



# SSCP (Systems Security Certified Practitioner)

Kelly Handerhan, Instructor  
[kellyhanderhan@gmail.com](mailto:kellyhanderhan@gmail.com)

# Introduction

- Welcome!
- Schedule
- Logistics
- Cell Phones, etc
- Introductions for students:
  - Name, Security Background, Certifications

# Domain 1 SSCP Exam and Exam Specifics

# SSCP Requirements

- One Year Experience in one or more domain
- Register for the exam [www.isc2.org](http://www.isc2.org)
- Legally commit to abide by the (ISC)<sup>2</sup> Code of Ethics
- Answer Four questions regarding criminal history and background
- TAKE THE TEST AND PASS IT!
- 60 Continuing Professional Education (CPE) credits every three years, with a minimum of 10 CPEs earned each year after certification.

# SSCP Exam Specifics

- **Exam Type:** Computer Based Provided by Pearson VUE
- Can be scheduled through ISC2.org website. Numerous testing locations available.
- **Number of questions:** 125
- Only 100 questions are graded. The other 25 questions are for research purposes, but they are mixed into the entire 125 questions so you won't know which questions are graded. You'll need to answer every question as if it's graded.
- **Type of Questions:** Multiple choice
- The questions are basic multiple choice questions. You may have some scenario-based items where you'll read a scenario and then answer two or more questions related to the scenario. You aren't penalized for wrong answers, so make sure you answer each question.
- **Passing score:** 700/1000
- The questions are weighted, so a score of 700 doesn't indicate that you need to get exactly 70 questions correct.
- **Time limit:** 3 hours
- Keep track of time. Allow yourself a little over a minute per question. Shoot for 50 questions per hour. This will allow you a little extra time for a break and to review.

# SSCP Exam Taking Tips

- Security Transcends Technology!
- Think like a manager.
- Look to fix the process, not the problem.
- Change Control and Documentation.
- How much security is enough?
- What's the trade-off?
- Who is responsible?
- Physical safety of employees always comes first.
- Don't just look for technical solutions. Think about a layered, comprehensive approach.

# Exam Objectives

- Access Controls
- Security Operations
- Monitoring and Analysis
- RISK!!!!
- Cryptography
- Networks and Communications
- Malicious Code and Activity

# Security Fundamentals

- C-I-A Triad
- Confidentiality
- Integrity
- Availability



# Confidentiality

- Prevent unauthorized disclosure
- Social Engineering
  - Training, Separation of Duties, Enforce Policies and Conduct Vulnerability Assessments
  - Phishing, Spear Phishing, Whaling
- Media Reuse
  - Proper Sanitization Strategies—Zeroization (Wiping), Degaussing (Magnetic), Physical Destruction, Cryptoshredding
- Eavesdropping
  - Encrypt
  - Keep sensitive information off the network

# Integrity

- Detect modification of information
- Corruption
- Unintentional or Malicious Modification
  - Message Digest (Hash)
  - MAC
  - Digital Signatures

# Availability

- Provide Timely and reliable access to resources
- Redundancy, redundancy, redundancy
- Prevent single point of failure
- Comprehensive fault tolerance (Data, Hard Drives, Servers, Network Links, etc)

# Defense in Depth

- Also Known as layered Defense
- No One Device will PREVENT an attacker
- Three main types of controls:
  - Technical (Logical)
  - Administrative
  - Physical

# The IAAA of Security

- Identification
- Authentication
- Authorization
- Accounting
- “Race” conditions exploit the order of events

# Nonrepudiation

- A sender can't deny having sent a message, nor the contents of the message.
- Being able to authoritatively link an action and its specifics back to an individual.
- Technical Controls are NOT enough

# Least Privilege/Need to Know

- Foundational principal of security
- Least Privelege-- Action
- Need to Know—Data
- Watch for “Privilege Creep”

# Separation of Duties

- Administrative Control
- Enforces Confidentiality
- Mitigates Conflict of Interest
- Allows Singleness of Purpose



# Liability

- Culpable Negligence
- Due Diligence
- Due Care
- Prudent Person rule

# Domain 2: Access Control

RESTRICTING SUBJECTS, OBJECTS AND THEIR  
INTERACTIONS

# Identification

- Making a claim
  - Username
  - Account Number
  - RFID
  - MAC address or IP address

# Authentication

- Support the Claim
- Three Types:
  - Type 1: Something You Know
  - Type 2: Something You Have
  - Type 3: Something You Are
- Multi-Factor Authentication
- Mutual Authentication

# Type 1: Something you Know

- Passwords are the most common
  - Why?
  - Strategies to secure:
    - Strong Passwords—use policy to enforce
    - Be careful of writing passwords down
    - Don't reuse (within reasonable timeframes)
    - Protect your passwords from others
    - Never walk away from a system without locking/logging off
    - Passwords should be audited

# Attacks on Passwords

- Password Guessing
- Dictionary Attacks
- Brute Force Attacks
- Rainbow Tables
- Replay Attacks—Remember an attacker doesn't want to know your password. He wants to use it.
- Spraying: Trying the same password on many different user accounts

## Type 2: Something you Have

- Keys
- Driver's License, Passport, ATM Card
- Proximity Cards
- Smart Cards: Often integrated with PKI
- Token Devices: Asynchronous vs. Synchronous
- Cryptographic Keys

# Type 3: Something you Are

- Biometrics
  - Physiological Characteristics
    - Fingerprints
    - Iris Scans
    - Retina Scans
  - Behavior Based
    - Signature
    - Keyboard Cadence
    - Gait



# Evaluating Biometrics


- Accuracy
  - Type I: False Rejection
  - Type II: False Acceptance
  - CER
- Acceptability
- Enrollment/Verification Time
- Biometrics are the best single factor authentication, but remember MULTI-FACTOR is best

# SSO (Single Sign On)

- Peer to Peer vs. Client-Server
- Kerberos
- Super Sign On

# Kerberos

- Authenticating Server (AS)
- Ticket Granting Server (TGS)
- Ticket Granting Ticket (TGT)
- Key Distribution Center (KDC)
- Tickets
- Principals (Users, Services, Systems)
- Federated systems



# Kerberos and Single Sign On (SSO)

# Learning Objectives

In this video, we will:

- 1 Discuss Single Sign On (SSO)
- 2 Examine the goals and components of Kerberos
- 3 Describe the Kerberos process



# Single Sign-On (SSO)

Allows a user to provide credentials to an authentication server and receive access to interconnected and disparate systems.

- Pros

- Ease of use for end users
- Centralized control
- Ease of administration

- Cons

- Single point of failure
- Standards necessary
- Keys to the kingdom

- Kerberos: SSO for networks

- LDAP: Directory Structure for authentication servers

# Kerberos

- A network authentication protocol designed from MIT's project Athena. Kerberos tries to ensure authentication security in an insecure environment
- Used in Windows 2000+ and some Unix
- Allows for single sign-on
- Never transfers passwords
- Uses symmetric encryption to verify identifications
- Avoids replay attacks

# Kerberos Components

## Essential Components:

- AS (Authentication Server): Allows authentication of the user and issues a TGT
- TGS: After receiving the TGT from the user, the TGS issues a ticket for a particular user to access a particular service
- KDC (Key Distribution Center): a system which runs the TGS (Ticket Granting Service) and the AS (Authentication Service)
- Ticket: Means of distributing Session Key
- Principles (users, applications, services)
- Kerberos Software (integrated into most Operating Systems. MS Windows 2000 and up support Kerberos)
- Main Goal: User needs to authenticate himself/herself without sending passwords across the network—needs to prove he/she knows the password without actually sending it across the wire.



# Summary

In this video, we covered:

