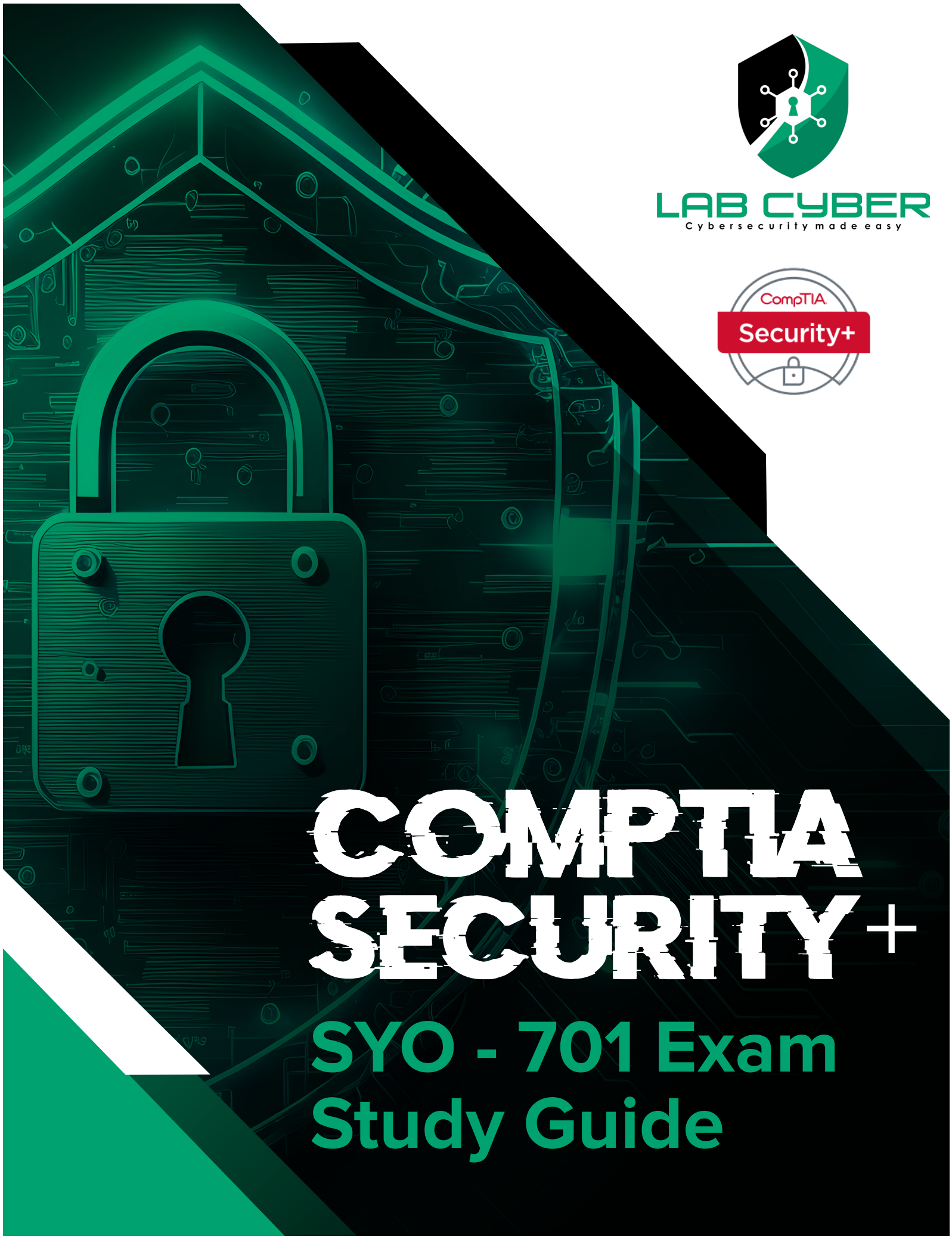


LAB CYBER

Cybersecurity made easy

CompTIA Security+

COMPTIA SECURITY+

SYO - 701 Exam Study Guide

Table of Contents

Section 1 -

Summarize Fundamental Security Concepts

Section 2 -

Explaining Threat Actors And Threat Vectors

Section 3 -

Explain Cryptographic Solutions

Section 4 -

Implement Identity and Access Management

Section 5 -

Secure Enterprise Network Architecture

Section 6 -

Secure Cloud Network Architecture

Section 7 -

Explain Resiliency and Site Security Concepts

Section 8 -

Explain Vulnerability Management

Section 9 -

Evaluate Network Security Capabilities

Section 10 -

Assess Endpoint Security Capabilities

Section 11 -

Enhance Application Security Capabilities

Section 12 -

Explain Incident Response and Monitoring Concepts

Section 13 -

Section 13 - Analyze Indicators of Malicious Activity

Section 14 -

Summarize Security Governance Concepts

Section 15 -

Explain Risk Management

Section 16 -

Summarize Data Protection and Compliance Concepts

SECTION 1 -

SUMMARIZE FUNDAMENTAL SECURITY CONCEPTS

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** - Hwwwwere 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 Gap Analysis

Gap analysis is a process that identifies how an organization's security systems deviate from those required or recommended by a framework. This will be performed when first adopting a framework or when meeting a new industry or legal compliance requirement. The analysis might be repeated every few years to meet compliance requirements or to validate any changes.

For each section of the framework, a gap analysis report will provide an overall score, a detailed list of missing or poorly configured controls associated with that section, and recommendations for remediation.

While some or all work involved in gap analysis could be performed by the internal security team, a gap analysis is likely to involve third-party consultants. Frameworks and compliance requirements from regulations and legislation can be complex enough to require a specialist. Advice and feedback from an external party can alert the internal security team to oversights and to new trends and changes in best practice.

