Comptia Security + (Syo-601 & Syo - 701) Exam Study Guide

Table of Contents

Section 1 - Intro To Information Security And Security Roles & Responsibilities

1.1 Introduction To Information Security

Information security is based on the cia and dad triads. information and cyber security professionals strive to accomplish the cia triad.

- Confidentiality - data is accessed by only those with the right permit and can be achieved with the use of encryption, passwords, biometrics, 2fa and so on.

- integrity - this ensures that data has not been tampered or altered in any way with the use of hashing, checksums etc

- availability - data and resources are available to be accessed or shared at all times. This can be achieved with network access, server and data availability.

Black hat hackers and cyber criminals aim for the dad triad.

- disclosure - here data is accessed by non-authorized users with the use of trojans, brute force attacks and theft

- alteration - this means data has been compromised or tampered with. This can be attained by malware, viruses and attacks like sql injection.

- deniability - this means data is not made available to those who need it with the use of attacks like dos and ddos as well as ransomware.

Non-repudiation - means a subject cannot deny something such as creating, modifying or sending a resource.

1.2 Cybersecurity Framework

Information security and cyber tasks can be classified as five functions following the framework developed by the national institute of standards and technology (nist).

The Nist Framework Has 5 Parts

- Identify - Evaluate Risks, Threats & Vulnerabilities And Recommend Security Controls To Mitigate Them.

- Protect - Procure/Develop, Install, Operate And Decommission It Hardware & Software Assets With Security As An Embedded Requirement At Every Stage.

- Detect - Perform Ongoing Proactive Monitoring To Ensure That Security Controls Are Effective And Capable Of Protection Against New Types Of Threats.

- Respond - Identify, Analyze, Contain And Eradicate Threats To Systems And Data Security

- Recover - Implement Cyber Security Resilience To Restore Systems And Data If Other Controls Are Unable To Prevent Attacks

1.3 Security Roles & Responsibilities

Security Professionals Must Be Competent In A Wide Range Of Disciplines From Network To Application Design And Procurement Of Security Resources.

- Participate In Risk Assessments
- Source, Install And Configure Security Devices And Software
- Set Up And Maintain Document Access Control
- Monitor Audit Logs And Review User Privileges
- Manage Security-Related Incident Response And Reporting
- Create And Test Business Continuity And Disaster Recovery Plans
- Participate In Security Training And Education Programs

A security policy is a formalized statement that defines how security will be implemented within an organization and can contain multiple individual policies.

Overall internal responsibility might be allocated to a dedicated department run by a director of security, chief security officer or chief information security officer

Managers may have responsibility for a domain such as building control, ict or even accounting.

Security Operations Center (Soc) - This Is A Location Where Security Professionals Monitor And Protect Critical Information Assets Across Other Business Functions Such As Finance, Operations And Marketing. Typically Employed By Larger Corporations Such As Government Agencies Or A Healthcare Company.

Devsecops - Devops is a cultural shift within an organization to encourage much more collaboration between developers and system admins. Devsecops extends the boundary to security specialists reflecting the principle that security is a primary consideration at every stage of software development (known as shift left)

Incident Response - A Dedicated Cyber Incident Response Team (Cirt) / Computer Security Incident Response Team (Csirt) / Computer Emergency Response Team (Cert) As A Single Point-Of-Contact For The Notification Of Security Incidents.

1.4 Security Control Categories

A Security Control Is Something Designed To Give A System Or Digital Asset The Properties Of Cia & Non-Repudiation.

There Are Three Main Security Control Categories

- Technical - Implemented As A System Such As Firewalls, Anti-Malware And Os Access Control. They Can Also Be Referred To As Logical Controls.
- Operational - Implemented Primarily By People Rather Than Systems E.G Security Guards And Training Programs
- Managerial - These Controls Give Oversight Of The Information System E.G Risk Identification Tools Or Security Policies.

1.5 Security Control Functional Types

- Preventive - These Controls Act To Eliminate Or Reduce The Likelihood That An Attack Can Succeed E.G Acls, Anti-Malware. Directives And Standard Operating Procedures (Sops) Can Be Regarded As Administrative Versions Of Preventative Controls.
- Detective - These Controls May Not Deter Access But Will Identify And Record Any Attempted Or Successful Intrusion E.G Logs & Audits
- Corrective - These Controls Act To Eliminate Or Reduce The Impact Of An Intrusion Event E.G Backups And Patch Management.
- Physical - These Include Alarms, Security Cameras And Guards And Can Be Used To Deter Physical Access To Premises And Hardware
- Deterrent - These Controls Can Psychologically Discourage An Attacker From Attempting An Intrusion E.G Signs And Warnings Of Legal Penalties.
- Compensating - These Controls Serve As A Substitute For A Principal Control By A Security Standard And Affords The Same (Or Better) Level Of Protection But Uses A Different Methodology Or Technology.

1.6 ISO and Cloud Frameworks

Iso 27k - The International Organization For Standardization (Iso) Has Produced A Cybersecurity Framework In Conjunction With The International Electrotechnical Commission (Iec).

Unlike The Nist Framework, The Iso 27001 Must Be Purchased. The Iso 27001 Is Part Of An Overall 27000 Series Of Information Security Standards Also Known As 27k.

There Are 3 Main Versions Of The Iso 27k

- 27002 - Security Controls
- 27017 & 27018 - Cloud Security
- 27701 - Personal Data & Privacy

Iso 31k - This Is An Overall Framework For Enterprise Risk Management (Erm). Erm Considers Risks And Opportunities Beyond Cybersecurity By Including Financial, Customer Service And Legal Liability Factors.

Cloud Security Alliance (Csa) - The Not-For-Profit Organization Produces Various Resources To Assist Cloud Service Providers (Csp) In Setting Up And Delivering Secure Cloud Platforms.

- Security Guidance - A Best Practice Summary Analyzing The Unique Challenges Of Cloud Environments And How On-Premises Controls Can Be Adapted To Them.
- Enterprise Reference Architecture - Best Practice Methodology And Tools For Csps To Use In Architecting Cloud Solutions.
- Cloud Controls Matrix - Lists Specific Controls And Assessment Guidelines That Should Be Implemented By Csps.

Statements On Standards For Attestation Engagements (Ssae) - the SSAE are audit specifications developed by the american institute of certified public accountants (aicpa). These audits are designed to assure consumers that service providers (notably cloud providers) meet professional standards.

Within Ssae No. 18, There Are Several Levels Of Reporting:

Service Organization Control (Soc2) - Soc2 Evaluates The Internal Controls Implemented By The Service Provider To Ensure Compliance With Trust Services Criteria (Tsc) When Storing And Processing Customer Data.

An Soc Type 1 Report Assesses The System Design, While A Type 2 Report Assesses The Ongoing Effectiveness Of The Security Architecture Over A Period Of 6-12 Months.

Soc2 Reports Are Highly Detailed And Designed To Be Restricted.

Soc 3 - A Less Detailed Report Certifying Compliance With Soc2. They Can Be Freely Distributed.

1.7 Bench Marks & Secure Configuration Guides

Although frameworks provide a "high-level" view of how to plan its services, they generally don't provide detailed implementation guidance.

At a system level, the deployment of servers and applications is covered by benchmarks and secure configuration guides.

Center For Internet Security (Cis)

A non profit organization that publishes the well-known (the cis critical security controls).

They also produce benchmarks for different aspects of cybersecurity e.g benchmarks for compliance with it frameworks include pci dss and iso 27000.

There are also product-focused benchmarks such as windows desktop, windows server, macos and web & email servers.

Os/Network Appliance Platform/Vendor-Specific Guides

Operating System (Os) Best Practice Configuration Lists The Settings And Controls That Should Be Applied For A Computing Platform To Work In Defined Roles Such As Workstation, Server, Network Switch/Router Etc.

Most Vendors Will Provide Guides, Templates And Tools For Configuring And Validating The Deployment Of Network Appliances And Operating Systems And These Configurations Will Vary Not Only By Vendor But By Device And Version As Well.

- Department Of Defense Cyber Exchange Provides Security Technical Implementation Guides (Stigs) With Hardening Guidelines For A Variety Of Software And Hardware Solutions.

- National Checklist Program (Ncp) By Nist Provides Checklists And Benchmarks For A Variety Of Operating Systems And Applications.

Application Servers

Most Application Architectures Use A Client/Server Model Which Means Part Of The Application Is A Client Software Program Installed And Run On Separate Hardware To The Server Application Code.

Attacks Can Therefore Be Directed At The Client, Server Or The Network Channel Between Them.

Open Web Application Security Project (Owasp)

A Non Profit Online Community That Publishes Several Secure Application Development Resources Such As The Owasp Top 10 That Lists The Most Critical Application Security Risks.

1.8 Regulations, Standards & Legislation

Key Frameworks, Benchmarks And Configuration Guides May Be Used To Demonstrate Compliance With A Country's Legal Requirements.

Due Diligence Is A Legal Term Meaning That Responsible Persons Have Not Been Negligent In Discharging Their Duties.

- Sarbanes-Oxley Act (Sox) Mandates The Implementation Of Risk Assessments, Internal Controls And Audit Procedures.
- The Computer Security Act (1987) Requires Federal Agencies To Develop Security Policies For Computer Systems That Process Confidential Information.
- In 2002, The Federal Information Security Management Act (Fisma) Was Introduced To Govern The Security Of Data Processed By Federal Government Agencies.

Some Regulations Have Specific Cybersecurity Control Requirements While Others Simply Mandate "Best Practice" As Represented By A Particular Industry Or International Framework.

Personal Data And General Data Protection Regulation (GDPR)

This legislation focuses on information security as it affects privacy or personal data.

GDPR means that personal data cannot be collected, processed or retained without the individual's informed consent.

Compliance issues are complicated by the fact that laws derive from different sources e.g gdpr does not apply to american data subjects but it does apply to american companies that collect or process the personal data of people in eu countries.

National, Territory Or State Laws

In the US there are federal laws such as the gramm-leach-bliley act (GLBA) for financial services and the health insurance portability and accountability act (HIPAA).

Section 2- Explaining Threat Actors And Threat Vectors

2.1 Vulnerability, Threat And Risk

Vulnerability - This Is A Weakness That Could Be Triggered Accidentally Or Exploited Intentionally To Cause A Security Breach. Threats Can Exist Even When There Are No Vulnerabilities.

Threats Can Exist Without Risks But A Risk Needs An Associated Threat To Exist

The Path Or Tool Used By A Malicious Threat Actor Can Be Referred To As The Attack Vector.

Risks Are Often Measured Based On The Probability That An Event Might Occur As Well As The Impact Of The Event On The Business.

Threat Assessment Is The Combination Of A Threat Actor’s Intentions To Harm Combined With An Assessment Of That Actor’s Capability To Carry Out Those Intentions.

Risk Assessment Involves Identification Of Security Risks Through The Analysis Of Assets, Threats And Vulnerabilities, Including Their Impacts And Likelihood.

Risks Are Event Focused (The Database Server Goes Down) While Threats Focus On Intentions (A Hacker Wants To Take Down The Database Server)

2.2 Attributes Of Threat Actors

Location - an external threat or actor is one that has no account or authorized access to the target system. such threats must use malware and or social engineering to infiltrate the security system. Conversely, an internal or insider threat actor is one that has been granted permissions on the system and typically means either an employee or a third party contractor.

Intent/motivation - intent describes what an attacker hopes to achieve from the attack while motivation is the reason for perpetuating the attack.motivation could be driven by greed, curiosity or grievance.

Threats can either be structured or unstructured. A criminal gang attempting to steal financial data is a structured targeted threat while a script kiddie launching a series of spam emails is unstructured and opportunistic.

Level of sophistication/capability - the technical abilities and resources/funding the adversary possesses must also be considered. capability refers to a threat actor's ability to craft novel exploit techniques and tools.

2.3 Threat Actors

- script kiddie - use hacker tools without necessarily understanding how they work or have the ability to craft new attacks.
- black hats - very skilled and have financial interests
- white hat - hack systems and networks with full authorization typically to discover vulnerabilities and test current security setup.
- gray hats - are very skilled and typically employ black hat tactics for white hat objectives
- hacktivists ** - hacking for a cause. they might attempt to obtain and release confidential information to the public or deface a website. (anonymous, wikileaks)

- state actors & advanced persistent threats - the term atp was coined to understand the behavior underpinning modern types of cyber adversaries. it refers to the ongoing ability of an adversary to compromise network security and maintain access by using a variety of tools and techniques.
- criminal syndicates - criminal syndicates can operate across the internet from different jurisdictions than its victim, increasing the complexity of prosecution.
- insider threats - these include, compromised employees, disgruntled employee (ex,) second streamer, spy/saboteur, shadow it, unintentional

2.4 Attack Surface & Attack Vectors

Attack Surface - this refers to all the points at which a malicious threat actor could try to exploit a vulnerability. The attack surface for an external actor is and should be far smaller than that for an insider threat. Minimizing the attack surface means restricting access so that only a few known endpoints, protocols/ports and services are permitted.

The attack vector is the path that a threat actor uses to gain access to a secure system and can include

- Direct Access
- Removable Media
- Email
- Remote & Wireless
- Supply Chain
- Web & Social Media
- Cloud

2.5 Threat Research Sources

Threat Research Is A Counterintelligence Gathering Effort In Which Security Companies And Researchers Attempt To Discover The Tactics, Techniques And Procedures (Ttps) Of Modern Cyber Adversaries.

Another Primary Source Of Threat Intelligence Is The Deep Web.

The Deep Web Is Any Part Of The World Wide Web That Is Not Indexed By A Search Engine E.G Registration Pages, Unlinked Pages And Pages That Block Search Indexing.

2.6 Threat Intelligence Providers

The outputs from the primary research undertaken by security solutions providers can take three main forms.

behavioral threat research - narrative commentary describing examples of attacks and TTPs gathered through primary research sources.

reputational threat intelligence - list of ip addresses and domains associated with malicious behavior

threat data - computer data that can correlate events observed on a customer's own networks and logs with known TTP and threat actor indicators.

Threat data can be packaged as feeds that integrate with a security information and event management (SIEM) platform.

These feeds are usually described as cyber threat intelligence (cti) data.

Threat intelligence platforms and feeds are supplied as one of four different commercial models

- closed/proprietary - the threat research and cti data is made available as a paid subscription to a commercial threat intelligence platform.
- vendor websites - this is proprietary threat intelligence that is not provided at a cost but is provided as a general benefit to customers e.g microsoft's security intelligence blog.
- public/private information sharing centers - in many critical industries, information sharing and analysis centers (isacs) have been set up to share threat intelligence and promote best practice.
- open source intelligence (OSINT) - some companies operate threat intelligence services on an open-source basis earning income from consultancy
- other threat intelligence research resources include - academic journals, conferences, request for comments (RFC) and social media

2.7 Tactics, Techniques & Procedures

A Tactic, Technique Or Procedure (Ttp) Is A Generalized Statement Of Adversary Behavior. Ttps Categorize Behaviors In Terms Of Campaign Strategy And Approach (Tactics), Generalized Attack Vectors (Techniques) And Specific Intrusion Tools And Methods (Procedures).

An Indicator Of Compromise (Ioc) Is A Residual Sign That An Asset Or Network Has Been Successfully Attacked. In Other Words, An Ioc Is Evidence Of A Ttp.

Examples Of Iocs Include

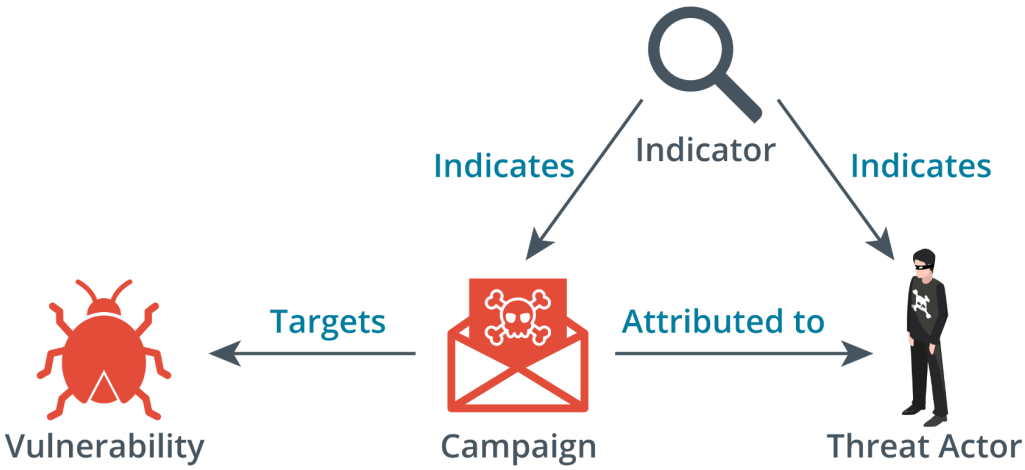
- Unauthorized Software And Files
- Suspicious Emails
- Suspicious Registry And File System Changes
- Unknown Port And Protocol Usage
- Excessive Bandwidth Usage
- Rouge Hardware
- Service Disruption And Defacement
- Suspicious Or Unauthorized Account Usage

Strictly Speaking An Ioc Is Evidence Of An Attack That Was Successful. The Term Indicator Of Attack (Ioa) Is Sometimes Also Used For Evidence Of An Intrusion Attempt In Progress.

2.8 Threat Data Feeds

There Are Various Ways That A Threat Data Feed Can Be Implemented.

Structured Threat Information Expression (Stix) - Describes Standard Terminology For Iocs And Ways Of Indicating Relationships Between Them.



Trusted automated exchange of indicator information (taxii) - protocol provides a means for transmitting cti data between servers and clients.

Automated indicator sharing (ais) - is a service offered by the dhs for companies to participate in threat intelligence sharing. ais is based on the stix and taxii standards and protocols.

Threat map - a threat map is an animated graphic showing the source, target and type of attacks detected by a cti platform.

File/code repositories - such a repository holds signatures of known malware code.

Vulnerability databases & feeds - another source of threat intelligence is identifying vulnerabilities in os, software applications and firmware code. vulnerability databases include the common vulnerabilities and exposure (CVE).

Artificial Intelligence - ai is the science of creating machine systems that can simulate or demonstrate a similar general intelligence capability to humans.

Predictive analysis - this refers to when a system can anticipate an attack and possibly identify the threat actor before the attack is fully realized.

Section 3- Performing Security Assessments

3.1 Network Reconnaissance Tools

Topology Discovery (Footprinting) Means Scanning For Hosts, Ip Ranges And Routes Between Networks To Map Out The Structure Of The Target Network.

- Ipconfig - Shows The Ip And Mac Addresses Assigned To Network Interfaces In Windows.
- Ifconfig - For Linux
- Ping - Probes A Host On A Particular Ip Address Or Host Name Using Icmp.
- Arp - Display's The Local Machine's Address Resolution Protocol (Arp) Cache Which Will Show The Mac Address Of The Interface Associated With Each Ip Address The Local Host Has Communicated With Recently.
- Route - View And Configure The Host's Local Routing Table
- Tracert (Windows) - Uses Icmp Probes To Report The Round Trip Time (Rtt) For Hops Between The Local Host And A Host On A Remote Network.
- Traceroute (Linux)- Uses Udp Probes Instead.
- Pathping (Windows) - Provides Stats For Latency And Packet Loss Along A Route Over A Longer Measuring Period.
- Mtr (Linux)

An Ip Scanner Performs Host Discovery And Identifies How The Hosts Are Connected Together In An Internetwork.

The Nmap Security Scanner Is One Of The Most Popular Open-Source Ip Scanners Which Can Use Diverse Methods For Host Discovery And Is Available For Windows, Linux And Macos.

Service Discovery & Nmap

- Tcp Syn (-Ss) - Fast Technique (Half Open) Where The Scanning Host Requests A Connection Without Acknowledging It. The Target's Response To The Scan's Syn Packet Identifies The Port State.
- Udp Scans (-Su) - Scan Udp Ports And Needs To Wait For A Response To Determine The Port State.
- Port Range (-P) - By Default, Nmap Scans 1000 Commonly Used Ports And -P Argument Can Be Used To Specify A Port Range.

Nmap Can Also Be Used For Fingerprinting Which Is The Process Of Discovering Detailed Analysis Of Services On A Particular Host.

Nmap Can Be Used To Discover:

- Protocols
- Application Name & Version
- Os Type And Version
- Device Type

Netstat And Nslookup

Netstat - Shows The State Of Tcp/Udp Ports On The Local Machine. Can Be Used On Both Windows And Linux.

You May Also Be Able To Identify Suspect Remote Connections To Services On The Local Host Or From The Host To Remote Ip Addresses.

Nslookup/Dig - Query Name Records For A Given Domain Using A Particular Dns Resolver Under Windows (Nslookup) Or Linux (Dig).

3.2 Other Reconnaissance & Discovery Tools

- Theharvester - A Tool For Gathering Open-Source Intelligence (Osint) For A Particular Domain Or Company.
- Dnsenum - Packages Queries For Name Requests And Hosting Details Into A Single Query
- Scanless - Provides The Option To Avoid Port Scanning Detection By Disguising The Source Of Probes.
- Curl - Command Line Client For Performing Data Transfers Over Many Types Of Protocols
- Nessus - A Very Powerful Vulnerability Scanner

Packet Capture And Tcpdump

Packet Analysis - Refers To Deep-Down Frame-By-Frame Scrutiny Of Captured Frames

Protocol Analysis - Means Using Statistical Tools To Analyze A Sequence Of Packets Or Packet Trace.

Packet And Protocol Analysis Depends On A Sniffer Tool To Capture And Decode The Frames Of Data. Network Traffic Can Be Captured From A Host Or From A Network Segment.

Tcpdump Is A Command Line Packet Capture Utility For Linux.

The Basic Syntax Of The Command Is Tcpdump -I Eth0 Where Eth0 Is The Interface To Listen On.

The Utility Will Then Display Captured Packets Until Halted Manually.

The Following Command Filters Frames To Those With The Source Ip 10.1.0.100 And Destination Port 53 Or 80:

Tcpdump -I Eth0 “Src Host 10.1.0.100 And (Dst Port 53 Or Dst Port 80)”

Packet Injection And Replay

Some Reconnaissance Techniques And Tests Depend On Sending Forged Or Spoofed Network Traffic. There Are Also Tools That Allow For Different Kinds Of Packets To Be Crafted And Manipulated.

Hping Is An Open-Source Spoofing Tool That Provides A Penetration Tester With The Ability To Craft Network Packets To Exploit Vulnerable Firewalls And Idss.

Exploitation Frameworks

A Remote Access Trojan (Rat) Is A Malware That Gives An Adversary The Means Of Remotely Accessing The Network.

An Exploitation Framework Uses The Vulnerabilities Identified By An Automated Scanner And Launches Scripts Of Software To Attempt To Deliver Matching Exploits. This Might Include Disruption To The Target, Including Service Failure And Risk Data Security.

The Framework Comprises A Database Of Exploit Code, Each Targeting A Particular Cve.

The Best Known Exploit Framework Is Metasploit. It’s Open Source But Also Has Pro And Express Commercial Editions Of The Framework.

Sn1per Is A Framework Designed For Penetration Test Reporting And Evidence Gathering. It Can Integrate With Tools Like Metasploit To Run Automated Suites Of Tests.

Other Exploitation Frameworks Include

- Fireelf
- Routersploit
- Browser Exploitation Framework (Beef)
- Zed Attack Proxy (Zap)
- Pacu

Netcat

This Is A Tool Used For Testing Connectivity Available On Both Windows And Linux And Can Also Be Used For Port Scanning And Fingerprinting.

The Following Command Attempts To Connect To The Http Port On A Server And Return Any Banner By Sending The “Head” Http Keyword.

Echo “Head” | Nc 10.1.0.1 -V 80

3.3 weak host & network configurations

Using the default manufacturer settings is an example of weak configuration. The root account or the default admin account typically has no restrictions set over system access and can have an extremely serious impact if an attacker gains control of it.

Open Permissions - this refers to provisioning data files or applications without differentiating access rights for user groups. This can lead to permitting unauthenticated guests to view confidential data or allowing write access to read only files. servers must operate with at least some open ports but security best practice dictates that these should be restricted to only necessary services.

Weak encryption - this can arise from the following:

- the key is generated from a simple password making it easy to brute-force
- the algorithm or cipher used for the encryption has known weaknesses
- the key is not distributed securely and can easily fall into the attacker's hands.

Errors - weakly configured applications may display unformatted error messages under certain conditions and can provide threat actors with valuable information.

3.4 Vulnerability Impacts

These Types Of Events Can Have Serious Impacts In Terms Of Cost And Damage To The Organization's Reputation.

- Data Breaches And Data Exfiltration Impacts
- Identity Theft Impacts
- Data Loss And Availability Loss Impacts
- Financial And Reputation Impacts

Data Breaches And Data Exfiltration Impacts

A Data Breach Event Is Where Confidential Data Is Read, Modified, Transferred To Deleted Without Authorization. A Privacy Breach Is Where Personal Data Is Not Collected, Stored Or Processed In Full Compliance With Laws Governing Personal Information.

Data Exfiltration Is The Methods And Tools By Which An Attacker Transfers Data Without Authorization From The Victim's System To An External Network Or Media.

Data Loss & Availability Loss Impacts

Compared To Data Breaches, Data Loss Is Where Information Is Unavailable And Can Result In The Company Unable To Perform Crucial Workflows.

3.5 Third Party Risks

Vendor Management Is The Process Of Choosing Supplier Companies And Evaluating The Risks Inherent In Relying On A Third Party Product Or Service.

Within Vendor Management, System Integration Refers To The Process Of Using Components From Multiple Vendors To Implement A Business Workflow.

There Are Two Main Data Risks When Using Third Parties

- Vendor May Need To Be Granted Access To Your Data
- The Vendor May Have To Be Used To Host The Data Or The Data Backups

Data Storage

The Following Precautions Should Be Taken:

- Ensure The Same Protections For Data As Though It Were Stored On-Premises.
- Monitor And Audit Third-Party Access To The Data
- Evaluate Compliance Impacts From Storing Personal Data On A Third-Party System

3.6 PenTest Attack Life Cycle

- *reconnaissance* - is typically followed by an initial exploitation phase where a software tool is used to gain some sort of access to the target's network.
- *persistence* - this is the tester's ability to reconnect to the compromised host and use it as a remote access tool (rat) or backdoor.
- *privilege escalation* - the tester attempts to map out the internal network and discover the services running on it.
- *lateral movement* - gaining control over other hosts and usually involves executing the attack or scripting tools such as powershell.
- *pivoting* - if a pen tester achieves a foothold on a perimeter server, a pivot allows them to bypass a network boundary and compromise servers on an inside network.
- *actions on objectives* - for a threat actor, this means stealing data while for a tester it would be a matter of the scope definition.
- *cleanup* - for an attacker, this means removing evidence of the attack while for a pen tester, this means removing any backdoors or tools and ensuring the system is not less secure than its pre-engagement state.

Section 4 - Social Engineering Techniques & Malware

4.1 - Intro To Social Engineering

This is the exploitation of human emotions and interactions to extract valuable information. more dangerous than traditional methods of hacking as it relies on human error which is subjective & less predictable than software/hardware vulnerabilities.

Social engineering relies heavily on human emotions such as fear, curiosity, excitement, anger and guilt.

phishing - relies on creating a sense of excitement or panic in the target using emails.

spear phishing - a phishing attack against a very specific individual or organization

angler phishing - a phishing attack directed specifically at social media users

whaling - a phishing attack targeted at senior executives of an organization

vishing - relies on creating a sense of excitement or panic in the target using a phone call

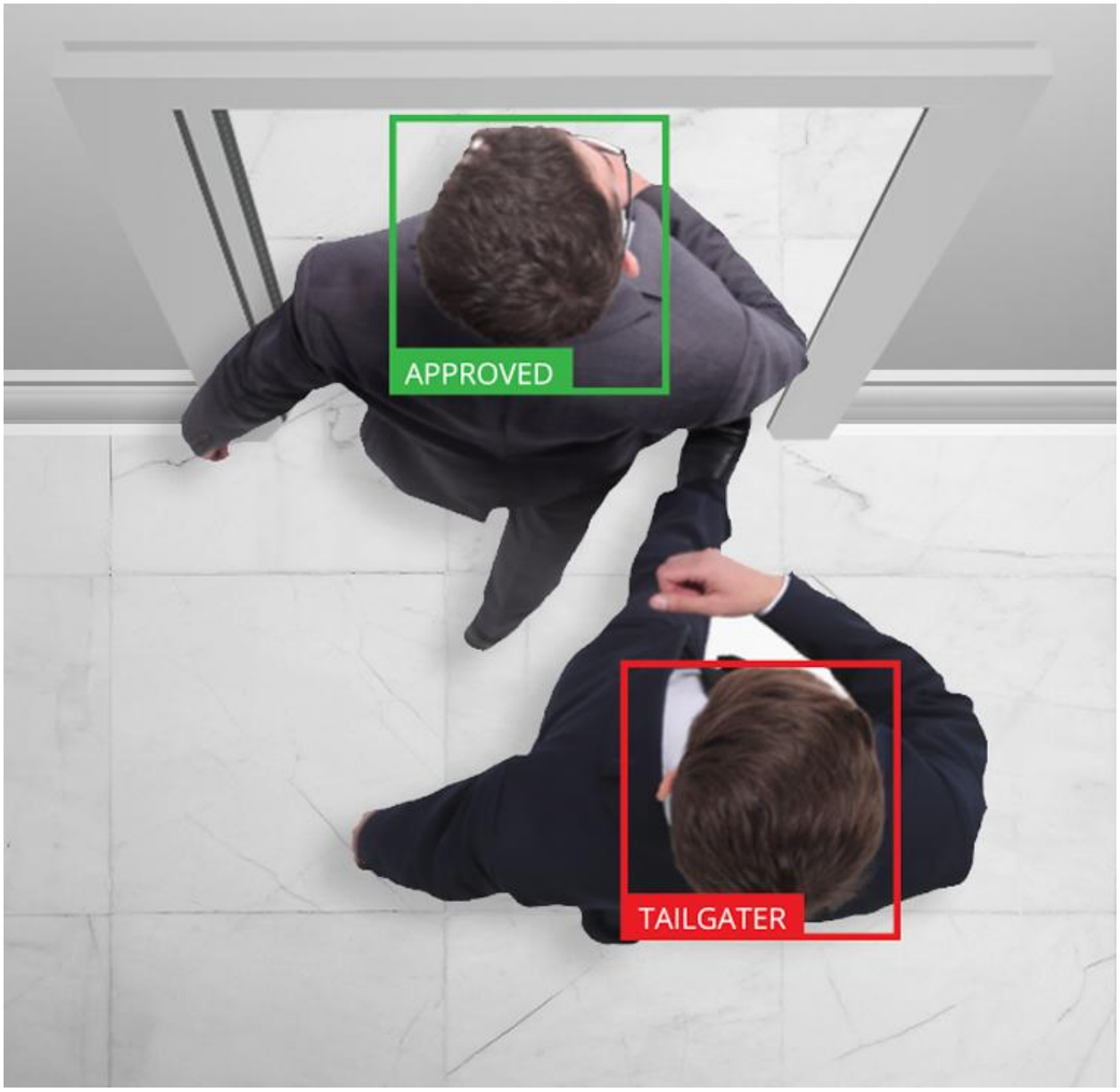
smishing - relies on creating a sense of excitement or panic in the target using a text message

hoaxes - the hacker impersonates an employee or angry customer

baiting - dropping infected usb drives in the parking lot to influence employees.

piggybacking - an attacker enters a secure building with the permission of an employee

tailgating - the attacker without access authorization closely follows an authorized person in a reserved area



shoulder surfing - obtaining sensitive information by spying

dumpster diving - obtaining sensitive information by going through the company trash

credential harvesting - using phishing emails and spamming campaigns to gather information which can then be sold.

pharming - redirecting victims to a malicious website using dns cache poisoning.

watering hole attack - an attack that aims to compromise a specific group of end-users by infecting existing websites or creating a new one that will attract them.

typo squatting/ url hijacking - hackers register misspelled domain names of popular websites hoping to capture sensitive information. e.g facbook.com. instagarm.com

influence campaigns - a major program launched by an adversary with a high level of capability such as a nation-state actor or terrorist group. the goal is to shift public opinion on some topic and when deployed along with espionage, disinformation/fake news and hacking, it can be characterized as hybrid warfare.

4.2 - Malware Classification

Some Malware Classifications Such As Trojan, Virus And Worm Focus On The Vector Used By The Malware. The Vector Is The Method By Which The Malware Executes On A Computer And Potentially Spreads To Other Network Hosts.