- SSO & Kerberos
- Kerberos Components
- Kerberos Process

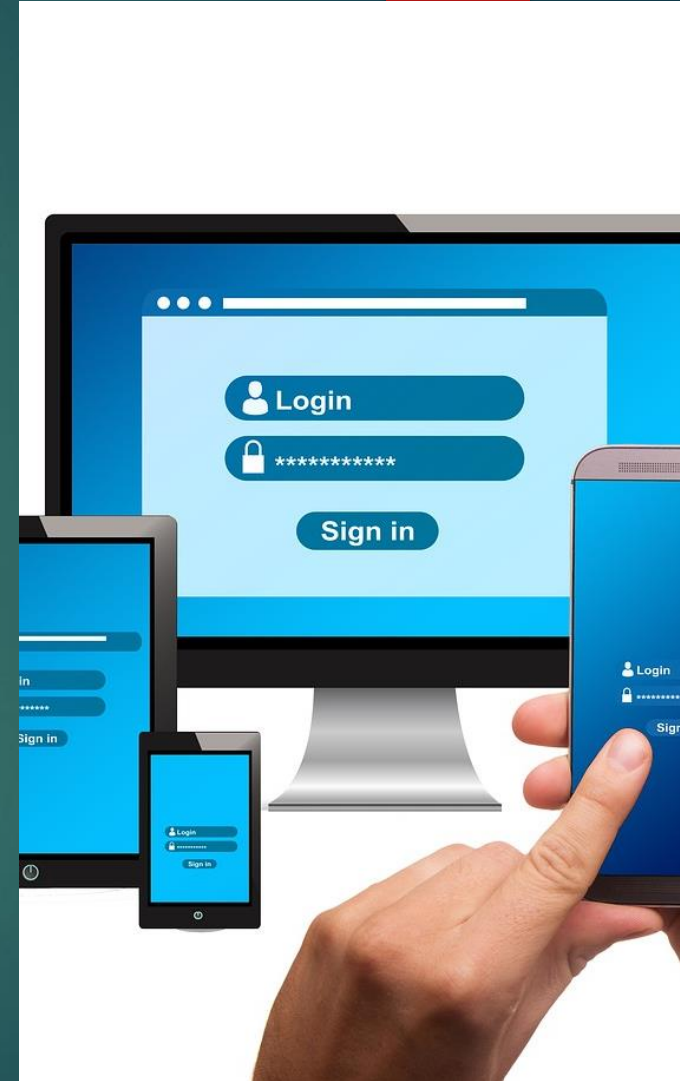


# The Kerberos Carnival

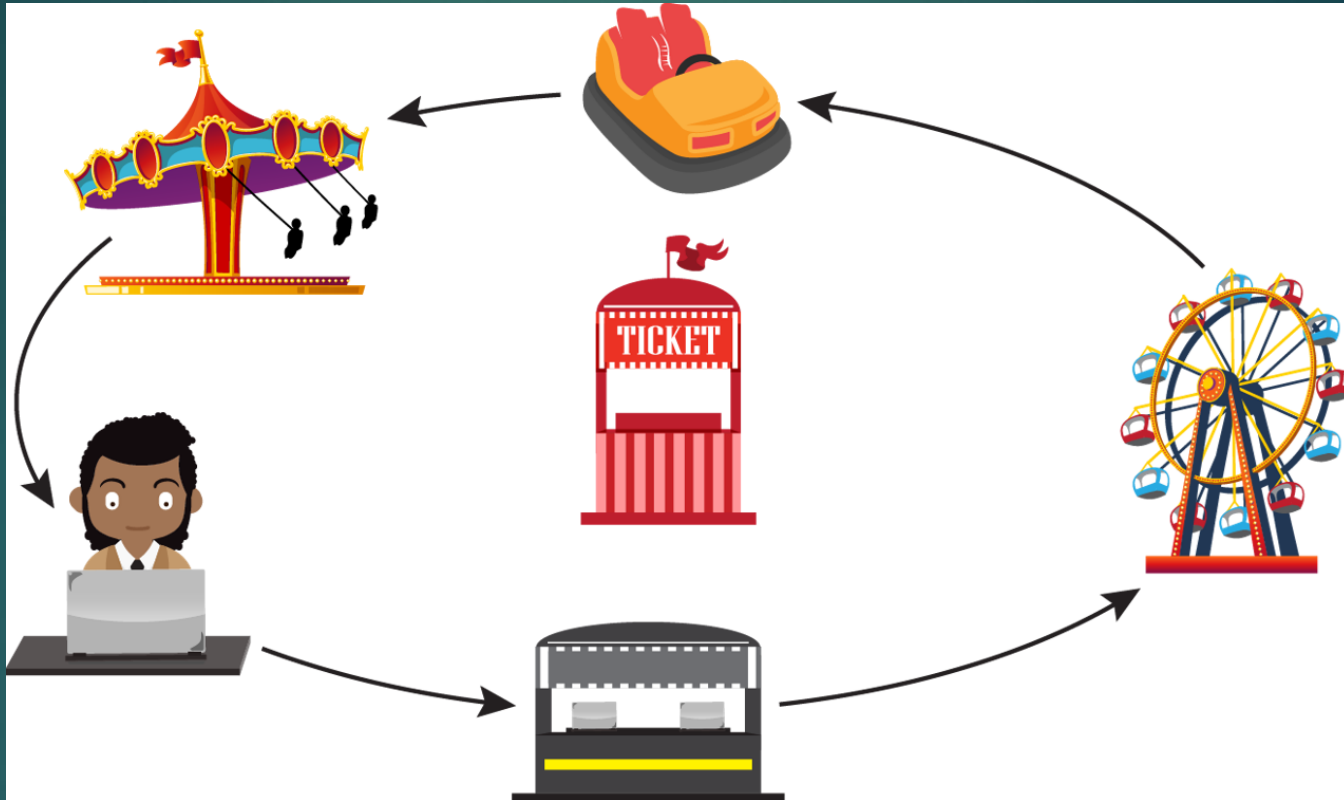
# Learning Objectives

In this video, we will:

- 1 Discuss the Kerberos Carnival
- 2 Examine the Kerberos concerns



# The Kerberos Carnival



# My Mom



Type text

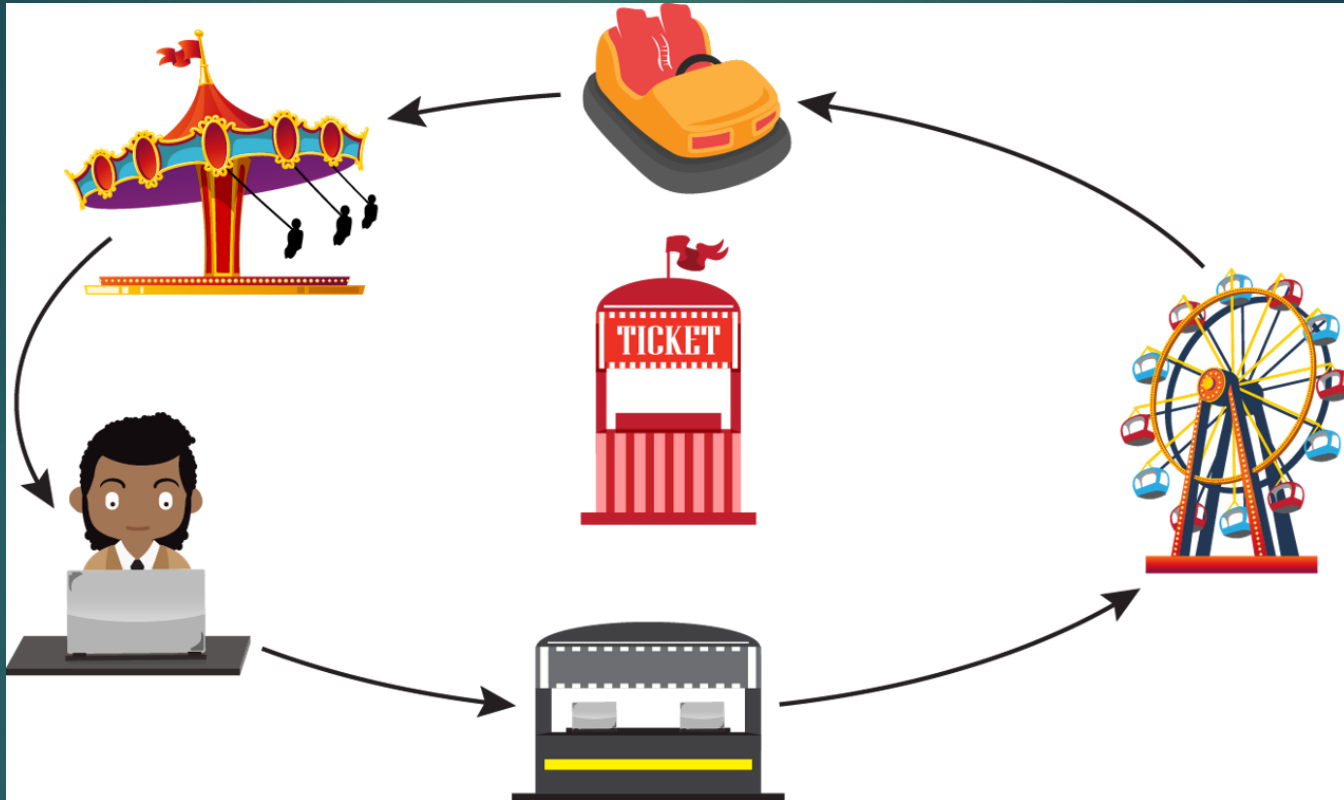


Type text

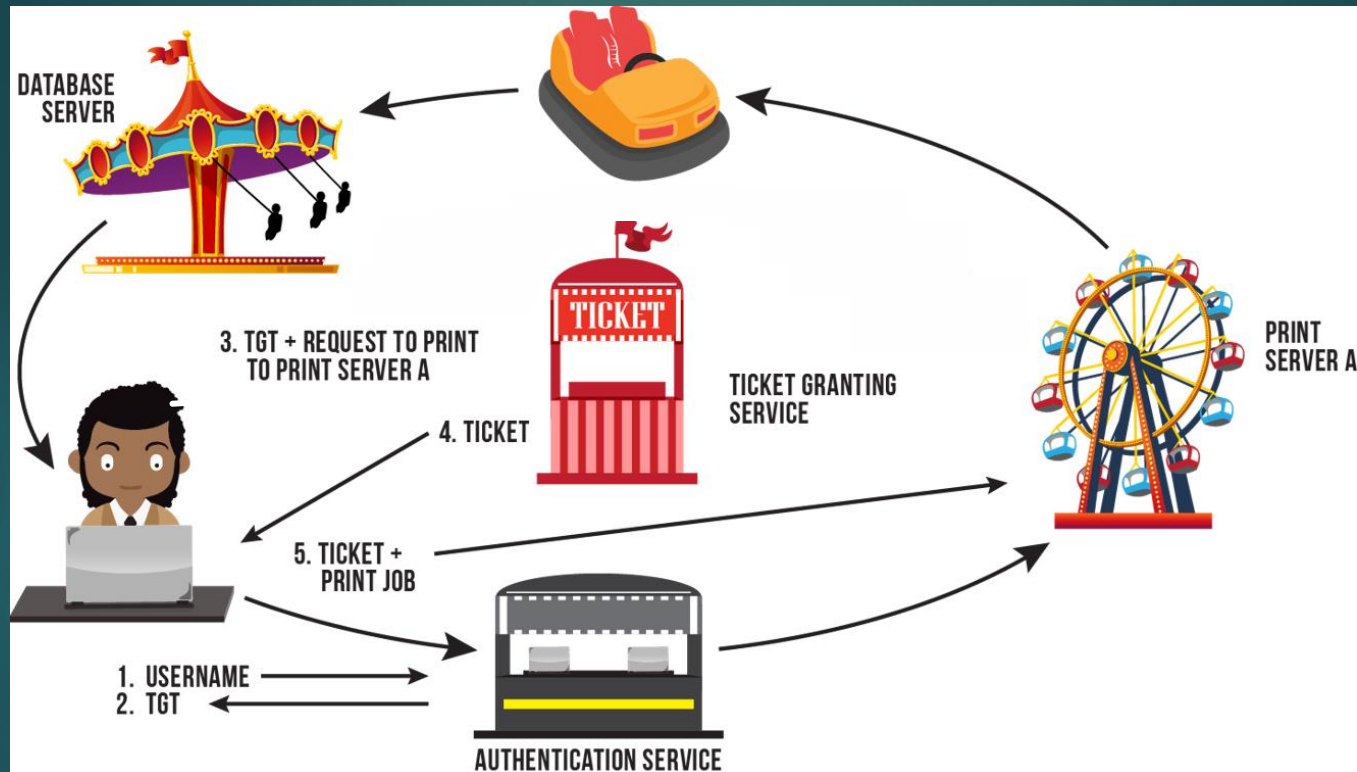


Type text

# The Kerberos Carnival



# The Kerberos Carnival



TICKET  
SKEY: 8675309  
encrypted with  
user's password  
SKEY: 8675309  
Encrypted with the  
service's key

# Kerberos Concerns

- Computers must have clocks synchronized within 5 minutes of each other
- Tickets are stored on the workstation. If the workstation is compromised your identity can be forged.
- If your KDC is hacked, security is lost
- A single KDC is a single point of failure and performance bottleneck
- Still vulnerable to password guessing attacks



# Summary

In this video, we covered:

- The Kerberos Carnival
- Kerberos Concerns

# Other Authentication Concerns

- Offline Authentication (Cached Credentials)
  - No network access
- One Time Passwords
  - Should be implemented with user password/PIN (to accomplish multi-factor)
  - Defense against sniffing passwords
  - Synchronous (OPIE One time Password In Everything) and S/Key
  - Asynchronous
    - Challenge Response

# Implementing Access Controls

- Subjects: Active Entities often controlled by accounts
  - Users
  - Computers
  - Application
  - Networks
- Context-based controls can be applied also:
  - Time, location, amount of usage, etc

# Implementing Access Controls Continued

- Objects: Passive Entity
  - Data
  - Hardware
  - Applications
  - Networks
  - Facilities
- Logical Control vs. Physical Control

# Reference Monitor and Security Kernel

- Handles all decisions in relation to subject/Object Access
- Reference Monitor: The law
- Security Kernel: The police

# Access Control Models: DAC

- DAC (Discretionary Access Control)
  - Owner of the object determines the security of the object
  - ACL (Access Control Lists)
  - Identity-based
  - Not designed for security, but ease of use

# MAC



- MAC (Mandatory Access Control)
  - Used for a secure environment
  - Uses Labels for both subject and object
  - Solaris with trusted extensions, SE Linux

# RBAC, ABAC, RuBAC



- ▶ RBAC (Role-based Access Control)
- ▶ ABAC (Attribute-based Access Control)
- ▶ RuBAC (Rule-based Access Control)



# Security Models

- Bell-Lapadula
- Biba
- Clark-Wilson
- Brewer-Nash (Chinese Wall)

# Bell-Lapadula

- Confidentiality: Designed to protect National Secrets
- MAC
- Simple Security Property: NO READ UP
- \*\_Security Property: NO WRITE DOWN

# Biba

- Integrity Model—Think academia
- Protects the sanctity of knowledge
- Down data's dirty
- Also a MAC
- Simple Integrity Axiom: NO READ DOWN
- \*\_Integrity Axiom: NO WRITE UP

