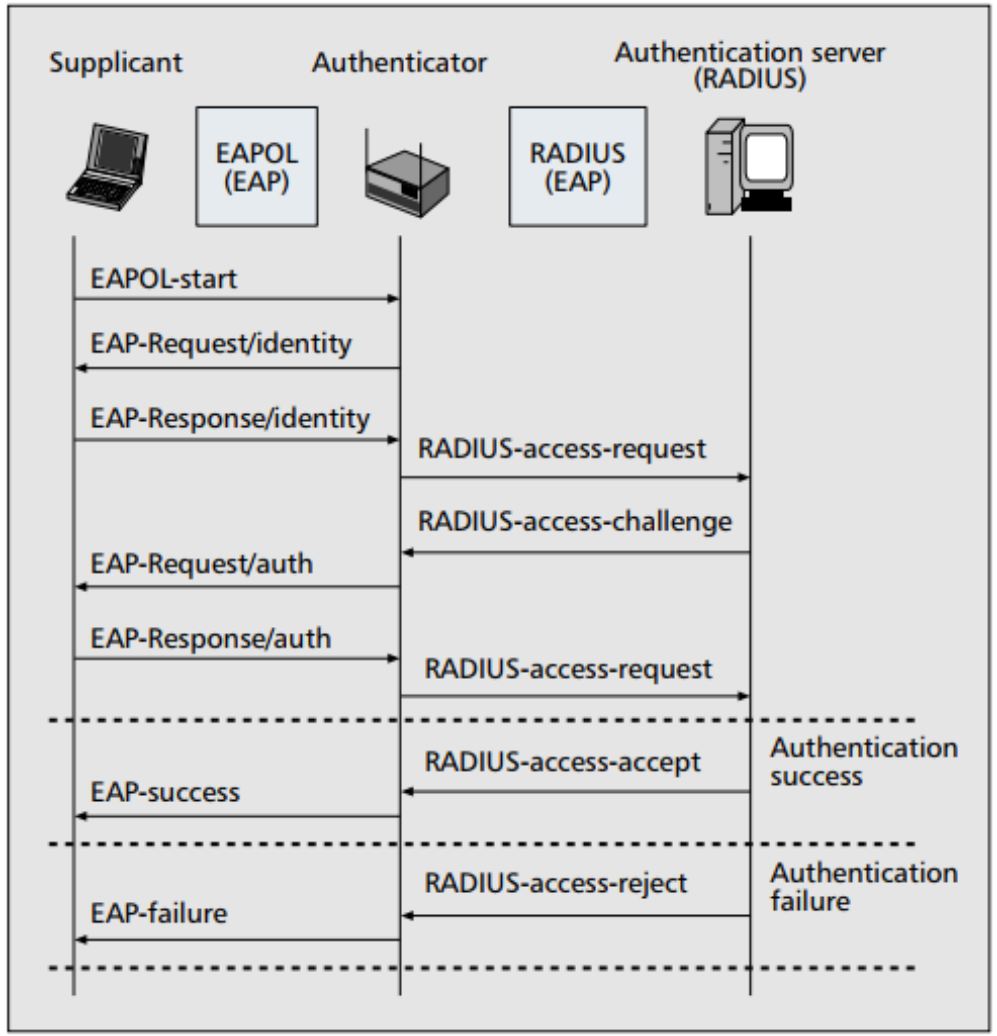
- "NAC 3.0" / Security Automation and Orchestration
- Non-traditional layer 3 devices
  - Printers
  - VoIP Phones
  - Cameras
- Unlikely to enforce device compliance
- Automated onboarding essential
- Poor NAC support



Credit: Juniper

802.1X Protocol

- Port-based NAC
- Main Components:
  - Supplicant
  - Authenticator
  - Authorization Server
- Utilizes Extensible Authentication Protocol (EAP)
- RADIUS Authentication
  - Allows for auditing
- Enforces Least Privilege Principle
  - Per Subject / User