1.4 Control Objectives

Controls are tactics or strategies that proactively minimize risk by reducing or eliminating:

- A vulnerability
- The likelihood that a threat actor will exploit a vulnerability
- The impact of an exploit

Countermeasures are controls implemented to address a **specific** threat.

Controls can be measured by

- **Functionality -** what the control does
- **Effectiveness -** how well a control works (consistency, reliability, timely)
- **Assurance -** a measure of confidence that intended security controls are effective in their application
- Cost-Benefit

Control objectives refer to a statement of a desired result that should be achieved by implementing a control or set of controls.

Defense-in-depth

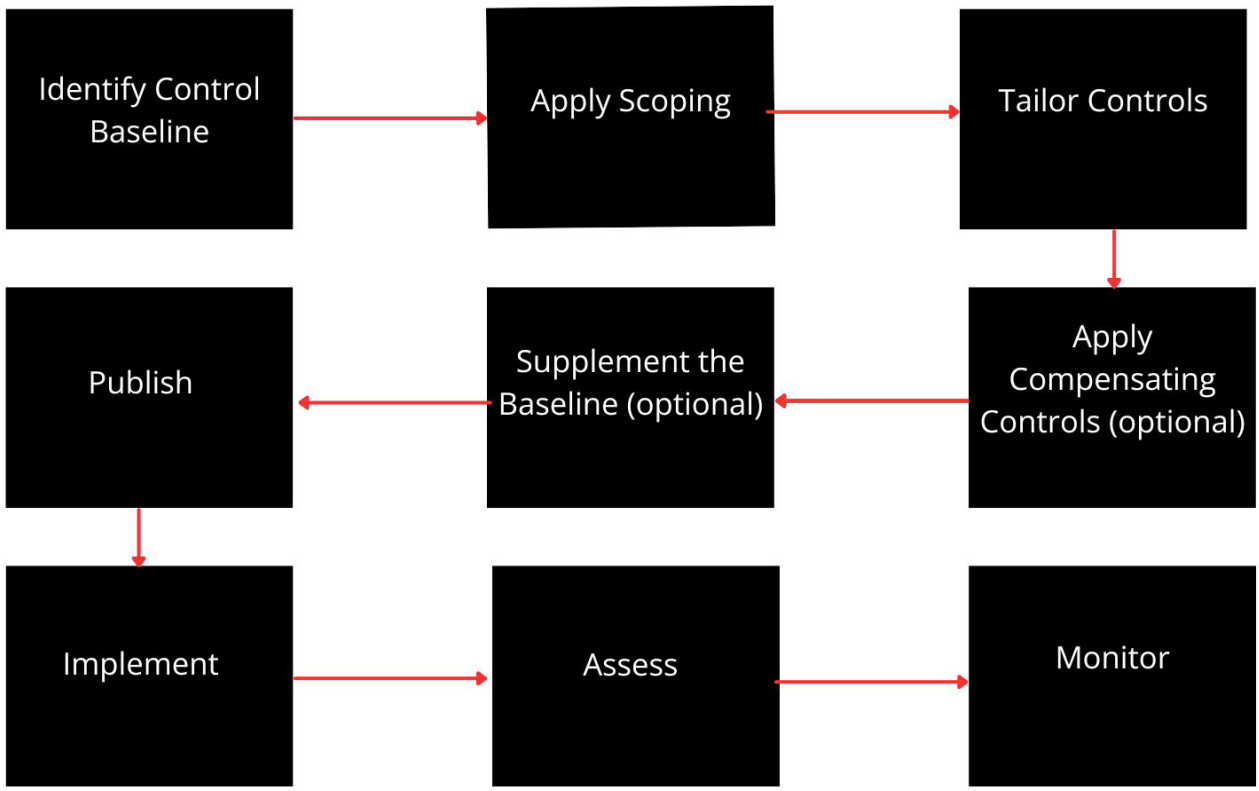
Design and implementation of multiple overlapping layers of diverse controls. Controls should maintain independence and not be subject to the cascading effect.

Security Control Baselines

These express the minimum standards for a given environment

Fine-Tuning Controls

- **Scoping -** Eliminating unnecessary baseline recommendations that are not applicable
- **Tailoring -** Customizing baseline recommendations to align with objectives
- **Compensating -** Substituting a recommended baseline control with a similar control
- **Supplementing -** Adding to the baseline recommendations



1.5 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.

1.6 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.

1.7 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.

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 Vulnerable Software & Network Vectors

Vulnerable software is one that contains a flaw in its code or design that can be exploited to circumvent access control or to crash the process.

Unsupported systems & applications - An unsupported system is one whose vendor no longer develops updates or patches for it.

One strategy for dealing with unsupported apps that cannot be replaced is to try to isolate them from other systems. The idea is to reduce opportunities for a threat actor to access the vulnerable app and run exploit code. Using isolation as a substitute for patch management is an example of a compensating control.