# Clark-Wilson

- Integrity of Data and protecting it's quality from improper access
- Enforces well-formed transactions through the use of an interface
- Not a MAC model
- Designed for commercial databases
- Designed to enforce well-formed transactions and separation of duty
- Uses Certification rules and Enforcement rules
- Access triple

# Brewer-Nash

- Also Known as the Chinese Wall model
- Not a MAC model
- Used in instances where database contains information from many competitors
- Used to prevent conflict of interest

# Identity Management in the Cloud

- Account provisioning
  - Creating accounts
  - Granting privileges
- Groups/Inheritance streamline this process
- Securing the process
  - Auditing
  - Policy )Password length, aging, history
  - Inactive accounts
  - Account lockouts and clipping levels
- Entitlements

# Today's Identity Management in the Cloud

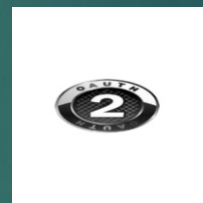
Provisioning  
Identities



Authentication

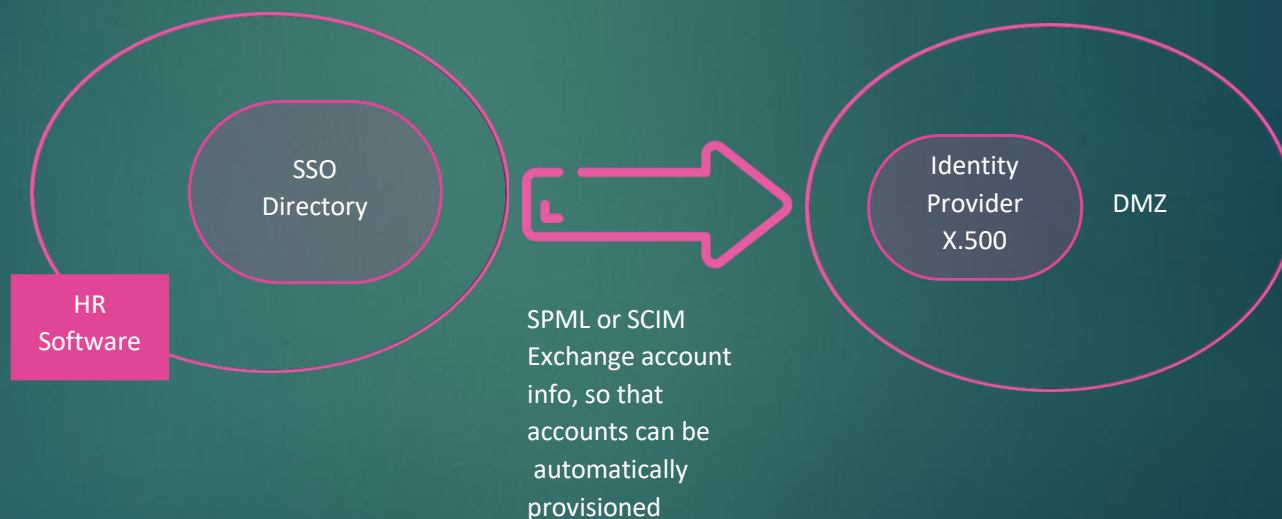


Authorization



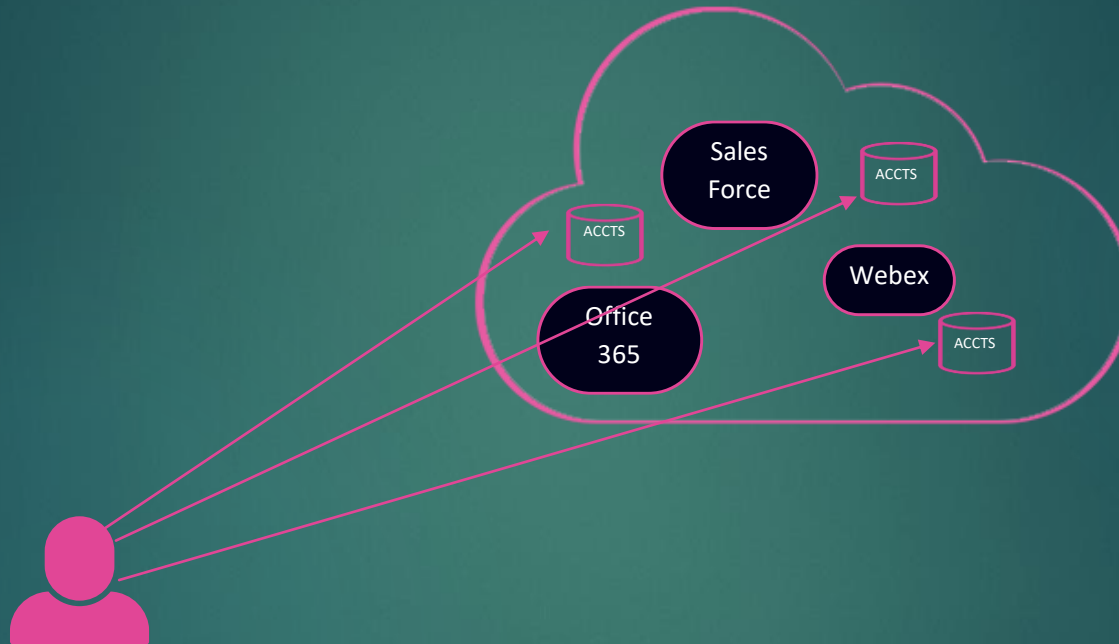
As a company on-boards and off-boards employees, they are added and removed from the company's electronic employee directory. As long as the service provider supports the SCIM standard, SCIM Could then be used to automatically add/delete (or, provision/de-provision) accounts for those users in external systems such as Google Apps for Work, Office 365, or Salesforce.com. Then, a new user account would exist in the external systems for each new employee, and the user accounts for former employees would be removed from those systems.