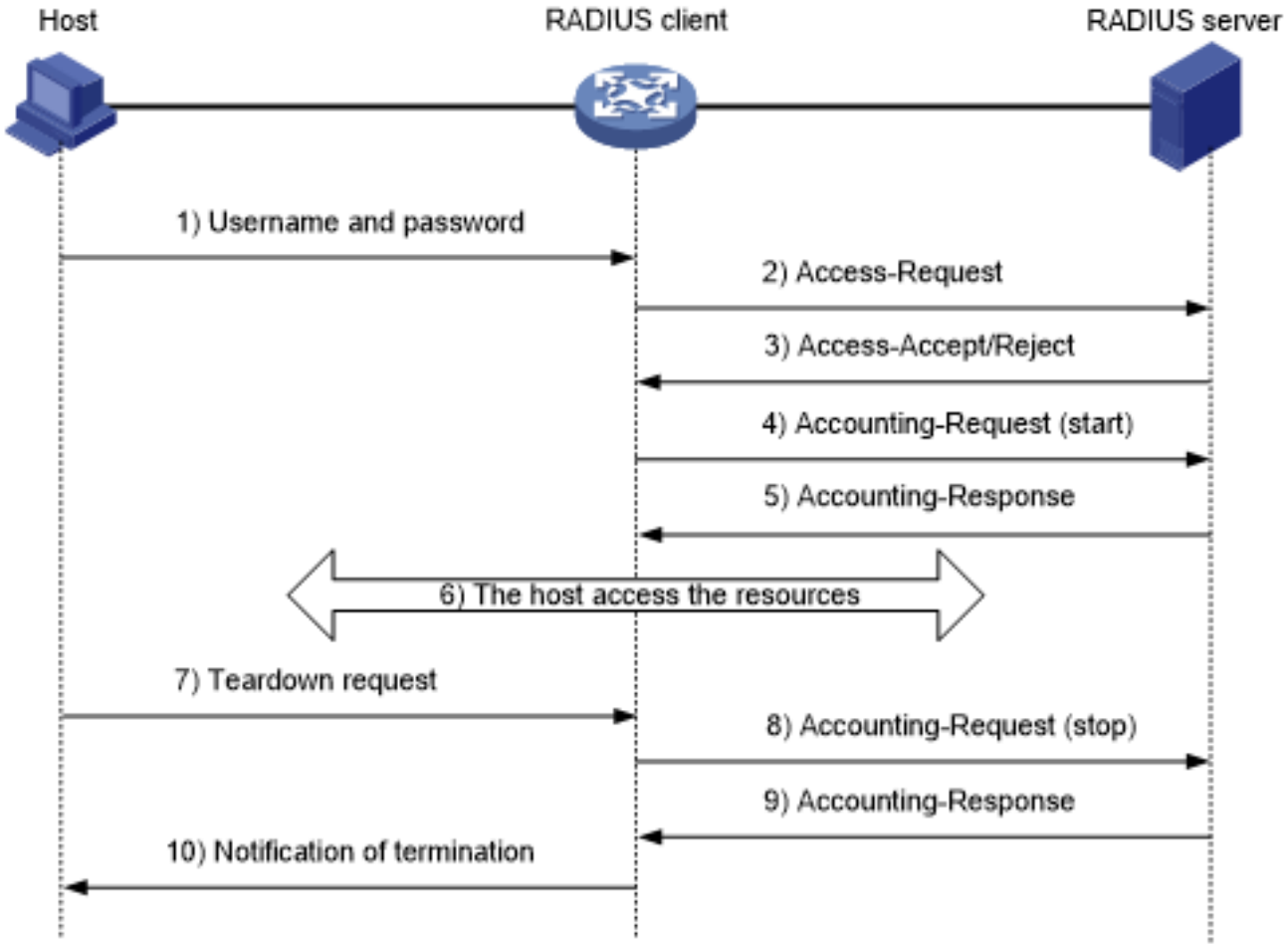


Credit: Chen, et al.

Definitions

- Supplicant
  - Subject requesting access
  - Device and software
- Authenticator
  - Pass-through device (e.g. router, access point)
  - Policy Enforcement Point (PEP)
- Authorization Server
  - Policy Decision Point (PDP)
  - e.g. RADIUS
- EAP (Extensible Authentication Protocol)
  - Authentication framework
  - Authentication initiated by the server (authenticator)
- RADIUS (Remote Authentication Dial-In User Service)
  - RADIUS Client = Networking device used to authenticate users
  - RADIUS Server = Central database of user profiles used to authenticate and authorize access