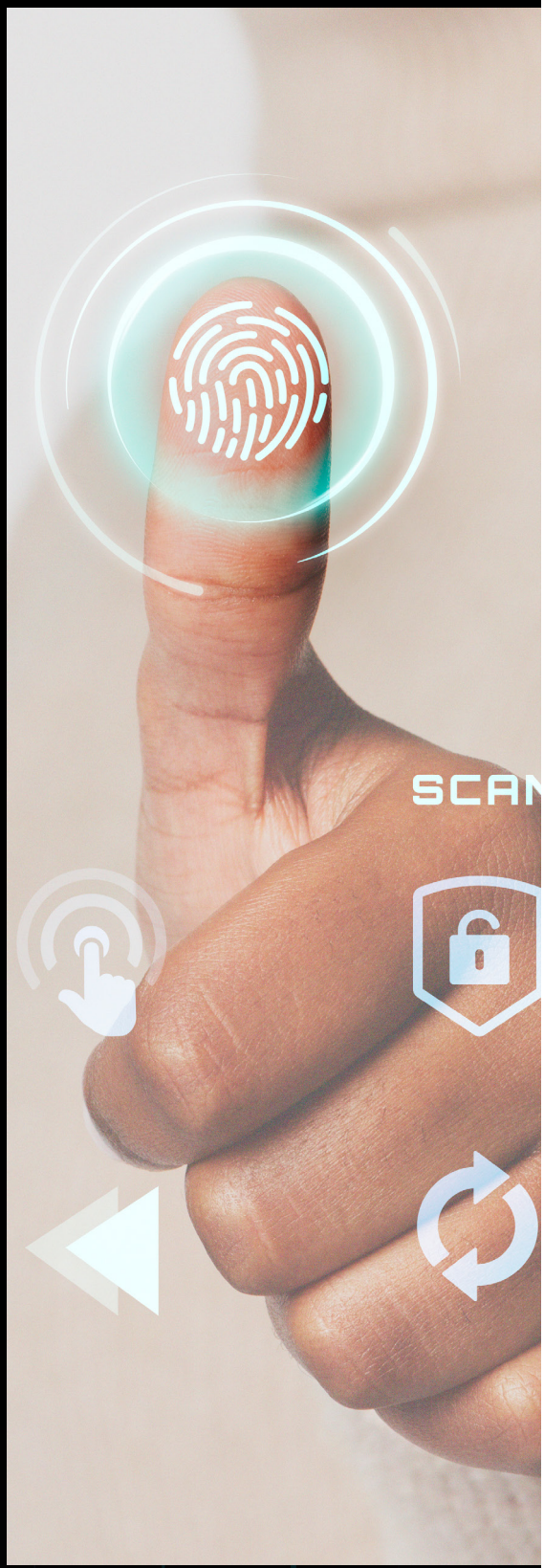
Network Vectors - An exploit technique for any given software vulnerability can be classed as either remote or local.

- Remote means the vulnerability can be exploited by sending code to the target over a network.
- Local means that the exploit code must be executed from an authenticated session on the computer.

An unsecure network is one that lacks the attributes of CIA while a secure network uses an access control framework and cryptographic solutions to identify, authenticate, authorize and audit network users, hosts and traffic.

Some specific threat vectors associated with unsecure networks are:

- **Direct Access -** Getting physical access to an unlocked workstation, stealing a PC or maybe using a boot disk to install malicious tools.
- **Wired Network -** A threat actor attaches an unauthorized device to a physical network port and is able to launch eavesdropping or DoS attacks.
- **Remote & Wireless Network -** The attacker either obtains credentials for a remote access or wireless connection to the network or cracks the security protocols used for authentication
- **Cloud Access -** The attacker is likely to target the accounts used to develop services in the cloud or manage cloud systems. They may also try to attack the cloud service provider (CSP) as a way of accessing the victim system.
- **Bluetooth Network -** The threat actor exploits a vulnerability or misconfiguration to transmit a malicious file to a user's device over the Bluetooth personal area wireless networking protocol.
- **Default Credentials -** The attacker gains control of a network device or app because it has been left configured with a default password
- **Open Service Port -** The threat actor is able to establish an unauthenticated connection to a logical TCP or UDP network port



2.6 Lure-Based & Message-Based Vectors

This is something superficially attractive that causes its target to want it even though it may be concealing something dangerous.

In cybersecurity terms, when the target opens the file bait, it delivers a malicious payload hook that will typically give the threat actor control over the system or perform service disruption

- **Removable Device -** The attacker conceals malware on a USB thumb drive or memory card and tries to trick employees into connecting the media to a PC or smartphone typically through a drop attack.
- **Executable File -** The threat actor conceals exploit code in a program file (Trojan Malware).
- **Document Files -** Malware is concealed by embedding it in word processing and PDF format files.
- **Image Files -** The exploit code is concealed in an image file that targets a vulnerability in browser or document editing software.

Message-Based Vectors

- **Email -** The attacker sends a malicious file attachment via email that allows attachments (phishing).
- Short Message Service (SMS)
- **Instant Messaging -** Most apps for this are more secure than SMS because they use encryption but they can still contain software vulnerabilities.
- **Web & Social Media -** Malware may be concealed in files attached to posts or presented as downloads.

The most powerful exploits are **zero-click** which means that simply receiving an attachment or viewing an image on a web page can trigger the exploit.

2.7 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

- The 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

2.8 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.