The Following Categories Describe Some Types Of Malware According To Vector:

- Viruses & Worms - Spread Without Any Authorization From The User By Being Concealed Within The Executable Code Of Another Process.
- Trojan - Malware Concealed Within An Installer Package For Software That Appears To Be Legitimate
- Potentially Unwanted Programs/Applications (Pups/Puas) - These Are Software Installed Alongside A Package Selected By The User. Unlike A Trojan, Their Presence Isn't Necessarily Malicious. They Are Sometimes Referred To As Grayware.

Other Classifications Are Based On The Payload Delivered By The Malware. The Payload Is The Action Performed By The Malware

Examples Of Payload Classification Include:

- Spyware
- Rootkit
- Remote Access Trojan (Rat)
- Ransomware

4.3 - Computer Viruses

This Is A Type Of Malware Designed To Replicate And Spread From Computer To Computer Usually By “Infecting” Executable Applications Or Program Code.

- Non-Resident/File Infector - The Virus Is Contained Within A Host Executable File And Runs With The Host Process. The Virus Will Try To Infect Other Process Images On Persistent Storage And Perform Other Payload Actions.
- Memory Resident - When The Host File Is Executed, The Virus Creates A New Process For Itself In Memory. The Malicious Process Remains In The Memory Even If The Host Process Is Terminated.
- Boot - The Virus Code Is Written To The Disk Boot Sector And Executes As A Memory Resident Process When The Os Starts.
- Script And Macro Viruses - The Malware Uses The Programming Features Available In Local Scripting Engines For The Os And/Or Browser Such As Powershell, Javascript, Microsoft Office Documents Or Pdf Documents With Javascript Enabled.

The Term *Multipartite* Is Used For Viruses That Use Multiple Vectors And *Polymorphic* For Viruses That Can Dynamically Change Or Obfuscate Their Code To Evade Detection. Viruses Must Infect A Host File Or Media. An Infected File Can Be Distributed Through Any Normal Means - On A Disk, On A Network, A Download From A Website Or Email Attachment.

4.4 - Computer Worms & Fileless Malware

Computer Worms - this is a memory resident malware that can run without user intervention and replicate over network resources. viruses need the user to perform an action but worms can execute by exploiting a vulnerability in a process and replicate themselves.

Worms can rapidly consume network bandwidth as the worm replicates and they may be able to crash an operating system or server application. worms can also carry a payload that may perform some other malicious action.

Fileless malware - as security controls got more advanced so did malware and this new sophisticated modern type of malware is often referred to as fileless.

- Fileless Malware Do Not Write Their Code To Disk. The Malware Uses Memory Resident Techniques To Run Its Own Process Within A Host Process Or

Dynamic Link Library (Dll). The Malware May Change Registry Values To Achieve Persistence.

- Fileless Malware Uses Lightweight Shellcode To Achieve A Backdoor Mechanism On The Host. The Shellcode Is Easy To Recompile In An Obfuscated Form To Evade Detection By Scanners. It Is Then Able To Download Additional Packages Or Payloads To Achieve The Actor's Objectives.
- Fileless Malware May Use "Live Off The Land" Techniques Rather Than Compiled Executables To Evade Detection. This Means That The Malware Code Uses Legitimate System Scripting Tools Like Powershell To Execute Payload Actions.

4.5 - Spyware, Keyloggers, Rootkits, Backdoors, Ransomware & Logic Bombs

spyware - this is malware that can perform adware-like tracking but also monitor local application activity, take screenshots and activate recording devices.

adware - grayware that performs browser reconfigurations such as allowing cookies, changing default search engines, adding bookmarks and so on.

tracking cookies - can be used to record pages visited, the user's ip address and various other metadata.

keylogger - spyware that actively attempts to steal confidential information by recording keystrokes.

backdoors & rats - a backdoor provides remote user admin control over a host and bypasses any authentication method. A remote access trojan is a backdoor malware that mimics the functionality of legitimate remote control programs but is designed specifically to operate covertly. a group of bots under the same control of the same malware are referred to as a botnet and can be manipulated by the herder program.

rootkits - this malware is designed to provide continued privileged access to a computer while actively hiding its presence. it may be able to use an exploit to escalate privileges after installation.software processes can run in one of several "rings".

- ring 0 is the most privileged and provides direct access to hardware

- ring 3 is where user-mode processes run
- ring 1 or 2 is where drivers and i/o processes may run.

ransomware - this type of malware tries to extort money from the victim by encrypting the victim's files and demanding payment. ransomware uses payment methods such as wire transfer or cryptocurrency.

logic bombs - logic bombs are not always malware code. a typical example is a disgruntled admin who leaves a scripted trap that runs in the event his or her account is disabled or deleted. anti-malware software is unlikely to detect this kind of script and this type of trap is also referred to as a mine.

4.6 - Malware Indicators & Process Analysis

There Are Multiple Indicators Of Malware:

- Antivirus Notifications
- Sandbox Execution
- Resource Consumption - Can Be Detected Using Task Manager Or Top Linux Utility.
- File System

because shellcode is easy to obfuscate, it can easily evade signature-based a-v products. Threat hunting and security monitoring must use behavioral-based techniques to identify infections.

Along with observing how a process interacts with the file system, network activity is one of the most reliable ways to identify malware.

Section 5 - Cryptographic Concepts, Hashing, Ciphers & Encryption

5.1 - Introduction To Cryptography And Hashing

Cryptography Is A Secure Communication Technique That Allows Only The Sender And Receiver Of A Message To View It.

Plaintext - An Unencrypted Message

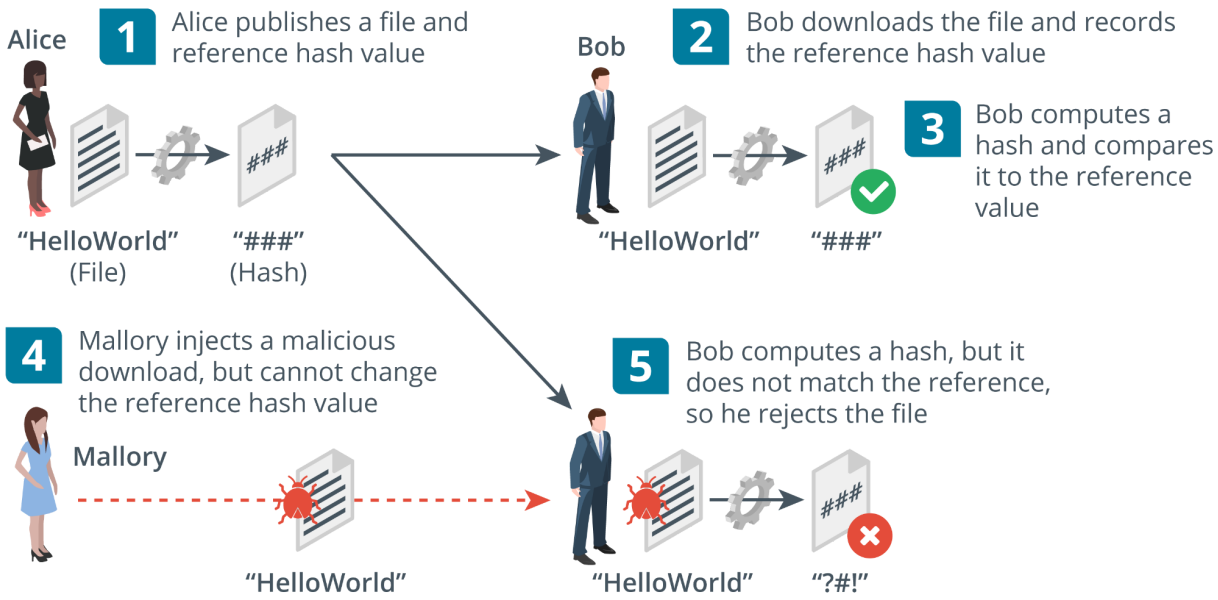
Ciphertext - An Encrypted Message

Cipher - The Process (Algorithm) Used To Encrypt And Decrypt A Message
Cryptanalysis - The Art Of Cracking Cryptographic Systems

There Are Three Main Types Of Cryptographic Algorithms:

- Hashing Algorithms
- Symmetric Encryption Cipher
- Asymmetric Encryption Cipher

Hashing Algorithms - The Simplest Type Of Cryptographic Operation And Produces A Fixed Length String From An Input Plaintext That Can Be Of Any Length. A *Hashing Collision* Occurs When Two Different Plain Texts Produce The Exact Same Hash Value. Encryption Algorithms Must Demonstrate Collision Avoidance.



Hashing Algorithms

- Secure Hash Algorithm (Sha) - Considered To Be The Strongest Algorithm With The Most Popular Being The Sha-256 Which Produces A 256-Bit Digest.
- Message Direct Algorithm #5 (Md5) - Produces A 128-Bit Digest

Birthday Attack - A Brute Force Attack Aimed At Exploiting Collisions In Hash Functions. Could Be Used For Forging A Digital Signature

5.2 - Encryption

An encryption algorithm is a type of cryptographic process that encodes data so that it can be recovered or decrypted.

the use of a key, with the encryption cipher ensures that decryption can only be performed by authorized persons.

A substitution cipher involves replacing units in the plaintext with different ciphertext. e.g rot13 rotates each letter 13 places so a becomes n

the ciphertext "uryyb jbeyq" means "hello world"

In contrast to substitution ciphers, the units in a transposition cipher stay the same in plaintext and ciphertext but their order is changed according to some mechanism.

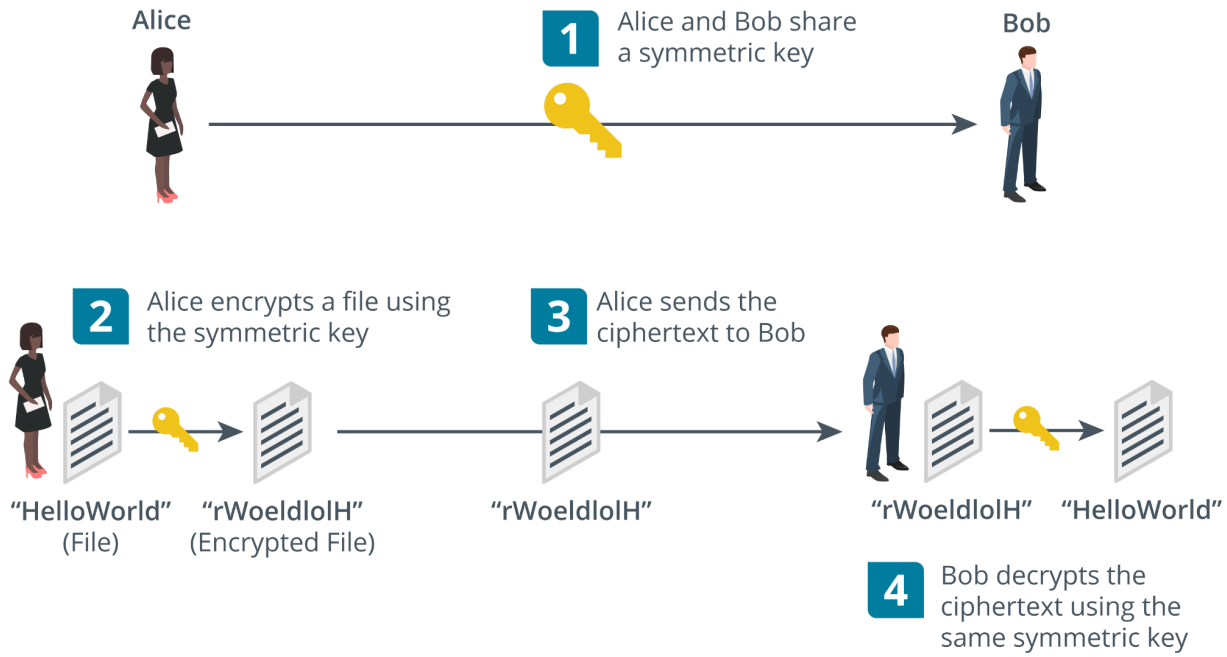
consider the ciphertext "hloolelwrd"

h l o o l

e l w r d

The letters are simply written as columns and the rows are concatenated.

symmetric encryption - here both encryption and decryption are performed by the same secret key and can be used for confidentiality. It is very fast and is used for bulk encryption of large amounts of data but can be vulnerable if the key is stolen.

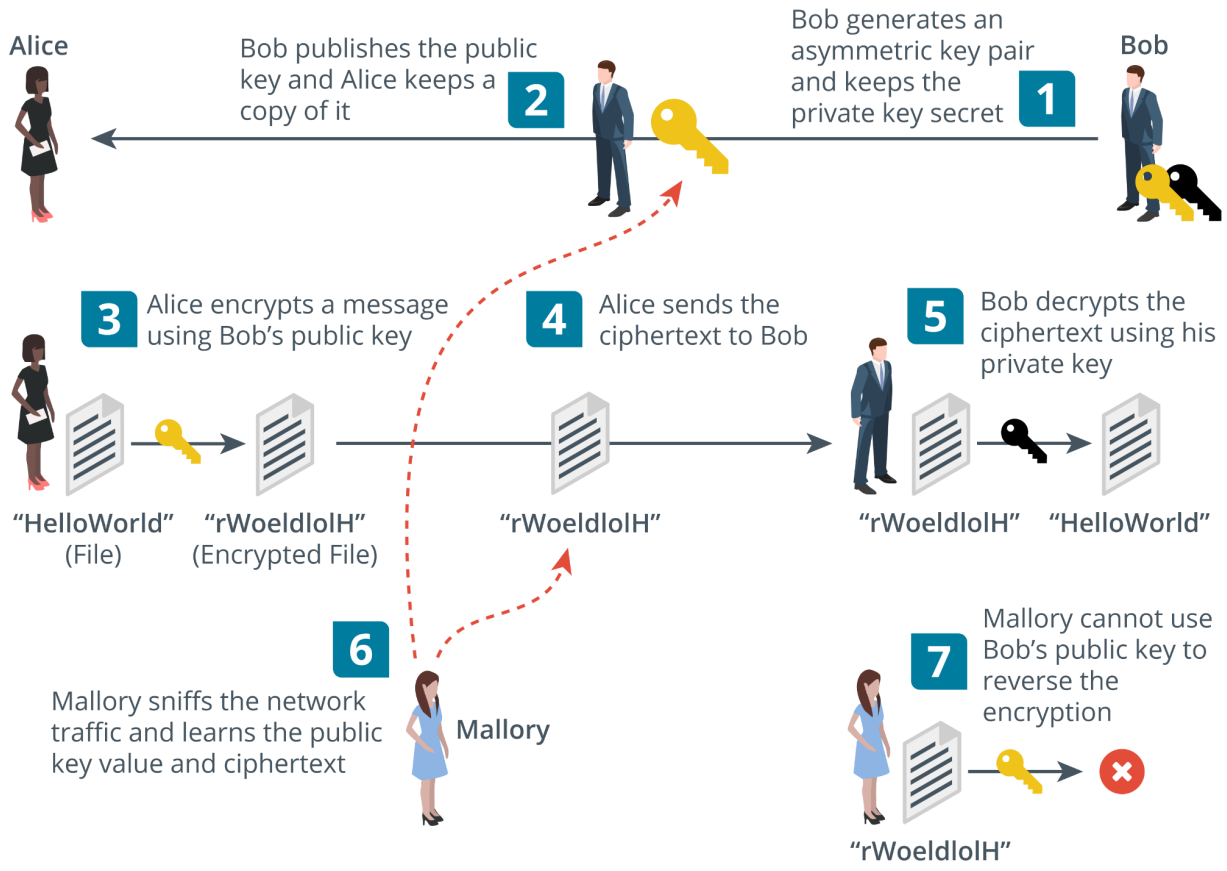


there are two types - stream ciphers & block ciphers

stream cipher - the plaintext is combined with a separate randomly generated message calculated from the key and an initialization vector (iv). each byte or bit of data is encrypted one at a time.

block cipher - the plaintext is divided into equal-size blocks (usually 128-bit). if there is not enough data in the plaintext, it is padded to the correct size. e.g, a 1200-bit plaintext would be padded with an extra 80 bits to fit into 10 x 128-bit blocks.

asymmetric encryption - here both encryption and decryption are performed by two different but related public and private keys in a key pair. Each key is capable of reversing the operation of its pair and they are linked in such a way as to make it impossible to derive one from the other.



Can Be Used To Prove Identity As The Holder Of The Private Key Cannot Be Impersonated By Anyone Else.

The Major Drawback Of This Encryption Is That It Involves Substantial Computing Resources.

Mostly Used For Authentication And Non-Repudiation And For Key Agreement And Exchange.

Asymmetric Encryption Is Often Referred To As Public Key Cryptography And The Products Are Based On The Rsa Algorithm.

Ron Rivest, Adi Shamir And Leonard Adleman Published The Rsa Cipher In 1977.

5.3 - Cryptographic Modes Of Operation & Cipher Suites

A Mode Of Operation Is A Means Of Using A Cipher Within A Product To Achieve A Security Goal Such As Confidentiality Or Integrity.

Public Key Cryptography Can Authenticate A Sender While Hashing Can Prove Integrity.

Both Can Be Combined To Authenticate A Sender And Prove The Integrity Of A Message And This Usage Is Called A Digital Signature.

Symmetric Encryption Can Encrypt And Decrypt Large Amounts Of Data But It's Difficult To Distribute The Secret Key Securely.

Asymmetric (Pkc) Encryption Can Distribute The Key Easily But Cannot Be Used For Large Amounts Of Data.

Digital Certificates - Public Keys Are Used And Are Freely Available But How Can Anyone Trust The Identity Of The Person Or Server Issuing A Public Key?

A Third Party Known As A Certificate Authority (Ca) Can Validate The Owner Of The Public Key By Issuing The Subject With A Certificate.

The Process Of Issuing And Verifying Certificates Is Called Public Key Infrastructure (Pki)

Cipher Suite - This Is The Combination Of Ciphers Supported And Is Made Up Of

- Signature Algorithm - Used To Assert The Identity Of The Server's Public Key And Facilitate Authentication
- Key Exchange/Agreement Algorithm - Used By The Client And Server To Derive The Same Bulk Encryption Symmetric Key.

5.4 - Cryptographic Use Cases

cryptography supporting authentication & non-repudiation - a single hash function, symmetric or asymmetric cipher is called a cryptographic primitive. a complete cryptographic system or product is likely to use multiple cryptographic primitives such as within a cipher suite.

authentication & non-repudiation depend on the recipient not being able to encrypt the message or the recipient would be able to impersonate the sender. Basically the recipient must be able to use the cryptographic process to decrypt authentication and integrity data but not to encrypt it.

cryptography supporting confidentiality - cryptography removes the need to store data in secure media as even if the ciphertext is stolen, the threat actor will not be able to understand or change what has been stolen.

cryptography supporting integrity & resiliency - integrity is proved by hashing algorithms which allow two parties to derive the same checksum and show that a message or data has not been tampered with. Cryptography can be used to design highly resilient control systems and secure computer code.

A developer can make tampering more difficult through obfuscation which is the art of making a message difficult to understand. Cryptography is a very effective way of obfuscating code but it also means the computer might not be able to understand and execute the code.

5.5 - Longevity, Salting , Stretching & Other Types Of Cryptographic Technologies

Longevity - This Refers To The Measure Of Confidence That People Have In A Given Cipher. In Another Sense, It Is The Consideration Of How Long Data Must Be Kept Secure.

Salting - Passwords Stored As Hashes Are Vulnerable To Brute Force And Dictionary Attacks. A Password Hash Cannot Be Decrypted As They Are One-Way. However, An Attacker Can Generate Hashes To Try And Find A Match For The Captured Password Hash Through A Brute Force Or Dictionary Attack.

A Brute Force Attack Will Run Through A Combination Of Letters, Numbers And Symbols While A Dictionary Attack Creates Hashes Of Common Words And Phrases.

Both Attacks Can Be Slowed Down By Adding A Salt Value When Creating The Hash.

(Salt + Password) * Sha = Hash

The Salt Is Not Kept Secret Because Any System Verifying The Hash Must Know The Value Of The Salt But It's Presence Means That An Attacker Cannot Use Pre-Computed Tables Of Hashes.

Key Stretching - This Takes A Key That's Generated From A User Password Plus A Random Salt Value And Repeatedly Converts It To A Longer And More Random Key. This Means The Attacker Will Have To Do Extra Processing For Each Possible Key Value Thus Make The Attack Even Slower.

This Can Be Performed By Using A Particular Software Library To Hash And Save Passwords When They Are Created. The Password-Based Key Derivation Function 2 (Pbkdf2) Is Widely Used For This Purpose.

Homomorphic Encryption - This Is The Conversion Of Data Into Ciphertext That Can Be Analyzed And Worked With As If It Were Still In Its Original Form.

It Enables Complex Mathematical Operations To Be Performed On Encrypted Data Without Compromising The Encryption.

Blockchain - this is a concept in which an expanding list of transactional records is secured using cryptography. Each record is referred to as a block and is run through a hash function. The hash value of the previous block in the chain is added to the hash calculation of the next block and thus ensures that each successive block is cryptographically linked.

Steganography - This is a technique for obscuring the presence of a message such as hiding a message in a picture. the container document or file is called the covertext.

Section 6 - Implementing Public Key Infrastructure

6.1 - Certificates, Pkis, Ras & Csrs

Public & Private Key Usage

When you want others to send you confidential messages, you give them your public key to encrypt the message and then you decrypt the message with your private key.

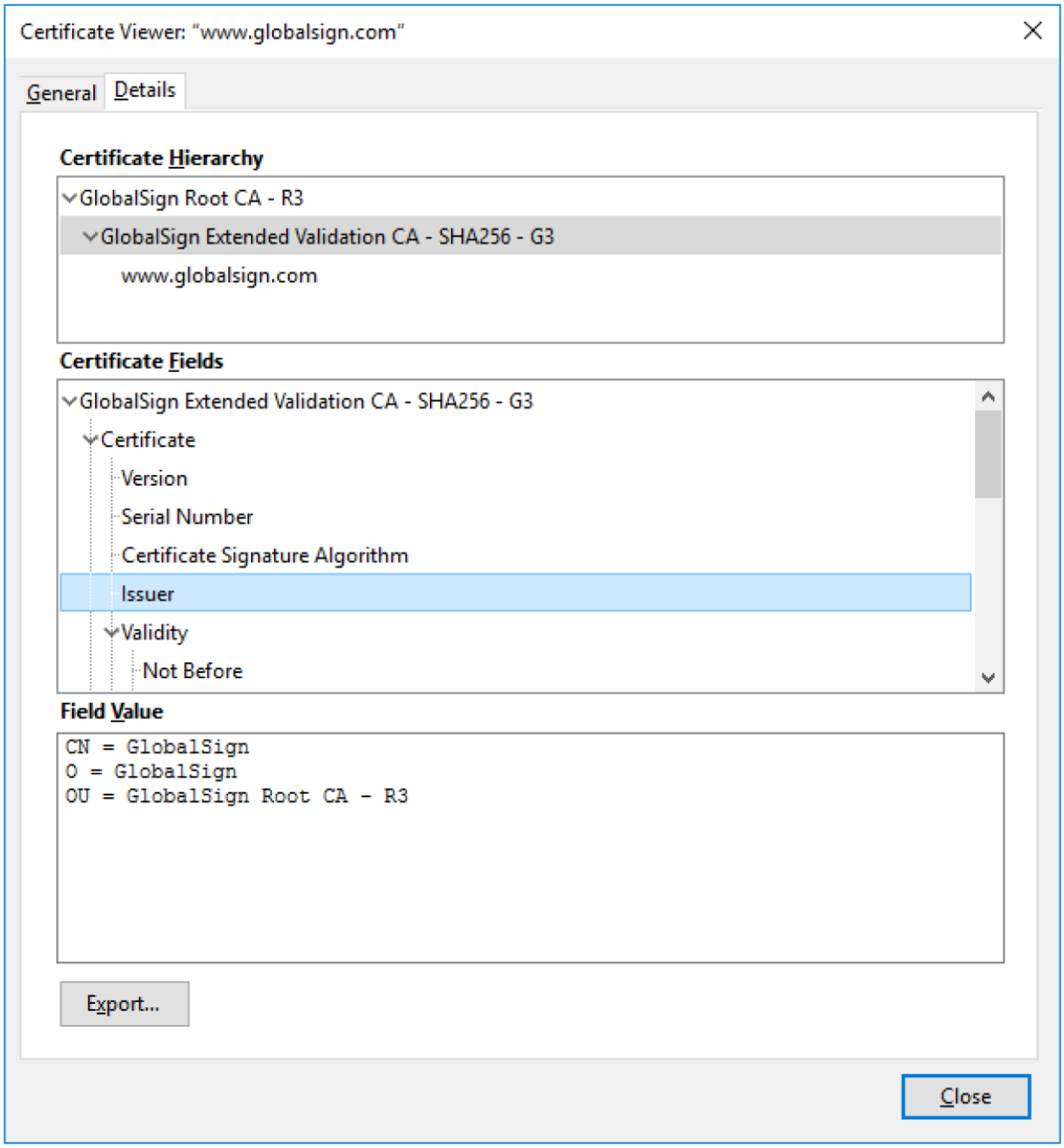
When You Want To Authenticate Yourself To Others, You Create A Signature And Sign It Using Your Private Key To Encrypt It. You Give Others Your Public Key To Decrypt The Signature.

Certificate Authority - This Is The Entity Responsible For Issuing And Guaranteeing Certificates.

Pki Trust Models Include:

- Single Ca - A Single Ca Issues Certificates To Users And The Users Trust Certificates By That Ca Exclusively. If The Ca Is Compromised, The Entire Pki Collapses

- Hierarchical (Intermediate Ca) - A Single Ca Called The Root Issues Certificates To Several Intermediate Cas. The Intermediate Cas Issue Certificates To Subjects (Leaf Or End Entities). Each Leaf Certificate Can Be Traced Back To The Root Ca Along The Certification Path And This Is Referred To As A Certificate Chain Or Chain Of Trust. The Root Is Still A Single Point Of Failure But It Can Be Taken Offline As Most Of The Regular Ca Activities Are Handled By The Intermediate Ca Servers.



- Online Versus Offline Cas - An online ca is one that is available to accept and process certificate signing requests and management tasks. Because of the high risk posed by a compromised root ca, a secure configuration will involve making the root an offline ca meaning it is disconnected from any network and only brought back online to add or update intermediate cas.

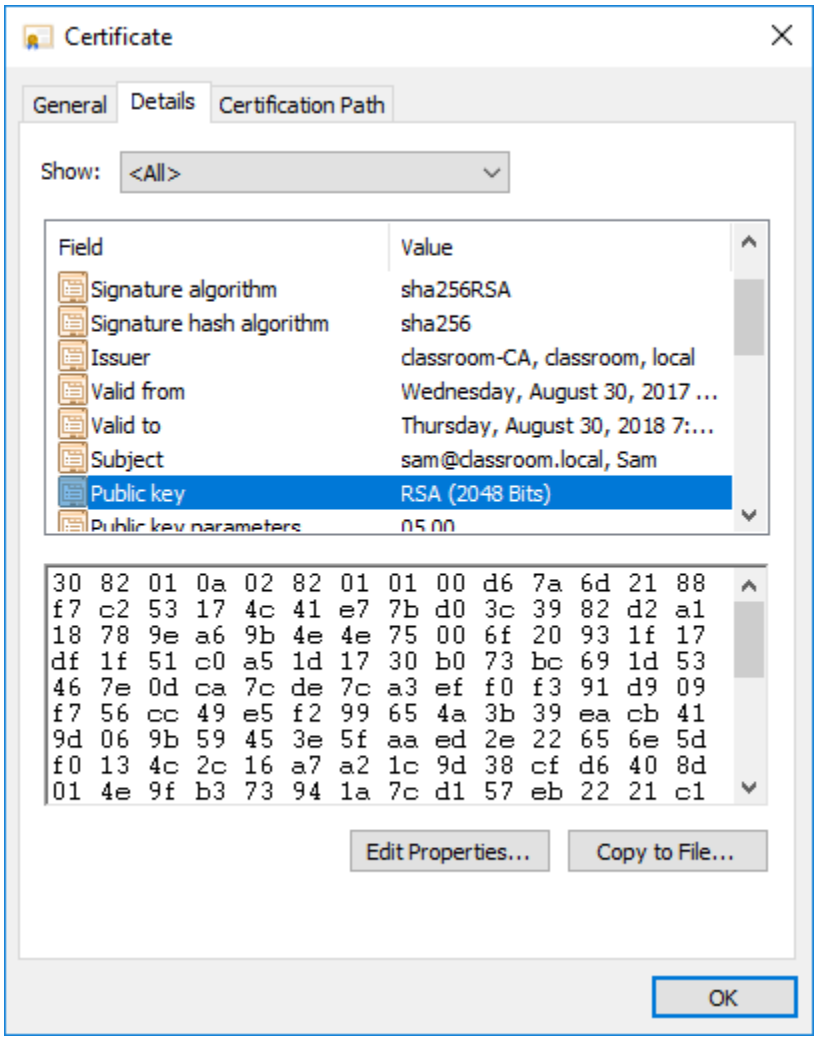
registration authorities and CSRS - registration is the process by which end users create an account with the CA and become authorized to request certificates.

When A Subject Wants To Obtain A Certificate, It Completes A Certificate Signing Request (Csr) And Submits It To The Ca.

The CA Reviews The Certificate And Checks That The Information Is Valid. If The Request Is Accepted, The CA Signs The Certificate And Sends It To The Subject.

6.2 - Digital Certificates

A Digital Certificate Is Essentially A Wrapper For A Subject's Public Key. As Well As The Public Key, It Contains Information About The Subject And The Certificate's Issuer.



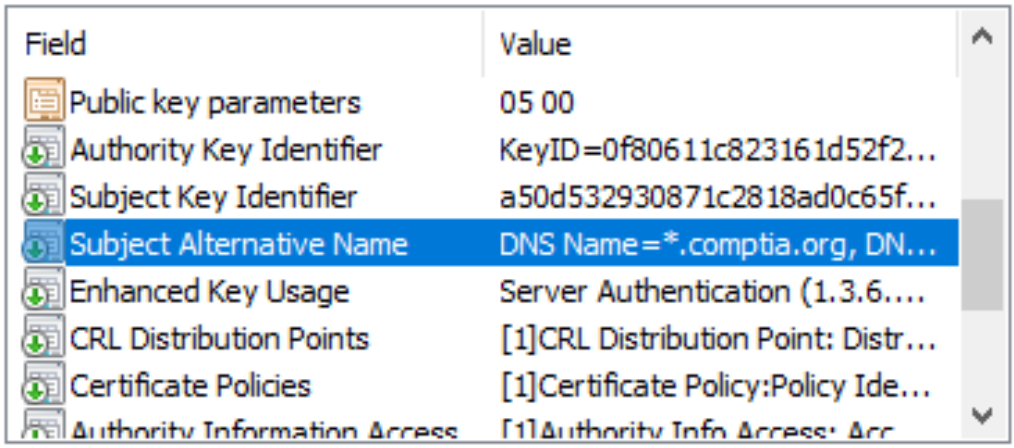
Certificate Attributes

Field	Usage
Serial number	A number uniquely identifying the certificate within the domain of its CA.
Signature algorithm	The algorithm used by the CA to sign the certificate.
Issuer	The name of the CA.
Valid from/to	Date and time during which the certificate is valid.
Subject	The name of the certificate holder, expressed as a distinguished name (DN). Within this, the common name (CN) part should usually match either the fully qualified domain name (FQDN) of the server or a user email address.
Public key	Public key and algorithm used by the certificate holder.
Extensions	V3 certificates can be defined with extended attributes, such as friendly subject or issuer names, contact email addresses, and intended key usage.
Subject alternative name (SAN)	This extension field is the preferred mechanism to identify the DNS name or names by which a host is identified.

When Certificates Were First Introduced, The Common Name (Cn) Attribute Was Used To Identify The Fqdn By Which The Server Is Accessed.

The Subject Alternative Name (San) Extension Field Is Structured To Represent Different Types Of Identifiers Including Domain Names.

A Wildcard Domain Such As *.Comptia.Org Means That The Certificate Issued To The Parent Domain Will Be Accepted As Valid For All Subdomains.



Eku Field - Can Have The Following Values

- Server Authentication
- Client Authentication
- Code Signing
- Email Protection

Web Server Certificate Types Include:

- Domain Validation (Dv) - Proves The Ownership Of A Particular Domain
- Extended Validation (Ev) - Subjecting To A Process That Requires More Rigorous Checks On The Subject's Legal Identity And Control Over The Domain.