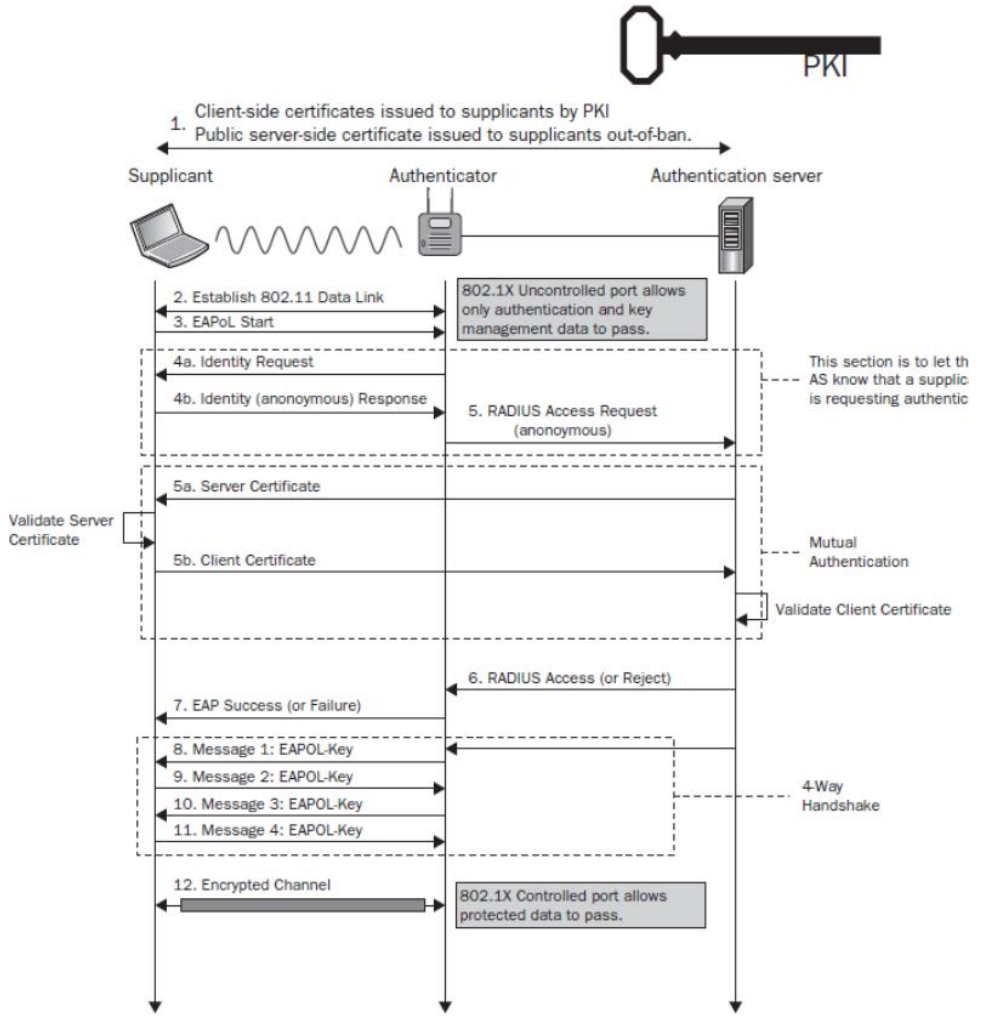
RADIUS Process



Source: https://techhub.hpe.com/eginfolib/networking/docs/switches/5130ei/5200-3946_security_cg/content/485047943.htm

EAP-TLS - Process

- Certificate distribution
- EAPoL used between Supplicant and Authenticator
- Mutual authentication
- Use of RADIUS for authorization
- Encrypted communication



Credit: Nayarisi (CWNE #153)

Need for Automation

- TLS certificate creation and distribution
- Policy compliance
- Increased usage of BYOD
- Increase in working remotely
  - Covid-19 effect
  - VPN connectivity
- IoT Devices
  - Many not compatible with 802.1X
  - Increased adoption among enterprise devices
  - Often positioned in non-secure areas

Need for 802.1X Capable IoT

- Security focused standards development
- Built-in support for 802.1X certificates
- Standardized API across manufacturers
  - Capable of handling auto-deployed client and server certificates
- Pre-enrollment mechanism
- Move beyond default security profiles to individual client authentication