# SPML (Service Provisioning Markup Language) and SCIM (System Cross-Domain Identity Management

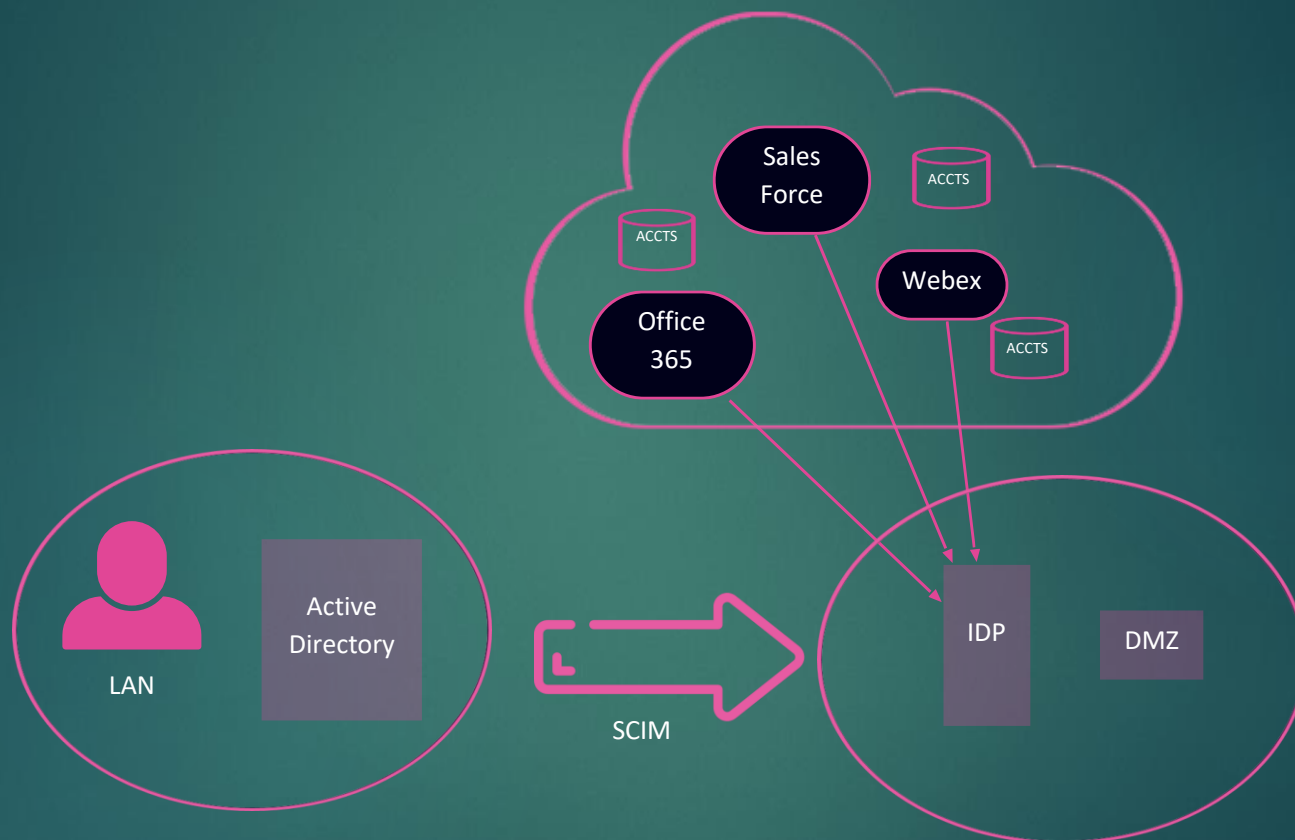




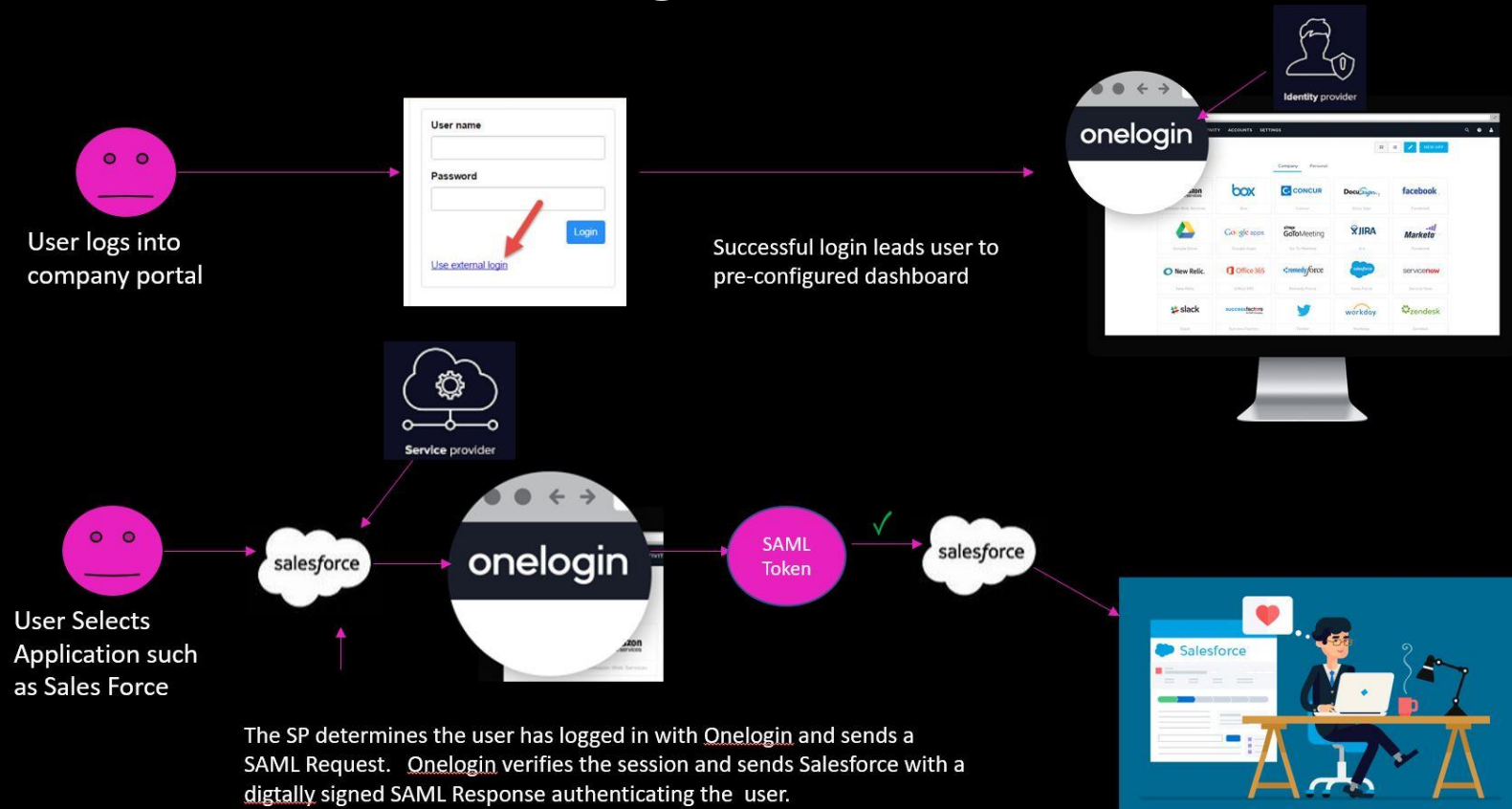
# The Problem with Authentication



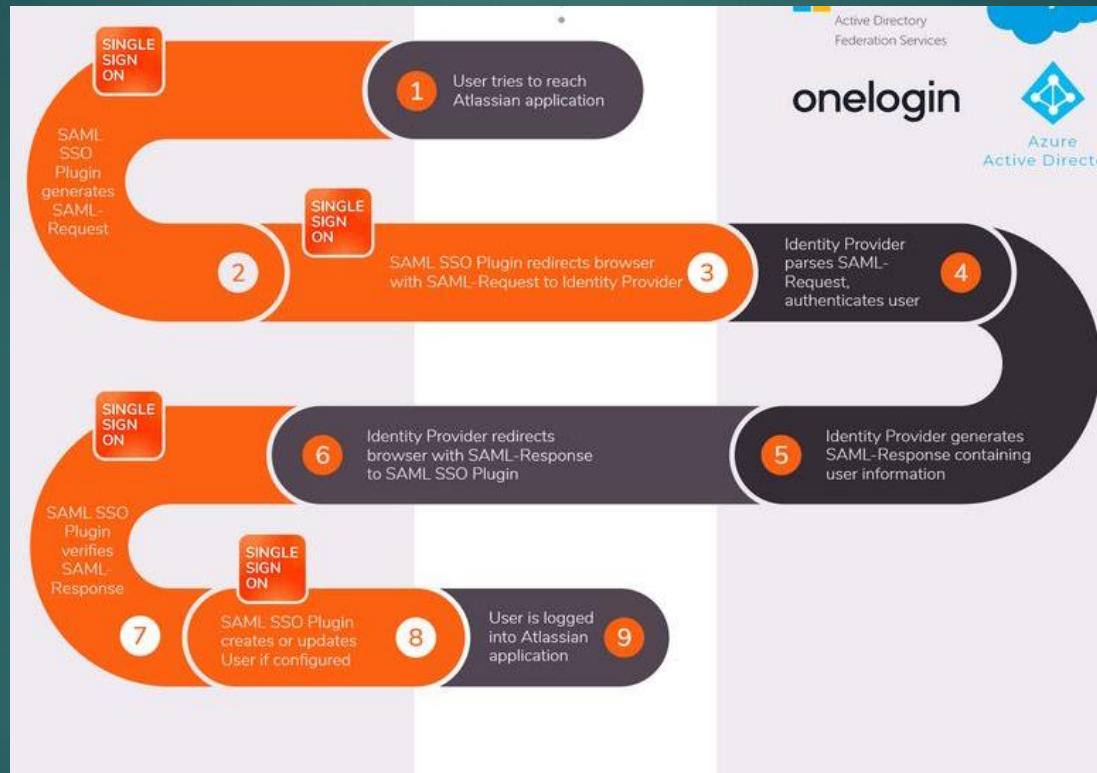
# The Problem with Authentication



# The Solution Through SAML/OPenID Connect



# Single Sign-on With SAML



# Authorization: OAuth 2.0

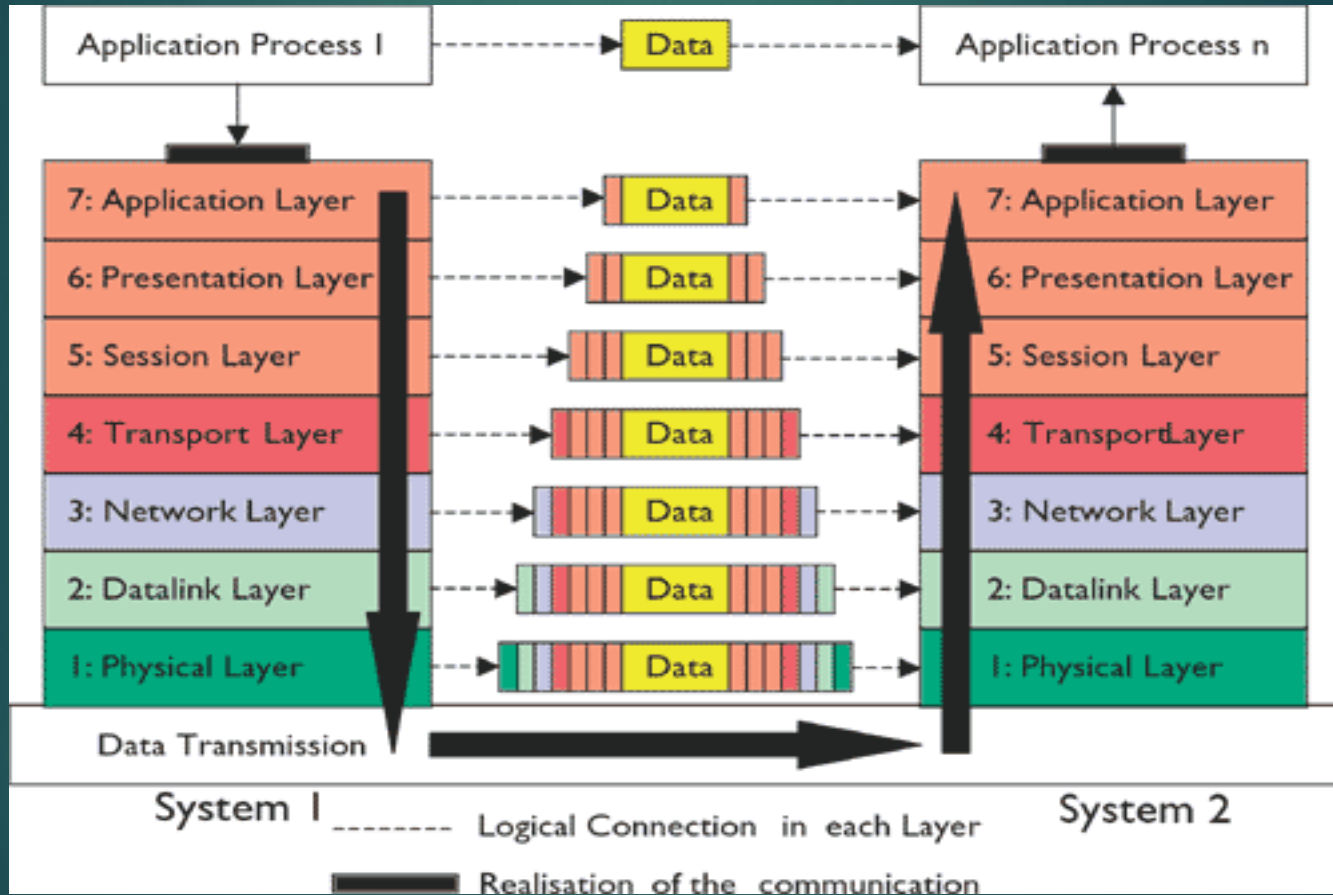
- OAuth (Open Standard for Authorization) has different intent
- Not designed for SSO
- Provides delegation of rights to applications
- In simplest terms, it means giving your access to someone you trust, so that they can perform the job on your behalf, e.g. updating status across Facebook, Twitter, Instagram, etc. with a single click.
- Could go to the sites manually, but easier to delegate access to an app that connect the above platforms
- Authenticate yourself to Facebook, Facebook provides a consent page stating you are about give this app rights to update status on your behalf. If you agree, the app gets an opaque access token from Facebook, app stores that access token, send the status update with access token to Facebook
- Facebook validates the access token (easy in this case as the token was issued by Facebook itself), and updates your status.

# Domain 3: Basic Networking and Communications

# OSI Reference Model

- Developed by ISO
- Designed to promote interoperability between vendors
- Breaks network functionality down into 7 layers
- For the exam know the names and numbers of each layer

# OSI Reference Model Encapsulation





# Layer 1: Physical Layer

- Network Media
  - Coaxial: (Traditionally used for LANs. Now used for WANs)
  - Twisted Pair: Least Secure
  - Fiber: Most secure and costly
  - Wireless: Easiest to Intercept
    - RF waves to transmit signals
    - WEP
    - WPA
    - WPA II

# Layer 2: Data Link Layer

- Two Sublayers:
  - LLC (Logical Link Control)
  - MAC (Media Access Control)
    - ARP
      - ARP Poisoning
- Switches
  - VLAN Switches

# Layer 3: Network Layer

- Routers
- Layer 3 switches
- IP Addressing
  - Spoofing
  - NAT
- All protocols that start with “I” for the purpose of class, EXCEPT “IMAP”

# Layer 4: Transport Layer

- End to end delivery
- The “Pony Express”
- Upper layer services and protocols “piggyback” on Layer 4 protocols UDP or TCP
  - UDP Connectionless
  - TCP Connection-oriented
    - Three-way handshake: Syn, Syn-ack, Ack
      - Syn Flood
  - SSL and TLS

# Layer 5 Session

- Client-side application opens session (connection) with a server-side application on the server
- Synchronization