Other Certificate Types Include:

- Machine/Computer Certificates
- Email/User Certificates
- Code Signing Certificates
- Root Certificate
- Self-Signed Certificates

6.3 - Key Management

This Refers To Operational Considerations For The Various Stages In A Key's Life Cycle And Can Be *Centralized* Meaning One Admin Controls The Process Or *Decentralized* In Which Each User Is Responsible For His Or Her Keys.

Key Life Cycle

- Key Generation
- Certificate Generation
- Storage
- Revocation
- Expiration And Renewal

If The Key Used To Decrypt Data Is Lost Or Damaged, Encrypted Data Cannot Be Recovered Unless A Backup Of The Key Exists. However Making Too Many Backups Can Make It More Difficult To Keep The Key Secure.

Escrow Means That Something Is Held Independently Which In Terms Of Key Management, Means A Third Party Is Trusted To Store The Key Securely.

6.4 - Certificate Management

When You Are Renewing A Certificate, It Is Possible To Use The Existing Key Referred To Specifically As Key Renewal Or Generate A New Key In Which Case, The Certificate Is Rekeyed.

Certificates Are Issued With A Limited Duration Set By The Ca Policy For The Certificate Type E.G A Root Certificate Might Have A 10 Year Expiry Date While A Web Server Certificate Might Be Issued For 1 Year Only.

A Certificate May Be Revoked Or Suspended. A Revoked Certificate Is No Longer Valid And Cannot Be Reinstated While A Suspended Certificate Can Be Re-Enabled.

A Certificate May Be Revoked Or Suspended For A Variety Of Reasons Such As The Private Key Compromise, Business Closure Or A User Leaving The Company. These Reasons Are Codified Under

- Unspecified
- Key Compromise
- Ca Compromise
- Superseded
- Cessation Of Operation

A Suspended Key Is Given The Code Certificate Hold

Section 7- Authentication Design Concepts

7.1 - Identity Access Management

Covers The Authentication & Authorization Aspects Of A System And How Privileged Users Are Managed.

There Are Four Phases Involved In Iam

- Identity - Supply Identification Information
- Authenticate - Identity Information Is Verified
- Authorize - Allows Actions Based On Verified Identification

- Audit - Keeps Track Of Actions Performed With The Identification

Identity & Access Threats

- Spoofing
- Identity Theft
- Keylogging
- Escalation Of Privilege
- Information Leakage

Im Tools & Techniques

- Identity Manager
- Fraud Analytics
- Multi Factor Authentication

Am Tools & Techniques

- Single Sign On
- Behavior Analytics
- Role Based Approach

7.2 - Authentication Factors, Design And Attributes

Authentication Factors

- Something You Know - This Includes Passwords, Passphrases Or Pins. A Knowledge Factor Is Also Used For Account Reset Mechanisms.

- Something You Have - An Ownership Factor Means That The Account Holder Possesses Something That No One Else Does Such As A Smart Card, Hardware Token Or Smartphone.

- Something You Are/Do - A Biometric Factor Uses Either Physiological Identifiers Like Fingerprints Or Behavioral Identifiers Such As The Way Someone Walks And Talks.

Multi Factor Authentication - This Combines The Use Of More Than One Authentication Factor And Can Either Be 2factor Or 3 Factor Authentication.

Multifactor authentication requires a combination of different technologies. for example, requiring a pin along with a date of birth isn't multifactor.

Authentication Attributes

Compared to the authentication factors, an authentication attribute is either a non-unique property or a factor that cannot be used independently.

- somewhere you are - this could be a geographic location measured using a device's location service or ip address. This isn't used as a primary authentication factor but may be used as a continuous authentication mechanism.

- something you can do - behavioral characteristics such as the way you walk or hold your smartphone can be used to identify you to a considerable degree of activity.

- something you exhibit - this also refers to a behavioral-based authentication and authorization with specific emphasis on personality traits such as the way you use smartphone apps or web search engines.

- someone you know - this uses a web of trust model where new users are vouched for by existing users.

7.3 - Password Attacks

Plain text/ unencrypted attacks - an attack that exploits unencrypted password storage such as those used in protocols like http, pap and telnet.

online attacks - the threat actor interacts directly with the authentication service using either a database of known passwords or a list of passwords that have been cracked online. This attack can be prevented with the use of strong passwords and restricting the number of login attempts within a specified period of time.

password spraying - a horizontal brute force attack where the attacker uses a common password (123456) and tries it with multiple usernames.

offline attacks - an offline attack means the attacker has gotten access to a database of password hashes e.g %systemroot%\system32\config\sam or %systemroot%\ntds\ntds.dit (the active directory credential store)

brute force attack - attempts every possible combination in the output space in order to match a captured hash and guess the plaintext that generated it. the more the characters used in the plaintext password, the more difficult it would be to crack.

rainbow table attack - a refined dictionary attack where the attacker uses a precomputed lookup table of all possible passwords and their matching hashes.

hybrid attack - uses a combination of brute force and dictionary attacks.

password crackers - there are some windows tools including cain and l0phtcrack but the majority of password crackers like hashcat run primarily on linux.

Password managers can be implemented with a hardware token or as a software app:

- password key - usb tokens for connecting to pcs and smartphones.
- password vault - software based password manager typically using a cloud service to allow access from any device.

7.4 - Authentication Technologies And Protocols

Smart-Card Authentication - This Means Programming Cryptographic Information Onto A Card Equipped With A Secure Processing Chip.

The Chip Stores:

- The User's Digital Certificate
- The Private Key Associated With The Certificate
- A Pin Used To Activate The Card

A hardware security module (HSM) is a network appliance designed to perform centralized PKI management for a network of devices which means it can act as an archive or escrow for keys in case of loss or damage.

Token Keys & Static Codes - The Use Of Tokens Avoids Some Of The Management Issues Of Using Digital Certificates.

A One-Time Password (Otp) Is One That Is Generated Automatically Rather Than Being Chosen By A User And Used Only Once. An Otp Is Not Vulnerable To Password Guessing Or Sniffing Attacks.

7.5 - Biometric Authentication

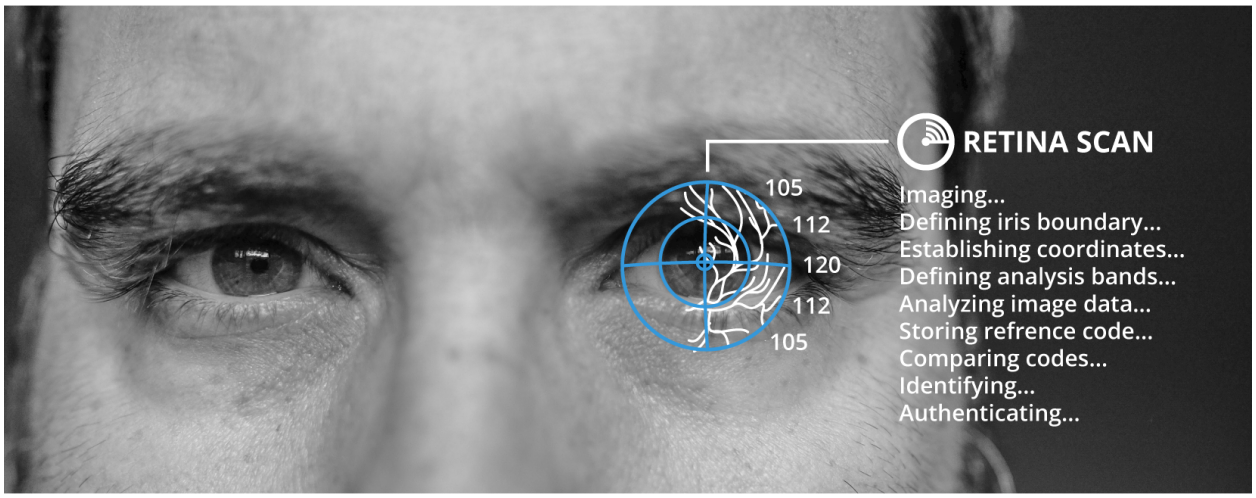
The first step is enrollment and the chosen biometric is scanned by a biometric reader and converted to binary information. The biometric template is kept in the authentication server database and when a user wants to access a resource, they are scanned and the scan is compared to the template to determine if access will be granted or denied.

- false rejection rate (FRR) - where a legitimate user is not recognized. also referred to as a type 1 error or false non-match rate (FNMR).

- false acceptance rate (FAR) - where an interloper is accepted. also referred to as type 2 error or false match rate (FMR)

- crossover error rate (CER) - the point at which FRR and FAR meet. the lower the CER, the more efficient and reliable the technology.

fingerprint & facial recognition - fingerprint recognition is the most widely used as it's inexpensive and non-intrusive. facial recognition records multiple factors about the size and shape of the face



Facial Recognition

- Retinal Scan - An Infrared Light Is Shone Into The Eye To Identify The Pattern Of Blood Vessels. It Is Very Accurate, Secure But Also Quite Expensive
- Iris Scan - Matches Patterns On The Surface Of The Eye Using Near-Infrared Imaging And Is Less Intrusive Than Retinal Scan.

Behavioral Technology - A Template Is Created By Analyzing A Behavior Such As Typing Or Walking.

- Voice Recognition - Relatively Cheap But Subject To Impersonation And Background Noise
- Gait Analysis - Human Movement
- Signature Recognition - Records The User Applying Their Signature (Stroke, Speed And Pressure Of The Stylus)
- Typing - Matches The Speed And Pattern Of A User's Input Of A Passphrase

Continuous Authentication Verifies That The User Who Logged On Is Still Operating The Device.

Section 8- Identity and Management Controls

8.1 - Identity Management Controls

Background Check & Onboarding Policies - Personnel Management Policies Are Applied In Three Phases

- Recruitment
- Operation
- Termination/Separation

A background check determines that a person is who they say they are and are not concealing criminal activity. Onboarding is the process of welcoming a new employee to the organization.

Onboarding Processes

- Secure Transmission Of Credentials - Creating An Initial Password Or Issuing A Smart Card Securely.
- Asset Allocation - Provision Of Computers Or Mobile Devices
- Training

Non-Disclosure Agreement (NDA) Might Be Incorporated Into The Employee Contract.

Personnel Policies For Privilege Management - Separation Of Duties Is A Means Of Establishing Checks And Balances Against The Possibility That Critical Systems Can Be Compromised By Insider Threats.

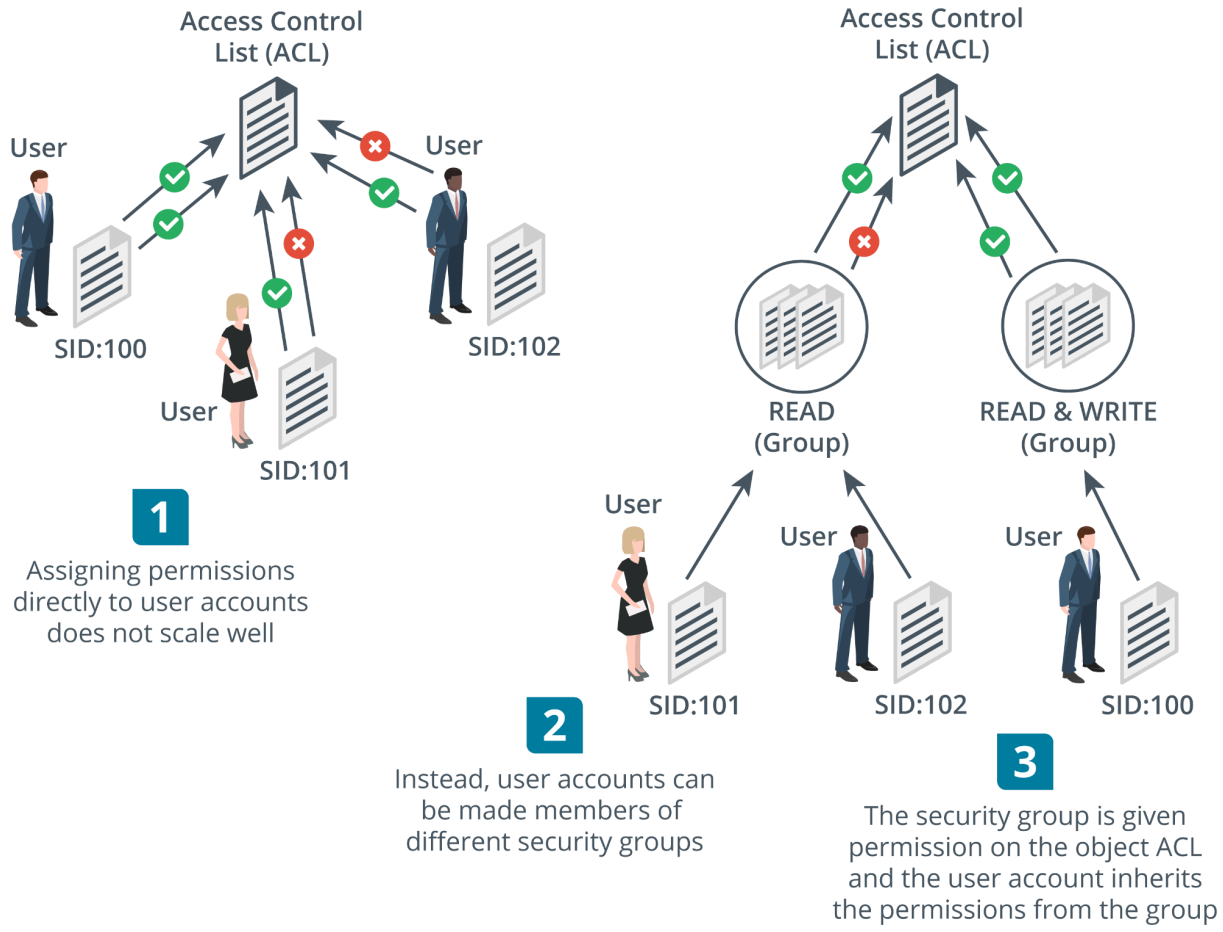
- Standard Operating Procedures (SOPS) Means That An Employee Has No Excuse For Following Protocols
- Shared Authority Means No One User Is Able To Make Changes On Their Own Authority

Offboarding Policies - Offboarding Is The Process Of Ensuring That An Employee Leaves A Company Gracefully.

- Account Management - Disable The User Account And Privileges
- Company Assets - Retrieve All Assets Previously Given To The Employee

- Personal Assets - Wipe Employee-Owned Devices Of Corporate Data And Applications.

Credential management policies - this is typically a password policy that will instruct users on best practices in choosing and maintaining passwords. the credential management policy also needs to alert users to diverse social engineering attacks and phishing attempts.



Administrator Credential Policies - The Default Superuser Should Be Replaced With One Or More Named Accounts With Sufficient Elevated Privileges For A Given Role.

In General, The Number Of Admin Accounts Should Be Restricted And Such Accounts Should Not Be Shared As This Would Compromise Accountability.

Service Accounts - These Are Used By Scheduled Processes And Application Server Software Such As Databases.

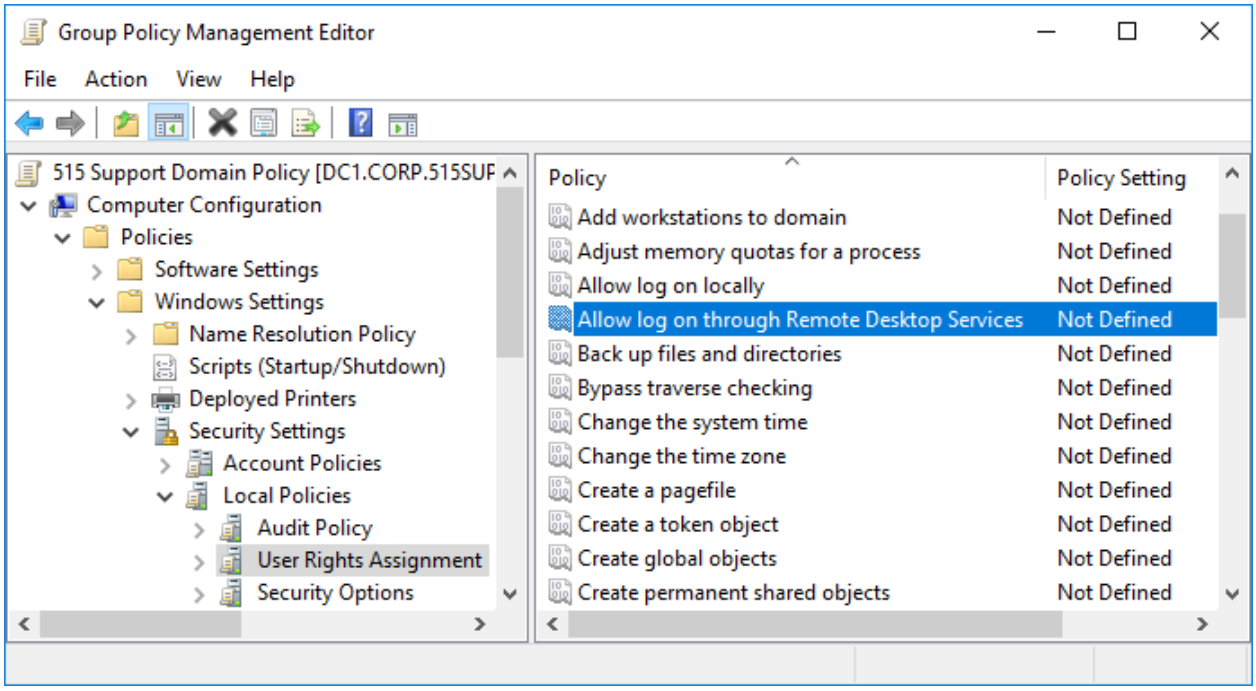
- System - Has The Most Privileges Of Any Windows Account
- Local Service - Has The Same Privileges As The Standard User Account But Can Only Access Network Resources As An Anonymous User
- Network Service - Has The Same Privileges As The Standard User Account But Can Present The Computer's Account Credentials When Accessing Network Resources.

Shared Accounts - This Is One Where Passwords (Or Other Authentication Credentials) Are Known To More Than One Person. A Shared Account Breaks The Principle Of Non-Repudiation And Makes An Accurate Audit Trail Difficult To Establish.

8.2 - Account Attributes & Access Policies

A user account is defined by a unique security identifier (sid), a name and a credential. Each account is associated with a profile which can be defined with custom identity attributes describing the user, such as full name, email address, contact number etc.

Each account can be assigned permissions over files and other network resources. These permissions might be assigned directly to the account or inherited through membership of a security group or role. on a windows active directory network, access policies can be configured via group policy objects (GPOS)



Account Password Policy Settings

- Password Length - Enforces A Minimum Length For Passwords.
- Password Complexity - Enforces Password Complexity Rules
- Password Aging - Forces The User To Select A New Password After A Set Period
- Password Reuse And History - Prevents The Selection Of A Password That Has Been Used Already.

Under The Most Recent Guidance Issued By Nist

- Complexity Rules Should Not Be Enforced And The Only Restriction Should Be To Block Common Passwords.
- Aging Policies Should Not Be Enforced. Users Should Be Able To Select If And When A Password Should Be Changed
- Password Hints Should Not Be Used.

Location-Based Policies - A User Or Device Can Have A Logical Network Location Identified By An Ip Address Which Can Be Used As An Account Restriction Mechanism.

The Geographical Location Of A User Or Device Can Be Calculated Using A Geographical Mechanism.

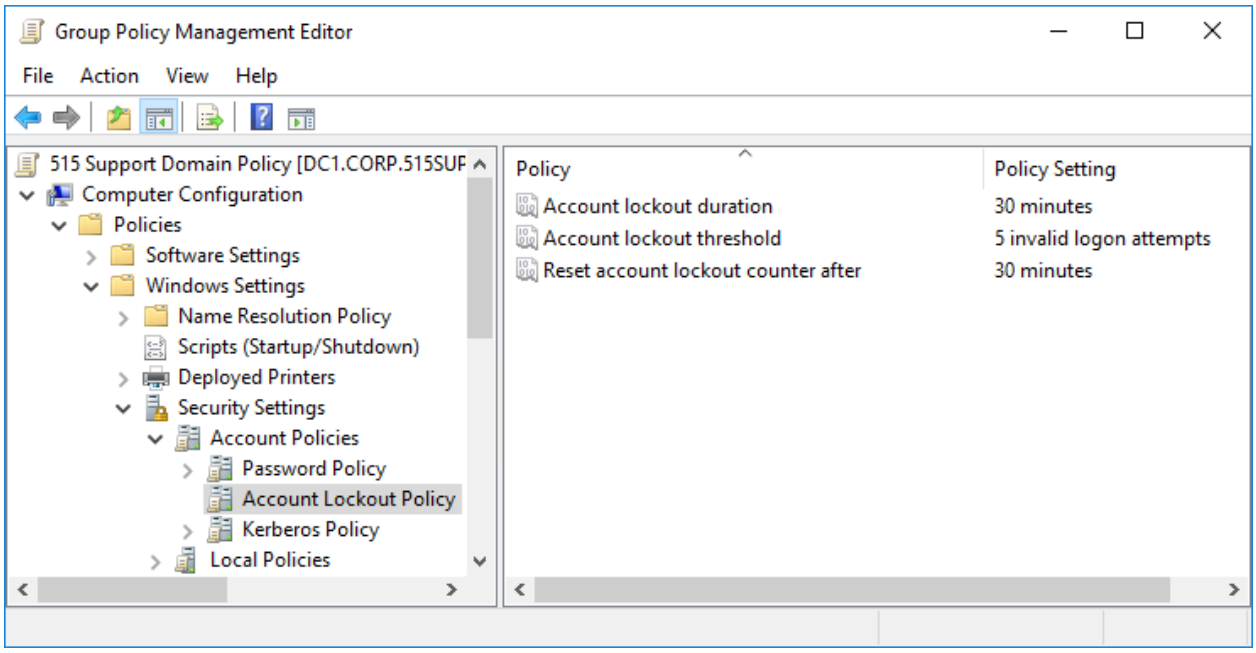
Geofencing Refers To Accepting Or Rejecting Access Requests Based On Location.

Time-Based Restrictions - There Are Three Main Types Of Time-Based Policies.

- A Time Of Day Policy Established Authorized Logon Hours For An Account
- A Time-Based Login Policy Established The Maximum Amount Of Time An Account May Be Logged In For
- An Impossible Travel Time/Risky Login Policy Tracks The Location Of Logon Events Over Time.

Account & Usage Audits - Accounting And Auditing Processes Are Used To Detect Whether An Account Has Been Compromised Or Is Being Misused. Usage Auditing Means Configuring The Security Log To Record Key Indicators And Then Reviewing The Logs For Suspicious Activity.

Account Lockout & Disablement - If Account Misuse Is Detected Or Suspected, The Account Can Be Manually Disabled By Setting An Account Property. An Account Lockout Means That Login Is Prevented For A Period



8.3 - Authorization Solutions - Part 1

An Important Consideration When Designing A Security System Is To Determine How Users Receive Rights Or Permissions.

The Different Models Are Referred To As Access Control Schemes.

Discretionary Access Control (Dac) - It Is Very Flexible But Also The Easiest To Compromise As It's Vulnerable To Insider Threats And Abuse Of Compromised Accounts.

This Is Based On The Primacy Of The Resource Owner And This Means The Owner Has Full Control Over The Resource And Can Decide Who To Grant Rights To.

Role-Based Access Control (Rbac) - Rbac Can Be Partially Implemented Through The Use Of Security Group Accounts.

This Adds An Extra Degree Of Centralized Control To The Dac Model Where Users Are Not Granted Rights Explicitly (Assigned Directly) But Rather Implicitly (Through Being Assigned A Role)

File System Permissions (Linux) - In Linux, There Are Three Basic Permissions:

- Read(R) - The Ability To Access And View The File
- Write(W) - The Ability To Modify The File
- Execute(X) - The Ability To Run A Script Or Program Or Perform A Task On That Directory.

These Permissions Can Be Applied In The Context Of The Owner User(U), A Group Account(G) And All Other Users/World(O).

D Rwx R-X R-X Home

The String Above Shows That For The Directory(D), The Owner Has Read, Write And Execute Permissions While The Group Context And Others Have Read And Execute Permissions

The Chmod Command Is Used To Modify Permissions And Can Be Used Either In Symbolic Or Absolute Mode.

In Symbolic Mode, The Command Works As Follows:

Chmod G+W, O-X Home

The Effect Of This Command Is To Append Write Permission To The Group Context And Remove Execute Permission From The Other Context.

By Contrast, The Command Can Also Be Used To Replace Existing Permissions.

Chmod U=Rwx, G=Rx, O=Rx Home

D Rwx R-X R-X Home

In Absolute Mode, Permissions Are Assigned Using Octal Notation Where R=4, W=2 And X=1

Chmod 755 Home

mandatory access control (mac) - this is based on the idea of security clearance levels (labels) instead of acls. in a hierarchical one, subjects are only permitted to access objects at their own clearance level or below.

attribute-based access control (abac) - this is the most fine-grained type of access control mode and it is capable of making access decisions based on a combination of subject and object attributes plus any system-wide attributes.

This system can monitor the number of events or alerts associated with a user account or track resources to ensure they are consistent in terms of timing of requests.

rule-based access control - this is a term that can refer to any sort of access control model where access control policies are determined by system-enforced rules rather than system users.

As such RBAC, ABAC and MAC are all examples of rule-based (or non-discretionary) access control.

8.4 - Authorization Solutions - Part 2

Directory Services - directory services are the principal means of providing privilege management and authorization on an enterprise network as well as storing information about users, security groups and services.

The types of attributes, what information they contain and the way object types are defined through attributes is described by the directory schema.

Cn - Common Name Ou - Organizational Unit C - Country Dc - Domain Component

E.G The Distinguished Name Of A Web Server Operated By Widget In The Uk Might Be:

Cn = Widgetweb, Ou = Marketing, O = Widget, C= Uk, Dc = Widget, Dc = Foo

federation - federation means that the company trusts accounts created and managed by a different network.

This is the notion that a network needs to be accessible to more than just a well-defined group of employees. In business, a company might need to make parts of its network open to partners, suppliers and customers.

cloud versus on-premises requirements - where a company needs to make use of cloud services or share resources with business partner networks, authorization and authentication design comes with more constraints and additional requirements.

oauth and openid connect - many public clouds use application programming interfaces (apis) based on representational state transfer (rest) rather than soap.

authentication and authorization for a restful api is often implemented using the open authorization (oauth) protocol. oauth is designed to facilitate sharing of information within a user profile between sites

8.5 - Personnel Policies

- Acceptable Use Policy (Aup)
- Code Of Conduct And Social Media Analysis
- Use Of Personally Owned Devices In The Workplace
- Clean Desk Policy

User And Role-Based Training - Appropriate Security Awareness Training Needs To Be Delivered To Employees At All Levels Including End Users, Technical Staff And Executives.

- Overview Of The Organization's Security Policies
- Data Handling
- Password & Account Management
- Awareness Of Social Engineering And Phishing

Diversity Of Training Techniques - Using A Diversity Of Training Techniques Helps To Improve Engagement And Retention.

- Phishing Campaigns
- Capture The Flag - Usually Used In Ethical Hacker Training Programs And Gamified Competitions.

- Computer-Based Training And Gamification

Section 9 - Implementing Secure Network Designs

9.1 - Secure Network Designs

switches - forward frames between nodes in a cabled network.

They work at layer 2 of the osi model and make forwarding messages based on the hardware or media access control (mac) address of attached nodes.

they can establish network segments that either map directly to the underlying cabling or to logical segments created in the switch configuration as virtual lans (VLANS)

wireless access points - provide a bridge between a cabled network and wireless clients or stations. They also work at layer 2 of the osi model.

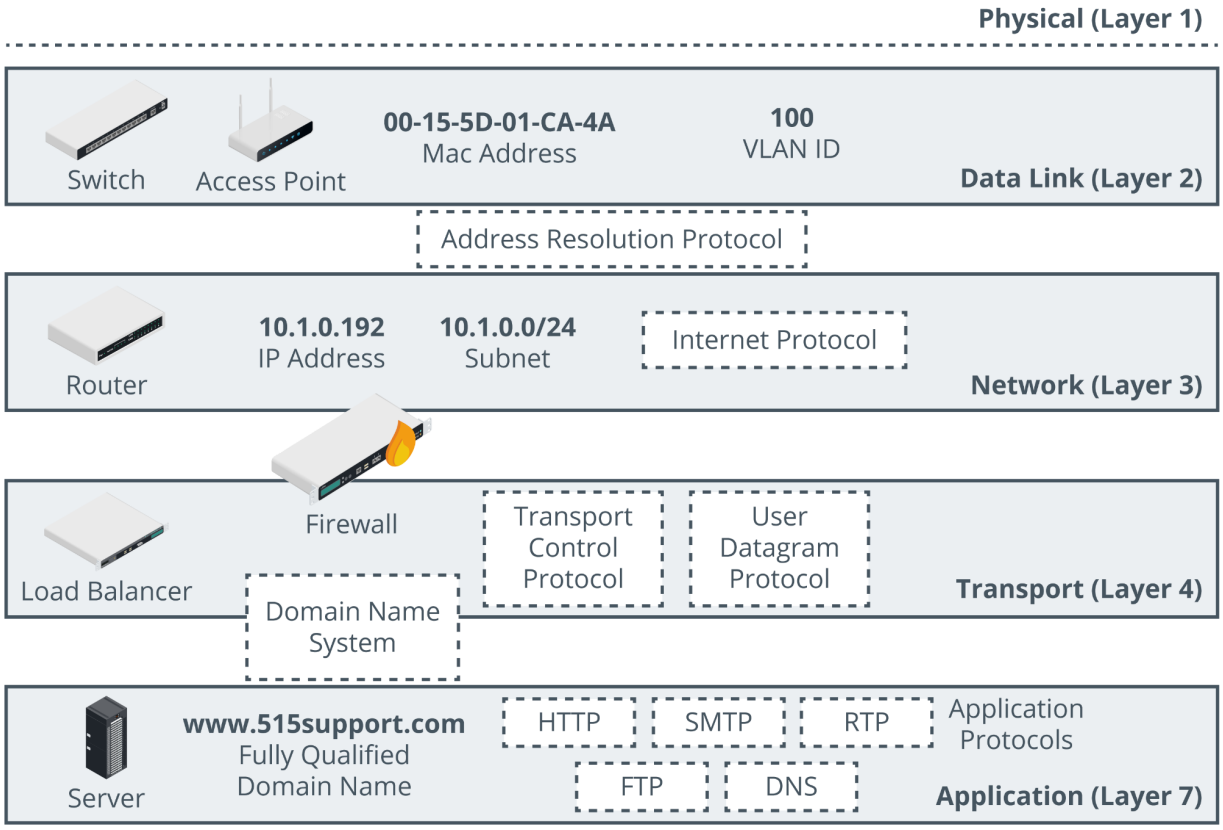
load balancers - distribute traffic between network segments or servers to optimize performance. they work at layer 4 of the osi model or higher

routers - forward packets around an internetwork, making forward decisions based on ip addresses. They work at layer 3 of the osi model. They can apply logical ip subnet addresses to segments within a network.

firewalls - they apply an access control list (acl) to filter traffic passing in or out of a network segment. they can work at layer 3 of the osi model or higher.

domain name system (DNS) servers - host name records and perform name resolution to allow applications and users to address hosts and services using fully qualified domain names (FQDNS) rather than IP addresses.

DNS works at layer 7 of the osi model.



9.2 - Network Segmentation, Topology & Dmzs

A Network Segment Is One Where All The Hosts Attached To The Segment Can Use Local (Layer 2) Forwarding To Communicate Freely With One Another.

Segregation Means That The Hosts In One Segment Are Restricted In The Way They Communicate With Hosts In Other Segments.

Freely Means That No Network Appliances Or Policies Are Preventing Communications.

A Network Topology Is A Description Of How A Computer Network Is Physically Or Logically Organized.

The Main Building Block Of A Topology Is A Zone Which Is An Area Of The Network Where The Security Configuration Is The Same For All Hosts Within It.

Zones Can Be Segregated With Vlans While The Traffic Between Them Can Be Controlled Using A Security Device, Typically A Firewall.

Network Zones

- Intranet (Private Network) - This Is A Network Of Trusted Hosts Owned And Controlled By The Organization.
- Extranet - This Is A Network Of Semi-Trusted Hosts Typically Representing Business Parties, Suppliers Or Customers.
- Internet/Guest - This Is A Zone Permitting Anonymous Access By Untrusted Hosts Over The Internet.