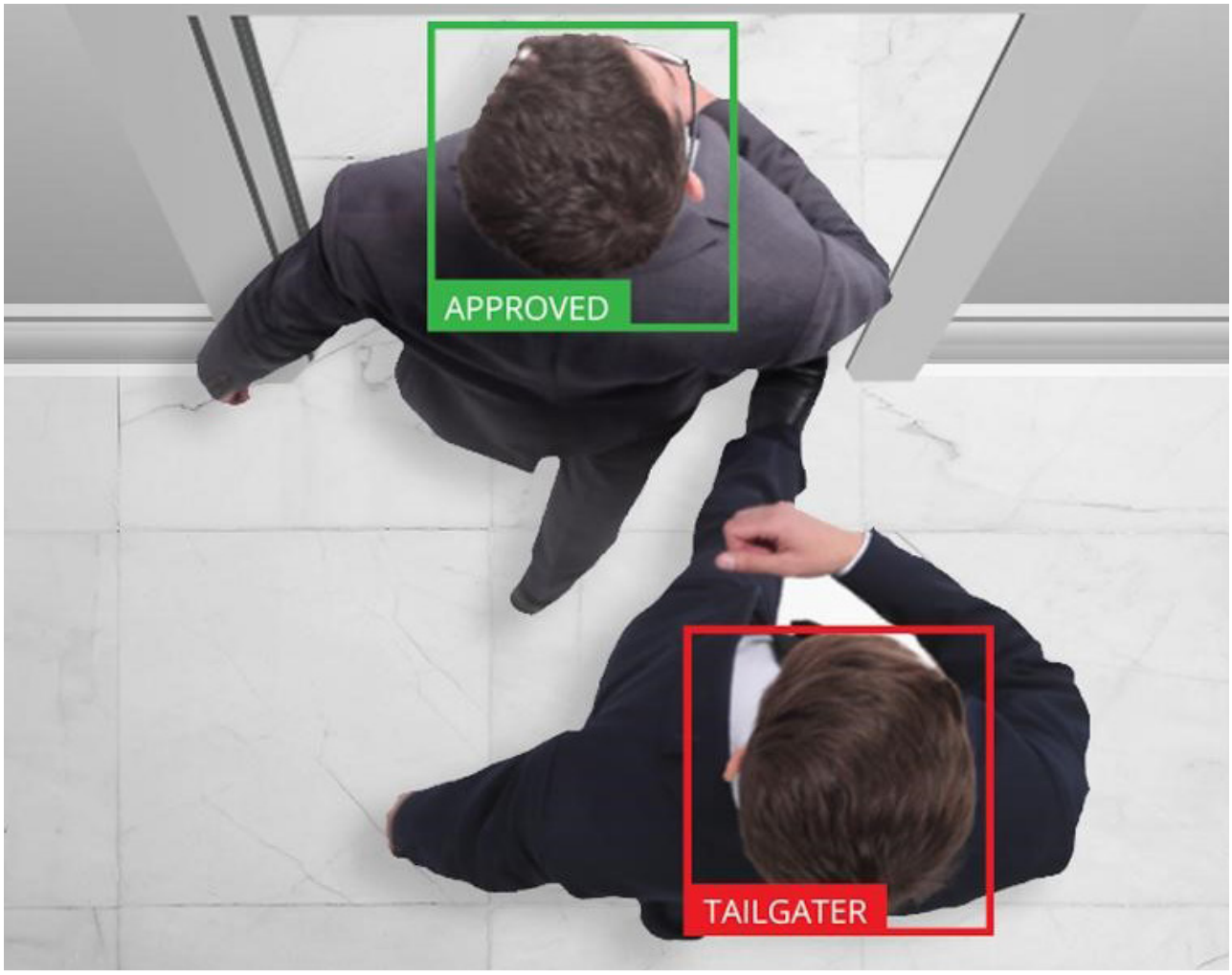
Phishing - Relies on creating a sense of excitement or panic in the target using emails.

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

Tailgating - The attacker without access authorization closely follows an authorized person in a reserved area



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

Shoulder Surfing - Obtaining sensitive information by spying

Dumpster Diving - Obtaining sensitive information by going through the company trash

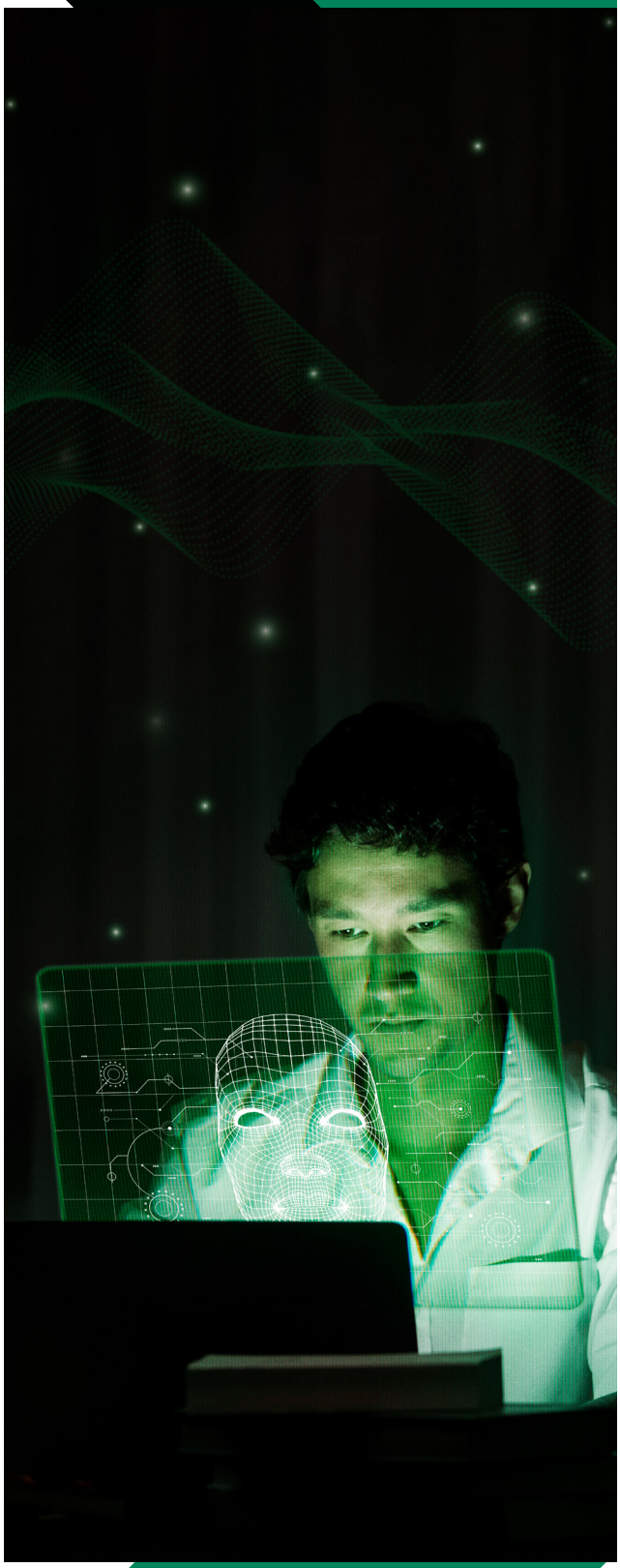
Credential Darvesting - Using phishing emails and spamming campaigns to gather information which can then be sold.