NAC Summary

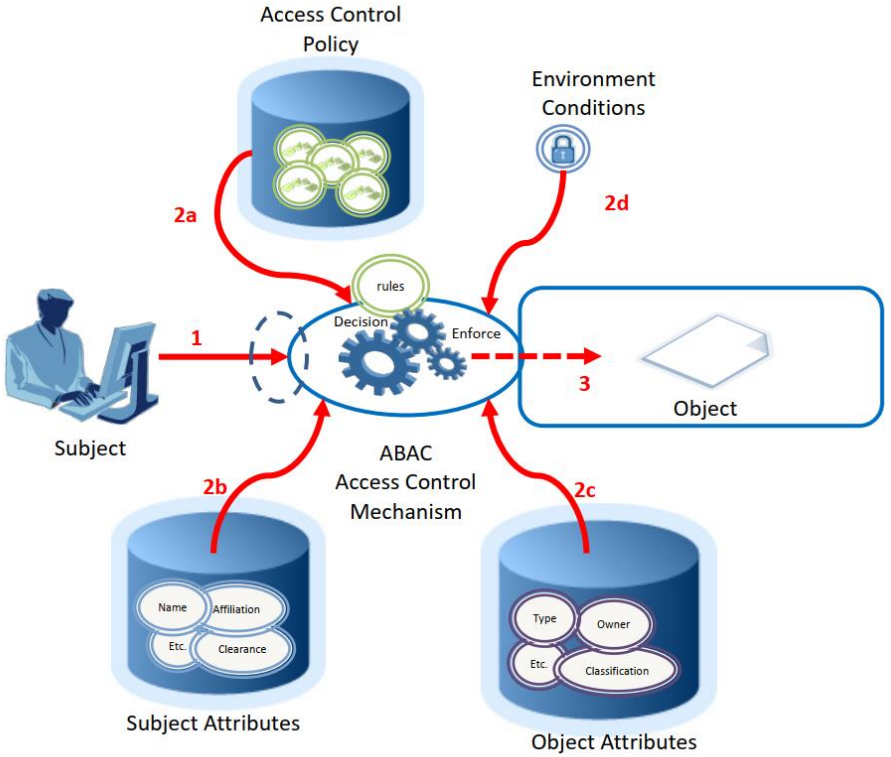
- Many components of NAC
  - All need to work together for comprehensive coverage
- Standardization for deployment/configuration of new network devices is key
  - Ad-hoc deployments complicate automation
- Trusted internal certificate authority is needed for EAP-TLS
  - Automated certificate deployment is needed (client and server)
  - Need to “auto-renew” certificates to avoid compromised certificates
- Current state of NAC for IoT devices is primarily profile based
  - Machine learning is helping to make this option more secure
- A well configured NAC includes auditable record keeping
  - Useful for auto-deployments, change management, and system recovery
- Points of Policy concept useful to consider when designing NAC workflow
  - Opens up path to use NAC increasingly for attribute-based authorizations

ABAC

- Attribute Based Access Control (ABAC)
  - "Access control method where subject requests to perform operations on objects are granted or denied based on assigned attributes of the subject, assigned attributes of the object, environmental conditions, and a set of policies that are specified in terms of those attributes and conditions."
  - Supports both Discretionary Access Control (DAC) and Mandatory Access Control (MAC)
- Components
  - Attributes: characteristics of the subject, object, and/or environmental conditions
  - Subject: human user or non-person entity (NPE)
  - Object: system resource for which access is managed by the ABAC system
    - e.g. devices, files, processes, networks, data, applications, etc.
  - Operation: execution of a function at the request of a subject upon an object
    - e.g. read, write, delete, copy, execute, or modify
  - Policy: representation of rules and/or relationships that determine if access should be allowed
  - Environmental Conditions: operational or situational context in which access requests occur
    - e.g. time, date, location, or threat level

Source: NIST SP 800-162

ABAC Model



1. Subject requests access to object
2. Access Control Mechanism evaluates a) Rules, b) Subject Attributes, c) Object Attributes, and d) Environment Conditions to compute a decision
3. Subject is given access to object if authorized

Figure 2: Basic ABAC Scenario

Source: NIST SP 800-162

ABAC (cont'd)

- Important Terms
  - Natural Language Policy (NLP): Human-readable statements regarding access to enterprise objects
  - Digital Policy (DP): Access control rules written as machine executable code (used by an access control mechanism)
    - Built using subject/object attributes, operations, and environmental conditions
  - Metapolicy (MP): Policy for managing policies. Used to resolve conflicts between DPs or other MPs in complex use cases
- Access Control Mechanism (ACM) Function Points
  - Policy Decision Point (PDP): Computes access decisions by evaluating application DPs and MPs
  - Policy Enforcement Point (PEP): Enforces policy decisions in response to a subject requesting access to a protected object
    - PEP enforces decisions made by the PDP
  - Policy Information Point (PIP): Source of information for attributes assigned to subjects and objects
    - Provides data to the PDP to make decisions
  - Policy Administration Point (PAP): User interface for creating, managing, and testing DPs and MPs