Demilitarized Zones (Dmzs) - The Most Important Distinction Between Different Security Zones Is Whether A Host Is Internet-Facing.

An Internet-Facing Host Accepts Inbound Connections From And Makes Connections To Hosts On The Internet.

Such Hosts Are Placed In A Dmz (Perimeter Or Edge Network). In A Dmz, External Clients Are Allowed To Access Data On Private Systems Such As Web Servers Without Compromising The Security Of The Internal Network As A Whole.

Triple-Homed Firewall - A Dmz Can Also Be Established Using One Router/Firewall Appliance With Three Network Interfaces, Referred To As Triple-Homed.

- One Interface Is The Dmz
- The Second Is The Public One
- The Third Connects To The Lan

East-West Traffic - Traffic That Goes To And From A Data Center Is Referred To As North-South. This Traffic Represents Clients Outside The Data Center Making Requests.

However In Data Centers That Support Cloud Services, Most Traffic Is Actually Between Servers Within That Data Center And This Traffic Is Referred To As East-West Traffic.

Zero Trust - This Is Based On The Idea That Perimeter Security Is Unlikely To Be Robust Enough. As Such In A Zero Trust Model, Continuous Authentication And Conditional Access Are Used To Mitigate Threats.

Zero Trust Also Uses A Technique Called Microsegmentation. This Is A Security Process That Is Capable Of Applying Policies To A Single Node As Though It Was In A Zone Of Its Own.

9.3 - Secure Switching And Routing

Man-In-The-Middle & Layer 2 Attacks - Most Attacks At Layer 1 And 2 Of The Osi Model Are Typically Focused On Information Gathering Through Network Mapping And Eavesdropping.

A MITM can also be performed on this layer due to the lack of security.

MAC cloning or MACaddress spoofing changes the hardware address of an adapter to an arbitrary one either by overriding the original address in software via os commands or with the use of packet crafting software.

arp poisoning attack - arp poisoning attack uses a packet crafter such as ettercap to broadcast unsolicited arp reply packets.

Because arp has no security mechanism, the receiving devices trust this communication and update their mac:ip address cache table with the spoofed address.

MAC flooding attacks - where arp poisoning is directed at hosts, mac flooding is used to attack a switch.

The idea here is to exhaust the memory used to store the switch's mac address table which is used by the switch to determine which port to use to forward unicast traffic to its correct destination.

overwhelming the table can cause the switch to stop trying to apply mac-based forwarding and simply flood unicast traffic out of all ports.

Router/Switch Security

- physical port security - access to physical switch ports and hardware should be restricted to authorized staff by using a secure server room or lockable hardware cabinets.
- mac limiting/filtering - configuring mac filtering on a switch means defining which mac addresses are allowed to connect to a particular port by creating a list of valid mac addresses. mac limiting involves specifying a limit to the number of permitted addresses that can connect to a port.

- dhcp snooping - dynamic host configuration protocol is one that allows a server to assign an ip address to a client when it connects to a network. dhcp snooping inspects this traffic arriving on access ports to ensure that a host is not trying to spoof its mac address. with dhcp snooping, only dhcp messages from ports configured as trusted are allowed.
- network access control - nac products can extend the scope of authentication to allow admins to devise policies or profiles describing a minimum security configuration that devices must meet to be granted network access. This is called a health policy.
- route security - a successful attack against route security enables the attacker to redirect traffic from its intended destination. routes between networks and subnets can be configured manually, but most routers automatically discover routes by communicating with each other.

routing is subject to numerous vulnerabilities

- spoofed routing information (route injection) - traffic is misdirected to a monitoring port (sniffing) or continuously looped around the network causing dos.
- source routing - this uses an option in the ip header to pre-determine the route a packet will take through the network. This can be used to spoof ip addresses and bypass router/firewall filters.
- software exploits in the underlying operating system - cisco devices typically use the internetwork operating system (ios) which suffer from fewer exploitable vulnerabilities than full network operating systems.

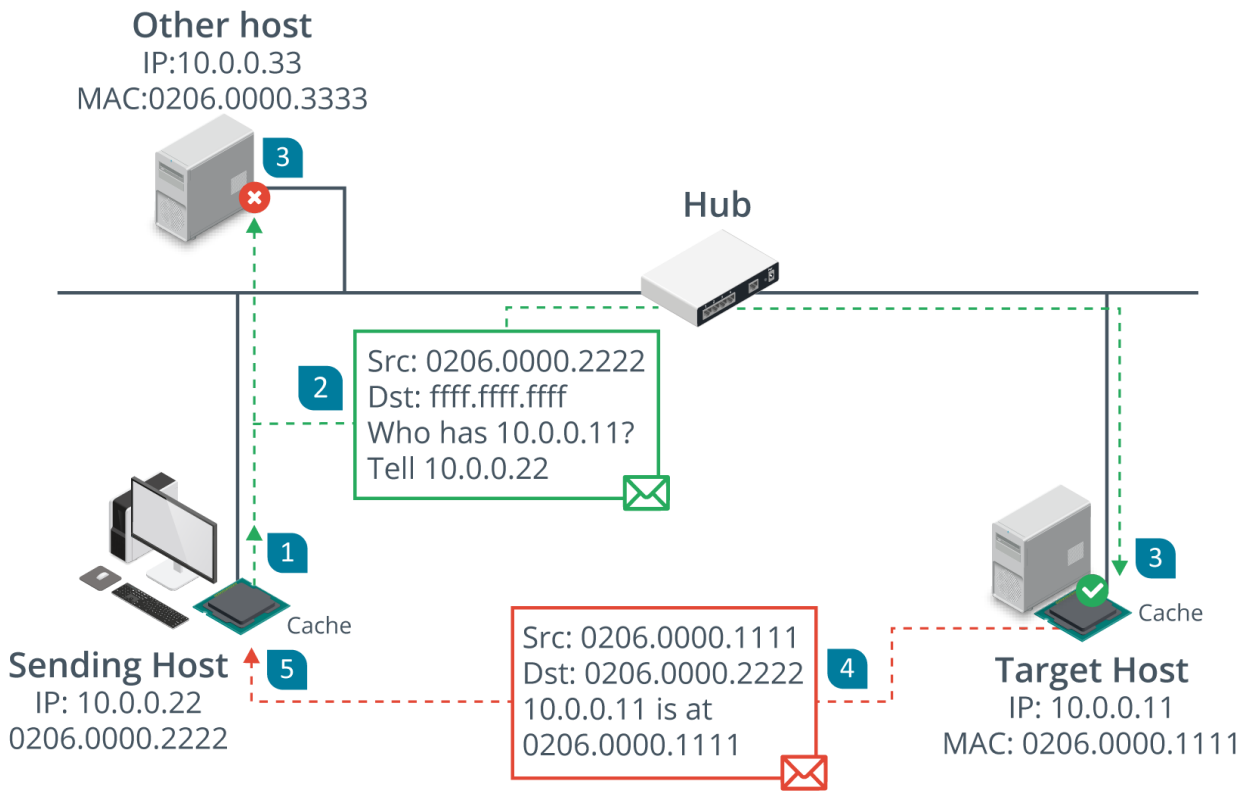
9.4 - Routing & Switching Protocols

Layer 3 Forwarding Or Routing Occurs Between Both Logically And Physically Defined Networks. A Single Network Divided Into Multiple Logical Broadcast Domains Is Said To Be Subnetted.

At Layer 3, Nodes Are Identified By Ip Addresses.

Address Resolution Protocol (Arp) - This Maps A Mac Address To An Ip Address.

Normally A Device That Needs To Send A Packet To An Ip Address But Does Not Know The Receiving Device's Mac Address Broadcasts Will Broadcast An Arp Request Packet And The Device With The Matching Ip Responds With An Arp Reply.



Internet Protocol (Ip)

This Provides The Addressing Mechanism For Logical Networks And Subnets.

172.16.1.101/16

The /16 Prefix Indicates That The First Half Of The Address (172.16.0.0) Is The Network Id While The Remainder Uniquely Identifies A Host On That Network. Networks Also Use 128-Bit Ipv6 Addressing.

2001:Db8::Abc:0:Def0:1234

The First 64-Bits Contain Network Information While The Last Are Fixed As The Host's Interface Id.

A Route To A Network Can Be Configured Statically But Most Networks Use Routing Protocols To Transmit New And Updated Routes Between Routers.

Some Common Routing Protocols Include

- Border Gateway Protocol (Bgp)
- Open Shortest Path First (Ospf)

- Enhanced Interior Gateway Routing Protocol (Eigrp)
- Routing Information Protocol (Rip)

9.5 - Wi-Fi Authentication Methods

Wi-Fi Authentication Comes In Three Types - Open, Personal And Enterprise.

Within The Personal Category, There Are Two Methods:

- Pre-Shared Key Authentication (Psk)
- Simultaneous Authentication Of Equals (Sae)

WPA2 pre-shared key authentication - in wpa2, pre-shared key (PSK) authentication uses a passphrase to generate the key for encryption.

The passphrase length is typically between 8 and 63 ascii characters and is then converted to a 256-bit HMAC value.

wpa3 personal authentication - wpa3 also uses a passphrase like wpa2 but it changes the method by which this secret is used to agree on session keys. this scheme is called password authenticated key exchange (PAKE)

wi-fi protected setup (wps) - this is a feature of both WPA and WPA2 that allows enrollment in a wireless network based on an 8-digit pin.

It is vulnerable to brute force attacks and is set to be replaced by the easy connect method in wpa3 which uses quick response (qr) codes of each device.

open authentication and captive portals - open authentication means that the client is not required to authenticate however it can be combined with a secondary authentication mechanism via a browser.

When the client launches the browser, the client is redirected to a captive portal or splash page where they will be able to authenticate to the hotspot provider's network.

enterprise/ieee 802.1x authentication - when a wireless station requests to join the network, its credentials are passed to an aaa server on the wired network for validation.

Once authenticated, the aaa server transmits a master key (mk) to the station and then both of them will derive the same pairwise master key (pmk) from the mk.

extensible authentication protocol (eap) - this defines a framework for negotiating authentication mechanisms rather than the details of the mechanisms themselves.

eap implementations can include smart cards, one-time passwords and biometric identifiers.

peap, eap-ttls and eap-fast - in protected extensible authentication protocol (peap), an encrypted tunnel is established between the supplicant and authentication server but only a server-side public key certificate is required.

eap with flexible authentication via secure tunneling (eap-fast) - is also similar to peap but instead of a server side certificate, it uses a protected access credential (pac) which is generated for each user from the authentication server's master key.

radius federation - most implementations of eap use a radius server to validate the authentication credentials for each user.

radius federation means that multiple organizations allow access to one another's users by joining their radius servers into a radius hierarchy or mesh.

rogue access points & evil twins - a rogue access point is one that has been installed on the network without authorization.

A rogue wap masquerading as a legitimate one is called an evil twin. an evil twin might have a similar ssid as the real one or the attacker might use some dos technique to overcome the legitimate wap.

A rogue hardware WAP can be identified through physical inspections. there are also various wi-fi analyzers that can detect rogue waps including inssider and kismet

disassociation and replay attacks - a disassociation attack exploits the lack of encryption in management frame traffic to send spoofed frames.

One type of disassociation attack injects management frames that spoof the mac address of a single victim causing it to be disconnected from the network.

Another variant broadcasts spoofed frames to disconnect all stations.

Jamming Attacks - A Wi-Fi Jamming Attack Can Be Performed By Setting Up A Wap With A Stronger Signal.

The Only Way To Defeat This Attack Is To Either Locate The Offending Radio Source And Disable It Or To Boost The Signal From The Legitimate Equipment.

9.6 - Network Attacks

Distributed Denial Of Service Attacks - Some Types Of Ddos Attacks Simply Aim To Consume Network Bandwidth Denying It To Legitimate Hosts While Others Cause Resource Exhaustion On The Hosts Processing Requests Consuming Cpu Cycles And Memory.

Syn Flood Attack - A Dos Attack Where The Attacker Sends Numerous Syn Requests To A Targeted Server Hoping To Consume Enough Resources To Prevent The Transfer Of Legitimate Traffic.

In A Distributed Reflection Dos (Drdos) Or Amplification Syn Flood Attack, The Threat Actor Spoofs The Victim's Ip Address And Attempts To Open Connections With Multiple Servers.

Those Servers Direct Their Syn/Ack Responses To The Victim Server Which Rapidly Consumes The Victim's Available Bandwidth.

Application Attacks - This Attack Targets Vulnerabilities In The Headers And Payloads Of Specific Application Protocols E.G Targeting Dns Services With Bogus Queries.

The Network Time Protocol (Ntp) Which Helps Servers On A Network To Keep The Correct Time Can Also Be Targeted With This Type Of Attack.

9.7 - Network Attacks Mitigation

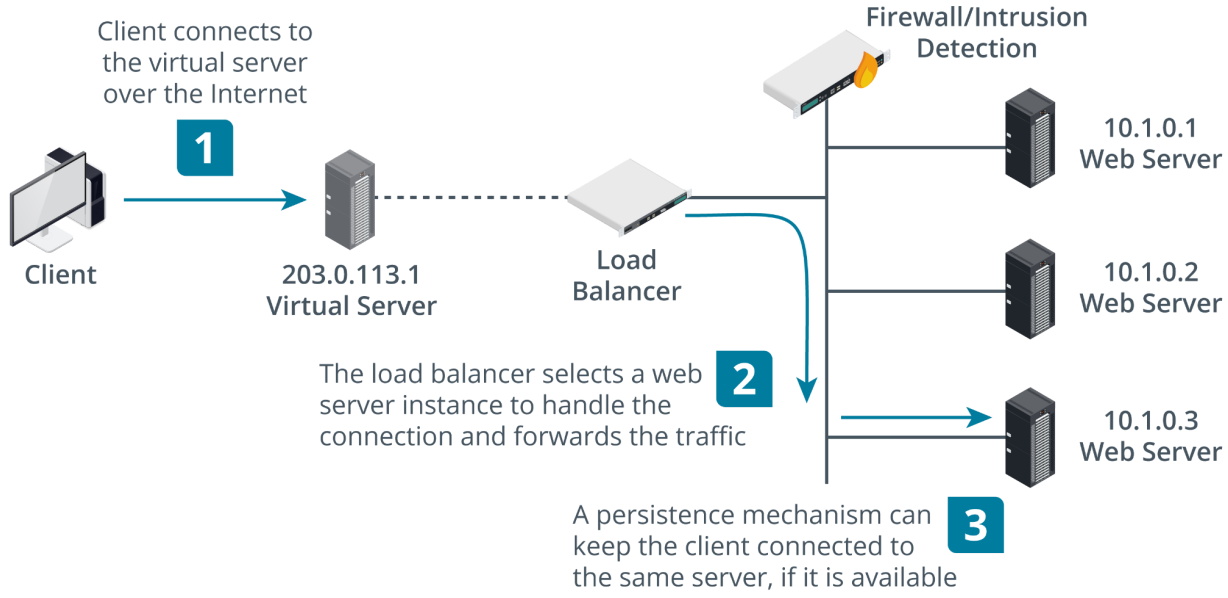
Ddos Attack Mitigation - DDOS attacks can be diagnosed by sudden huge traffic spikes and can be countered by load balancing or cluster services.

In some cases, a stateful firewall can detect a ddos attack and automatically block the source but in many other cases, the source addresses will be spoofed making it difficult to locate the real source. Another option is to use sinkhole routing so that the traffic flooding a particular ip address is routed to a different network where it can be analyzed.

Load Balancing - A Load Balancer Distributes Client Requests Across Available Server Nodes In A Farm Or Pool And Also Helps With Fault Tolerance. There Are Two Main Types Of Load Balancers:

- Layer 4 - Basic Load Balancers Make Forwarding Decisions On Ip Address And Tcp/Udp Port Values Working At The Transport Layer.

- Layer 7 - More Advanced Load Balancers That Make Forward Decisions Based On Application-Level Data Such As Request For Data Types Like Audio Or Video.



Source Ip Affinity & Session Persistence - Source Ip Or Session Affinity Is A Layer 4 Approach To Handling User Sessions And It Means That When A Client Establishes A Session, It Becomes Stuck To The Node That First Accepted The Request.

An Application Layer Can Use Persistence To Keep A Client Connected To A Session When It Is Necessary.

Clustering - This Allows Multiple Redundant Processing Nodes That Share Data With One Another To Accept Connections Thus Providing Redundancy. If One Of The Nodes In The Cluster Stops Working, Connections Can Failover To A Working Node.

Active/Passive (A/P) Clustering - In A/P, One Node Is Active While The Other Is Passive. Here The Performance Is Not Affected During Failover But The Operating Costs Can Be Higher Because Of The Unused Capacity.

Active/Active (A/A) Clustering - In A/A, Both Nodes Are Processing Connections Concurrently And This Allows The Admin To Use The Maximum Capacity From The Available Hardware But Performance Is Degraded When A Failover Occurs.

Quality Of Service - This Is A Framework For Prioritizing Traffic Based On Its Characteristics.

- Latency - The Time It Takes For A Transmission To Reach The Recipient Measured In Milliseconds
- Jitter - A Variation In The Delay Or An Inconsistent Rate Of Packet Delivery

Section 10 - Firewalls and Proxy Servers

10.1 - Firewalls

Packet filtering firewalls - these are the earliest type of firewalls and are configured by specifying a group of rules called an access control list (acl).

Each rule defines a specific type of data packet and the appropriate action to take when a packet matches the rule. an action can either be to deny or to accept the packet.

This firewall can inspect the headers of ip packets meaning that the rules can be based on the information found in those headers.in certain cases, the firewall can control only inbound or both inbound and outbound traffic and this is often referred to as ingress and egress traffic or filtering.

A basic packet filtering firewall is stateless meaning that it does not preserve any information about network sessions. The least processing effort is required for this but it can be vulnerable to attacks that are spread over a sequence of packets.

Stateful inspection firewalls - this type of firewall can track information about the session established between two hosts and the session data is stored in a state table.

When a packet arrives, the firewall checks it to confirm that it belongs to an existing connection and if it does then the firewall would allow the traffic to pass unmonitored to conserve processing effort.

Stateful inspection can occur at two layers: transport and application.

Transport layer (osi layer 4) - here, the firewall examines the tcp three-way handshake to distinguish new from established connections.

syn > syn/ack > ack

any deviations from this sequence can be dropped as malicious flooding or session hijacking attempts.

application layer (osi layer 7) - this type of firewall can inspect the contents of packets at the application layer and one key feature is to verify the application protocol matches the port e.g http web traffic will use port 80.

ip tables - *iptables* is a command on linux that allows admins to edit the rules enforced by the linux kernel firewall.

iptables works with chains which apply to the different types of traffic such as the input chain for traffic destined for the local host. Each chain has a default policy set to drop or allow traffic that does not match a rule.

The rules in this example will drop any traffic from the specific host 10.1.0.192 and allow icmp echo requests (pings), dns and http/https traffic either from the local subnet (10.1.0.0/24) or from any network (0.0.0.0/0)

```
Chain INPUT (policy DROP)

# target prot opt source   destination

1 DROP  all -- 10.1.0.192  0.0.0.0/0

2 ACCEPT icmp -- 10.10.0.0/24 0.0.0.0/0 icmptype 8

3 ACCEPT udp -- 0.0.0.0/0  0.0.0.0/0  udp dpt:53

4 ACCEPT tcp -- 0.0.0.0/0  0.0.0.0/0  tcp dpt:53

5 ACCEPT tcp -- 10.1.0.0/24 0.0.0.0/0  tcp dpt:80

6 ACCEPT tcp -- 10.1.0.0/24 0.0.0.0/0  tcp dpt:443

7 ACCEPT all -- 0.0.0.0/0  0.0.0.0/0  ctstate RELATED,ESTABLISHED
```

10.2 - Firewall Implementation

Firewall Appliances - This Is A Stand-Alone Firewall Deployed To Monitor Traffic Passing Into And Out Of A Network Zone. It Can Be Deployed In Two Ways:

- Routed (Layer 3) - The Firewall Performs Forwarding Between Subnets
- Bridged (Layer 2) - The Firewall Inspects Traffic Between Two Nodes Such As A Router And A Switch.

Application-Based Firewalls

- Host-Based (Personal) - Implemented As A Software Application Running On A Single Host Designed To Protect The Host Only.

- Application Firewall - Software Designed To Run On A Server To Protect A Particular Application Only

- Network Operating System (Nos) Firewall - A Software Based Firewall Running Under A Network Server Os Such As Windows Or Linux.

Proxies And Gateways - A Firewall That Performs Application Layer Filtering Is Likely To Be Implemented As A Proxy.

Proxy Servers Can Either Be Non-Transparent Or Transparent.

- Non-Transparent Means The Client Must Be Configured With The Proxy Server Address And Port Number To Use It

- Transparent (Forced Or Intercepting) Intercepts Client Traffic Without The Client Having To Be Reconfigured

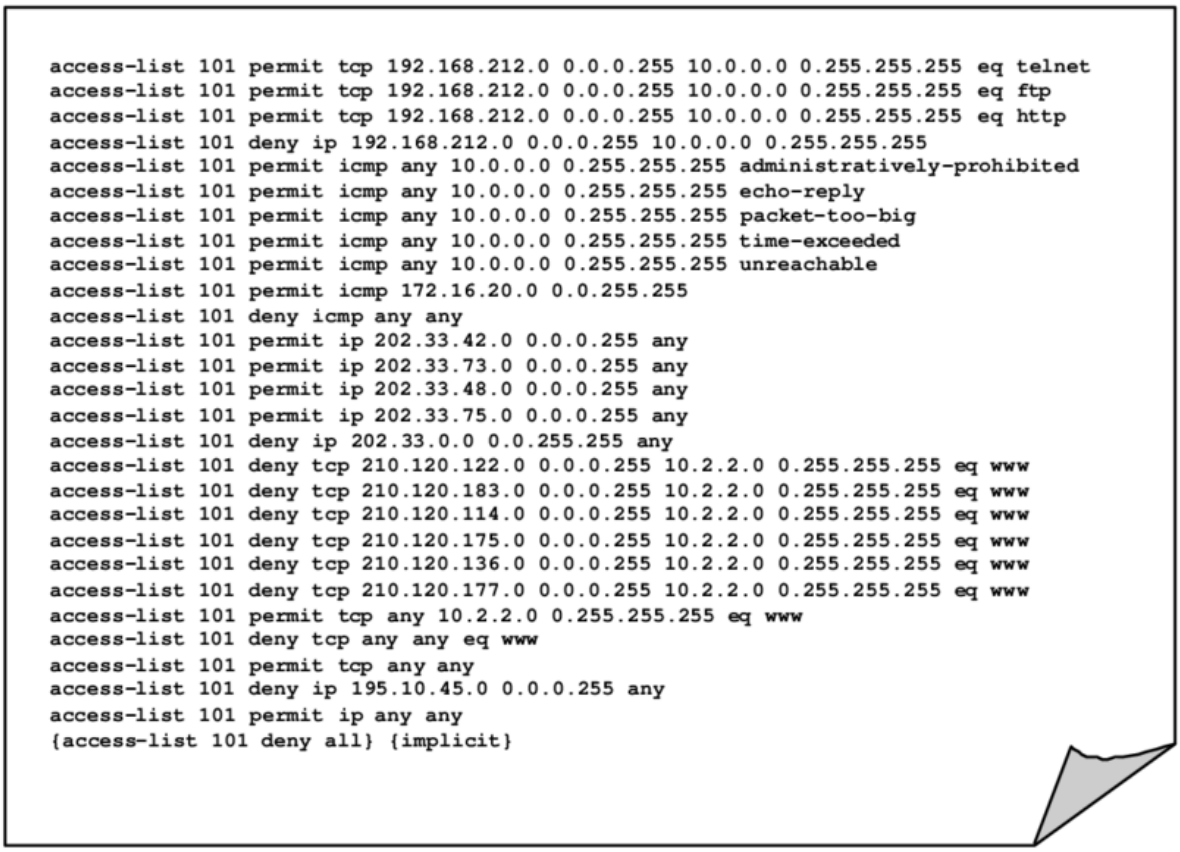
Reverse Proxy Servers - These Provide For Protocol-Specific Inbound Traffic.

A Reverse Proxy Can Be Deployed On The Network Edge And Configured To Listen For Client Requests From A Public Network

10.3 - ACLs, Nat & Virtual Firewalls

Access Control Lists - These Are Configured On The Principle Of Least Access (Least Privilege); Only Allow The Minimum Amount Of Traffic Required For The Operation Of Network Services.

The Most Specific Rules Are Placed At The Top And The Final Default Role Is Typically To Block Any Traffic That Has Not Matched A Rule (Implicit Deny)



Each Rule Can Specify Whether To Block Or Allow Traffic Based On Several Parameters, Often Referred To As Tuples.

Tuples Can Include Protocol, Source And Destination Address, Source And Destination Port.

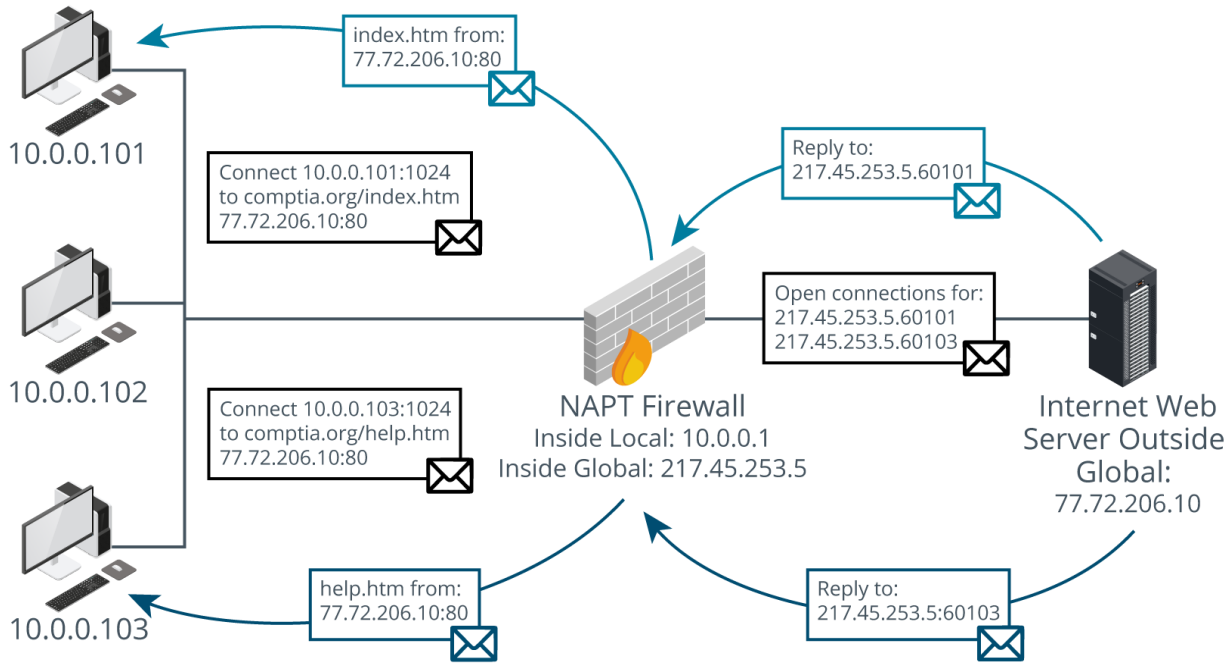
Network Address Translation (Nat) - This Was Devised As A Way Of Freeing Up Scarce Ip Addresses For Hosts Needing Internet Access. A Private Network Will Typically Use A Private Addressing System To Allocate Ip Addresses To Hosts.

- 10.0.0.0 To 10.255.255.255 (Class A)
- 172.16.0.0 To 172.31.255.255 (Class B)
- 192.168.0.0 To 192.168.255.255 (Class C)

There Are Several Types Of Nat

- Static & Dynamic Source Nat - Performs 1:1 Mappings Between Private And Public Addresses. The Mappings Can Be Static Or Dynamically Assigned

- Overloaded Nat/Network Address Port Translation(Napt)/Port Address Translation (Pat) - Provides A Means For Multiple Private Ip Addresses To Be Mapped Onto A Single Public Address.



- Destination Nat/Port Forwarding - Uses The Router's Public Address To Publish A Web Service But Forwards Incoming Requests To A Different Ip.

Port Forwarding Means That The Router Takes Requests From The Internet For A Particular Application (Http/Port 80) And Sends Them To A Designated Host And Port In The Dmz Or Lan

Virtual Firewalls - These Are Usually Deployed Within Data Centers And Cloud Services And Can Be Implemented In Three Different Ways.

- Hypervisor-Based - This Means That Filtering Functionality Is Built Into The Hypervisor Or Cloud Provisioning Tool.

- Virtual Appliance - This Refers To Deploying A Vendor Firewall Appliance Using Virtualization

- Multiple Context - This Refers To Multiple Virtual Firewall Instances Running On A Hardware Firewall Appliance.

10.4 - Network Security Monitoring

network-based intrusion detection systems - an ids is a means of using software tools to provide real-time analysis of either network traffic or system and application logs. a network-based ids captures traffic via a packet sniffer referred to as a sensor. when traffic matches a detection signature, it raises an alert but will not block the source host.

taps & port mirrors - typically the packet capture sensor is placed inside a firewall or close to an important server and the idea is to identify malicious traffic that has managed to get past the firewall. depending on network size and resources, one or just a few sensors will be deployed to monitor key assets and network paths.

network-based intrusion prevention systems (ips) - an ips provides an active response to any network threat.

typical responses to a threat can include blocking the attacker's ip address (shunning), throttling the bandwidth to attacking hosts and applying complex firewall filters.

Next generation firewall (NGFW) - HGFW is a product that combines application-aware filtering with user account-based filtering and the ability to act as an ips.

Unified threat management (UTM) - this refers to a security product that centralizes many types of security controls - firewall, antimalware, spam filtering, vpn etc into a single appliance. The downside is that this creates a single point of failure that can affect the entire network. they can also struggle with latency issues if they are subject to too much network activity.

content/url filter - a firewall typically has to sustain high loads of traffic which can increase latency and even cause network outages. a solution is to treat security solutions for server traffic differently from that of user traffic.

A Content Filter Is Designed To Apply A Number Of User-Focused Filtering Rules Such As Applying Time-Based Restrictions To Browsing.

Content Filters Are Now Implemented As A Class Of Product Called Secure Web Gateway (Swg) Which Can Also Integrate Filtering With The Functionality Of Data Loss Prevention.

Host-Based Ids - A Host-Based Ids (Hids) Captures Information From A Single Host. The Core Ability Is To Capture And Analyze Log Files But More Sophisticated Systems Can Also Monitor Os Kernel Files, Monitor Ports And Network Interfaces.

One Other Core Feature Is File Integrity Monitoring (Fim). Fim Software Will Audit Key System Files To Make Sure They Match The Authorized Versions.

Web Application Firewall (Waf) - A Waf Is Designed To Specifically Protect Software Running On Web Servers And Their Back-End Databases From Code Injection And Dos Attacks.

They Use Application-Aware Processing Rules To Filter Traffic And Perform Application-Specific Intrusion Detection.

10.5 - Monitoring Services & Siem

Packet Capture - Data Captured From Network Sensors/Sniffers Provides Both Summary Statistics About Bandwidth And Protocol Usage And The Opportunity For Detailed Analysis.

Network Monitors - These Collect Data About Network Appliances Such As Switches, Access Points, Routers, Servers And Firewalls.

They Are Used To Monitor Load Status For Cpu/Memory, State Tables, Disk Capacity, Fan Speeds/Temperature And So On. This Information Can Be Collected Using The Simple Network Management Protocol (Snmp).

Logs - Very Valuable And Can Be Used To Diagnose Availability Issues And Record Both Authorized And Unauthorized Uses Of A Resource Or Privilege. Reviewing Logs Are A Crucial Part Of Security Assurance.

Security Information & Event Management (Siem) - This Is Software Designed To Assist With Managing Security Data Inputs And Provide Reporting And Alerting.

The Core Function Is To Aggregate Traffic Data And Logs From The Os, Routers, Firewalls, Switches, Malware Scanners, Databases Etc.

Log Aggregation - Log Aggregation Refers To Normalizing Data From Different Sources So That It Is Consistent And Searchable.

User And Entity Behavior Analytics (UEBA) - A UEBA Solution Supports Identification Of Malicious Behaviors From Comparison To A Baseline. The Analytics Software Tracks User Account Behavior Across Different Devices And Cloud Services.

Security Orchestration, Automation And Response (Soar) - Soar Is Designed As A Solution To The Problem Of The Volume Of Alerts Overwhelming Analysts Ability To Respond.