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.



SECTION 3 -

EXPLAIN CRYPTOGRAPHIC SOLUTIONS

3.1 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

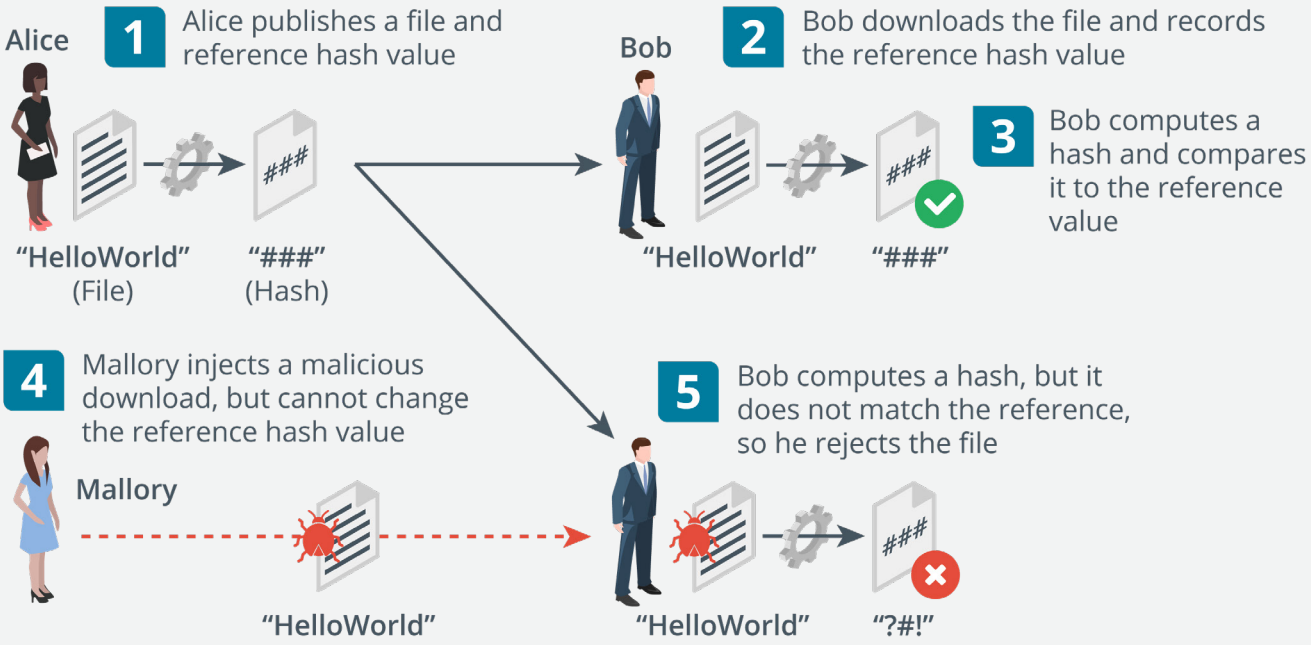
Cipher - The Process (Algorithm) Used to Encrypt and Decrypt a Message

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

3.2 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 plain text with different cipher text. e.g rot13 rotates each letter 13 places so a becomes n

The cipher text "uryyb jbeyq" means "hello world"

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

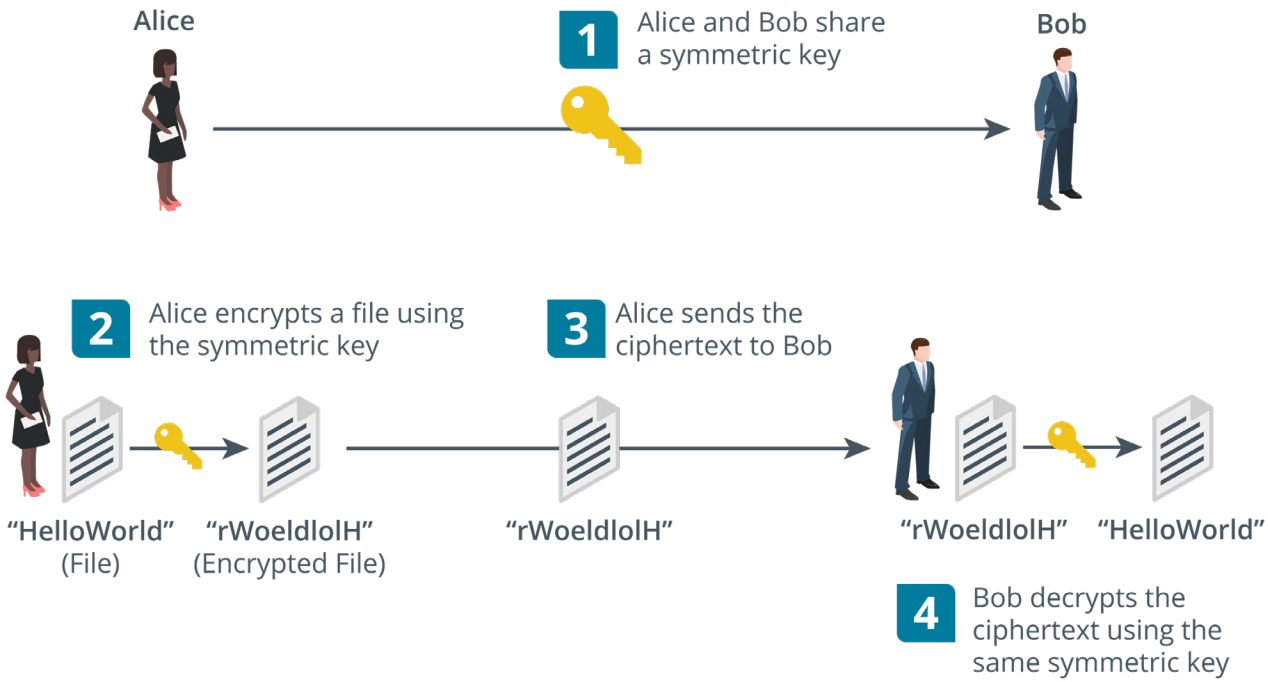
Consider the cipher text “hloolelwrd”

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 ast and is used or bulk encryption of large amounts of data but can be vulnerable if the key is stolen.