# Layer 6: Presentation Layer

- Formatting
- Compression
- Encryption

# Layer 7 Application

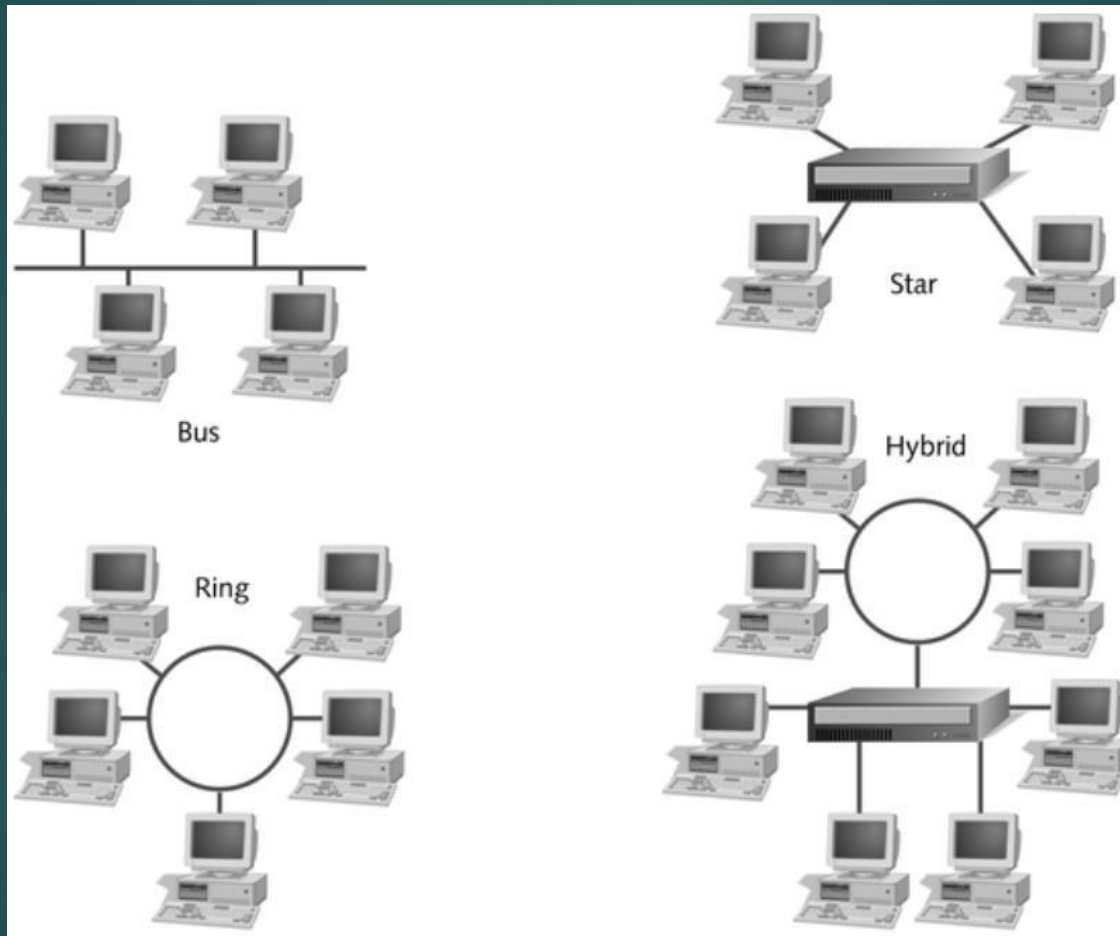
- Content Access
- Non-Repudiation
- Certificates
- HTTP, HTTPS, FTP, Telnet, and many others

# Media Access Methods

- CSMA/CD (Carrier Sense Multiple Access with Collision Detection): Ethernet
- CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance): Wireless
- Token Passing: Token Ring, FDDI (Fiber Distributed Data Interface)



# Network Topologies



# Basic Protocols

- Arp
  - Arp Poisoning
- ICMP
  - Ping Floods, Pings of Death, Smurf Attacks
- IGMP
  - Unicast, Multicast, Broadcast Addresses
- DHCP

# Basic Protocols Continued

- HTTP/HTTPS
- SSL/TLS
- DNS
- NFS
- FTP/TFTP
- Tunneling Protocols
  - PPTP, L2TP
- SSH
- Mail Protocols
  - SMTP, POP, IMAP

# IPSEC

- Tunnel Mode
- Transport Mode
- Subprotocols
  - AH (Authentication Header)
  - ESP (Encapsulating Security Payload)
  - IKE (Internet Key Exchange))

# Well-Known Ports

- FTP 20, 21
- Telnet 23
- SMTP 25
- **AH PROTOCOL ID 51**
- **ESP PROTOCOL ID 50**
- HTTP 80
- HTTPS 443

# Comparing Internet Architecture

- Intranet
- Extranet
- Internet
- DMZ

# IP Addresses

- Public
- Private
- Network Address Translation (NAT)
- IPv6
  - Limited Address Space
  - Integrated Security

# Wireless Technologies

- Using Radio Frequency to transmit data
- Key Components
  - WAP
    - Service Set ID
    - Broadcasts by default
    - Weak by Default



# Wireless Security

- WEP
- WPA
  - Personal
  - Enterprise
- WPAII
  - Personal
  - Enterprise

# Domain 4: Advanced Networking

# Understanding Telecommunications

- Transmission of signal used for communications
- Phones, Cables, Fiber Optics, Satellites, etc

# Connecting to the Internet

- Phones (PSTN/POTS)
- Dial Up
- ISDN
- ADSL
- Broadband Cable
- Wireless
- Satellite

# VOIP (Voice over IP)

- Telephony
- Analog voice over digital lines
- Easily intercepted/eavesdropped
- SRTP (Secure Real Time Protocol) can be used to apply security. It provides Confidentiality, Authentication, and replay protection

# Private Branch Exchange (PBX)

- Business Telephone System-Telco switch on the business property allows many functions
  - Transfer call
  - Voice Mail
  - Auditing
- Security Strategies
  - Physical Security—Protect the PBX/wiring
  - Strong administrative passwords
  - Restrict numbers for call forwarding
  - Restrict long distance or require access codes

# Firewalls

- Separate Trusted from less trusted
- Inspects Traffic (filters traffic) based on rules configured by an administrator (Often called ACLs, or Access Control Lists)
- Software vs. Hardware Firewalls
-

# Packet Filtering Firewalls

- Filters Traffic at Layer 3 of the OSI model
  - IP Address
  - Port Number
  - Protocol
- Very low-end decision making capability, but very fast.
- Deny all (White listing)
  - “Deny any” as the last rule



# Stateful Inspection

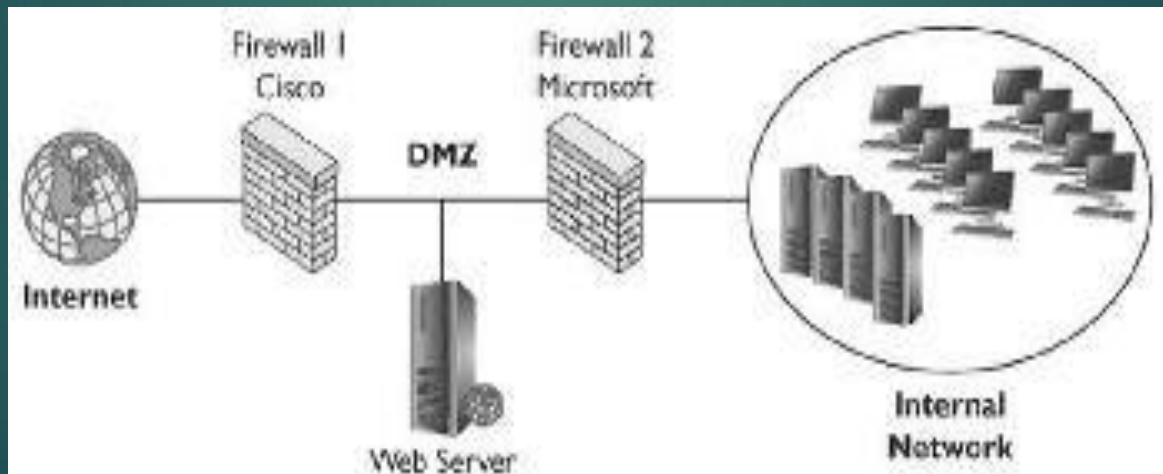
- Only traffic that is part of an active connection or that is initiating a new connection is allowed by a stateful inspection firewall. It will reject traffic that is not part of an active connection or that is initiating a new connection.
- Gibson, Darriil (2011-12-08). SSCP Systems Security Certified Practitioner All-in-One Exam Guide (Kindle Locations 2714-2715). McGraw-Hill Education. Kindle Edition.

# Application Firewall

- Inspects traffic at Layer 7—full content inspection
- Has different engines for different protocols
  - HTTP
  - SMTP
  - FTP
- Can also be called an Application Proxy or an Application Gateway
- Defense Diversity—don't rely on a single vendor for all your protection needs, particularly with firewalls

# DMZ

- Gibson, Darril (2011-12-08). SSCP Systems Security Certified Practitioner All-in-One Exam Guide (Kindle Locations 2738-2740). McGraw-Hill Education. Kindle Edition.



# Host Based vs. Network Based

- Host based Systems
  - Inspects traffic destined for a specific machine
  - Run on internal computers to inspect traffic coming to a particular system's NIC
  - Many operating systems include host-based firewalls, like Windows Firewall
- Network based firewalls
  - provide a point of separation from network to network (Used to create a DMZ also)
  - Protect internal networks from the untrusted internet
- Both are needed for Defense in Depth

# Proxy Server

- Implements NAT (Network Address Translation)
- Acts on behalf of clients
- Can inspect their requests and block them based on rule set
- Can inspect responses and block them based on rule set
- Can cache and filter
- Administrators can purchase lists of websites to block from various vendors (Shopping, games sites, inappropriate material, etc)

# Remote Access

- Dial Up
  - RAS Servers
    - War Dialing
      - Call Back
      - Caller ID
      - Telephone Number of RAS
- VPN (Virtual Private Network)
  - Tunneling Protocols (encapsulation)
    - PPTP—initial handshaking not secure
    - L2F/L2TP—uses IPSec for security
    - SSTP (uses port 443)
  - SSH Not used for VPNs—used to secure Telnet, FTP

# IPSec

- Tunnel Mode
- Transport Mode
- AH
- ESP
- IKE

# Authentication Protocols

- PAP—clear text
- CHAP
  - MSCHAP v1 (no longer used)
  - MSCHAP v2 (Mutual Authentication)
- EAP/EAP-TLS
  - Smart cards, biometrics, tokens, etc



# Central Authentication for Remote Access

- Radius
  - Provides Central Point of Authentication for Remote Access Devices
  - Only encrypts the password
- TACACS+
  - From Cisco
  - Performs the services of RADIUS
  - Encrypts entire session instead of just the password

# Network Access Control (NAC)

- Inspects a system's health
  - Anti-virus software
  - Firewall
  - Anti-spyware
  - Up to date on patches, service packs, updates
- Can provide remediation

# Cloud Computing

- Services provided across the internet
- Software as a Service (SaaS)
  - Gmail, Google Docs, MS Office 365
- Platform as a Service (PaaS)
  - Platform provided primarily for software development
  - Testing environments, tools, etc. Google Apps, Amazon Cloud Computing
- Infrastructure as a Service (IaaS)
  - Sometimes called Hardware as a Service
  - Servers, storage, network services
- Security Considerations
  - Privacy
  - Compliance
  - Availability (pros and cons)

# Virtualization

- Isolation
- Cost benefit
- Threats
  - Scooby Doo, Red Pill sniff out virtual machines
  - VM Escape to access host and all guest vms.