The Basis Of Soar Is To Scan The Organization's Store Of Security And Threat Intelligence Then Analyze It Using Machine/Deep Learning Techniques And Then Use That Data To Automate And Provide Data Enrichment For Incident Response And Threat Hunting.

Section 11 - Implement Secure Network Operations Protocols

11.1 - Secure Network Operations Protocols

Network Address Allocation - In A Network, The Interface Address For Routers, Firewalls And Some Servers Are Best Assigned And Managed Manually, However For Client Workstations, Their Addresses Can Be Assigned Dynamically With The Use Of The Dynamic Host Configuration Protocol (Dhcp)

Dhcp Starvation Is A Type Of Dos Attack Where A Rogue Client Repeatedly Requests New Ip Addresses Using Spoofed Mac Addresses With The Aim Of Exhausting The Ip Address Pool Of The Dhcp Server.

As A Result, Clients Seeking An Ip Address Might Be Forced To Use A Rogue Dhcp Server That Has Been Setup By The Attacker.

Domain name resolution - the domain name system (dns) resolves fully qualified domain names (FQDNS) to ip addresses by making use of a distributed database

system that contains information on domains and hosts within those domains. Name servers work over port 53.

Domain hijacking - this is an attack where an adversary acquires a domain for a company's trading name or trademark or perhaps some spelling variation thereof. This can happen because domain names need to be re-registered every year.

uniform resource locator (url) redirection - a url is an address for the pages and files published as a website and consists of a FQDN, file path and script parameters.

url redirection refers to the use of http redirects to open a page other than the one the user requested.this is often used for legitimate purposes like redirecting a user from a broken link to the updated link.

However, if the redirect is not properly validated by the web application, an attacker can craft a phishing link that might appear legitimate to a naive user.

https://trusted.foo/login.php?url = "https://tru5ted.foo"

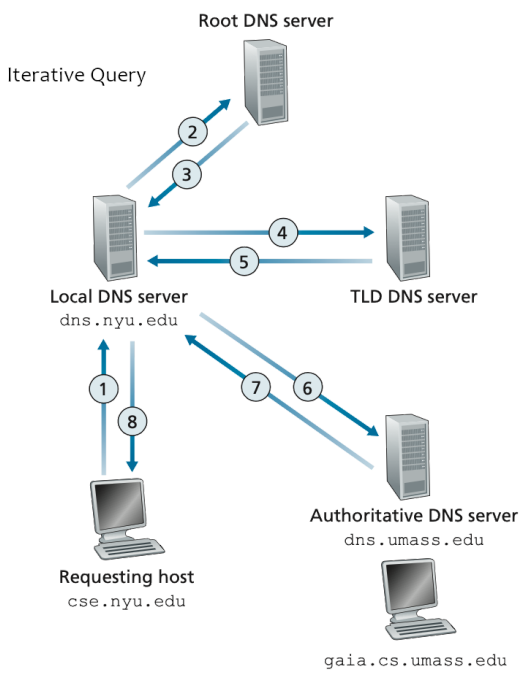
domain reputation - if a domain website has been hijacked and used for spam or distributing malware, the domain could end up being blacklisted.

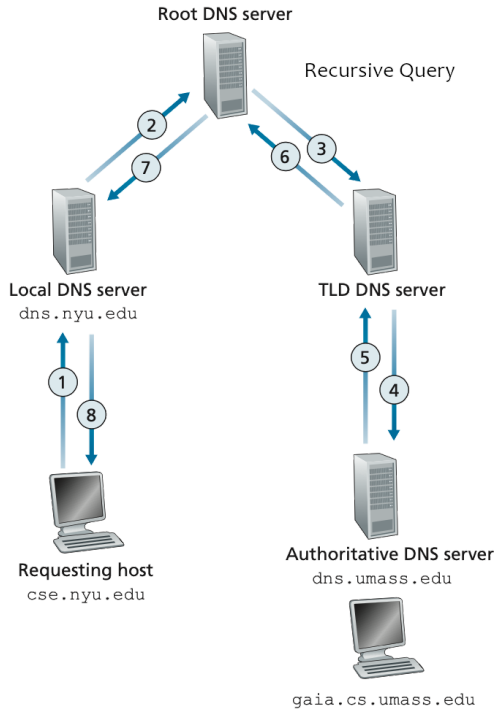
dns poisoning - this is an attack that compromises the process by which clients query name servers to locate the ip address for a fqdn.

- man in the middle - if the attacker has access to the same local network as the victim, the attacker can use arp poisoning to respond to dns queries from the victim with spoofed replies.

- dns client cache poisoning - here the attacker inserts fake information into the dns or web cache for the purpose of diverting traffic from a legitimate server to a malicious one. The attack is aimed primarily at the hosts text file.

- dns server cache poisoning - this aims to corrupt the records held by the dns server itself. This can be accomplished by performing dos against the server that holds the authorized records for the domain and then spoofing replies to requests from other name servers. the nslookup or dig tool can be used to query the name records and cached records held by a server to discover whether any false records have been inserted.





11.2 - Dns Security, Directory Services & Snmp

Dns Security - To Ensure Dns Security On A Private Network, Local Dns Servers Should Only Accept Recursive Queries From Local Authenticated Hosts And Not From The Internet.

Clients Should Be Restricted To Using Authorized Resolvers To Perform Name Resolution. Dns Footprinting Means Obtaining Information About A Private Network By Using Its Dns Server To Perform A Zone Transfer (All The Records In A Domain) To A Rogue Dns.

Dns Security Extensions (Dnssec) - These Help To Mitigate Against Spoofing And Poisoning Attacks By Providing A Validation Process For Dns Responses.

Secure Directory Services - A Network Directory Lists The Subjects (Users, Computers And Services) And Objects (Directories And Files) Available On The Network Plus The Permissions Subjects Have Over Objects.

Most Directory Services Are Based On The Lightweight Directory Access Protocol (Ldap) Running Over Port 389.

Authentication Referred To As Binding To The Server Can Be Implemented By:

- No Authentication - Anonymous Access Is Granted
- Simple Bind - The Client Must Supply Its Distinguished Name And Password In Plaintext
- Simple Authentication And Security Layer (Sasl) - The Client And Server Negotiate The Use Of A Supported Authentication Mechanism Such As Kerberos.
- Ldap Secure (Ldaps) - The Server Is Installed With A Digital Certificate Which It Uses To Setup A Secure Tunnel For The User Credential Exchange. Ldaps Use Port 636.

Generally Two Levels Of Access To The Directory Can Be Granted Which Are Read-Only Access (Query) And Read/Write Access (Update) And Is Implemented Using An Access Control Policy.

Time Synchronization - Many Network Applications Are Time Dependent And Time Critical. The Network Time Protocol (Ntp) Provides A Transport Over Which To Synchronize These Time Dependent Applications

Ntp Works Over Udp On Port 123.

Ntp Has Historically Lacked Any Sort Of Security Mechanism But There Are Moves To Create A Security Extension For The Protocol Called Network Time Security.

Simple Network Management Protocol (Snmp) Security - This Is A Widely Used Framework For Management And Monitoring And Consists Of An Snmp Monitor And Agents. The Agent Is A Process (Software Or Firmware) Running On A Switch, Router, Server Or Other Snmp-Compatible Network Device.

This Agent Maintains A Database Called A Management Information Base (Mib) That Holds Statistics Relating To The Activity Of The Device. The Agent Is Also Capable Of Initiating A Trap Operation Where It Informs The Management System Of A Notable Event Like Port Failure.

11.3 - Secure Application Operations Protocols

Hypertext Transfer Protocol & Web Services - Http Enables Clients To Request Resources From An Http Server. The Server Acknowledges The Request And Responds With The Data Or An Error Message.

Http Is A Stateless Protocol Which Means The Server Preserves No Information About The Client During A Session.

Transport Layer Security - To Implement Tls, A Server Is Assigned A Digital Certificate Signed By Some Trusted Ca. The Certificate Proves The Identity Of The Server And Validates The Server's Public/Private Key Pair.

The Server Uses Its Key Pair And The Tls Protocol To Agree Mutually Supported Ciphers With The Client And Negotiate An Encrypted Communications Session.

Ssl/Tls Version - A Server Can Provide Support For Legacy Clients Meaning A Tls 1.2 Server Could Be Configured To Allow Clients To Downgrade To Tls 1.1 Or 1.0

Cipher Suites - This Is A Set Of Algorithms Supported By Both The Client And Server To Perform The Different Encryption And Hashing Operations Required By The Protocol.

Prior To Tls 1.3, A Cipher Suite Would Be Written Like This

Ecdhe-Rsa-Aes128-Gcm-Sha256

This Means That The Server Can Use Elliptic Curve Diffie-Hellman Ephemeral Mode For A Session Key Agreement, Rsa Signatures, 128-Bit Aes-Gcm (Galois Counter Mode) For Symmetric Bulk Encryption And 256-Bit Sha For Hmac Functions.

11.4 - Remote Access Architecture

Most Remote Access Is Implemented As A Virtual Private Network (Vpn) Running Over The Internet But It Can Be More Difficult To Ensure The Security Of Remote Workstations And Servers Than Those On The Lan. A Vpn Can Also Be Deployed In A Site-To-Site Model To Connect Two Or More Private Networks And Is Typically Configured To Operate Automatically

Openvpn - This Is An Open Source Example Of A Tls Vpn. Openvpn Can Work In Tap (Bridged) Mode To Tunnel Layer 2 Frames Or In Tun (Routed) Mode To Forward Ip Packets.

Another Option Is Microsoft's Secure Sockets Tunneling Protocol (Sstp) Which Works By Tunneling Point-To-Point Protocol (Ppp) Layer 2 Frames Over A Tls Session.

Internet Protocol Security (Ipsec) - Tls Is Applied At The Application Level Either By Using A Separate Secure Port Or By Using Commands In The Application Protocol To Negotiate A Secure Connection.

Ipsec Operates At The Network Layer (Layer 3) So It Can Operate Without Having To Configure Specific Application Support.

Authentication Header (Ah) - This Performs A Cryptographic Hash On The Whole Packet Including The Ip Header Plus A Shared Secret Key And Adds This Hmac In Its Header As Integrity Check Value (Icv)

The Recipient Performs The Same Function On The Packet And Key And Should Derive The Same Value To Confirm That The Packet Has Not Been Modified.

Encapsulation Security Payload (Esp) - This Provides Confidentiality And/Or Authentication And Integrity. It Can Be Used To Encrypt The Packet Rather Than Simply Calculating An Hmac.

Esp Attaches Three Fields To The Packet: A Header, A Trailer (Providing Padding For The Cryptographic Function) And An Icv.

Ipsec Transport And Tunnel Modes - Ipsec Can Be Used In Two Modes:

- Transport Mode - This Mode Is Used To Secure Communications Between Hosts On A Private Network. Here The Ip Header For Each Packet Is Not Encrypted, Just The Payload Data. If Ah Is Used In This Mode, It Can Provide Integrity For The Ip Header.

- Tunnel Mode - This Mode Is Used For Communications Between Vpn Gateways Across An Unsecure Network And Is Also Referred To As Router

Implementation. With Esp, The Whole Ip Packet (Header And Payload) Is Encrypted And Encapsulated As A Datagram With A New Ip Header.

Internet Key Exchange (Ike) - Ipsec's Encryption And Hashing Functions Depend On A Shared Secret. The Secret Must Be Communicated To Both Hosts And The Hosts Must Confirm One Another's Identity (Mutual Authentication) Otherwise The Connection Is Vulnerable To Mitm And Spoofing Attacks. The Ike Protocol Handles Authentication And Key Exchange Referred To As Security Associations (Sa).

Ike Negotiations Take Place Over Two Phases:

- Phase 1 Establishes The Identity Of The Two Hosts And Performs Key Agreement Using The Dh Algorithm To Create A Secure Channel. Digital Certificates And Pre-Shared Key Are Used For Authenticating Hosts.
- Phase 2 Uses The Secure Channel Created In Phase 1 To Establish Which Ciphers And Key Sizes Will Be Used With Ah And/Or Esp In The Ipsec Session.

Vpn Client Configuration - To Configure A Vpn Client, You May Need To Install The Client Software If The Vpn Type Is Not Natively Supported By The Os.

Always-On Vpn - This Means That The Computer Establishes The Vpn Whenever An Internet Connection Over A Trusted Network Is Detected, Using The User's Cached Credentials To Authenticate.

When A Client Connected To A Remote Access Vpn Tries To Access Other Sites On The Internet, There Are Two Ways To Manage The Connection:

Split Tunnel - The Client Accesses The Internet Directly Using Its "Native" Ip Configuration And Dns Servers.

Full Tunnel - Internet Access Is Mediated By The Corporate Network, Which Will Alter The Client's Ip Address And Dns Servers And May Use A Proxy.

Full Tunnel Offers Better Security But The Network Address Translations And Dns Operations Required May Cause Problems With Some Websites Especially Cloud Services.

Out-Of-Band Management - Remote Management Methods Can Be Described As Either In-Band Or Out-Of-Band (Oob).

An In-Band Management Link Is One That Shares Traffic With Other Communications On The "Production" Network While A Serial Console Or Modem Port On A Router Is A Physically Out-Of-Band Management Method.

Secure Shell - This Is The Principal Means Of Obtaining Secure Remote Access To A Command Line Terminal. Mostly Used For Remote Administration And Secure File Transfer (Sftp).

Ssh Servers Are Identified By A Public/Private Key Pair (The Host Key).

Section 12 - Implement Host Security Solutions

12.1 - Hardware Root Of Trust & Boot Integrity

A hardware root of trust (rot) or trust anchor is a secure subsystem that is able to provide attestation. attestation means that a statement made by the system can be trusted by the receiver.

The ROT is usually established by a cryptoprocessor known as a trusted platform module (TPM) which is implemented either as part of the chipset or as an embedded function of the cpu.

Each TPM is hard-coded with a unique unchangeable asymmetric private key called the endorsement key which can be used to create various other types of subkeys used in key storage, signature and encryption operations.

In windows, a TPM can be managed via the tpm.msc console or through group policy.

A major concern with establishing a rot is that devices are used in environments where anyone can get complete control over them.

UEFI - most pcs and smartphones implement the unified extensible firmware interface (uefi). uefi provides the code that allows the host to boot to an os and can also enforce a number of boot integrity checks.

secure boot - this is designed to prevent a computer from being hijacked by a malicious os.

UEFIis configured with digital certificates from valid OS vendors so the system firmware will check the OS boot loader and kernel using the stored certificate to ensure that it has been digitally signed by the OS vendor.

measured/trusted boot - this uses platform configuration registers (PCRS) in the TPM at each stage in the boot process to check whether hashes of key system state data (boot firmware, boot loader, os kernel and critical drivers) have changed.

it won't prevent the system from booting but will record the presence of unsigned kernel-level code.

boot attestation - this is the capability to transmit a boot log report signed by the TPM via a trusted process to a remote server.

This report can be analyzed for signs of compromise and the host can be prevented from accessing the network if it does not meet the required health policy or if no attestation report is received.

12.2 - Disk Encryption

Full Disk Encryption (Fde) - This Means That The Entire Contents Of The Drive Including System Files And Folders Are Encrypted. Fde Requires The Secure Storage Of The Key Used To Encrypt The Drive Contents And Is Normally Stored In A Tpm.

A Drawback Of Fde Is That Performance Is Reduced Because The Os Performs The Cryptographic Operations. This Issue Can Be Mitigated By Self-Encrypting Drives (Sed) Where The Cryptographic Operations Are Done By The Drive Controller.

Self-Encrypting Drives (Sed) - Sed Uses A Symmetric Data/Media Encryption Key (Dek/Mek) For Bulk Encryption And Stores The Dek Securely By Encrypting It With An Asymmetric Key Pair Called The Authentication Key Or Key Encryption Key (Kek)

Usb & Flash Drive Security

- Devices Of An Unknown Origin Or History Should Not Be Plugged In.
- Hosts Should Always Be Configured To Prevent Autorun When Usb Devices Are Attached.
- Usb Ports Can Also Be Blocked Using Most Types Of Hids.

12.3 - Third-Party Risk Management & Security Agreements

A Root Of Trust Is Only Trustworthy If The Vendor Has Implemented It Properly. Anyone With Time And Resources To Modify The Computer's Firmware Could Create Some Sort Of Backdoor Access.

For A Tpm To Be Trustworthy, The Supply Chain Of Chip Manufacturers, Firmware Authors And The Administrative Staff Responsible For Providing The Computing Device To The User Must All Be Trustworthy.

When Assessing Suppliers For Risk, It Is Helpful To Distinguish Two Types Of Relationship

- Vendor - This Means A Supplier Of Commodity Goods And Services Possibly With Some Level Of Customization And Direct Support.
- Business Partner - This Implies A Closer Relationship Where Two Companies Share Quite Closely Aligned Business Goals.

End Of Life Systems - When A Manufacturer Discontinues The Sales Of A Product, It Enters An End Of Life (Eol) Phase In Which Support And Availability Of Spares And Updates Become More Limited.

An End Of Service Life (Eosl) System Is One That Is No Longer Supported By Its Developer Or Vendor.

Windows Versions Are Given Five Years Of Mainstream Support And Five Years Of Extended Support (During Which Only Security Updates Are Provided).

Organizational Security Agreements - It Is Important To Remember That Although One Can Outsource Virtually Any Service To A Third Party, One Cannot Outsource Legal Accountability For These Services.

Issues Of Security Risk Awareness, Shared Duties And Contractual Responsibilities Can Be Set Out In A Formal Legal Agreement.

- memorandum of understanding (MOU) - a preliminary agreement to express an intent to work together. They are usually intended to be relatively informal and not contract binding.

- business partnership agreement (BPA) - the most common model of this in it are the agreements between large companies and their resellers and solution providers.

- nondisclosure agreement (NDA) - used between companies and employees/contractors/other companies as a legal basis for protecting information assets.

- service level agreement (SLA) - a contractual agreement describing the terms under which a service is provided.

- measurement systems analysis (MSA) - a means of evaluating the data collection and statistical methods used by a quality management process to ensure they are robust.

12.4 - Endpoint Security

Hardening - This Is The Process Of Putting An Os Or Application In A Secure Configuration However Hardening Must Be Balanced Against The Access Requirements And Usability In A Particular Situation.

The Essential Principle Is Of Least Functionality Meaning The System Should Run Only The Protocols And Services Required By Legit Users And No More.

Interfaces, Services And Application Service Ports Not In Use Should Be Disabled.

Patch Management - On Residential And Small Networks, Hosts Can Be Configured To Auto-Update Either By The Windows Update Process Or In Linux With The Commands Yum-Cron Or Apt Unattended-Upgrades Depending On The Package Manager Used By The Distribution.

Patches Can Become Incompatible With A Particular Application And Cause Availability Issues. Update Repositories Can Also Be Infected With Malware That Can Then Be Spread Via Automatic Updates.

Antivirus (A-V)/ Anti-Malware - First Generation Of Antivirus Scanned For Only Viruses But Today They Can Perform Generalized Malware Detection.

While A-V Software Remains Important, Signature-Based Detection Is Widely Regarded To Be Insufficient For The Prevention Of Data Breaches.

Host-Based Intrusion Detection/Prevention (Hids/Hips) - Hids Provide Threat Detection Via Logs And File System Monitoring. Other Products May Also Monitor Ports And Network Interfaces And Process Data And Logs Generated By Specific Applications Such As Http Or Ftp.

Endpoint Protection Platform (Epp) - An Epp Is A Single Agent Performing Multiple Security Tasks, Including Malware/Intrusion Detection And Prevention But Also Other Features Such As Firewall, Web Content Filtering And File/Message Encryption.

Sandboxing - This Is A Technique That Isolates An Untrusted Host Or App In A Segregated Environment To Conduct Tests. Sandbox Offers More Than Traditional Anti-Malware Solutions Because You Can Apply A Variety Of Different Environments To The Sandbox Instead Of Just Relying On How The Malware Might Exist In Your Current Configuration.

12.5 - Embedded Systems

This Is A Complete System Designed To Perform A Specific Dedicated Function.

These Systems Can Be A Microcontroller In A Small Device Or Could Be As Large And Complex As The Network Of Control Devices Managing A Water Treatment Plant.

Embedded Systems Are Characterized As Static Environments While A Pc Is A Dynamic Environment Because Both Software And Hardware Changes Can Be Made By The User.

Embedded Systems Are Usually Constrained By:

- Processor Capability
- System Memory
- Persistent Storage
- Cost
- Power (Battery)

- Authentication Technologies
- Cryptographic Identification
- Network And Range Constraints

System On Chip - This Is A System Where All Processors, Controllers And Devices Are Provided On A Single Processor Die Or Chip. This Is Often Very Power Efficient And Is Commonly Used With Embedded Systems.

Raspberry Pi And Arduino Are Examples Of Soc Boards Initially Devised As Educational Tools But Now Widely Used For Industrial Applications And Hacking.

Field Programmable Gate Array (Fpga) - As Many Embedded Systems Perform Simple And Repetitive Operations, It Is More Efficient To Design The Hardware Controller To Perform Only The Instructions Needed.

An Example Of This Is The Application-Specific Integrated Circuits (Asics) Used In Ethernet Switches But They Can Be Quite Expensive And Work Only For A Single Application.

An Fpga Solves The Problem Because The Structure Is Not Fully Set At The Time Of Manufacture Giving The End Customer The Ability To Configure The Programming Logic Of The Device To Run A Specific Application.

Operational Technology (Ot) Networks - These Are Cabled Networks For Industrial Applications And Typically Use Either Serial Data Protocols Or Industrial Ethernet.

Industrial Ethernet Is Optimized For Real-Time And Deterministic Transfers.

Cellular Networks - A Cellular Network Enables Long-Distance Communication Over The Same System That Supports Mobile And Smartphones.

Also Known As Baseband Radio And There Are Two Main Radio Technologies:

- Narrowband-Iot (Nb-Iot) - This Refers To Low-Power Version Of The Long Term Evolution (Lte) Or 4g Cellular Standard.
- Lte Machine Type Communication (Lte-M) - This Is Another Low-Power System But Supports Higher Bandwidth (Up To About 1 Mbps)

Any Lte-Based Cellular Radio Uses A Subscriber Identity Module (Sim) Card As An Identifier. The Sim Is Issued By A Cellular Provider With Roaming To Allow The Use Of Other Supplier's Tower Relays.

12.6 - Industrial Control Systems & Internet Of Things

Industrial Systems Have Different Priorities To It Systems And Tend To Prioritize Availability And Integrity Over Confidentiality (Reversing The Cia Triad As The Aic Triad)

Workflow And Process Automation Systems - Industrial Control Systems (Icss) Provide Mechanisms For Workflow And Process Automation And These Systems Control Machinery Used In Critical Infrastructure Like Power And Water Suppliers And Health Services.

An Ics Comprises Plant Devices And Equipment With Embedded PLCs.

Supervisory Control And Data Acquisition (SCADA) - A SCADA System Takes The Place Of A Server In Large Scale Multiple-Site Icss. Scada Typically Run As Software On Ordinary Computers, Gathering Data From And Managing Plant Devices And Equipment With Embedded Plcs Referred To As Field Devices.

Ics/Scada Applications - These Types Of Systems Are Used Within Many Sectors Of Industry

- Power Generation And Distribution
- Mining And Refining Raw Materials
- Fabrication And Manufacturing
- Logistics
- Site And Building Management Systems

Internet Of Things (Iot) - This Is Used To Describe A Global Network Of Appliances And Personal Devices That Have Been Equipped With Sensors, Software And Network Connectivity.

12.7 - Specialized Systems

A Specialized System Refers To The Use Of Embedded Systems And/Or Iot Devices For A Specific Purpose Or Application. They Can Be Used In

- Building Automation System (Bas)
- Smart Meters
- Surveillance Systems
- Multifunction Printers (Mfps)
- Voice Over Ip (Voip)

- Automobiles And Uavs
- Medical Devices

Security For Embedded Systems Include:

- Network Segmentation
- Wrappers
- Firmware Code Control & Inability To Patch

Section 13 - Implement Secure Mobile Solutions

13.1 - Mobile Device Management

Mobile Device Deployment Models Include

- Bring Your Own Device (BYOD) - The Mobile Device Is Owned By The Employee And Will Have To Meet Whatever Security Profile Is Required. It's The Most Common Model For Employees But Poses The Most Difficulties For Security Managers.

- Corporate Owned Business Only (COBO) - The Device Is Owned By The Company And May Only Be Used For Company Business.

- Corporate Owned, Personally-Enabled (COPE) - The Employee May Use It To Access Personal Email ,Social Media Accounts And For Some Personal Web Browsing.

- Choose Your Own Device (CYOD) - Very Similar To Cope Except That Here, The Employee Is Given A Choice Of Device From A List.

Enterprise Mobility Management (EMM) - This Is A Class Of Management Software Designed To Apply Security Policies To The Use Of Mobile Devices And Apps In An Enterprise.

- Mobile Device Management (Mdm) - Sets Device Policies For Authentication, Feature Use (Camera And Microphone) And Connectivity. Mdm Also Allows Device Resets And Remote Wipes.
- Mobile Application Management (Mam) - Sets Policies For Apps That Can Process Corporate Data And Prevents Data Transfer To Personal Apps.

ios in the enterprise - in apple's ios ecosystem, third-party developers can create apps using apple's software development kit available only on macos.

Corporate control over ios devices and distribution of corporate and b2b apps is facilitated by participating in the device enrollment program, the volume purchase program and the developer enterprise program.

android in the enterprise - android is open source meaning there is more scope for vendor-specific versions and the app model is far more relaxed.

The sdk is available on linux, windows and macos.

mobile access control systems - if a threat actor is able to gain access to a smartphone, they might be able to gain access to plenty of confidential data as well as cached passwords for email, social media etc.

smartphone authentication - access control can be implemented by configuring a screen lock that can be bypassed using a password, pin or swipe pattern. Some devices also support biometrics like fingerprint readers.

screen lock - the screen lock can also be configured with a lockout policy. For example, the device can be locked out for a period of time after a certain number of incorrect password attempts.

context-aware authentication - smartphones now allow users to disable screen locks when the device detects it is in a trusted location (home) however an enterprise may seek more stringent access controls to prevent misuse of a device.

For example, even if a device has been unlocked, the user might need to reauthenticate in order to access the corporate workspace.

remote wipe - if the phone is stolen, it can be set to factory defaults or cleared of any personal data with the use of the remote wipe feature. it can also be triggered by several incorrect password attempts.

In theory, the thief could prevent the remote wipe by ensuring the phone cannot connect to the network then hacking the phone and disabling its security.

full device encryption & external media - in ios, there are various levels of encryption:

- all user data on the device is always encrypted but the key is stored on the device. It's this key that is deleted in a remote wipe to ensure the data is inaccessible.
- Email data and any apps using the "data protection" option are subject to a second round of encryption using a key derived from the user's credential.

location services - location services make use of two systems:

- global positioning system (gps) - means of determining the device's latitude and longitude based on information received from satellites via a gps sensor.
- indoor positioning system (ips) - works out a device's location by triangulating its proximity to other radio sources such as cell towers and wi-fi access points.

geofencing and camera /microphone enforcement - geofencing is the practice of creating a virtual boundary based on real-world geography and can be a useful tool for controlling the use of camera or video functions or applying context-aware authentication.

GPS tagging - this is the process of adding geographical identification metadata such as latitude and longitude, photographs, sms messages, video and so on.

GPS tagging is highly sensitive personal information and potentially confidential organizational data also.

content management - containerization allows the employer to manage and maintain the portion of the device that interfaces with the corporate network. a container can also enforce storage segmentation where the container will be associated with a directory.

rooting & jailbreaking

- rooting - associated with android devices and typically involves using custom firmware
- jailbreaking - associated with ios and is accomplished by booting the device with a patched kernel
- carrier unlocking - for either ios or android and it means removing the restrictions that lock a device to a single carrier.

Rooting or jailbreaking mobile devices involves subverting the security measures on the device to gain super administrative access to it but also has the side effect of permanently disabling certain security features.

13.2 - Secure Mobile Device Connections

Personal Area Networks (PANs) - these enable connectivity between a mobile device and peripherals. ad hoc (peer-to-peer) networks between mobile devices or between mobile devices and other computing devices can also be established

For corporate security, these peer-to-peer functions should generally be disabled.

ad hoc wi-fi and wi-fi direct - an ad hoc network involves a set of wireless stations establishing peer-to-peer connections with one another rather than using an access point.

wi-fi directly allows one-to-one connections between stations though one of them will serve as a soft access point.

tethering and hotspots - a smartphone can share its internet connection with other devices via wi-fi making it a hotspot.

where the connection is shared by connecting the smartphone to a pc via usb or bluetooth, it can be referred to as tethering.

bluetooth connection methods

- device discovery - allows the device to connect to any other bluetooth devices nearby.
- authentication & authorization - use of a simple passkey to "pair" connecting devices
- malware

Bluetooth connection methods - discoverable devices are vulnerable to bluejacking, where the spammer sends unsolicited messages to the device.

bluesnarfing refers to using an exploit in bluetooth to steal information from someone else's phone.

Infrared & rfid connection methods - infrared has been used for pan but it's use in modern smartphones and wearable technology focuses on two other uses:

- ir blaster - this allows the device to interact with an ir receiver and operate a device such as a tv as though it were the remote control.
- ip sensor - these are used as proximity sensors and to measure health information (heart rate & blood oxygen levels).

radio frequency id (rfid) is a means of encoding information into passive tags which can easily be attached to devices, clothing and almost anything else.

Skimming involves using a fraudulent rfid reader to read the signals from a contactless bank card

Microwave radio connection methods - microwave radio is used as a backhaul link from a cell tower to the service provider's network and these links are important to 5g where many relays are required and provisioning fiber optic cable backhaul can be difficult.

a microwave link can be provisioned in two modes:

- point-to-point (p2p) - microwave uses high gain antennas to link two sites and each antenna is pointed directly at the other. It's very difficult to eavesdrop on the signal as an intercepting antenna would have to be positioned within the direct path.

- point-to-multipoint (p2m) - microwave uses smaller sectoral antennas each covering a separate quadrant. p2m links multiple sites to a single hub and this can be cost-efficient in high density urban areas.

Section 14 - Application Attacks

14.1 - Privilege Escalation & Error Handling

Application Attack - This Attacks A Vulnerability In An Os Or Application And A Vulnerability Refers To A Design Flaw That Can Cause The Application Security System To Be Circumvented Or To Crash. The Purpose Of This Attack Is To Allow The Attacker To Run His/Her Own Code On The System And This Is Referred To As Arbitrary Code Execution.

Where The Code Is Transmitted From One Computer To Another, This Is Referred To As Remote Code Execution.

Privilege Escalation - A Design Flaw That Allows A Normal User Or Threat Actor To Suddenly Gain Extended Capabilities Or Privileges On A System.

- Vertical Privilege Escalation - The User Or Application Is Able To Gain Access To Functionality Or Data That Shouldn't Be Available To Them.
- Horizontal Privilege Escalation - The User Or Application Is Able To Access Data Or Functionality Intended For Another User.

Error Handling - An Application Attack May Cause An Error Message. As Such Applications In The Event Of An Error Should Not Reveal Configuration Or Platform Details That Can Help The Attacker.

Improper Input Handling - Good Programming Practice Dictates That Any Input Accepted By A Program Or Software Must Be Tested To Ensure That It Is Valid. Most Application Attacks Work By Passing Invalid Or Maliciously Constructed Data To The Vulnerable Process.

14.2 - Overflows, Resource Exhaustion, Memory Leaks & Race Conditions

Buffer overflow - a buffer is an area of memory reserved by the application to store working data. the attacker passes data that deliberately overfills the buffer. One of the most common vulnerabilities is stack overflow.

Integer overflow - an integer is a whole number and integers are used as a valid data type with fixed lower and upper bounds. an integer flow attack causes the target software to calculate a value that exceeds these bounds and can even cause a positive number to become negative.

eternal blue is an example of an attack that uses vulnerabilities in integer overflow to gain system privileges on a windows host.

null pointer dereferencing & race conditions - in c/c++ programming, a pointer is a variable that stores a memory location rather than a value. attempting to read/write that memory address via the pointer is called dereferencing.

if the memory location is invalid or null this can create a null pointer dereference and cause the process to crash and in other cases might allow the threat actor to run arbitrary code.

A race condition is a way of engineering a null pointer dereference exception.