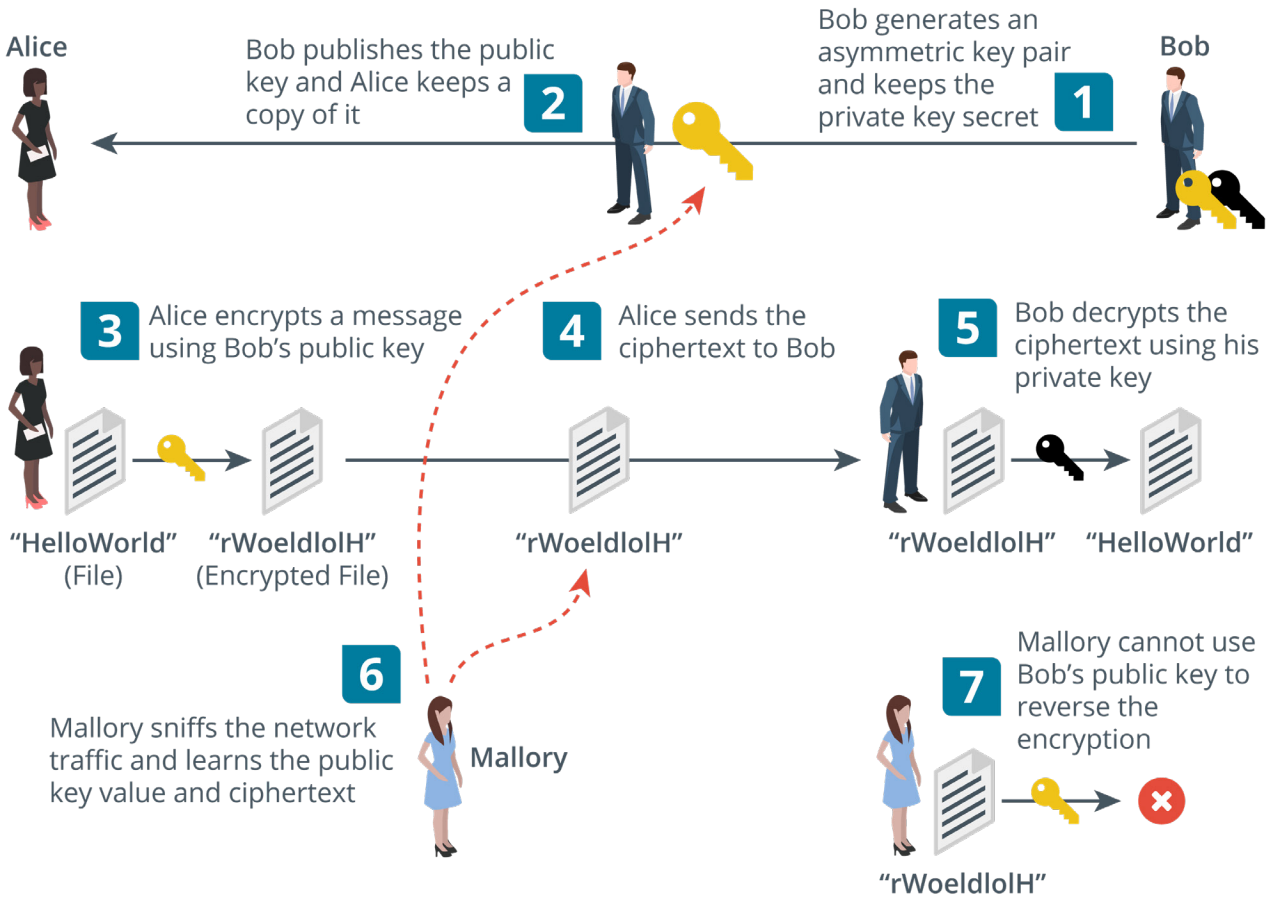


There are two types - Stream ciphers & block ciphers

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.

3.3 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.

3.4 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 cipher text 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.

3.5 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 Cipher text 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 cover text.