# Domain 5: Attacks

# Hackers/Crackers

- Hacker (White Hat)
- Crackers (Black Hat)
- Grey Hat
- Attacker

# Insider Threat

- Greatest loss comes from internal employees
- Both intentional and accidental
- Phishing Emails
- Forwarding Spam/Hoaxes/Malware
- Unauthorized data access/loss
- Loss of Hardware
- Fraud
  - Separation of Duties, Job rotation, Mandatory Vacations

# Other Attackers

- Script Kiddies
- Phreaks
- Advanced Attackers: APT (Advanced Persistent Threats)

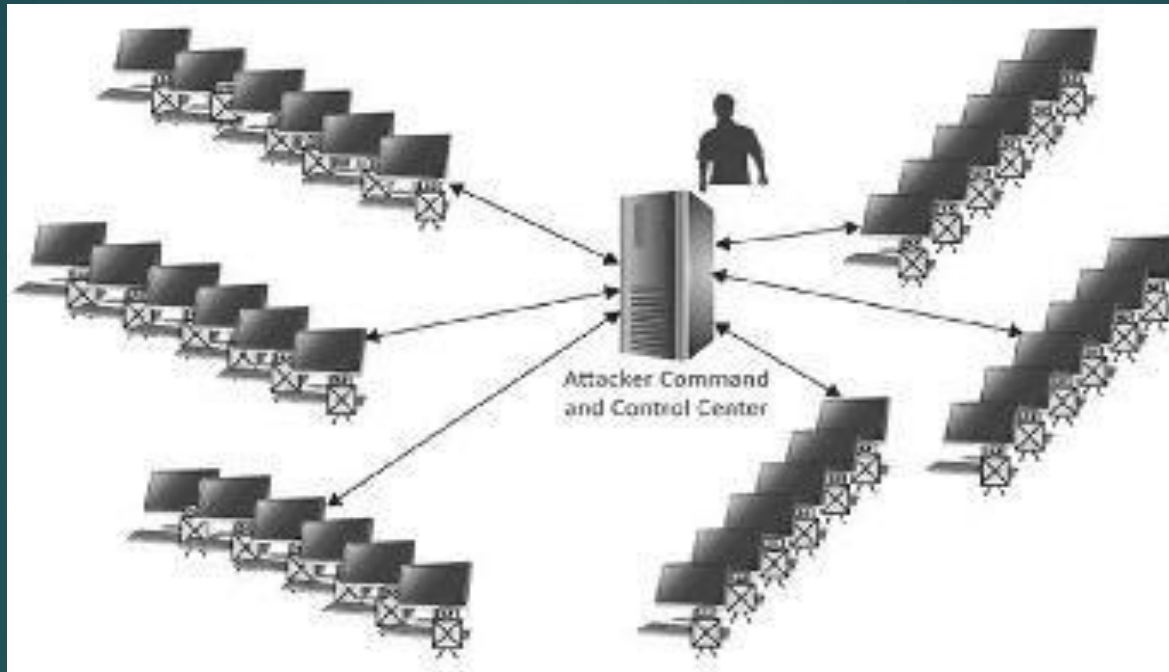


# DoS, DDoS (Denial of Service, Distributed Denial of Service)

- DoS attempts to make a system or service unavailable
- Often attempts to overwhelm a system so it can no longer respond to legitimate requests.
  - Syn Flood—exploits TCP handshake (can be called a TCP SYN, TCP Flood)
  - Ping flood--Exploits ICMP (ping)
  - Ping of Death -Exploits ICMP (ping)
  - LAND
  - Smurf
  - Fraggle

# DDos (Distributed Denial of Service)

- Botnets/Zombies: The goal is to commandeer unsuspecting systems to carry out the attack. Compromise as many systems as possible—this is the first step.
  - Drive-by Downloads—malicious websites where downloads happen automatically, often without users knowledge
  - Trojan Horses/Trojans



Gibson, Darril (2011-12-08). SSCP Systems Security Certified Practitioner All-in-One Exam Guide (Kindle Location 3306). McGraw-Hill Education. Kindle Edition.

# Spam

- Unsolicited Emails sent in bulk
- Can overwhelm mail servers
- Can include phishing attempts
- Anytime you provide your email address you increase your risk for spam. Consider having a separate email just for websites that require email

# Sniffers

- Protocol Analyzers
- Intercept traffic on the network
- Encrypt or keep sensitive information off the network
- Wire shark

# Sniffing through Hubs vs. Switches

- Sniffing through hubs is easy. Hubs send all data out all ports all the time.
- Sniffer is a system with a NIC in promiscuous mode (can capture traffic regardless of it's destination address).
- Switches, however, only send traffic out the appropriate port.
  - Port Span

# Looking for Information

- Foot Printing: Learn the network
  - Ping Sweeps
- Fingerprinting
  - Port Scans

# Additional Attacks

- Salami
- MITM (Man in the Middle)
  - Passive: Sniffing
  - Active: Targeted: Session Hijack (captures cookies with web session information) TIP A cookie is a text file stored on a user's system. When a user visits a website, the website is able to read the cookie and use it to identify the user. The cookie also includes a session ID used to identify the current session to the web server.
  - Gibson, Darril (2011-12-08). SSCP Systems Security Certified Practitioner All-in-One Exam Guide (Kindle Locations 3430-3431). McGraw-Hill Education. Kindle Edition.



# Additional Attacks

- Replay: Needs uniqueness information to prevent
- Buffer Overflow: Exploits a programming error.
  - Denial of Service
  - Gain elevated privilege on a system
  - The best defense is to keep systems updated This is a important step for protecting against many attacks
  - Covert Channel
    - Loki Attack
- Scareware/Ransomware

# Password Attacks

- Dictionary
- Brute Force
- Rainbow tables-Very fast and very efficient
  - Applications should “salt” the password
- Social Engineering is the easiest!

# Additional Attacks

- Cramming
- Zero Day Exploits
- APT (Advanced Persistent Threats)

# Social Engineering

- Impersonation
- Dumpster Diving
- Piggy Backing
- Shoulder Surfing
- Phishing
  - Spear Phishing
  - Whaling
  - Smishing
  - Vishing
- Pharming
- User Awareness Training to Modify Behavior!!!

# Domain 6: Malicious Code and Activity

# Virus

- Needs a host and a user action to spread
- Armored virus: Had mechanisms to thwart removal
- **Macro Virus: easy to create because of the simplicity of the macro languages**
- **Boot Sector Virus: malicious code inserted into the disk boot sector**
- **Compression Virus: when decompressed, it initializes and attacks the host system**
- **Stealth Virus: hides its footprints and changes that it has made**
- **Polymorphic Virus: makes copies and changes the copies in some way – uses a mutation engine**
- **Multi-Partite Virus: infects both boot sector and hard drive (the file system)**

# Worm

- Doesn't need a host or user interaction
- Can spread across a network, from computer to computer once the network is infected. Self-replicating

# Other Malware

- Trojan/Trojan Horse:
  - Looks like one thing, contains something else (screensavers that contain malicious code, etc)
  - Usually a means of distributing malware
- Logic Bomb: Lays dormant until an event
- Keyloggers: Hardware or software. Sometimes called shims.
- Rootkits: Integrated with the kernel of an Operating system. Can be very difficult to get rid of.
- Backdoor/Trapdoor: Entry way into a system to bypass normal authentication controls
- Spyware: Tracks user action



# Mobile Code

- Client Side Processing
- JavaScript
- Active X
- Java
- Protect your system:
  - Don't download if not digitally signed
  - Java code should run in the “sandbox”
- Documents including Macros (vbscript)

# Threats to Web Servers

- Server-side processing
- Web Forms
- SQL Code Injection
  - Input Validation
    - Data Length
    - Data Type
    - Data control Languagei
- Command Injection: Attempt to attack Operating System of web server.
  - Dir command
  - Deltree

# Cross Site Scripting (XSS)

- Attempts to insert malicious code on legitimate websites that don't have security controls
- When the user goes to the website, the code runs on the user's system
- Can be used to discover passwords and cause other harm like infecting the client system

# Cross Site Request Forgery (CSRF or XSRF) Pronounced

- User is tricked into clicking a link that includes a command for an action.
- If a user has logged on to a banking site, for instance another web-site or chat could include a link that would cause an action on that website to run as the legitimate user.

# Defense Against Malicious Code

- • Install antivirus software on all systems. •
  - Install antivirus and antispam software on e-mail servers. •
  - Install antivirus and content filter software on firewalls.
  - Keep all antivirus software up to date.
  - Keep all systems up to date.
  - Educate users.
  - Content-filtering appliance
  - Principle of least privilege
- 
- Gibson, Darril (2011-12-08). SSCP Systems Security Certified Practitioner All-in-One Exam Guide (Kindle Locations 4358-4362). McGraw-Hill Education. Kindle Edition.

# Educate Users

- Use spam filters and AV software. •
- Don't open attachments from unsolicited e-mails. •
- Don't click on links from any unsolicited e-mails. •
- Identify actual links sent within an e-mail (even from people you know, because their system can become infected). •
- Don't send sensitive data via e-mail (unless you are able to encrypt it). •
- Limit personal information provided online.
- Check source of links and be wary of shortened links
- Gibson, Darril (2011-12-08). SSCP Systems Security Certified Practitioner All-in-One Exam Guide (Kindle Locations 4535-4539). McGraw-Hill Education. Kindle Edition.

# Stay in “The Know”

- Sign up for email alerts and bulletins
- Review MITRE’s CVE (common vulnerabilities and exploits)

# Antimalware Software

- Signature Based
- Behavior (heuristics) based
- Should be used to inspect any content downloaded from the web, as well as email attachments
- Real-time scanning
- On-Demand Scanning
- Scheduled Scanning



# Domain 7: Risk

# Risk Definitions

- Asset: Anything of Value to the company
- Vulnerability: A weakness; the absence of a safeguard
- Threat: Something that could pose loss to all or part of an asset
- Threat Agent: An attacker or his software that carries out the attack
- Exploit: An instance of compromise
- Risk: The probability of a threat compromising an Vulnerability.

# Risk

- Determine the value of your assets
- Look to identify the potential for loss
- Find cost effective solution reduce risk to an acceptable level (rarely can we eliminate risk)
- Safeguards are proactive
- Countermeasures are reactive

# Sources of Vulnerabilities

- Weak or non-existing anti-virus software
- Disgruntled employees
- Poor physical security
- Weak access control
- No change management
- No formal process for hardening systems
- Lack of redundancy
- Poorly trained users

# Probability and Impact

- Probability: How likely is the threat to materialize?
- Impact: How much damage will there be if it does?

# Managing Risk

- Avoid
  - Transfer
  - Mitigate
  - Accept
- 
- Secondary Risks
  - Residual Risks

# Risk Assessment

- Looks at risks for a specific period in time and must be reassessed periodically
- Risk Management is an ongoing process
- The following steps are part of a Risk Assessment per NIST 800-30
  - System Characterization
  - Threat Identification
  - Vulnerability Identification
  - Control Analysis
  - Likelihood Determination
  - Impact analysis
  - Risk determination
  - Control Recommendation
  - Results Documentation

# Risk Analysis

- Qualitative Analysis (subjective, judgment-based)
  - Probability and Impact Matrix
- Quantitative Analysis (objective, numbers driven)
  - AV (Asset Value)
  - EF (Exposure Factor)
  - ARO (Annual Rate of Occurrence)
  - SLE (Single Loss Expectancy)= $AV * EF$
  - ALE (Annual Loss Expectancy)  $SLE * ARO$
  - Cost of control should be the same or less than the potential for loss



# Responding to Incidents

- Events: Any observable occurrence on a system or a network
- Adverse events have negative impact or consequence
- A computer security incident is specifically a violation or imminent threat of a violation of computer security policy
  - DoS
  - Malware
  - Inappropriate Usage
  - Unauthorized access.
- The first thing after event detection is to limit it's scope (contain the incident)

# Computer Incident Response Team (CIRT)

- Preparation is Key
  - Contact Information
  - Reporting forms
  - War room
  - Forensic Tools
  - Documentation Process
  - Software and Hardware
  - Well Documented Procedures
  - Well Trained Staff

# Incident Response

- Detection and Analysis
- Containment
- Eradication
- Recovery
- Post-incident Debriefing (lessons learned and Documentation)

# Domain 8: Monitoring and Analysis

# Intrusion Detection System

- Inspects traffic and documents suspicious behavior
- NIC must be in promiscuous mode
- Passive devices that document attacks
- IPS Stops the attack and is active
- HIDS (Host IDS)
- NIDS (Network IDS)
  - Agents loaded on routers, switches
  - Management Console is a central location to configure and review
  - Analysis Engine
- Alerts
  - False Positive
  - False Negative

# Analysis Engines

- Signature Based(Knowledge Based)
  - Must be frequently updated
  - No good against Zero Day attacks
  - Anomaly Based (Heuristic or Behavior)
    - Can have false positives
    - Must be rebaselined with changes
- Hybrid

# Detecting Unauthorized Changes

- File Integrity Checkers for Logs
- Monitor for Unauthorized Connections
- Deploy a Honeypot or a HoneyNet
  - Distract attackers
  - Learn their tools/techniques
  - Never entrap. Only entice.