This occurs when the outcome from an execution process is directly dependent on the order and timing of certain events and those events fail to execute in the order and timing intended by the developer.

memory leaks & resource exhaustion - a process should release its block of memory used when it no longer requires it but if it doesn't, it can lead to memory leaks. such a situation can lead to less memory available for other applications and could lead to a system crash.

resources refer to cpu time, system memory, fixed disk capacity & network utilization. a malicious process could spawn multiple looping threads to use cpu time or write thousands of files to disk.

dll injection & driver manipulation - dll (dynamic link library) is a binary package that implements some sort of standard functionality such as establishing a network connection or performing cryptography.

The main process of a software application is likely to load several DLLS during the normal course of operations.

DLL injection is a vulnerability where the OS allows one process to attach to another and a malware can force a legitimate process to load a malicious link library.

To perform dll injection, the malware must already be operating with sufficient privileges and evade detection by anti-virus software.

Avoiding detection is done through a process called code refactoring where the code performs the same function by using different methods (variable types and control blocks).

pass the hash attack - pth is the process of harvesting an account's cached credentials when the user is logged into a single sign-on (sso) system so the attacker can use the credentials on other systems.

If the attacker can obtain the hash of the user password, it is possible to use it (without cracking) to authenticate to network protocols that accept ntlm (windows new technology lan manager) hashes as authentication credentials.

14.3 - Uniform Resource Locator Analysis & Percent Encoding

Uniform Resource Locator Analysis - Besides Pointing To The Host Or Service Location On The Internet, A Url Can Encode Some Action Or Data To Submit To The Server Host. This Is A Common Vector For Malicious Activity.

Http Methods - It Is Important To Understand How Http Operates.

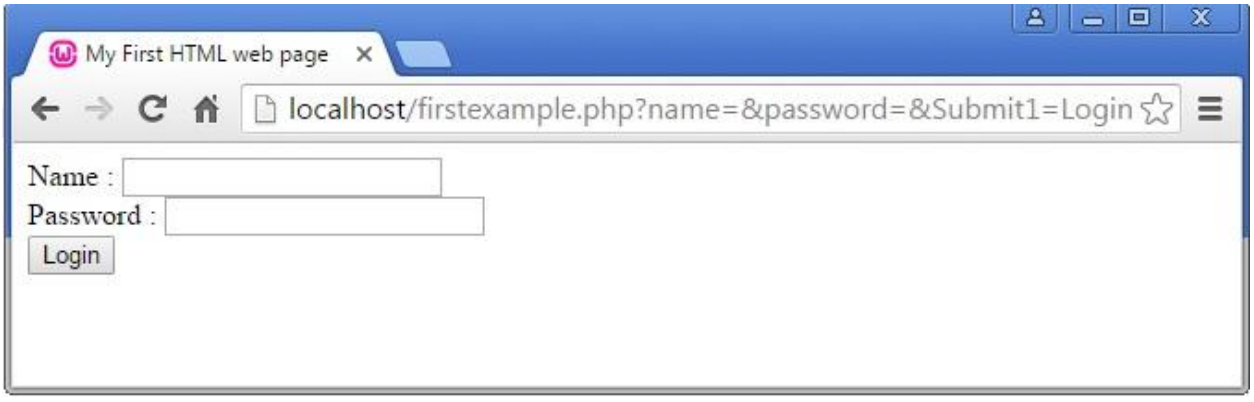
- An Http Session Starts With A Client (Web Browser) Making A Request To An Http Server.
- The Connection Establishes A Tcp Connection
- The Connection Can Be Used For Multiple Requests Or A Client Can Start New Tcp Connections For Different Requests.

A Request Typically Contains A Method, Resource (Url Path), Version Number, Headers And Body. The Principal Method Is Get But Other Methods Include:

- Post - Send Data To The Server For Processing By The Requested Resource
- Put - Create Or Replace The Resource. Delete Can Be Used To Remove The Resource
- Head - Retrieve The Headers For A Resource Only (Not The Body)

Data Can Be Submitted To The Server Using A Post Or Put Method And The Http Headers And Body Or By Encoding The Data Within The Url Used To Access The Resource.

Data Submitted Via A Url Is Delimited By The ? Character Which Follows The Resource Path And Query Parameters Are Usually Formatted As One Or More Name=Value Pairs, With Ampersands Delimiting Each Pair.



Percent Encoding - A Url Can Contain Only Unreserved And Reserved Characters From The Ascii Set. Reserved Ascii Characters Are Used As Delimiters Within The Url Syntax.

Reserved Characters : / ? # [ ] @ ! $ & ' ( ) * + , ; =

There Are Also Unsafe Characters Which Cannot Be Used In A Url. Control Characters Such As Null String Termination, Carriage Return, Line Feed, End Of File And Tab Are Unsafe.

Character	Percent Encoding
null	%00
space	%20
CR (Carriage Return)	%0D
LF (Line Feed)	%0A
+	%2B
%	%25
/	%2F
\	%5C
.	%2E
?	%3F
"	%22
'	%27
<	%3C
>	%3E
&	%26
|	%7C

14.4 - Api & Replay Attacks, Cross-Site Request Forgery, Clickjacking & Ssl Strip Attacks

Application Programming Interface Attacks - Web Applications And Cloud Services Implement Application Program Interfaces (Apis) To Allow Consumers To Automate Services.

If The Api Isn't Secure, Threat Actors Can Easily Take Advantage Of It To Compromise The Services And Data Stored On The Web Application. Api Calls Over Plain Http Are Not Secure And Could Easily Be Modified By A Third Party.

Some Other Common Attacks Against Apis Include

- Ineffective Secrets Management, Allowing Threat Actors To Discover An Api Key And Perform Any Action Authorized To That Key.
- Lack Of Input Validation Allowing The Threat Actor To Insert Arbitrary Parameters Into Api Methods And Queries. This Is Often Referred To As Allowing Unsanitized Input.
- Error Messages Revealing Clues To A Potential Adversary. (Username/Password)
- Denial Of Service (Dos) By Bombarding The Api With Bogus Calls.

Replay Attacks - Session Management Enables Web Applications To Uniquely Identify A User Across A Number Of Different Actions And Requests.

To Establish A Session, The Server Normally Gives The Client Some Type Of Token And A Replay Attack Works By Sniffing Or Guessing The Token Value And Then Submitting It To Re-Establish The Session Illegitimately.

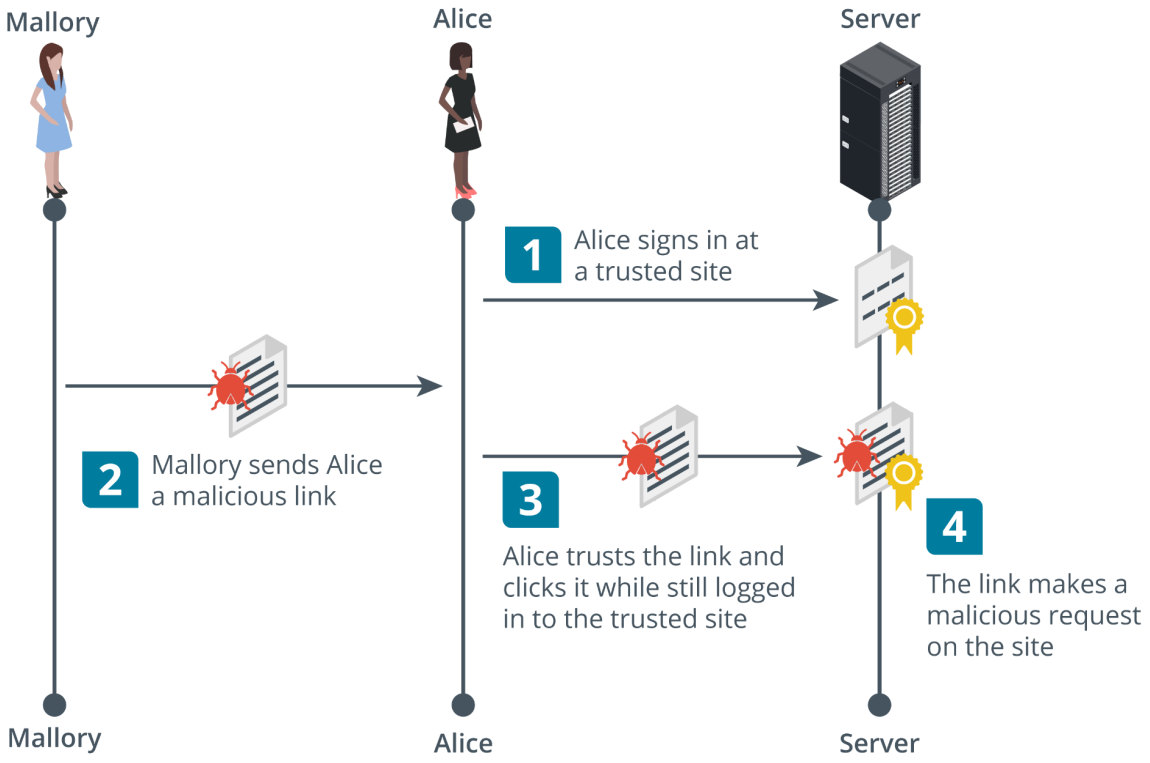
Http By Default Is A Stateless Protocol Meaning The Server Preserves No Information About The Client But Cookies Allow For The Preservation Of Data.

A Cookie Has A Name, Value And Optional Security And Expiry Attributes. Cookies Can Either Be Persistent And Non-Persistent.

Cross-Site Request Forgery - A Client-Side Or Cross-Site Request Forgery (Csrf Or Xsrf) Can Exploit Applications That Use Cookies To Authenticate Users And Track Sessions.

In Order To Work, The Attacker Must Convince The Victim To Start A Session With The Target Site. The Attacker Must Then Pass An Http Request To The Victim's

Browser That Spoofs An Action On The Target Site Such As Changing A Password Or An Email Address.



If The Target Site Assumes The Browser Is Authenticated Because There Is A Valid Session Cookie, It Will Accept The Attacker's Input As Genuine.

This Is Also Referred To As A Confused Deputy Attack.

Clickjacking - This Is An Attack Where What The User Sees And Trusts As A Web Application With Some Sort Of Login Page Or Form Contains A Malicious Layer Or Invisible Iframe That Allows An Attacker To Intercept Or Redirect User Input.

Clickjacking Can Be Launched Using Any Type Of Compromise That Allows The Adversary To Run Arbitrary Code As A Script. It Can Be Mitigated By Using Http Response Headers That Instruct The Browser Not To Open Frames From Different Origins

Ssl Strip - This Is Launched Against Clients On A Local Network As They Try To Make Connections To Websites. The Threat Actor First Performs A Mitm Attack Via Arp Poisoning To Masquerade As The Default Gateway.

When A Client Requests An Http Site That Redirects To An Https Site In An Unsafe Way, The Sslstrip Utility Proxies The Request And Response, Serving The Client The Http Site With An Unencrypted Login Form Thus Capturing Any User Credentials.

14.5 - Injection Attacks

XML and LDAP injection attacks - an injection attack can target other types of protocols where the application takes user input to construct a query, filter or document.

extensible markup language (xml) injection - xml is used by apps for authentication and authorizations and for other types of data exchange and uploading.

lightweight directory access protocol (ldap) injection - ldap is another example of query language. ldap is specifically used to read and write network directory databases. a threat actor could exploit either unauthenticated access or a vulnerability in a client app to submit arbitrary ldap queries. This could allow accounts to be created or deleted or for the attacker to change authorizations and privileges.

for example a web form could construct a query from authenticating the valid credentials for bob and pa$$w0rd like this:

(& (username = bob)(password = pa$$w0rd))

if the form input is not sanitized, the threat actor could bypass the password check by entering a valid username plus an ldap filter string

(& (username = bob)(&))

Directory traversal & command injection attacks - directory traversal is another type of injection attack performed against a web server.

The threat actor submits a request for a file outside the web server's root directory by submitting a path to navigate to the parent directory (../)

The threat actor might use a canonicalization attack to disguise the nature of the malicious input.

canonicalization refers to the way the server converts between different methods by which a resource (file path or url) may be represented and submitted to the simplest method used by the server to process the input.

server-side request forgery (SSRF) - SSRF causes the server application to process an arbitrary request that targets another service either on the same host or a different one.

It exploits both the lack of authentication between the internal servers and services and weak input validation allowing the attacker to submit unsanitized requests or api parameters.

14.6 - Secure Coding Techniques

Input Validation - Malicious Input Could Be Crafted To Perform An Overflow Attack Or Some Type Of Script Or Sql Injection Attack.

To Mitigate This, There Should Be Routines To Check User Input And Anything That Does Not Conform To What Is Required Must Be Rejected.

Normalization And Output Encoding - Normalization Means That A String Is Stripped Of Illegal Characters Or Substrings And Converted To The Accepted Character Set. This Ensures That The String Is In A Format That Can Be Processed Correctly By The Input Validation Routines.

Output Encoding Means That A String Is Re-Encoded Safely For The Context In Which It Is Being Used.

Server-Side Versus Client-Side Validation - A Web Application Can Be Designed To Perform Code Execution And Input Validation Locally (On The Client) Or Remotely (On The Server).

The Main Issue With Client-Side Validation Is That The Client Will Always Be More Vulnerable To Some Sort Of Malware Interfering With The Validation Process.

Main Issue With Server-Side Validation Is That It Can Be Time-Consuming As It May Involve Multiple Transactions Between The Server And Client.

Client-Side Validation Is Usually Restricted To Informing The User That There Is Some Sort Of Problem With The Input Before Submitting It To The Server. Relying On Client-Side Validation Only Is Poor Programming Practice.

Web Application Security In Response Headers

A Number Of Security Options Can Be Set In The Response Header

- Http Strict Transport (Hsts) - Forces Browser To Connect Using Https Only, Mitigating Downgrade Attacks Such As Ssl Stripping.
- Content Security Policy (Csp) - Mitigates Clickjacking, Script Injection And Other Client-Side Attacks.
- Cache Control - Sets Whether The Browser Can Cache Responses. Preventing Caching Of Data Protects Confidential And Personal Information Where The Client Device Might Be Shared By Multiple Users.

Data Exposure And Memory Management - Data Exposure Is A Fault That Allows Privileged Information Such As A Password Or Personal Data To Be Read Without Being Subject To The Appropriate Access Controls.

A Well-Written Application Must Be Able To Handle Errors And Exceptions Gracefully. Ideally The Programmer Should Have Written A Structured Exception Handler (Seh) To Dictate What The Application Should Then Do.

The Error Must Not Reveal Any Platform Information Or Inner Workings Of The Code To An Attacker.

Secure Code Usage - A Program May Make Use Of Existing Code In The Following Ways:

- Code Reuse - Using A Block Of Code From Elsewhere In The Same Application Or From Another Application To Perform A Different Function.
- Third-Party Library - Using A Binary Package (Such As A Dynamic Link Library) That Implements Some Sort Of Standard Functionality Such As Establishing A Network Connection.
- Software Development Kit (Sdk) - Using Sample Code Or Libraries Of Pre-Built Functions From The Programming Environment Used To Create The Software.
- Stored Procedures - Using A Pre-Built Function To Perform A Database Query.

unreachable code and dead code

unreachable code is a part of application source code that can never be executed (if ... then conditional logic that is never called because the conditions are never met).

dead code is executed but has no effect on the program flow (a calculation is performed but the result is never stored as a variable or used to evaluate a condition).

static code analysis - this is performed against the application code before it is packaged as an executable process. The software will scan the source code for signatures of known issues.

Human analysis of software source code is described as a manual code review. It is important that the code be reviewed by developers other than the original coders to try to identify oversights, mistaken assumptions or a lack of experience.

dynamic code analysis - static code review will not reveal any vulnerabilities that exist in the runtime environment. dynamic analysis means that the application is tested under real world conditions using a staging environment.

fuzzing is a means of testing that an application‘s input validation routines work well. fuzzing will deliberately generate large amounts of invalid or random data and record the responses made by the application.

associated with fuzzing is the concept of stress testing an application to see how an application performs under extreme performance or usage scenarios.

Finally, the fuzzer needs some means of detecting an application crash and recording which input sequence generated the crash.

14.7 - Implementing Secure Script Environments

Automation Using Scripting Means That Each Configuration Is Performed By A Block Of Code. A Script Will Use The Following:

- Parameters That The Script Takes As Input Data
- Branching And Looping Statements That Can Alter The Flow Of Execution Based On Logic Conditions
- Validation And Error Handlers To Check Inputs And Ensure Robust Execution
- Unit Tests To Ensure That The Script Returns The Expected Outputs Given The Expected Inputs.

Powershell Script Environment - Powershell Is The Preferred Method Of Performing Windows Administration Tasks.

Cmdlets And Functions - A Cmdlet Is A Compiled Library That Exposes Some Configuration Or Administrative Task. Most Powershell Usage Is Founded On Cmdlets. Powershell Also Supports A Wider Range Of Branching And Looping Structures Than Python Including The Switch And Do Statements.

Execution Control - This Is The Process Of Determining What Additional Software Or Scripts May Be Installed Or Run On A Host Beyond Its Baseline.

- Allow List - A Highly Restrictive Policy That Means Only Running Authorized Processes And Scripts.
- Block List - A Permissive Policy That Only Prevents Execution Of Listed Processes And Scripts. It Is Vulnerable To Software That Has Not Previously Been Identified As Malicious.

Code Signing - This Is The Principal Means Of Proving The Authenticity And Integrity Of Code. The Developer Creates A Cryptographic Hash Of The File Then Signs The Hash Using His/Her Private Key.

The Program Is Shipped With A Copy Of The Developer's Code Signing Certificate Which Contains A Public Key That The Destination Computer Uses To Read And Verify The Signature.

Os-Based Execution Control - Execution Control Is Often Enforced By A Third-Party Product But There Are Some Built-In Windows Features That Can Perform The Task.

- Software Restriction Policies (Srp)
- Applocker - Improves Configuration Options And Default Usage Of Srp.
- Windows Defender Application Control (Wdac) - Can Be Used To Create Code Integrity (Ci) Policies Which Can Be Used On Their Own Or In Conjunction With Applocker.
- Unit Tests To Ensure That The Script Returns The Expected Outputs Given The Expected Inputs.

In Linux, Execution Control Is Normally Enforced By Using A Mandatory Access Control (Mac) Kernel Module Or Linux Security Module (Lsm). The Two Main Lsms Are Selinux And Apparmor.

Malicious Code Indicators

- Shellcode - Minimal Program Designed To Exploit A Buffer Overflow Or Similar Vulnerability To Gain Privileges
- Credential Dumping - Malware Might Try To Access The Credentials File Or Sniff Them In The Memory.
- Lateral Movement/Insider Attack - The General Process Is To Use The Foothold To Execute A Process Remotely Then Try To Widen Access By Changing The System Configuration.
- Persistence - Allows The Threat Actor's Backdoor To Be Restarted If The Host Reboots Or The User Logs Off And On.

Man-In-The-Browser Attack - A Mitb Attack Is A Specific Type Of On-Path Attack Where The Web Browser Is Compromised. Depending On The Level Of Privilege Obtained, The Attacker May Be Able To Inspect Session Cookies, Certificates And Data, Change Browser Settings And Inject Code.

The Attack May Be Accomplished By Installing Malicious Plug-Ins Or Scripts Or Intercepting Calls Between The Browser Process And Dlls.

14.8 - Deployment And Automation Concepts

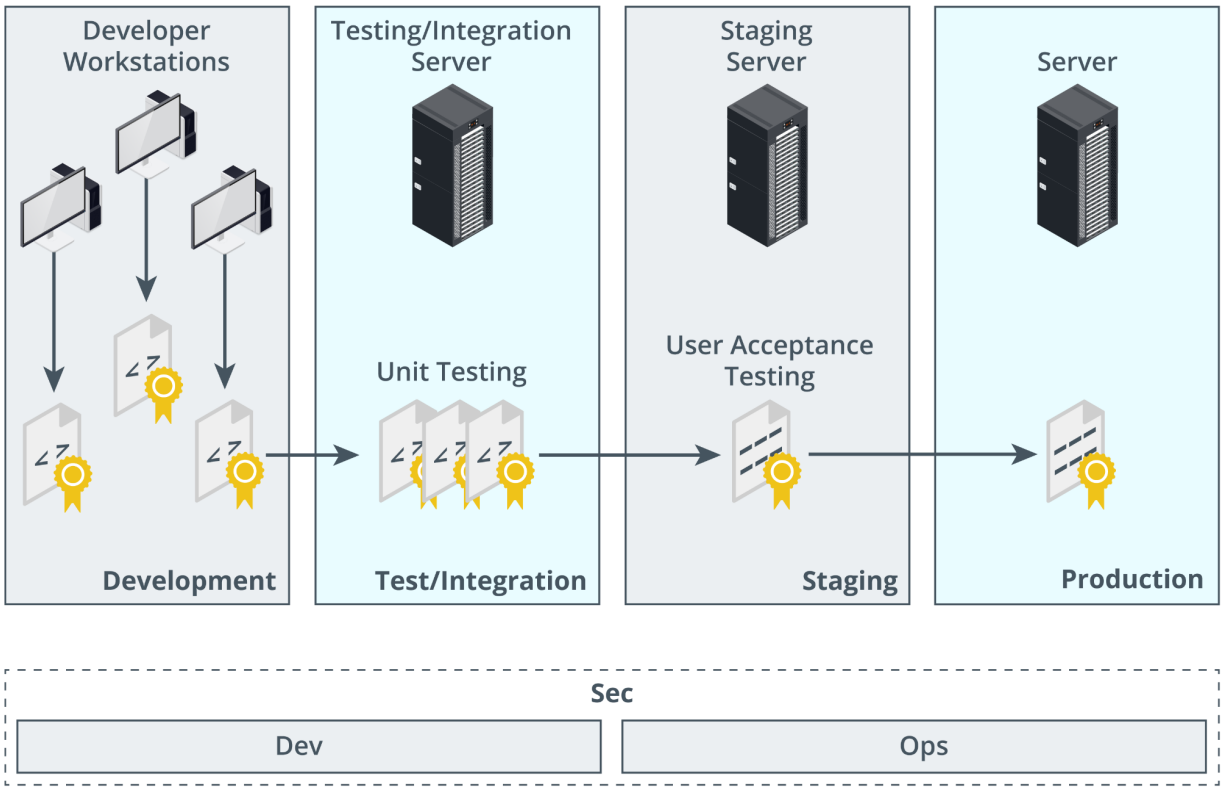
A Devsecops Culture Gives Project Teams A Broad Base Of Development, Security, And Operations Expertise And Experience. This Promotes An Environment In Which Security Tasks Make Increased Use Of Automation.

Automation Provides Better Scalability And Elasticity Than Manual Configuration.

- Scalability - Means That The Costs Involved In Supplying The Service To More Users Are Linear (Double Users = Double Cost)
- Elasticity - Refers To The Ability Of The Team To Handle Changes On Demand In Real Time.

Quality Assurance (Qa) - Requirements And Expectations Can Be Driven By Risk-Based Assessments Or They Can Be Driven By Internal And External Compliance Factors Such As Industry Regulations.

Secure Application Development Environments - Code Is Normally Passed Through Several Different Environments.



It Is Important To Be Able To Validate The Integrity Of Each Coding Environment.

- sandboxing - each development environment should be segmented from the others. only the minimum tools and services necessary to perform code development and testing should be allowed in each sandbox.

- secure configuration baseline - each development environment should be built to the same specification possibly using automated provisioning.

- integrity measurement - this process determines whether the development environment varies from the configuration baseline.

Provisioning - This Is The Process Of Deploying An Application To The Target Environment, Such As Enterprise Desktops, Mobile Devices Or Cloud Infrastructure. It Could Also Include Os And Applications And Provisioning Must Ensure Any Version Changes To These Applications Are Updated.

Deprovisioning - This Is The Process Of Removing An Application From Packages Or Instances. This Might Be Necessary If Software Has To Be Completely Rewritten Or No Longer Satisfies Its Purpose.

any configurations that were made to support the application should also be removed.

version control - this is an id system for each iteration of a software product.

When a developer commits new or changed code to a product, the new source code is tagged with an updated version number and the old version archived. This allows changes to be rolled back if a problem is discovered.

automation/scripting release paradigms - coding projects are managed using different life cycle models. The waterfall model software development life cycle (sdlc) is an older paradigm that focuses on the successful completion of monolithic projects that progress from stage-to-stage.

The more recent agile paradigm uses iterative processes to release well-tested code in smaller blocks or units. In this model, development and provisioning tasks are conceived as continuous.

continuous integration (ci) - ci is the principle that developers should commit and test updates often every day or sometimes even more frequently. This is designed to reduce the chances of two developers spending time on code changes that are later found to conflict with one another.

continuous delivery - this is about testing all of the infrastructure that supports the app including networking, database functionality, client software and so on.

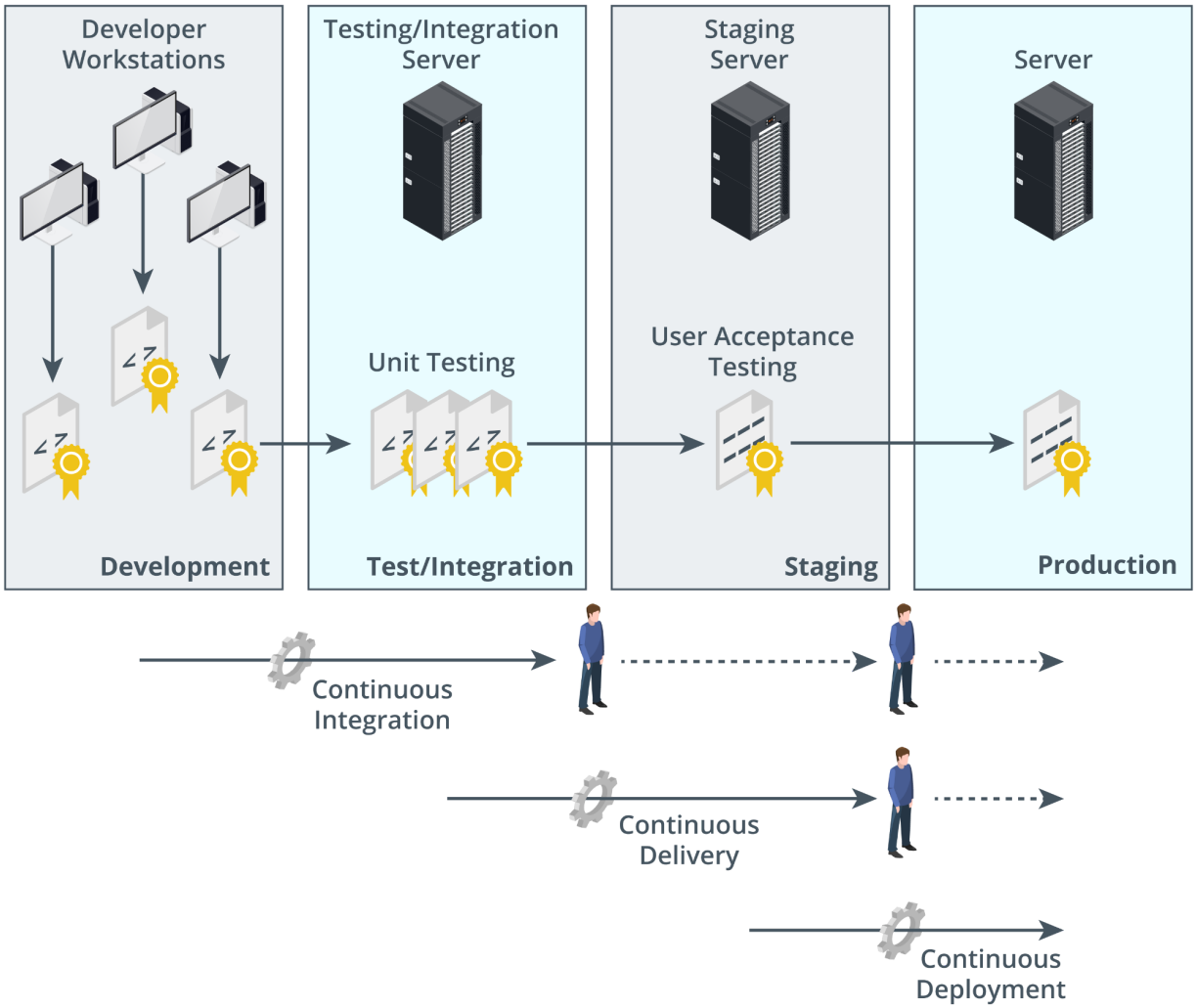
continuous deployment - this is the separate process of actually making changes to the production environment to support the new app version.

continuous monitoring and automated courses of action - continuous monitoring might use a locally installed agent or heartbeat protocol or may involve checking availability remotely. courses of action that the monitoring system takes can also be automated.

continuous validation - verification is a compliance testing process to ensure that the product or system meets its design goals while validation is the process of determining whether the application is fit for purpose.

software diversity - this can refer to obfuscation techniques to make code difficult to detect as malicious. This is widely used by threat actors in the form of shellcode compilers to avoid signature detection but can also be used as a defensive technique.

obfuscating api methods and automation code makes it harder for a threat actor to reverse engineer and analyze the code to discover weaknesses.



Section 15 - Implement Secure Cloud Solutions

15.1 - Cloud Deployment Models

Public (Multi-Tenant) - A Service Offered Over The Internet By Cloud Service Providers (Csps) To Cloud Consumers

Hosted Private - Hosted By A Third Party For The Exclusive Use Of An Organization. Better Performance But More Expensive Than Public.

Private - Cloud Infrastructure That Is Completely Private And Owned By The Organization. Geared More Towards Banks And Governmental Services Where Security And Privacy Is Of Utmost Importance.

Community - Several Organizations Share The Costs Of Either A Hosted Private Or Fully Private Cloud.

Cloud Service Models

Cloud Services Can Also Be Differentiated On The Level Of Complexity And Pre-Configuration Provided (Sometimes Referred To As Anything As A Service Xaas)

Most Common Implementations Are Infrastructure, Software And Platform.

Infrastructure As A Service (Iaas) - It Resources (Servers, Load Balancers And San) Are Provided Here. Examples Include Amazon Elastic Compute Cloud, Oracle Cloud And Microsoft Azure Virtual Machines.

Software As A Service (Saas) - Provisioning Of Software Applications And Can Be Purchased On A Pay-As-You-Go Or Lease Arrangement. Examples Are Microsoft 365, Salesforce And Adobe Creative Cloud.

Platform As A Service (Paas) - Provides Resources Somewhere Between Saas And Iaas. A Typical Paas Solution Would Provide Servers And Storage Network Infrastructure And Also A Web-Application Or Database Platform On Top.

Examples Include Oracle Database, Microsoft Azure Sql Database And Google App Engine.

Security As A Service

- Consultants - Can Be Used For Framework Analysis Or For More Specific Projects.
- Managed Security Services Provider (Mssp) - Fully Outsourcing Responsibility For Information Assurance To A Third Party. Can Be Expensive But A Good Fit For An Sme That Has No In-House Security Capability.
- Security As A Service (Secaas) - Can Mean A Lot Of Things But Typically Means Implementing A Particular Security Control Such As Malware Scanning In The Cloud. Examples Include Cloudflare, Mandiant/Fireeye And Sonicwall.

15.2 - Virtualization Techs & Hypervisor Types

Virtualization - Means That Multiple Operating Systems Can Be Installed And Run Simultaneously On A Single Computer.

- Host Hardware - The Platform That Will Host The Virtual Environment
- Hypervisor/Virtual Machine Monitor (Vmm) - Manages The Virtual Machine Environment
- Guest Operating Systems/ Virtual Machines

Virtual Desktop Infrastructure (Vdi) & Thin Clients - Vdi Refers To Using A Vm As A Means Of Provisioning A Corporate Desktops.

In A Typical Vdi, Desktop Computers Are Replaced By Low-Spec, Low-Power Thin Client Computers. When The Thin Client Starts, It Boots A Minimal Os Allowing The User To Log Onto A Vm Stored On The Company Server Infrastructure. The User Connects To The Vm Using Some Sort Of Remote Desktop Protocol.

With vdi, it is a lot easier for a company to completely offload their IT infrastructure to a third-party company but could lead to downtime if the server and network infrastructure fails.

Application virtualization & container virtualization - application virtualization is a more limited type of vdi where instead of the whole client desktop running as a virtual platform, the client either accesses an application hosted on a server or streams the application from the server to the client for local processing.

Containerization is used in many cloud services like serverless architecture and also used to implement corporate workspaces on mobile devices.

vm escape protection - vm escaping refers to malware running on a guest os jumping to another guest or to the host and must identify that it is running in a virtual environment.

Timing attack - the attacker sends multiple usernames to the authentication server and measures the server responses times.