3.6 Certificates, Pkis, Ras & Csrs

Public & Private Key Usage

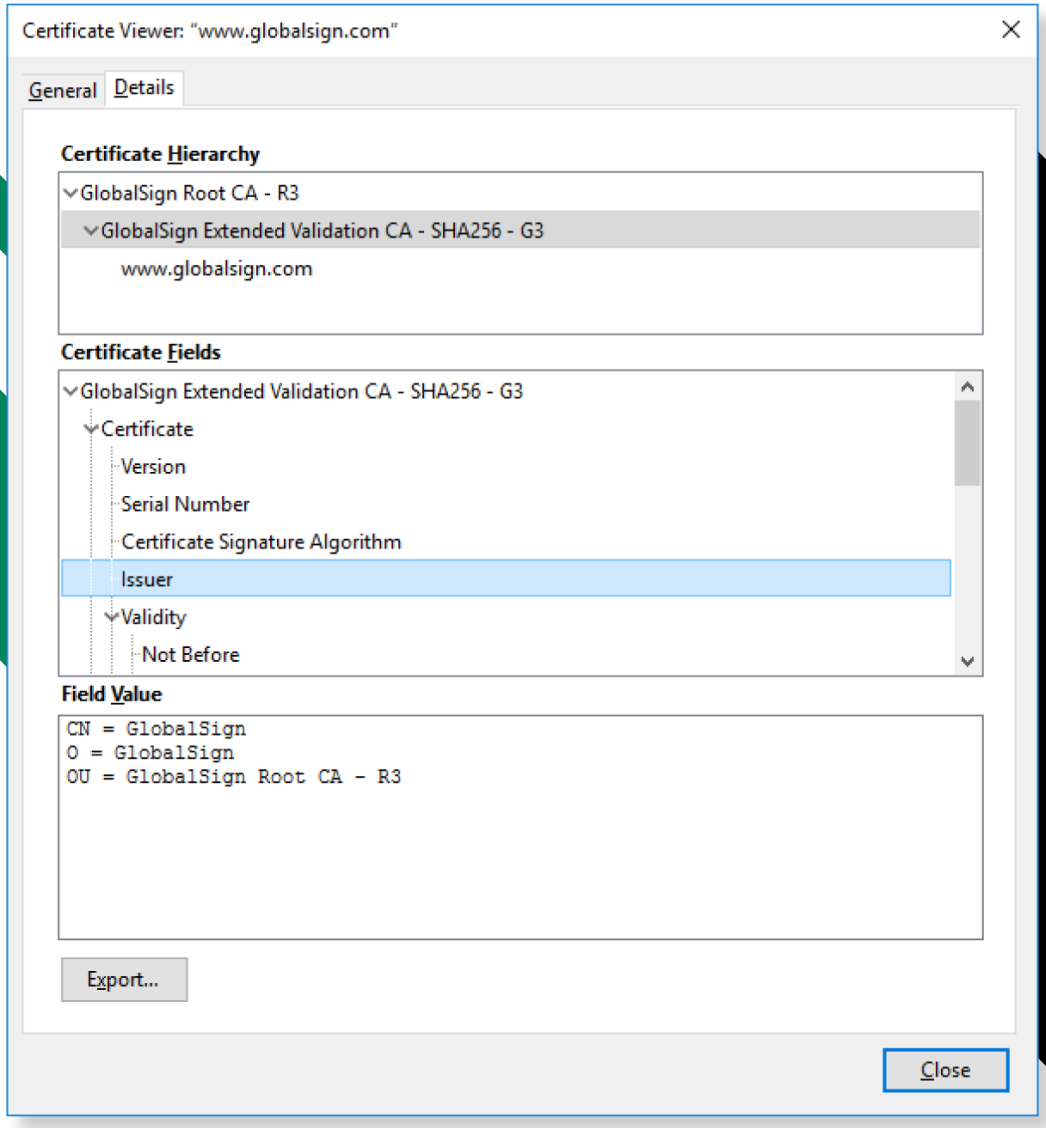
When you want others to send you confidential messages, you give them your public key to encrypt the message and then you decrypt the message with your private key.

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 off-line 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 off-line CA meaning it is disconnected from any network and only brought back on line to add or update intermediate CAs.

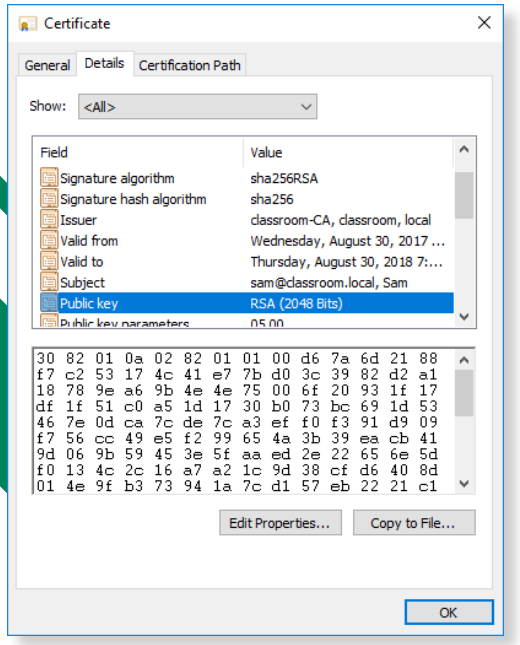
Registration authorities and CSRS - registration is the process by which end users create an account with the CA and become authorized to request certificates.

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.

3.7 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.

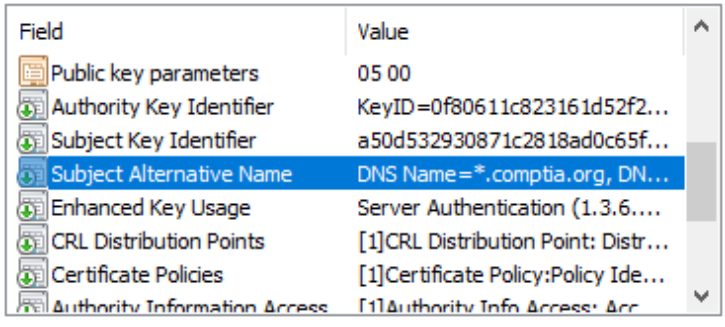


Field	Usage
Serial number	A number uniquely identifying the certificate within the domain of its CA.
Signature algorithm	The algorithm used by the CA to sign the certificate.
Issuer	The name of the CA.
Valid from/to	Date and time during which the certificate is valid.
Subject	The name of the certificate 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

3.8 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.

3.9 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 4 -

IMPLEMENT IDENTITY AND ACCESS MANAGEMENT

4.1 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

4.2 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.