# SEMs, SIMs, and SIEM

- SEM (System Event Managers)/SIM (Security Information Manager)/SEIM (Security Information and Event Manager)
- Monitoring tools for large organizations that massive amounts of information that needs to be analyzed
  - Single interface
  - Database
  - Fine-tune for specific needs
  - Alerting capabilities
  - Secure storage of data



# Security Assessments

- Vulnerability Assessments
- Penetration testing (Pen Test)
- Types
  - White Box (Full Knowledge: designed to test an insider's ability to compromise a system or network)
  - Black Box (Zero Knowledge: designed to test and external attacker's success likelihood)
  - Grey Box (Partial Knowledge: designed to test someone with some knowledge of the organization but without full administrative access)
- All types of testing should be implemented.

# Vulnerability Scans

- Nessus
  - IP Ping sweep
  - Port Scans
  - Network mapping
  - Password Cracking
- Part of demonstrating compliance checking and due diligence for organizations that must show they monitor for compliance

# Steps for Vulnerability Assessments

1. Permission from Management
2. Discovery: Scan the network
3. Analyze Results
4. Document vulnerabilities
5. Identify and recommend corrective actions
6. Present recommendations to management
7. Remediate

# Steps for Penetration Testing

1. Get WRITTEN permission
2. Perform vulnerability assessment
3. Attempt to exploit vulnerabilities (do no harm!)
4. Report findings to Management

# Domain 8 Monitoring and Analysis Review

Questions page 242

# Domain 9: Controls and Countermeasures

# Using Controls, Safeguards and Countermeasures

- Controls are mitigating strategies we implement to reduce risk to an acceptable level
- Safeguards are proactive
- Countermeasures are reactive
- Use Defense in Depth (aka Layered Defense)
  - Management (Focus is on management of risk and IT Security)
  - Technical (Hardware, software, firmware)
  - Operational (Implemented by people, not systems)

# Steps for Control Implementation

- 1. Prioritize Actions
- 2. Evaluate Recommended Controls
- 3. Cost/Benefit Analysis
- 4. Select the Control
- 5. Assign Responsibility
- 6. Develop an Implementation Plan
- 7. Implement Controls



# Three Primary Goals of Controls

- Prevent
- Detect
- Correct

# Other Control Functions

- Compensating
- Directive
- Recovery
- Deterrent

# Classes of Controls

- Management: Policies, procedures, standards, guidelines
- Technical: Encryption, firewalls, IDS, etc
- Operational: Training users, Change management practices

# System Hardening

- Also called “reducing the attack surface”
- Remove unnecessary services
- Apply the latest security patches
- Change default settings
- Enable firewalls
- Enable anti-virus

# Policies, Standards, Procedures and Guidelines

- Policies: Authoritative in nature and come from senior management.
  - Acceptable Use Policy (AUP)
  - Backup Policy
- Standards provide the specifics of policy
- Procedures: Step by step instructions
- Baseline: Minimum acceptable security Configuration

# Change Control and Configuration Management

- Ensure that changes to systems are formally approved, tested, documented prior to implementation
- Promotes consistency and stability of systems

# Patching Systems

- Close critical security vulnerabilities
- Ensure systems are able to detect mitigate current risks
- A process for testing, approving, and documenting patches must be in place.

# USB Devices

- Most organizations restrict use of USB devices
- Easily used to infect systems
- Can also be used for data exfiltration



# Fault Tolerance (Redundancy)

- RAID

- RAID 0: Disk Striping
- RAID 1: Mirroring
- RAID 5: Disk Striping with Parity
- RAID 10 (Disk striping set mirrored to a second set of drives)

# Clustering

- Redundancy for entire servers and services
- Multiple physical nodes (servers) participate in a single logical unit called a cluster
- Also called a server farm
- Appears as a single server to users
  - Web Servers and Database servers are often implemented in a cluster

# Backups

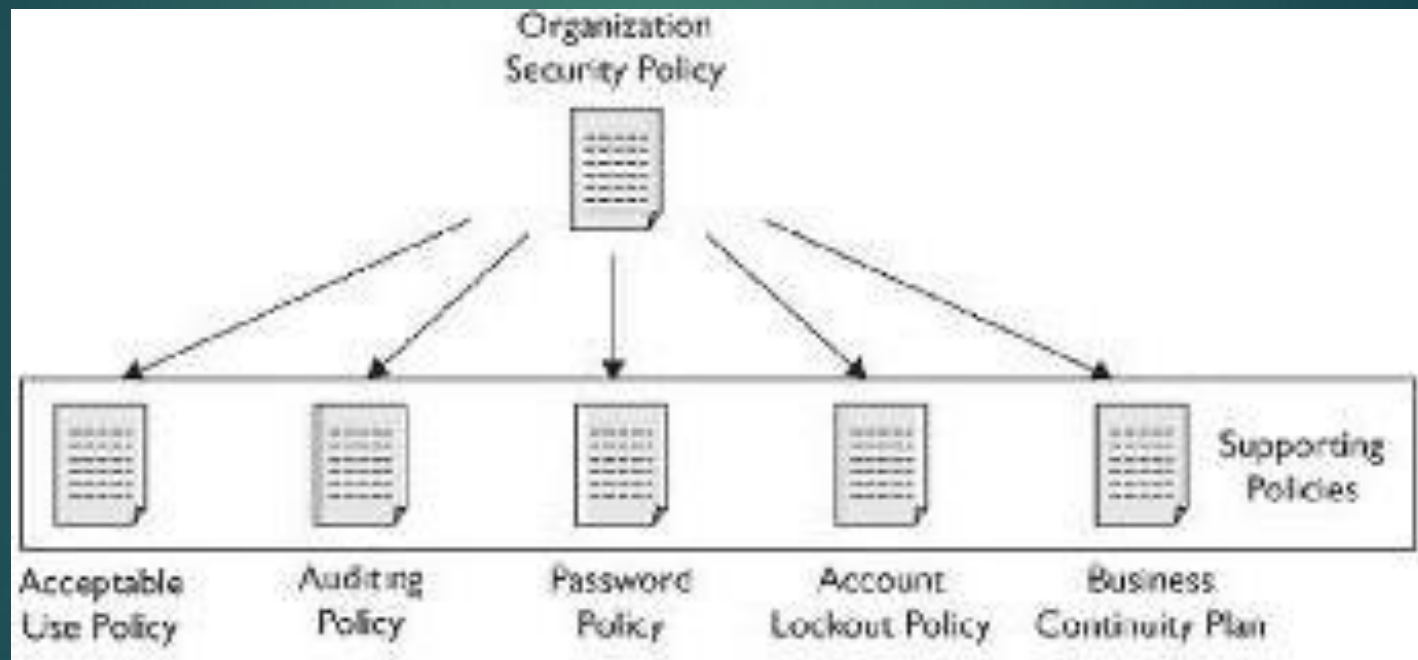
- Full: All Data is backed up. The archive bit is cleared (reset)—In a restore situation, only the most recent full backup will need to be restored.
- Incremental: Backs up all data that has changed since the last backup of any kind. The archive bit is cleared (reset). In a restore situation, all tapes will need to be restored, including the full backup and each day's incremental
- Differential: Backs up all data that has changed since the last FULL backup. Archive bit is NOT cleared (not reset) In a restore situation, only two tapes will need to be restored. The full backup and the most recent differential.

# Domain 12: Security Administration and Planning

# Security Policies

- Security Policy is a high-level document providing the organization with a view of the security goals for the company.
- The organizational policy is supported by subordinate policies
- Sized based on the needs of the company
- Part of Due Care
- Awareness: Designed to modify behavior
  - Training
  - Warning Banners
  - Posters

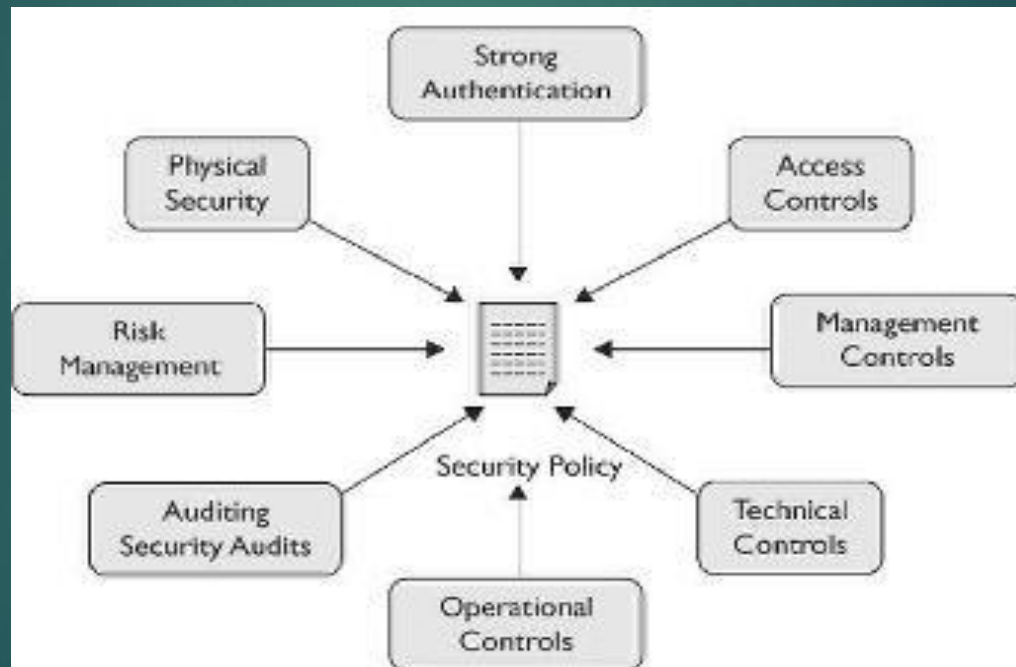
# Subordinate Policy



# Often included in Security Policy

- Organization mission statement
- Statement of accountability
- Data classification
- Classification of resources
- Network access
- Risk management
- Business Continuity
- Incident response
- Physical security
- Acceptable Use
- Enforcement
- Authentication requirement
- Hardware usage
- Ethics statement

# Enforcement of Policy





# Updating/Maintaining Security Policies

- Should be reviewed at least once per year
- Also reviewed in the event of a major change
- Supporting policies should also be reviewed
- Reexamine after a security breach

# Business Continuity Plan

- Protects the organization when risk management fails
- Disasters/Disruptions come from many different areas
  - Natural Disasters
  - Accidents
  - Human Error
  - Malicious Attacks