A wrong username will be rejected quickly but a valid one will take longer allowing the attacker to harvest a list of valid usernames.

Malware can use the timing attack to determine if it is in a virtual environment because certain operations will take longer to complete in a virtual environment than in a real one.

VM sprawl avoidance - apart from patching the hypervisor, each vm should be treated as any other network host meaning security policies and controls must be applied to them.

VM sprawl occurs when a system is brought up for "just a minute" to test something but ends up languishing for months undocumented and unsecured.

virtual machine life cycle management (vmlm) software can be deployed to enforce vm sprawl avoidance as it provides a centralized dashboard for maintaining and monitoring all the virtual environments.

15.3 - Cloud Security Solutions

Cloud computing is also a means of transferring risk and as such it is important to identify which risks are being transferred and what responsibilities both the company and service provider will undertake.

a company will always still be held liable for legal and regulatory consequences in case of a security breach though the service provider could be sued for the breach.

the company will also need to consider the legal implications of using a csp if its servers are located in a different country.

Application security in the cloud refers both to the software development process and to the identify and access management (IAM) features designed to ensure authorized use of applications.

cloud provides resources abstracted from physical hardware via one or more layers of virtualization and the compute component provides process and system memory (ram) resources as required for a particular workload.

high availability - one of the benefits of using the cloud is the potential for providing services that are resilient to failures at different levels.

In terms of storage performance, high availability (ha) refers to storage provisioned with a guarantee of 99.99% uptime or better and the csp typically uses redundancy to make multiple disk controllers and storage devices available to a pool of storage resources.

replication - data replication allows businesses to copy data to where it can be utilized most effectively and the cloud may be used as a central storage area.

The terms hot and cold storage refer to how quickly data is retrieved and hot storage is quicker but also more expensive to manage.

- local replication - replicates data within a single data center in the region where the storage account was created.
- regional replication - replicates data across multiple data centers within one or two regions.
- geo-redundant storage (GRS) - replicates data to a secondary region that is distant from the primary region. This safeguards data in the event of a regional outage or a disaster.

virtual private clouds (VPCs) - each customer can create one or more VPCs attached to their account. By default, a VPC is isolated from other csp accounts and from other VPCs operating in the same account.

Each subnet within a VPC can either be private or public. for external connectivity that isn't appropriate for public.

Routing can be configured between subnets in a vpc and between vpcs in the same account or with vpcs belonging to different accounts.

configuring additional vpcs rather than subnets within a vpc allows for a greater degree of segmentation between instances.

A vpc endpoint is a means of publishing a service that is accessible by instances in other vpcs using only the aws internal network and private ip addresses. there are two types - gateway and interface

cloud firewall security - filtering decisions can be made based on packet headers and payload contents at various layers

- network layer 3 - the firewall accepts/denies connections based on the ip addresses or address ranges and tcp/udp port numbers (actually contained in layer 4 headers but the functionality is still always described as layer 3 filtering).
- transport layer 4 - the firewall can store connection states and use rules to allow established traffic.
- application layer 7 - the firewall can parse application protocol headers and payloads and make decisions based on their contents.

Firewalls in the cloud can be implemented in several ways to suit different purposes.

- as software running on an instance
- as a service at the virtualization layer to filter traffic between vpc subnets and instances. This equates to an on-premises network firewall.

cloud access security brokers (casb) -CASBs provide you with visibility into how clients and other network nodes are using cloud services.

- enable single sign-on authentication and enforces access controls and authorizations from the enterprise network to the cloud provider
- scan for malware and rouge devices
- monitor and audit user and resource activity
- mitigate data exfiltration

casbs are implemented in one of three ways:

- forward proxy - positioned at the client network edge that forwards user traffic to the cloud network
- reverse proxy - positioned at the cloud network edge and directs traffic to cloud services
- api

15.4 - Infrastructure As Code Concepts

Service-Oriented Architecture (Soa) - This Conceives Of Atomic Services Closely Mapped To Business Workflows. Each Service Takes Defined Inputs And Produces Defined Outputs.

Service Functions Are Self-Contained, Do Not Rely On The State Of Other Services And Expose Clear Input/Output (I/O) Interfaces.

Microservices - Microservice-Based Development Shares Many Similarities With Agile Software Project Management And The Processes Of Continuous Delivery And Deployment.

The Main Difference From Soa Is That While Soa Allows A Service To Be Built From Other Services, Each Microservice Should Be Capable Of Being Developed, Tested And Deployed Independently (Highly Decoupled)

Services Integration - Service Integration Refers To Ways Of Making These Decoupled Services Work Together To Perform A Workflow. Where Soa Used The Concept Of An Enterprise Service Bus, Microservices Integration And Cloud Services/Virtualization, Integration Generally Is Very Often Implemented Using Orchestration Tools.

Automation Focuses On Making A Single Discrete Task Easily Repeatable While Orchestration Performs A Sequence Of Automated Tasks.

Cloud Orchestration Platforms Connect To And Provide Administration, Management And Orchestration For Many Popular Cloud Platforms And Services.

Application Programming Interfaces (Api) - Soa, Microservices, Service Integration, Automation And Orchestration All Depend On Apis

- Simple Object Access Protocol (Soap) - Uses Xml Format Messaging And Has A Number Of Extensions In The Form Of Web Services Standards That Support Common Features Such As Authentication, Transport Security And

Asynchronous Messaging.

- Representational State Transfer (Rest) - A Much Looser Architectural Framework Also Referred To As Restful Api. Soap Requests Must Be Sent In Correctly Formatted Xml Document While Rest Requests Can Be Submitted As An Http Operation.

serverless architecture - this is a modern design pattern for service delivery and is strongly associated with modern web applications - netflix.

billing is based on execution time rather than hourly charges and this type of service provision is also called function as a service (FAAS).

Serverless architecture eliminates the need to manage physical or virtual server instances so there is no need for software and patches or file system security monitoring.

infrastructure as code - an approach to infrastructure management where automation and orchestration fully replace manual configuration is referred to as infrastructure as code (IAC)

The main objective of iac is to eliminate snowflake systems which are basically systems that are different from others and this can happen when there is a lack of consistency in terms of patch updates and stability issues.

By rejecting manual configuration of any kind, iac ensures idempotence which means making the same call with the same parameters will always produce the same result.

iac means using carefully developed and tested scripts and orchestration runbooks to generate consistent builds.

fog & edge computing - traditional data center architecture sensors are quite likely to have low bandwidth and higher latency WAN links to data networks.

Fog computing developed by cisco addresses this by placing fog node processing resources close to the physical location for the iot sensors. The sensors communicate with the fog node using wi-fi or 4g/5g and the fog node prioritizes traffic, analyzes and remediates alertable conditions.

Edge Computing Is A Broader Concept Partially Developed From Fog Computing.

- Edge Devices Collect And Depend Upon Data For Their Operation.

- Edge Gateways Perform Some Pre-Processing Of Data To And From Edge Devices To Enable Prioritization.
- Fog Nodes Can Be Incorporated As A Data Processing Layer Positioned Closed To The Edge Gateways.
- The Cloud Or Data Center Layer Provides The Main Storage And Processing Resources Plus Distribution And Aggregation Of Data Between Sites.

Instead of depending on a cluster of clouds for computing and data storage, edge computing leverages local computing (routers, PCs, smartphones) to produce shorter response time as the data is processed locally.

Section 16 - Data Privacy & Protection Concepts

16.1 - Privacy & Sensitive Data Concepts

The Value Of An Information Asset Can Be Determined By How Much Damage Its Compromise Would Cause The Company.

It Is Important To Consider How Sensitive Data Must Be Secured Not Just At Rest But Also In Transit.

Information Life Cycle Management

- Creation/Collection
- Distribution/Use
- Retention
- Disposal

Data roles & responsibilities - a data governance policy describes the security controls that will be applied to protect data at each stage of its life cycle.

data owner - a senior executive role with ultimate responsibility for maintaining the cia of the information asset. The owner also typically chooses a steward and custodian and directs their actions and sets the budget and resource allocation for controls.

data steward - primarily responsible for data quality. ensuring data is labeled and identified with appropriate metadata and that it is stored in a secure format

data custodian - this role handles managing the system on which the data assets are stored. This includes responsibility for enforcing access control, encryption and backup measures.

data privacy officer (DPO) - this role is responsible for oversight of any personally identifiable information (PII) assets managed by the company.

in the context of legislation and regulations protecting personal privacy, the following two institutional roles are important

data controller - the entity responsible for determining why and how data is stored, collected and used for ensuring that these purposes and means are lawful. the controller has ultimate responsibility for privacy breaches and is not permitted to transfer that responsibility.

data processor - an entity engaged by the data controller to assist with technical collection, storage or analysis tasks. a data processor follows the instructions of a data controller with regard to collection or processing.

Data Classifications - Data Can Be Classified Based On The Degree Of Confidentiality Required.

- Public (Unclassified) - No Restrictions And Can Be Viewed By The Public. Poses No Real Risk To The Company.

- Confidential (Secret) - Highly Sensitive Information To Be Viewed Only By Authorized People And Possibly By Trusted Parties Under An Nda.

- Critical (Top Secret) - Extremely Valuable Information And Viewing Is Severely Restricted.

Data Can Also Be Classified Based On The Kind Of Information Asset.

- Proprietary/Intellectual Property (Ip) - Information Created And Owned By The Company Typically About The Products They Make.
- Private/Personal Data - Information That Relates To An Individual Identity.

- Sensitive - Refers To Company Data That Could Cause Serious Harm Or Embarrassment If It Is Leaked To The Public. Sensitive Personal Data Includes Political Opinions, Sexual Orientation, Health Records , Tax Records Etc.

Data Types

Personally Identifiable Information (Pii) - This Is Data That Can Be Used To Identify, Contact Or Locate An Individual Such As A Social Security Number.

An Ip Address Can Also Be Used To Locate An Individual And Could Be Considered To Be A Type Of Pii.

Customer Data - This Can Be Institutional Information But Also Personal Information About The Customer's Employees Such As Sales And Technical Support Contacts.

Financial Information - This Refers To Data Held About Bank And Investment Accounts Plus Tax Returns And Even Credit/Debit Cards. The Payment Card Industry Data Security Standard (Pci Dss) Defines The Safe Handling And Storage Of This Information.

Government Data - Government Agencies Have Complex Data Collection And Processing Requirements. The Data May Sometimes Be Shared With Companies For Analysis Under Very Strict Agreements To Preserve Security And Privacy.

Data Retention - This Refers To Backing Up And Archiving Information Assets In Order To Comply With Business Policies And Applicable Laws And Regulations.

16.2 - Data Sovereignty, Privacy Breaches & Data Sharing

Data Sovereignty & Geographical Considerations - Some States And Nations May Respect Data More Or Less Than Others And Likewise Some Nations May Disapprove Of The Nature And Content Of Certain Data.

Data Sovereignty Refers To A Jurisdiction Preventing Or Restricting Processing And Storage From Taking Place On Systems That Do Not Physically Reside Within That Jurisdiction. For Example Gdpr Protections Are Extended To Any Eu Citizen While They Are Within The Eu Borders.

Geographic Access Requirements Fall Into Two Different Scenarios

- Storage Locations Might Have To Be Carefully Selected To Mitigate Data Sovereignty Issues. Most Cloud Providers Allow Choice Of Data Centers For Processing And Storage, Ensuring That Information Is Not Illegally Transferred From A Particular Privacy Jurisdiction Without Consent.

- Employees Needing Access From Multiple Geographic Locations. Cloud-Based File And Database Services Can Apply Constraint-Based Access Controls To Validate The User's Geographic Location Before Authorizing Access.

A Data Breach Occurs When Information Is Read, Modified Or Deleted Without Authorization.

Notification & Escalation - Responses To A Data Breach Must Be Configured So The Appropriate Personnel Are Notified Immediately Of The Breach.

The First Responders Might Be Able To Handle The Incident If Its A Minor Issue However In More Serious Cases, The Case May Need To Be Escalated To A More Senior Manager.

In Certain Cases, A Timescale Might Also Be Applied. For Example With Gdpr, All Affected Individuals Must Be Informed Of The Breach Within 72 Hours After The Breach Occurred.

Data Sharing & Privacy Terms Of Agreement

- Service Level Agreement (Sla) - A Contractual Agreement Setting Out The Detailed Terms Under Which A Service Is Provided.

- Interconnection Security Agreement (Isa) - Isas Set Out A Security Risk Awareness Process And Commits The Agency And Supplier To Implementing Security Controls.

- Nondisclosure Agreement (Nda) - This Is A Legal Basis For Protecting Information Assets.

- Data Sharing And Use Agreement - personal data can only be collected for a specific purpose but data sets can be subject to deidentification to remove personal data. however there are risks of re identification if combined with other data sources. A data sharing and use agreement is a legal means of preventing this risk. it can specify terms for the way a data set can be analyzed and proscribe the use of re identification techniques.

16.3 - Privacy And Data Controls

Data Can Be Described As Being In One Of Three States:

- Data At Rest - Data Is In Some Sort Of Persistent Storage Media. This Data Can Be Encrypted And Acls Can Also Be Applied To It

- Data In Transit - This Is The State When Data Is Transmitted Over A Network. In This State It Can Be Protected By A Transport Encryption Protocol Such As Tls Or Ipsec.

- Data In Use/Processing - This Is The State When Data Is Present In Volatile Memory Such As The Ram Cache. Trusted Execution Environment (Tee) Mechanisms E.G Intel Software Guard Extensions Are Able To Encrypt The Data As It Exists In Memory.

Data Exfiltration - Data Exfiltration Can Take Place Via A Wide Variety Of Mechanisms:

- Copying The Data To Removable Media Such As Usb Drive Or Smartphone
- Using A Network Protocol Such As Ftp, Http Or Email
- Communicating It Orally Over A Phone Or Even With The Use Of Text Messaging.

Data Protection Against Exfiltration

- All Sensitive Data Is Encrypted At Rest
- Create And Maintain Offsite Backups Of Data
- Ensure That Systems Storing Or Transmitting Sensitive Data Are Implementing Access Controls.
- Restrict The Types Of Network Channels That Attackers Can Use To Transfer Data From The Network To The Outside.
- Train Users About Document Confidentiality And The Use Of Encryption To Store And Transmit Data Securely.

Data Loss Prevention

DLP Products Automate The Discovery And Classification Of Data Types And Enforce Rules So That Data Is Not Viewed Or Transferred Without Proper Authorization.

- Policy Server - To Configure Classification, Confidentiality And Privacy Rules And Policies, Log Incidents And Compile Reports
- Endpoint Agents - To Enforce Policy On Client Computers Even When They Are Not Connected To The Network
- Network Agents - To Scan Communications At Network Borders And Interface With Web And Messaging Servers To Enforce Policy.

Remediation Is The Action The Dlp Software Takes When It Detects A Policy Violation.

- Alert Only
- Block - The User Is Prevented From Copying The Original File But Retains Access To It. User May Not Alerted To The Policy Violation But It Will Be Logged As An Incident By The Management Engine.
- Quarantine - Access To The Original File Is Denied To The User.
- Tombstone - The Original File Is Quarantined And Replaced With One Describing The Policy Violation And How The User Can Release It Again.

Privacy Enhancing Technologies - Data Minimization Is The Principle That Data Should Only Be Processed And Stored If That Is Necessary To Perform The Purpose For Which It Is Collected.

Data Minimization Affects The Data Retention Policy And Its Necessary To Track How Long A Data Point Has Been Stored For And Whether Continued Retention Is Necessary For A Legitimate Processing Function.

Pseudo-Anonymization Modifies Identifying Information So That Reidentification Depends On An Alternate Data Source Which Must Be Kept Separate. With Access To The Alternated Data, Pseudo-Anonymization Methods Are Reversible.

Database Identification Methods

Data Masking - Can Mean That All Or Part Of The Contents Of A Field Are Redacted By Substituting All Character Strings With "X".

Tokenization - Means That All Or Part Of Data In A Field Is Replaced With A Randomly Generated Token. The Token Is Stored With The Original Value On A Token Server Or Vault Separate To The Production Database. It's Often Used As A Substitute For Encryption.

Aggregation/Binding - Another Identification Technique Is To Generalize The Data Such As Substituting A Specific Age With A Broader Age Band.

Hashing & Salting - a cryptographic hash produces a fixed-length string from arbitrary-length plaintext data using an algorithm such as sha. if the function is secure, it should not be possible to match the hash back to a plaintext. a salt is an additional value stored with the hashed data field. The purpose of salt is to frustrate attempts to crack the hashes.

Section 17 - Incident Response Procedures

17.1 - Incident Response Process

This is a set of policies and procedures that are used to identify, contain, and eliminate cyberattacks. The goal is to allow an organization to quickly detect and stop attacks, minimize damage and prevent future attacks of the same type.

principal stages in incident response life cycle

- preparation - makes the system resilient to attack. this includes: hardening systems, writing policies and procedures,and creating incident response resources and procedures
- identification - determine whether an incident has taken place, assess how severe it might be and then notify the appropriate personnel.
- containment - limits the scope and magnitude of the incident. The main aim of incident response is to secure data while limiting the immediate impact on customers and business partners.
- eradication - once the incident is contained, the vulnerability/issue is removed and the affected systems are restored to a secure state.
- recovery - the restored system is then reintegrated back into the business process that it supports
- lessons learned - analyze the incident and responses to identify whether procedures or systems could be improved. It is also imperative to document the incident.

17.2 - Cyber Incident Response Team

Preparing For Incident Response Means Establishing The Policies And Procedures For Dealing With Security Breaches And The Personnel And Resources To Implement Those Policies.

First Task Is To Define And Categorize Types Of Incidents. In Order To Identify And Manage Incidents, You Should Develop Some Method Of Reporting, Categorizing And Prioritizing Them.

An Incident Response Team Can Be Referred To As A Cyber Incident Response Team (Cirt), Computer Security Incident Response Team (Csirt) Or Computer Emergency Response Team (Cert).

For Major Incidents, Expertise From Other Business Divisions Might Be Needed

- Legal - The Incident Can Be Evaluated From The Perspective Of Compliance With Laws And Industry Regulations.
- Human Resources (Hr) - Incident Prevention And Remediation Actions May Affect Employee Contracts, Employment Law And So On.
- Marketing - The Team Is Likely To Require Marketing Or Public Relations Input So Any Negative Publicity From A Serious Incident Can Be Managed.

Incident Response Policies Should Establish Clear Lines Of Communication Both For Reporting Incidents And For Notifying Affected Parties.

Status And Event Details Should Be Circulated On A Need-To-Know Basis And Only To Trusted Parties Identified On A Call List.

Trusted Parties Might Include Both Internal And External Stakeholders.

Obligations To Report The Attack Must Be Carefully Considered And It May Be Necessary To Inform Affected Parties During Or Immediately After The Incident So That They Can Perform Their Own Remediation E.G " Change Your Passwords Immediately "

17.3 - Incident Response Plan

This Lists The Procedures, Contacts And Resources Available To Responders For Various Incident Categories.

A Playbook Is A Data-Driven Standard Operating Procedure (Sop) To Assist Junior Analysts In Detecting And Responding To Specific Cyberthreat Scenarios

One Challenge In Incident Management Is To Allocate Resources Efficiently And There Are Several Factors That Can Affect This Process.

- Data Integrity - The Most Important Factor In Prioritizing Incidents
- Downtime - An Incident Can Either Degrade Or Interrupt The Availability Of An Asset Or System.
- Economic/Publicity - Both Data Integrity And Downtime Will Have Important Economic Effects. Short-Term Might Involve Lost Business Opportunity While Long-Term May Involve Damage To Reputation And Marketing Standing.
- Scope - Refers To The Number Of Affected Systems In An Incident
- Detection Time - Research Has Shown That More Than Half Of Data Breaches Are Not Detected For Weeks Or Months. This Demonstrates That Systems Used To Search For Intrusions Must Be Thorough.
- Recovery Time - Some Incidents Require Lengthy Remediation As The System Changes Required Are Complex To Implement.

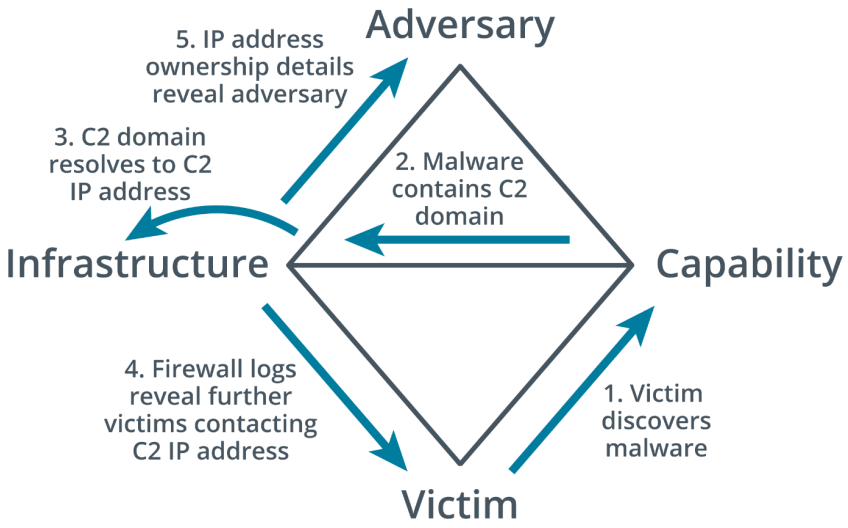
A Key Tool For Threat Research Is A Framework To Use To Describe The Stages Of An Attack And These Stages Are Referred To As A Cyber Kill Chain.

Mitre Att&Ck - An Alternative To The Kill Chain Is The Mitre Corporation's Adversarial Tactics, Techniques And Common Knowledge

It Provides Access To A Database Of Known Ttps And Tags Each Technique With A Unique Id And Places It In One Or More Tactic Categories Such As Initial Access , Persistence Or Command & Control.

Diamond Model Of Intrusion Analysis - This Suggests A Framework To Analyze An Intrusion Event (E) By Exploring The Relationships Between Four Core Features: Adversary, Capability, Infrastructure And Victim.

Each Event May Also Be Described By Meta-Features Such As Date/Time, Kill Chain Phase Etc.



17.4 - Incident Response Exercises, Recovery And Retention Policy

Training On Specific Incident Response Scenarios Can Use Three Forms

- Tabletop - Least Costly Where The Facilitator Presents A Scenario And The Responders Explain What Action They Would Take To Identify, Contain And Eradicate The Threat. Flashcards Are Used In Place Of Computer Systems.

- Walkthroughs - Similar To Tabletop Except Here The Responders Demonstrate What Actions They Would Take In Response Such As Running Scans And Analyzing Sample Files.

- Simulations - A Team Based Exercise Where The Red Team Attempts An Intrusion, The Blue Team Operates Response And Recovery Controls And The White Team Moderates And Evaluates The Exercise.

disaster recovery plan - also called the emergency response plan. This is a document meant to minimize the effects of a disaster or disruption. meant for short term events and implemented during the event itself.

business continuity plan - identifies how business processes should deal with both minor and disaster-level disruption. a continuity plan ensures that business processes can still function during an incident even if at a limited scale.

continuity of operation planning (COOP) - this terminology is used for government facilities but is functionally similar to business continuity planning. In some definitions, coop refers specifically to backup methods of performing mission functions without IT support.

retention policy - a retention policy for historic logs and data captures sets the period of which these are retained. indicators of a breach might be discovered only months after the breach and this would not be possible without the retention policy to keep logs and other digital evidence.

17.5 - Incident Identification

Identification - This Is The Process Of Collating Events And Determining Whether Any Of Them Should Be Managed As Incidents Or As Possible Precursors To An Incident.

- Using Logs, Error Messages And Ids/Firewall Alerts
- Comparing Deviations To Established Metrics To Recognize Incidents And Their Scopes
- Manual Or Physical Inspections Of Site, Premises, Networks And Hosts
- Notification By An Employee, Customer Or Supplier
- Public Reporting Of New Vulnerabilities

Correlation - This Means Interpreting The Relationship Between Individual Data Points To Diagnose Incidents Of Significance To The Security Team.

A SIEM (Security Information And Event Management System) Correlation Rule Is A Statement That Matches Certain Conditions.

These Rules Use Logical Expressions Such As And And Or And Operators (==, <,>, In)

A Single-User Logon Failure Might Not Raise An Alert However Multiple Failed Logins For The Same Account Over A Short Period Of Time Should Raise One.

Error.Logonfailure > 3 And Logonfailure.Alice And Duration < 10 Minutes

One of the biggest challenges in operating a SIEM is tuning the system sensitivity to reduce false positive indicators being reported as an event.

The correlation rules are likely to assign a criticality level to each match.

- log only - an event is produced and added to the siem's database but automatically classified
- alert - the event is listed on a dashboard or incident handling system for an agent to assess.
- alarm - the event is automatically classified as critical and a priority alarm is raised.

trend analysis - this is the process of detecting patterns or indicators within a data set over a time series and using those patterns to make predictions about future events.

- frequency-based trend analysis establishes a baseline for a metric such as number of errors per hour of the day. if the frequency exceeds the threshold for the baseline, then an alert is raised.

- volume-based trend analysis - this can be based on logs growing much faster than usual. This analysis can also be based on network traffic and endpoint disk usage.

- statistical deviation analysis can show when a data point should be treated as suspicious. For example, a data point that appears outside the two clusters for standard and admin users might indicate some suspicious activity by that account.

logging platforms - log data from network appliances and hosts can be aggregated by a siem either by installing a local agent to collect the data or by using a forwarding system to transmit logs directly to the siem server.

syslog - provides an open format, protocol and server software for logging event messages and it's used by a very wide range of host types.

a syslog message comprises a pri code, a header containing a timestamp and host name and a message part. usually uses UDP port 514

- rsyslog uses the same configuration file syntax but can work over tcp and use a secure connection.
- syslog-ng uses a different configuration file syntax but can also use tcp/secure communications and more advanced options for message filtering.

In linux, rather than writing events to syslog-format text files, logs from processes are written to a binary-format called journald.

Events captured by journald can be forwarded to syslog and to view events in journald directly, you can use journalct command to print the entire journal log.

system & security logs - the five main categories of windows event logs are:

- application - events generated by applications and services
- security - audit events such as a failed logon or denied access to a file
- system - events generated by the os and its services such as storage volume health checks
- setup - events generated during the windows installation
- forwarded events - events that are sent to the local log from other hosts.

network logs can be generated from routers, firewalls, switches and access points.

authentication attempts for each host are likely to be written to the security log.

DNS event logs may be logged by a dns server while web servers are typically configured to log http traffic that encounters an error or traffic that matches some predefined rule set.

The status code of a response can reveal something about both the request and the server's behavior.

- codes in the 400 range indicate client-based errors
- codes in the 500 range indicate server-based errors
- "403" may indicate that the server is rejecting a client's attempts to access resources they are not authorized to.
- "502" (bad gateway) response could indicate that communications between the target server and its upstream server are being blocked or the upstream server is down.

dump files - a system memory dump creates an image file that can be analyzed to identify the processes that are running, the contents of temporary file systems, registry data, network connections and more.

It can also be a means of accessing data that is encrypted when stored on a mass storage device.

metadata - this the properties of data as it is created by an application stored on media or transmitted over a network. Metadata sources are useful during an investigation as they can establish timeline questions as well as containing other types of evidence.

file - file metadata is stored as attributes. The file system tracks when a file was created, accessed and modified. The acl attached to a file showing its permissions also represents another type of attribute.

web - when a client requests a resource from a web server, the server returns the resource plus headers setting or describing its properties. headers describe the type of data returned.

email - an email's internet header contains address information for the recipient and sender plus details of the servers handling transmission of the message between them.

mobile - phone metadata comprises call detail records (CDRs) of incoming, outgoing and attempted calls and sms text time, duration and the opposite party's number. meta data will also record data transfer volumes and the location history of the device can be tracked by the list of cell towers it has used to connect to the network.

netflow/ipfix - a flow collector is a means of recording metadata and statistics about network traffic rather than recording each frame.

flow analysis tools can provide features such as:

- highlighting trends and patterns in traffic generated by particular applications, hosts and ports.
- alerting based on detection of anomalies or custom triggers
- identification of traffic patterns revealing rouge user behavior or malware in transit

17.6 - Mitigation Controls

- Isolation-Based Containment - Isolation Involves Removing An Affected Component From Whatever Larger Environment It Is A Part Of. A Simple Option Is To Disconnect The Host From The Network Completely Either By Pulling The Network Plug Or Disabling Its Switch Port.
  If A Group Of Hosts Are Affected, They Could Be Isolated Into A Black Hole.

  Finally, Isolation Could Also Refer To Disabling A User Account Or Application Service.

- Segmentation-Based Containment - This Is A Means Of Achieving The Isolation Of A Host Or Group Of Hosts Using Network Technologies And Architecture. Segmentation Uses Vlans, Routing/Subnets And Firewall Acls To Prevent A Host Or Group Of Hosts From Communicating Outside The Protected Segment.

Incident Eradication & Recovery - Eradication Involves Completely Removing The Cause Of The Incident However It Is Not The Last Step In Incident Response.

Recovery Means Restoring The Affected Systems Back To Their Original Working State Before The Incident And Ensuring That The System Cannot Be Attacked Again Using The Same Attack Vector.

Eradication And Recovery Generally Involves Three Steps

- Reconstitution Of Affected Systems - Removing Malicious Files Or Restoration Through The Use Of Backups.
- Reaudit Security Controls
- Ensure That Affected Parties Are Notified And Provided With The Means To Remediate Their Own Systems. (Change Your Passwords !!!)

Update Or Revoke Certificates - Compromise Of The Private Key Represented By A Digital Certificate Or The Ability To Present Spoofed Certificates As Trusted Is A Critical Security Vulnerability.

- Remove Compromised Root Certificates
- Revoke Certificates On Compromised Hosts

Endpoint Configuration Changes - If Endpoint Security Is Breached, There Are Several Classes Of Vector To Consider For Mitigation:

- Social Engineering

- Vulnerabilities
- Lack Of Security Controls
- Configuration Drift
- Weak Configuration

Another element of endpoint configuration is an execution control policy that defines which applications can or can't run.

an update to this policy might be needed in response to an incident.

quarantine might be a last resort if all mitigation efforts have failed.

security orchestration, automation & response (SOAR) - automation is the action of scripting a single activity while orchestration is the action of coordinating multiple automations to perform a complex multistep task.

The purpose of SOAR is to solve the problem of the volume of alerts overwhelming the analyst's ability to respond. An incident response workflow is usually defined as a playbook. A playbook is a checklist of actions to perform to detect and respond to a specific type of incident.

When a playbook is implemented with a high degree of automation from a SOAR system, it can be referred to as a runbook.

Section 18 - Digital Forensics

18.1 - Digital Forensics Documentation

Digital Forensics Is The Practice Of Collecting Evidence From Computer Systems To A Standard That Will Be Accepted In A Court Of Law.

Prosecuting External Threat Sources Can Be Difficult As The Threat Actor May Be In A Different Country Or Have Taken Effective Steps To Disguise Their Location.

Like Dna Or Fingerprints, Digital Evidence Is Latent Meaning That The Evidence Cannot Be Seen With The Naked Eye; Rather It Must Be Interpreted Using A Machine Or Process.

Due Process - Term Used In Us And Uk Common Law That Requires That People Only Be Convicted Of Crimes Following The Fair Application Of The Laws Of The Land.

The First Response Period Following Detection And Notification Is Often Critical. To Gather Evidence Successfully, It's Vital That Staff Do Not Panic Or Act In A Way That Would Compromise The Investigation.

Legal Hold - This Refers To The Fact That Information That May Be Relevant To A Court Case Must Be Preserved. This Means That Computer Systems May Be Taken As Evidence With All The Obvious Disruption To A Network That Entails.

Chain Of Custody - This Documentation Reinforces The Integrity And Proper Handling Of Evidence From Collection, To Analysis, To Storage And Finally To Presentation. It Is Meant To Protect An Organization Against Accusations That Evidence Has Been Tampered With During A Trial.

Digital Forensics Reports - A Report Summarizes The Significant Contents Of The Digital Data And The Conclusions From The Investigator's Analysis.

- Analysis Must Be Performed Without Bias. Conclusions And Opinions Should Be Formed Only From The Direct Evidence Under Analysis.
- Analysis Methods Must Be Repeatable By Third Parties With Access To The Same Evidence
- Ideally, The Evidence Must Not Be Changed Or Manipulated.

E-Discovery - This Is A Means Of Filtering The Relevant Evidence Produced From All The Data Gathered By A Forensic Examination And Storing It In A Database In A Format Such That It Can Be Used As Evidence In A Trial.