ACM Example

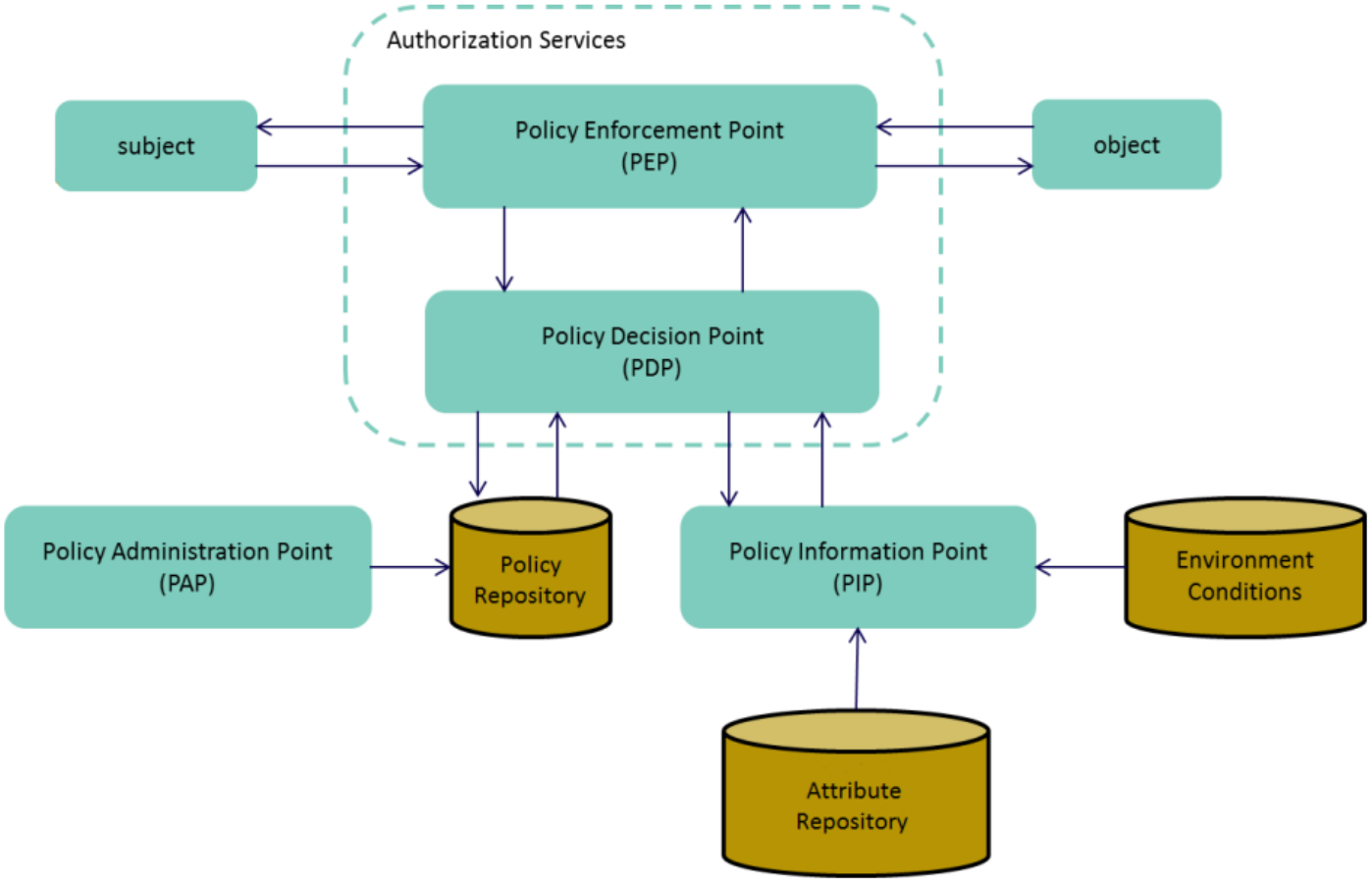


Figure 5: An Example of ACM Functional Points

Source: NIST SP 800-162