# Elements of a BCP

- Business Impact Analysis
- Develop Recovery Strategies
- Develop Recovery Plans
- Test Recovery Plans
- Train Personnel and Maintain Plans

# Business Impact Analysis (BIA)

- Identifies and Prioritizes Business Processes for Criticality
- Identifies Acceptable Outage Times
  - MAO (Maximum Acceptable Outage)
    - Can also be called MTO or MTD
  - RPO (Recovery Point Objective)

# Disaster Recovery Plan

- Deals with the immediacy of the disaster
- First priority is human safety
- Identifies how one or more individual systems can be recovered after a failure

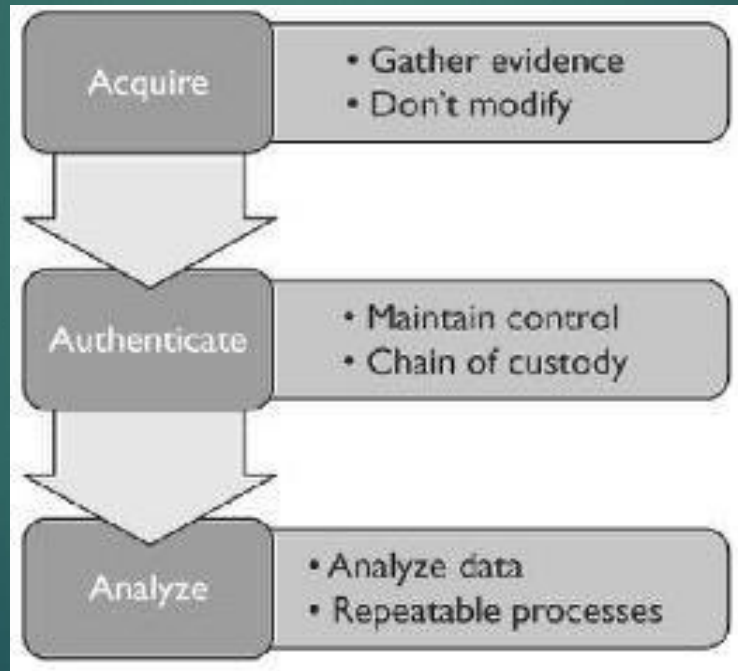
# Alternate Locations

Alternative	Time to Occupy	Readiness	Cost
Mirrored Site	Within 24 hours	Fully redundant in every way	Highest
Hot Site	Within 24 hours	Fully configured equipment and communications links; need only load most recent data	Higher
Rolling Hot Site	Usually 24 hours	Similar to hot site, but supports data center operations only	High
Warm Site	Within a week	Between a hot and cold site. Partially configured equipment and does not contain any live data; some activation activity needed	Medium
Cold Site	Within 30 days	Typically contains the appropriate electrical and heating/air conditioning systems, but does not contain equipment or active communication links	Lowest

# Exploring Computer Forensics

- Computer forensics is the science of examining and inspecting computer systems for evidence about an event or crime.
- First Responders are tasked with preserving the evidence.
- It is extremely important that data doesn't get modified as part of collection.
- Don't work on originals. Always make a copy

# Three Phases of a Computer Forensics





# Chain of Custody

- One of the reasons that evidence is frequently ruled inadmissible.
- Must account for how evidence is handled and by whom.

There should be no gaps in the Chain of Custody

- Document, document, document
- Who, what, when, where

# IOCE (International Organization of Computer Evidence)

- Digital evidence must follow the same principals as with more traditional evidence.
- If a person handles original evidence, they must be trained to do so.
- All activity relating to the seizure, access, storage or transfer of evidence must be documented and preserved
- An individual must be responsible for all actions taken with respect to the digital evidence
- Any agency that is responsible for seizing, accessing, storing or transferring evidence is responsible for compliance with these principles

# Volatile Evidence

- Evidence is easily destroyed
- Capture Screen Contents
- Dump contents of RAM
- Don't power down system

# Comparing Abuse vs. Crime

Computer Abuse	Computer Crime
Counter to established policies	Breaks a law
Misuse Unethical use	Theft Destruction

# Elements of a Crime

- Motive
- Opportunity
- Means

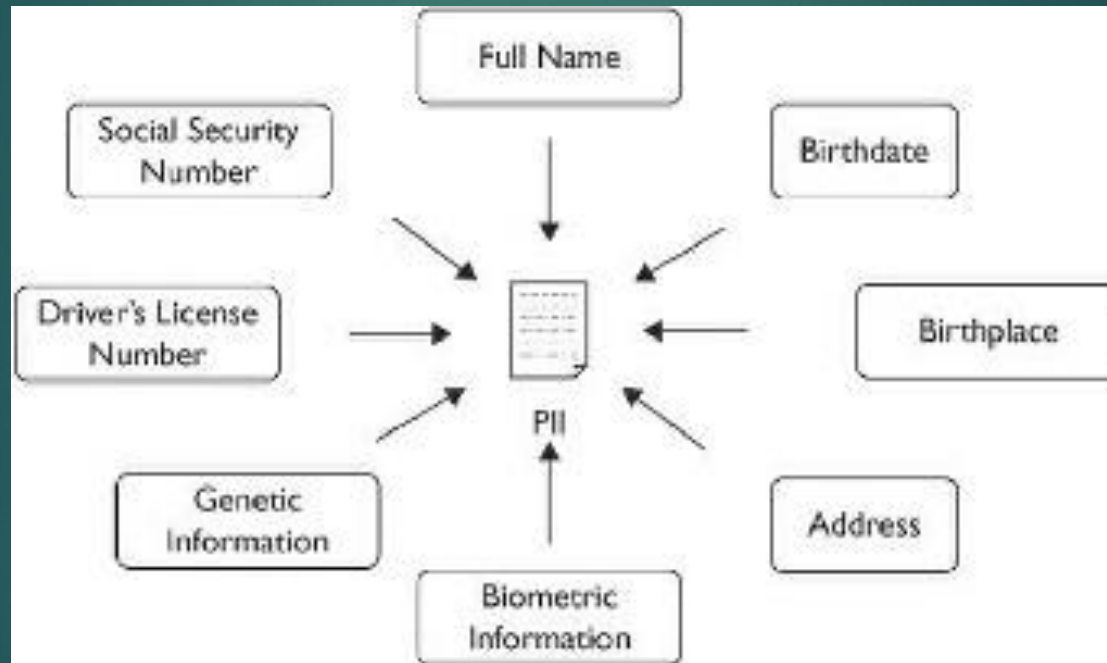
# Fraud and Embezzlement

- Fraud is the use of deception for unlawful gain or unjust advantage
- Embezzlement is a specific type of financial fraud where an individual steals money or property from an employer, company, clients, customers, or partners
- Misappropriation of funds.

# Controls to Prevent Fraud

- Separation of Duties
- Mandatory Vacations
- Job Rotation
- Principle of Least privilege
- Due Diligence and Due Care

# Copy of PII





# European Directives

- Data Protection Directive
  - Regulates personal data protection
- E-privacy Directive
  - Regulates use of cookies

# Privacy

- California Supreme Court rules zip codes are PII
- Connecticut's Public Act
  - SSNumbers
  - Any one in possession of personal information of another person's data shall safeguard that data
- Children's Online Privacy Protections (COPPA)
  - Prevents collection of information on children under 13
- California Online Privacy Protection Act
  - requires operators of commercial websites to post comply with a privacy policy if they collect PII on any visitors who reside in California.

# Domain 14

## Cryptography

# Cryptography

## Definitions/Concepts

- Plaintext + Initialization Vector + Algorithm + Key  
=

Ciphertext

Initialization Vector: Adds randomness to the beginning of the process

Algorithm: Math Functions

Key: Instructions on how the algorithm will work

Cryptanalysis: Science of breaking the secrecy of the algorithm

# The P.A.I.N of Cryptography

- Privacy
- Authenticity
- Integrity
- Non-Repudiation

# Integrity

- Integrity provides assurance that the message has not been modified
- The sender hashes the document and the receiver hashes the document. If the two hashes match, we get assurance the document hasn't changed
- Hashing algorithms create one-way message digests (hashes)
- MD-5 128 bit hash
- SHA-1 256 bit hash
- Sha-2 256 bit hash

# Privacy

- Encryption
  - Symmetric
  - Asymmetric
  - Hybrid

# Symmetric Cryptography

- Same Key is used to decrypt that was used to encrypt
- Two parties must share the same key
  - Can be called Private Key, Shared Key, Secret Key
- Cryptography
- Block
  - Chunks data into blocks and encrypts the entire block at a time
  - Complex, good security, slow
- Stream
  - Encrypts one bit at a time
  - Fast, efficient, not secure (RC-4)



# Pros and Cons of Symmetric Cryptography

- Cons
  - No easy way to exchange the key between the two parties
  - Not scalable
  - Only provides Privacy, no other security services
- Pros
- Fast
- Fast
- Fast
- Very desirable to use it to exchange data because of its speed, but there needs to be some way to resolve the other problems.

# Asymmetric

- Every user is granted a key pair. One is a public key. The other is a private key
- The keys are mathematically related in such a way that anything encrypted with one key can only be decrypted with the other
- Solves scalability problem, as every user has only two keys
- Solves key exchange problem, as nothing secret needs to traverse the network.

# Asymmetric

- **Privacy:** Always encrypt with the receiver's PUBLIC key. Receiver decrypts with receiver's PRIVATE key which only that receiver has.
- **Authenticity:** Sender will encrypt "something" with the sender's PRIVATE key. When the receiver is able to successfully decrypt that "something" with that sender's PUBLIC key, that proves it was encrypted with the sender's PRIVATE key, which only the sender has.
- **Integrity:** Create a message digest (hash) with a hashing algorithm (MD5, SHA-1, SHA 256)
- **Non-Repudiation.** Sender encrypts hash with the sender's private key. Receiver decrypts hash with sender's public key. Receiver hashes document—if hashes match, receiver gets a guarantee that message has not been modified. This is called a digital signature.

# Hybrid Cryptography

- SSL is a great example of hybrid cryptography
  1. Client requests a secure connection to a server using the https protocol
  2. Server responds by sending it's public key to the client
  3. The client generates a symmetric session key
  4. The client encrypts the session key with the server's public key and sends it to the server.
  5. The server decrypts the session key (using it's private key) and has the session key to use for communications.
  6. A "secure channel" has been created

# Symmetric Algorithms

- DES was the defacto standard for many years, but today can be broken easily
- 3DES: More secure than DES but requires a ton of processing power
- AES: Most commonly used
- IDEA, Twofish, Blowfish, RC-5, CAST and many others

# Asymmetric

- Diffie Hellman: Key Exchange
- DSA: was originally used for digital signatures
- RSA: Used for digital signatures and is based on factorization
- El Gamal
- ECC (Elliptical Curve Cryptography)
- Knapsack: Obsolete

# Certificates

- Allow a guarantee of identity and verification of a public key
- Signed by an issuing authority (Certificate Authority)
- Is only as trusted as the issuing authority
- Require a PKI (Public Key Infrastructure)

# Email Security

- S/MIME (Secure Multi-Part Internet Mail Extensions)
  - Standards based
  - Uses X.509 certificates
- PGP (Pretty Good Privacy)
  - Proprietary
  - Web of Trust
  - Key Ring file



# Steganography

- A message hidden inside another format (an image file, a sound file, even a text file).
- Special software embeds one message into the other by using redundant or LSBs (Least significant bits)

# Cryptanalytic Attack

- Known Plaintext
- Known Ciphertext

# Cryptography Review