Some Of The Functions Of E-Discovery Suites Are:

- Identify And De-Duplicate Files And Metadata
- Search - Allows Investigators To Locate Files Of Interest To The Case.
- Tags - Apply Standardized Keywords Or Labels To Files And Metadata To Help Organize The Evidence.
- Security - At All Points Evidence Must Be Shown To Have Stored, Transmitted And Analyzed Without Tampering.

- Disclosure - An Important Part Of The Trial Procedure Is That Evidence Is Made Available To Both Plaintiff And Defendant.

Video and witness interviews - the first phase of a forensics investigation is to document the scene by taking photographs and ideally audio and video.

As well as digital evidence, an investigator should interview witnesses to establish what they were doing at the scene and whether they observed any suspicious behavior or activity.

timelines - a very important part of a forensic investigation will involve tying events to specific times to establish a consistent and verifiable narrative. This visual representation of events in a chronological order is called a timeline.

Operating systems and files use a variety of methods to identify the time at which something occurred but the benchmark time is coordinated universal time (utc).

Local time will be offset from UTC by several hours and this local time offset may also vary if a seasonal daylight saving time is in place.

NTFSuses utc “internally“ but many OS and file systems record timestamps as the local system time and when collecting evidence, it is vital to establish how a timestamp is calculated and note the offset between the local system time and utc.

Event logs and network traffic - an investigation may also obtain the event logs for one or more network appliances and/or server hosts. network captures might provide valuable evidence.

For forensics, data records that are not supported by physical evidence (data drive) must meet many tests to be admissible in court. if the records were captured by a SIEM, it must demonstrate accuracy and integrity.

The intelligence gathered from a digital forensic activity can be used in two different ways:

- counterintelligence - identification and analysis of specific adversary tactics, techniques and procedures (TTPS) provides information on how to configure and audit systems so they are better able to capture evidence of attempted and successful intrusions.
- strategic intelligence - data that has been analyzed to produce actionable insights. These insights are used to inform risk management and security control provisioning to build mature cybersecurity capabilities.

18.2 - Digital Forensics Evidence Acquisition

Acquisition is the process of obtaining a forensically clean copy of data from a device held as evidence. if the system is not owned by the organization then the seizure could be challenged legally (BYOD)

Data acquisition is also more complicated when capturing evidence from a digital scene compared to a physical one (evidence may be lost due to system glitches or loss of power).

Data acquisition usually proceeds by using a tool to make an image from the data held on the target device. the image can be acquired from either volatile or nonvolatile storage.

Digital acquisition and order of volatility - the general principle is to capture evidence in the order of volatility from more volatile to less volatile.

According to the ISOC, the order is as follows

- cpu registers and cache memory
- contents of ram including routing table, arp cache, kernel statistics
- data on persistent mass storage devices like hard drives, usbs
- remote logging and monitoring data
- physical configuration and network topology
- archival media and printed documents

Digital forensics software include:

- encase forensic is a digital forensics case management product. contains workflow templates showing the key steps in diverse types of investigation.
- the forensic toolkit (ftk) from accessdata. a commercial investigation suite designed to run on windows server.
- the sleuth kit - an open source collection of command line tools and programming libraries for disk imaging and file analysis. autopsy is the gui that sits on top of the kit and is accessed through a web browser.
- winhex - a commercial tool for forensic recovery and analysis of binary data, with support for a range of file systems and memory dump types.
- the volatility framework which is widely used for system memory analysis.

system memory acquisition - system memory is volatile data held in the ram modules. A system memory dump creates an image file that can be analyzed to

identify the processes that are running, the contents of temporary file systems, registry data, network connections and more.

There are three main ways to collect the contents of the system memory

- live acquisition
- crash dump
- hibernation file and pagefile

Disk image acquisition refers to acquiring data from non-volatile storage. it could also be referred to as device acquisition meaning the ssd storage in a smartphone or media player.

There are three device states for persistent storage acquisition

Live acquisition - means copying the data while the host is still running. this may capture more evidence or more data for analysis and reduce the impact on overall services. however the data on the actual disks will have changed so this method may not produce legally acceptable evidence.

Static acquisition by shutting down the host - runs the risk that the malware will detect the shut-down process and perform anti-forensics to try and remove traces of itself.

Static acquisition by pulling the plug - this means disconnecting the power at the wall socket. This will likely preserve the storage device in a forensically clean state but there is the risk of corrupting data.

Whichever method is chosen, it is important to document the steps taken and supply a timeline of all actions.

Preservation and integrity of evidence - it is vital that the evidence collected at the crime scene conform to a valid timeline. recording the whole process establishes provenance of the evidence as deriving directly from the crime scene.

To obtain a clean forensic image from a non-volatile storage, you need to ensure nothing you do alters the data or metadata on the source disk or file system. A write blocker can ensure this by preventing any data from being changed by filtering write commands.

The host devices and media taken from the crime scene should be labeled, bagged and sealed using tamper-evident bags. bags should have anti-static shielding to reduce the possibility that data will be damaged or corrupted on the electronic media by electrostatic discharge.

The evidence should be stored in a secure facility.

Acquisition of other data types includes:

- network - packet captures and traffic flows can contain evidence. most networks will come from a SIEM.
- cache - software cache can be acquired as part of a disk image. the contents of hardware cache are generally not recoverable.
- artifacts and data recovery - artifact refers to any type of data that is not part of the mainstream data structures of an os. Data recovery refers to analyzing a disk for file fragments that might represent deleted or overwritten files. The process of recovering them is referred to as carving.
- snapshot - is a live acquisition image of a persistent disk and may be the only means of acquiring data from a virtual machine or cloud process.
- firmware - is usually implemented as flash memory. Some types like the pc firmware can potentially be extracted from the device or from the system memory using an imaging utility.

Section 19 - Risk Management Processes & Concepts

19.1 - Risk management process

Risk management involves all processes from assessing the risk to managing it.

- identify assets - humans, data, emails, hardware (scoping)
- identify vulnerabilities - weak passwords, unpatched systems
- identify exploits & threats - hackers, natural disasters
- determine safeguards & countermeasures - security policies, backups, patches, updates etc
- determine which risks are acceptable or not

Enterprise risk management - risk management is treated very differently in companies of different sizes and compliance requirements. most companies will

institute enterprise risk management (erm) policies and procedures based on frameworks such as nist's rmf

Risk Types

- external
- internal
- multiparty (supply chain attack)
- intellectual property (ip) theft
- software compliance/licensing
- legacy systems

Quantitative risk assessment - this aims to assign concrete values to each risk factor:

- single loss expectancy (sle) - the amount that would be lost in a single occurrence of the risk factor. it's calculated by multiplying the value of the asset by an exposure factor (ef). ef is the percentage of the asset value that would be lost.
- annualized loss expectancy (ale) - the amount that would be lost over the course of a year. done by multiplying the sle by the annualized rate of occurrence (aro)

it's important to realize that the value of an asset isn't just about its material value but also the damage its compromise could cost the company (e.g a server is worth more than its cost).

Qualitative risk assessment - seeks out people's opinions of which risk factors are significant. assets and risks may be placed in categories such as high, medium or low value and critical, high, medium or low probability respectively.

Risk Factor	Impact	ARO	Cost of Controls	Overall Risk
Legacy Windows Clients				
Untrained Staff				
No Antivirus Software				

19.2 - Risk Controls

Risk Mitigation - This Is The Most Common Method Of Handling Risk And Typically Involves The Use Of Countermeasure Or Safe Guards. The Likelihood Of The Risk Occurring Must Be Reduced To The Absolute Minimum.

Risk Avoidance - The Cost Of The Risk Involved Is Too High And Must Be Avoided. Mitigation Means The Risk Probabilities Are Reduced To The Maximum While Avoidance Means The Risk Is Eliminated Completely

Risk Transference - This Involves Assigning Or Transferring The Risk To Another Entity Or Organization. In Other Words, The Risk Is Outsourced Because The Organization Cannot Mitigate The Risk On It's Own Due To Cost.

Risk Acceptance - The Cost Of Mitigating The Risk Outweighs The Cost Of Losing The Asset. Risk Can Also Be Accepted When There Isn't A Better Solution.

Risk Appetite & Residual Risk - Where Risk Acceptance Has The Scope Of A Single System, Risk Appetite Has A Project Or Institution-Wide Scope And Is Typically Constrained By Regulation And Compliance. Where Inherent Risks Are The Risks Before Security Controls Have Been Applied, Residual Risks Are Those Carried Over After The Controls Have Been Applied.

Control Risk Is A Measure Of How Much Less Effective A Security Control Has Become Over Time E.G Antivirus.

Risk Register - A Document Showing The Results Of Risk Assessments In A Comprehensible Format.

Business Impacts and Risk Value								
	Risk Criticality	**Overall Projected Loss**	**Critical Systems Downtime**	**Non-Critical Systems Downtime**	**Data Leak**	**Brand Damage**	**Compliance**	**Calculated Value**
5	Critical	>50 M	>30 min	>24 Hrs	Highly sensitive PII for more than 5 people	Re-branding, loss of major accounts	Major (Ex. License loss)	$100 M
4	High	5-50 M	Up to 30 min	5-24 Hrs	Detailed PII for multiple people	Major damage sustained for years	Fines >$200k, investigation impacting business	$50 M
3	Medium	500k-5 M	None	1-5 Hrs	General PII for multiple people or senstive PII for up to 5	Moderate reputational damage	Fines $200k-2 M, investigation not impacting business	$5 M
2	Low	50k-500k	None	Up to 1 Hr	None	Minor	Fines <$10k	$500k
1	Very Low	<50k	None	None	None	None	None	$5k

19.3 - Business Impact Analysis

business impact analysis (BIA) - this is the process of assessing what losses might occur for a range of threat scenarios.

Where BIA identifies risks, the business continuity plan (BCP) identifies controls and processes that enable an organization to maintain critical workflows in the face of an incident.

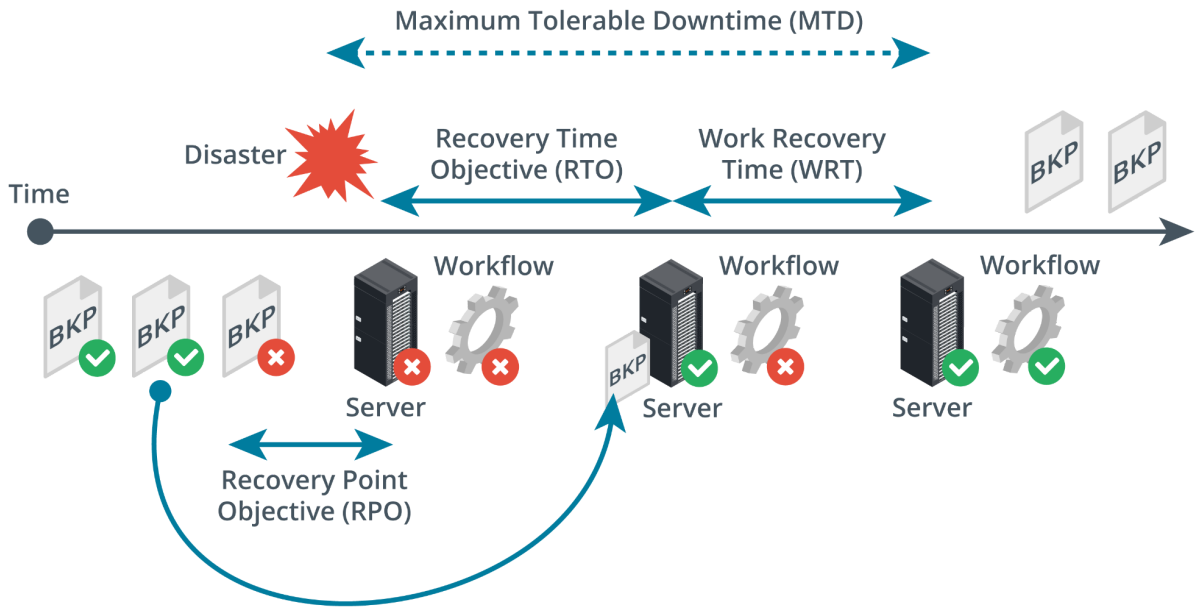
mission essential function (MEF) - this is one that cannot be deferred. the business must be able to perform the function as close to continually as possible.

maximum tolerable downtime (MTD) - the maximum amount of time a business can be down before it can no longer recover in a reasonable time or manner.

recovery time objective (RTO) - the targeted amount of time to recover business operations after a disaster.

work recovery time (WRT) - following systems recovery, there may be additional work to reintegrate different systems, test overall functionality and brief system users on any changes.

recovery point objective (RPO) - refers to the maximum amount of data that can be lost after recovery from a disaster before the loss exceeds what is tolerable to an organization.



Identification Of Critical Systems - Asset Types Include:

- People
- Tangible Assets
- Intangible Assets (Ideas, Reputation, Brand)
- Procedures (Supply Chains, Critical Procedures)

Single Points Of Failure - A SPOF Is An Asset That Causes The Entire Workflow To Collapse If It Is Damaged Or Unavailable. Can Be Mitigated By Provisioning Redundant Components.

Mean Time To Failure (Mttf) and Mean Time Between Failures (Mtbf) Represent The Expected Lifetime Of A Product. Mttf Should Be Used For Non-Repairable Assets

For Example, A Hard Drive Can Be Described With An Mttf While A Server With Mtbf.

- Calculation For Mtbf Is The Total Time Divided By The Number Of Failures. For Example 10 Devices That Run For 50 Hours And Two Of Them Fail, The Mtbf Is 250.
- Calculation For Mttf For The Same Test Is The Total Time Divided By Number Of Devices So 50 Hours/Failure.

Mean Time To Repair (Mttr) Is A Measure Of The Time Taken To Correct A Fault So That The System Is Restored To Full Operation. This Metric Is Important For Determining The Overall Rto.

Disasters

- Internal Vs External - Internal Could Be System Faults Or Malicious/Accidental Act By An Employee
- Person-Made - War, Terrorism, Pollution
- Environmental - Natural Disaster

A Site Risk Assessment Should Be Conducted To Identify Risks From These Factors.

Disaster Recovery Plans

- Identify Scenarios For Natural And Non-Natural Disasters And Options For Protecting Systems
- Identify Tasks, Resources And Responsibilities For Responding To A Disaster
- Train Staff In The Disaster Planning Procedures And How To React Well To Change.

Functional Recovery Plans

- Walkthroughs, Workshops And Seminars
- Tabletop Exercises - Staff "Ghost" The Same Procedures As They Would In A Disaster Without Actually Creating Disaster Conditions.
- Functional Exercises - Action Based Sessions Where Employees Can Validate The Drp By Performing Scenario-Based Activities In A Simulated Environment
- Full-Scale Exercises - Action Based Sessions That Reflect Real Situations. Held On Site And Uses Real Equipment And Real Personnel.

Section 20 - Implement Cyber Security Resilience

20.1 - Implementing Redundancy Strategies

High Availability - A Key Property Of Any Resilient System And Is Typically Measured Over A Period Of One Year.

The Maximum Tolerable Downtime (Mtd) Metric Expresses The Availability Requirement For A Particular Business Function.

High Availability Also Means That A System Is Able To Cope With Rapid Growth In Demand.

Scalability Is The Capacity To Increase Resources To Meet Demands With Similar Cost Ratios

- To Scale Out Is To Add More Resources In Parallel With Existing Resources
- To Scale Up Is To Increase The Power Of Existing Resources.

Elasticity Refers To The System's Ability To Handle These Changes On Demand In Real Time.

Fault Tolerance & Redundancy - A System That Can Experience Failures And Continue To Provide The Same Or Nearly The Same Level Of Service Is Said To Be Fault Tolerant.

Fault Tolerance Is Often Achieved By Provisioning Redundancy For Critical Components And Single Points Of Failure.

Power Redundancy

- Dual Power Supplies
- Managed Power Distribution Units (Pdus)
- Battery Backups And Upss
- Generators

A Ups Is Always Required To Protect Against Any Interruption As A Backup Generator Cannot Be Brought Online Fast Enough To Respond To A Power Failure.

Network Redundancy - Network Interface Card (Nic) Teaming Means The Server Is Installed With Multiple Nics Or Nics With Multiple Ports Or Both. Each Port Is Connected To Separate Network Cabling.

For Example Four 1gb Ports Gives An Overall Bandwidth Of 4gb So If One Port Goes Down, 3gb Of Bandwidth Will Still Be Provided.

Switching & Routing - Network Cabling Should Be Designed To Allow For Multiple Paths Between The Various Switches And Routers So That During A Failure Of One Part Of The Network, The Rest Remains Operational.

Load Balancers - Nic Teaming Provides Load Balancing At The Adapter Level, Load Balancing And Clustering Can Also Be Provisioned At A Service Level.

- A Load Balancing Switch Distributes Workloads Between Available Servers.
- A Load Balancing Cluster Enables Multiple Redundant Servers To Share Data And Session Information To Maintain A Consistent Service If There Is Failover From One Server To Another.

Disk Redundancy - Redundant Array Of Independent Disks (Raid) - Here Many Disks Can Act As Backups For Each Other To Increase Reliability And Fault Tolerance.

There Are Several Raid Levels Numbered 0 To 6

RAID Level	Fault Tolerance
Level 1	Mirroring means that data is written to two disks simultaneously, providing redundancy (if one disk fails, there is a copy of data on the other). The main drawback is that storage efficiency is only 50%.
Level 5	Striping with parity means that data is written across three or more disks, but additional information (parity) is calculated. This allows the volume to continue if one disk is lost. This solution has better storage efficiency than RAID 1.
Level 6	Double parity, or level 5 with an additional parity stripe, allows the volume to continue when two devices have been lost.
Nested (0+1, 1+0, or 5+0)	Nesting RAID sets generally improves performance or redundancy. For example, some nested RAID solutions can support the failure of more than one disk.

Geographical Redundancy & Replication - Data Replication Can Be Applied In Many Contexts:

- Storage Area Networks - Redundancy Can Be Provided Within The San And Replication Can Also Take Place Between Sans Using Wan Links.
- Database

- Virtual Machine - The Same Vm Instance Can Be Deployed In Multiple Locations. This Can Be Achieved By Replicating The Vm's Disk Image And Configuration Settings.

Geographical Dispersal Refers To Data Replicating Hot And Warm Sites That Are Physically Distant From One Another. This Means That Data Is Protected Against A Natural Disaster Wiping Out Storage At One Of The Sites.

Asynchronous & Synchronous Replication

- Synchronous Replication Is Designed To Write Data To All Replicas Simultaneously Therefore All Replicas Should Always Have The Same Data All The Time.
- Asynchronous Replication Writes Data To The Primary Storage First And Then Copies Data To The Replicas Scheduled Intervals. It Isn't A Good Choice For A Solution That Requires Data In Multiple Locations To Be Consistent

20.2 - Backup Strategies & Storage

Backups & Retention Policies - As Backups Take Up Space, There Is The Need For Storage Management Routines While Also Giving Adequate Coverage Of The Required Window.

The Recovery Window Is Determined By The Recovery Point Objective (Rpo) Which Is Determined Through Business Continuity Planning.

Backup Types

- full includes all files and directories while incremental and differential check the status of the archive attribute before including a file. The archive attribute is set whenever the file is modified so the backup software knows which files have been changed and need to be copied.

- incremental makes a backup of all new files as well as files modified since the last backup while differential makes a backup of all new and modified files since the last full backup. Incremental backups save backup time but can be more time-consuming when the system must be restored. The system is restored first from the last full backup set and then from each incremental backup that has subsequently occurred.

Snapshots And Images - Snapshots Are Used For Open Files That Are Being Used All The Time Because Copy-Based Mechanisms Are Not Able To Backup Open Files.

In Windows, Snapshots Are Provided For On Ntfs By The Volume Shadow Copy Service (Vss).

Backup Storage Issues - Backups Require Cia As Well And Must Be Secured At All Times. Natural Disasters Such As Fires And Earthquakes Must Also Be Accounted For.

Distance Consideration Is A Calculation Of How Far Offsite Backups Need To Be Kept Given Different Disaster Scenarios However They Mustn't Be Too Far To Slow Down A Recovery Operation.

The 3-2-1 Rule States That You Should Have 4 Copies Of Your Data Across Two Media Types With One Copy Held Offline And Offsite.

Backup Media Types

- disk
- network attached storage (nas) - an appliance that is a specially configured type of server that makes raid storage available over common network protocols
- tape - very cost effective and can be transported offsite but slow compared to disk-based solutions especially for restore operations
- san & cloud

Restoration order - if a site suffers an uncontrolled outage, ideally processing should be switched to an alternate site. However, if an alternate processing site is not available, then the main site must be brought back online as quickly as possible to minimize service disruption.

A complex facility such as a data center or campus network must be reconstituted according to a carefully designed order of restoration.

- enable and test power delivery systems (grid power, ups, secondary generators and so on)
- enable and test switch infrastructure then routing appliances and systems
- enable and test network security appliances (firewalls, ids)
- enable and test critical network servers (dhcp. dns, ntp and directory services)
- enable and test back-end and middleware (databases). verify data integrity
- enable and test front-end applications

- enable client workstations and devices and client browser access.

non-persistence

- snapshot/revert to known state - a saved system state that can be reapplied to the instance.
- rollback to known configuration
- live boot media - an instance that boots from read-only storage to memory rather than being installed on a local read/write hard disk.

when provisioning a new or replacement instance automatically, the automation system may use one of two types of mastering instructions.

- master image - the "gold copy" of a server instance with the os applications and patches all installed and configured.
- automated build from a template - similar to a master image and is the build instructions for an instance. rather than storing a master image, the software may build and provision an instance according to the template instructions.

20.3 - Cyber Security Resilient Strategies

Configuration management - configuration management ensures that each component of ict infrastructure is in a trusted state that has not diverged from its documented properties.

Change control and change management reduce the risk that changes to these components could cause service disruption.

Asset management - an asset management process tracks all the organization's critical systems, components, devices and other objects of value in an inventory.

An asset management database can be configured to store as much or as little information as it deemed necessary though typical data would be type, model, serial number, asset id, location, user(s), value and service information.

Asset identification & standard naming conventions - tangible assets can be identified using a barcode label or frequency id (rfid) tag attached to the device. the rfid tag is a chip programmed with asset data and can help to also track the location of the device making theft more difficult.

a standard naming convention for hardware and digital assets such as accounts and virtual machines makes the environment more consistent. This means errors are easier to spot and it's easier to automate through scripting.

The naming strategy should allow admins to identify the type and function of any particular resource or location at any point in the network directory.

Change control & change management - a change control process can be used to request and approve changes in a planned and controlled way. change requests are usually generated when

- something needs to be corrected
- when something changes
- where there is room for improvement in a process or system currently in place.

In a formal change management process, the need or reasons for change and the procedure for implementing the change is captured in a request for change (rfc) document and submitted for approval.

The implementation of changes should be carefully planned, with consideration for how the change will affect dependent components.

For major changes, a trial change should be attempted first and every change should be accompanied by a rollback plan so the change can be reversed if it has a negative impact.

site resiliency - an alternate processing site might always be available and in use while a recovery site might take longer to set up or only be used in an emergency.

- a hot site can failover almost immediately.
- a warm site could be similar but with the requirement that the latest data set will need to be loaded.
- a cold site takes longer to set up and could be an empty building waiting to have whatever equipment that is needed to be installed in it.

diversity and defense in depth - layered security is typically seen as improving cybersecurity resiliency because it provides defense in depth (multiple security controls).

Allied with defense in depth is the concept of security through diversity. Technology diversity refers to a mix of oss, applications, coding languages and so on while control diversity means that the layers of controls should combine different

classes of technical and administrative controls with the range of control functions to prevent, detect, correct and deter.

Vendor diversity - as well as deploying multiple types of controls, there are also advantages in leveraging vendor diversity.

While single vendor solutions provide interoperability and can reduce training and support costs, it does have several disadvantages.

- not obtaining best-in-class performance
- less complex attack surface.
- less innovation

Deception and disruption strategies

Active defense means an engagement with the adversary and can mean the deployment of decoy assets to act as lures or bait.

A honey pot is a system set up to attract threat actors, with the intention of analyzing attack strategies and tools to provide early warnings of attack attempts. it could also be used to detect internal fraud, snooping and malpractice.

A honeynet is an entire decoy network.

On a production network, a honeypot is more likely to be located in a dmz, or on an isolated segment on the private network if the honeypot is seeking to draw out insider threats.

A honeypot or honeynet can be combined with the concept of a honeyfile which is convincingly useful but actually fake data.

Some examples of disruption strategies include:

- using bogus dns entries to list multiple non-existent hosts
- configuring a web server with multiple decoy directories
- using port triggering or spoofing to return fake telemetry data when a host detects port scanning activity. This will result in multiple ports being falsely reported as open.
- using a dns sinkhole to route suspect traffic to a different network such as a honeynet.

Section 21 - Implement Physical Security

21.1 - Physical Security Controls

Physical access controls - these are security measures that restrict and monitor access to specific physical areas or assets. They can control access to buildings, server rooms, data centers, finance or legal areas and so on.

Physical access controls depend on the same access control fundamentals as network or os security:

- authentication - create lists of approved people
- authorization - create barriers around a resource so access to it is controlled through defined entry and exit points
- accounting - keep a record of when entry/exit points are used and detect security breaches.

Site layout, fencing & lighting - given constraints of cost and existing infrastructure, try to plan the site using the following principles

- locate secure zones
- use a demilitarized zone design for the physical space and position public access areas so that guests do not pass near secure zones.
- use signage and warnings to enforce the idea that security is tightly controlled.
- entry points to secure zones should be discreet. do not allow an intruder the opportunity to inspect security mechanisms.
- try to minimize traffic having to pass between zones. the flow should be "in and out" rather than "across and between"
- give high traffic public areas high visibility
- in secure zones, do not display screens facing toward pathways or windows. alternatively use one-way glass so that no one can look in through windows.

Gateways and locks - in order to secure a gateway, it must be fitted with a lock. lock types can be categorized as follows:

- physical - a conventional lock that prevents the door handle from being operated without the use of a key.

- electronic - rather than a key, the lock is operated by entering a pin on an electronic keypad. This type of lock is also referred to as cipher, combination or keyless.
- biometric - a lock may be integrated with biometric scanner

Physical attacks against smart cards and usb - smart cards used to bypass electronic locks can be vulnerable to cloning and skimming attacks.

- card cloning -making one or more copies of an existing card. a lost or stolen card with no cryptographic protections can be physically duplicated.
- skimming - refers to using a counterfeit card to capture card details which are then used to program a duplicate.

Malicious usb charging cables and plugs are also a widespread problem. a usb data blocker can provide mitigation against "juice-jacking" attacks by preventing any sort of data transfer when the smartphone is connected to a charge point.

alarm systems & sensors - there are five main types of alarms

- circuit - a circuit-based alarm sounds when the circuit is opened or closed depending on the type of alarm. could be caused by a door or window opening or by a fence being cut.
- motion detection - a motion-based alarm is linked to a detector triggered by any movement within an area.
- noise detection - an alarm triggered by sounds picked up by a microphone.
- proximity - rfid tags and readers can be used to track the movement of tagged objects within an area.
- duress - this type of alarm is triggered manually by staff if they come under threat.

Security guards & cameras - surveillance is typically a second layer of security designed to improve the resilience of perimeter gateways.

Security guards can be placed in front of secure and important zones and can act as a very effective intrusion detection and deterrence mechanism but can be expensive.

CCTV is a cheaper means of providing surveillance than using security guards.

The other big advantage is that movement and access can also be recorded but the main drawback is that response times are longer and security may be compromised if not enough staff are present to monitor the camera feeds.

Reception personnel & id badges - a very important aspect of surveillance is the challenge policy and can be quite effective against social engineering attacks.

An access list can be held at the reception area for each secure area to determine who is allowed to enter.

Reception areas for high-security zones might be staffed by at least two people at all times

21.2 - physical host security controls

Secure areas - a secure area is designed to store critical assets with a higher level of access protection than general office areas. The most vulnerable point of the network infrastructure will be the communications or server room.

Air gap/ DMZ - an air gapped host is one that is not physically connected to any network. such a host would normally have stringent physical access controls.

an air gap within a secure area serves the same function as a DMZ. as well as being disconnected from any network, the physical space around the host makes it easier to detect unauthorized attempts to approach the asset.

Protected distribution & faraday cages - a physically secure cabled network is referred to as protected cable distribution or as a protected distribution system (pds). there are two main risks:

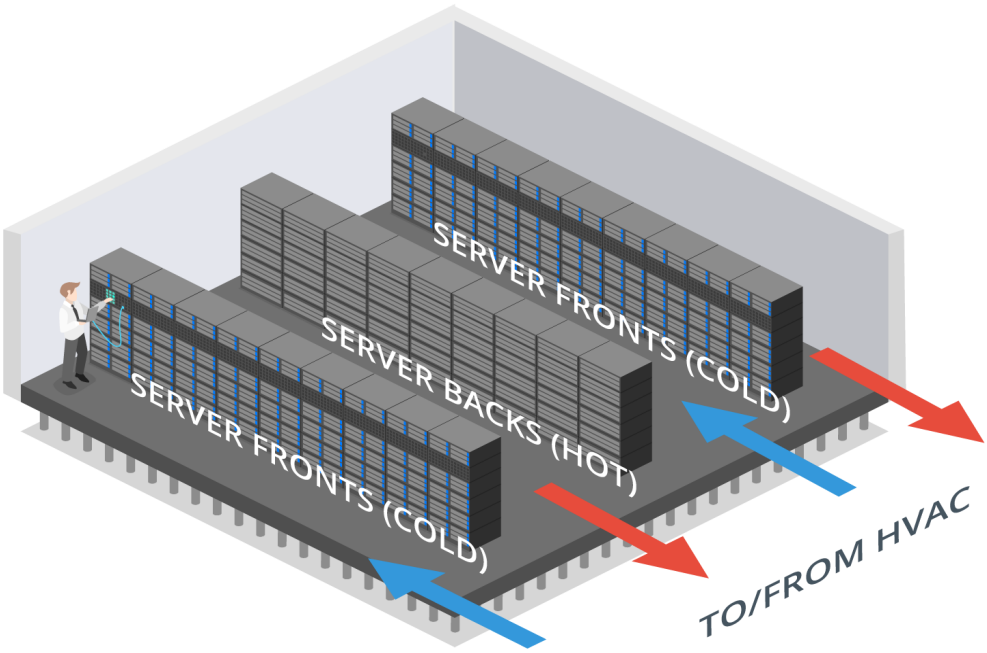
- an attacker could eavesdrop using a tap
- an attacker could cut the cable (dos)

heating, ventilation & air conditioning - environmental controls mitigate the loss of availability through mechanical issues with equipment such as overheating.

For computer rooms and data centers, the environment is typically kept at a temperature of about 20-22 degrees centigrade and relative humidity of 50%.

Hot and cold aisles - a server room or data center should be designed in such a way as to maximize air flow across the server or racks.

The servers are placed back-to-back not front-to-back so that the warm exhaust from one bank of servers is not forming the air intake for another bank. This is referred to as a hot/cold aisle arrangement.



Fire detection & suppression - fire suppression systems work on the basis of the fire triangle. This triangle works on the principle that a fire requires heat, oxygen and fuel to ignite and burn so removing any one of them will suppress the fire.

Overhead sprinklers may also be installed but there is the risk of a burst pipe and accidental triggering as well as the damage it could cause in the event of an actual fire.

secure data destruction - physical security controls also need to take account of the disposal phase of the data life cycle. Media sanitization and remnant removal refer to erasing data from hard drives, flash drives and tape media before they are disposed of.

there are several physical destruction options:

- burning
- shredding and pulping
- pulverization
- degaussing - exposing a hard disk to a powerful electromagnet disrupts the magnetic pattern that stores the data.

Data sanitization tools - the standard method of sanitizing an hdd is called overwriting. This can be performed using the driver's firmware tools or a utility program.

The most basic type of overwriting is called zero filling which just sets each bit to zero. Single pass zero filling can leave patterns that can be read with specialist tools.

secure erase (se) - since 2001, the sata and serial attached scsi (sas) specifications have included a secure erase (se) command. This command can be invoked using a drive/array utility or the hdparm linux utility. on HDDS, this performs a single pass of zero-filling.

Instant secure erase (ise) - hdds and ssds that are self-encrypting drives (seds) support another option invoking a sanitize command set in sata and sas standards from 2012 to perform a crypto ease. Drive vendors implement this as ise. with an ise, all data on the drive is encrypted using media encryption key (mek) and when the erase command is issued, the mek is erased rendering the data unrecoverable.