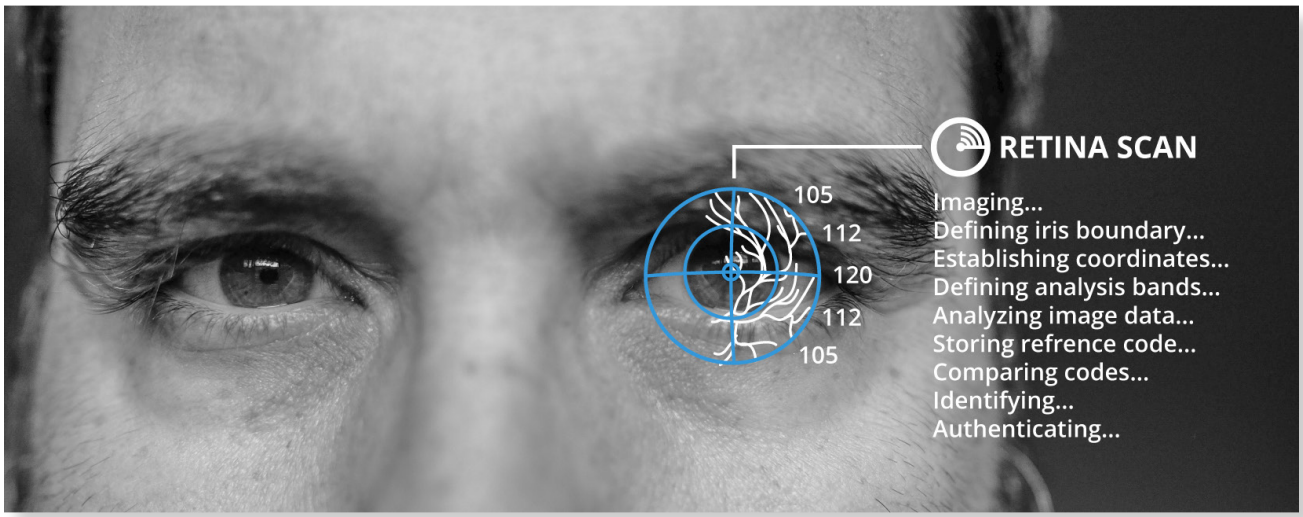
- **Somewhere you are -** This could be a geographic location measured using a device's location service or ip address. This isn't used as a primary authentication factor but may be used as a continuous authentication mechanism.
- **Something you can do -** Behavioral characteristics such as the way 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.

4.3 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.

4.4 Password Concepts

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 **NIST** guidelines:

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.

Password Managers - These are used to mitigate poor credential management practices that are hard to control.

The main risks involved are selection of a weak master password, compromise of the vendor's cloud storage or systems and impersonation attacks designed to trick the manager into filling a password to a spoofed site.

4.5 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.

4.6 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.

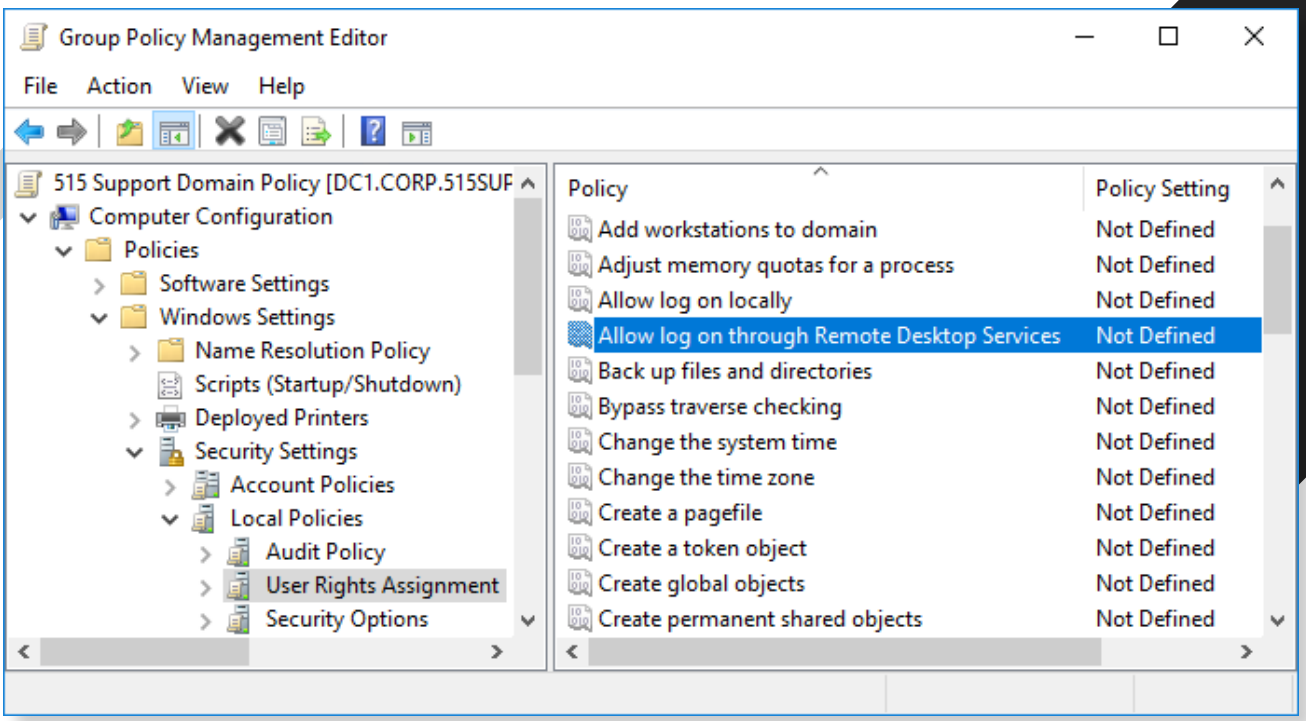
Oauth and openid connect - Many public clouds use application programming interfaces (apis) based on representational state transfer (rest) rather than soap.

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.

4.7 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)



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.

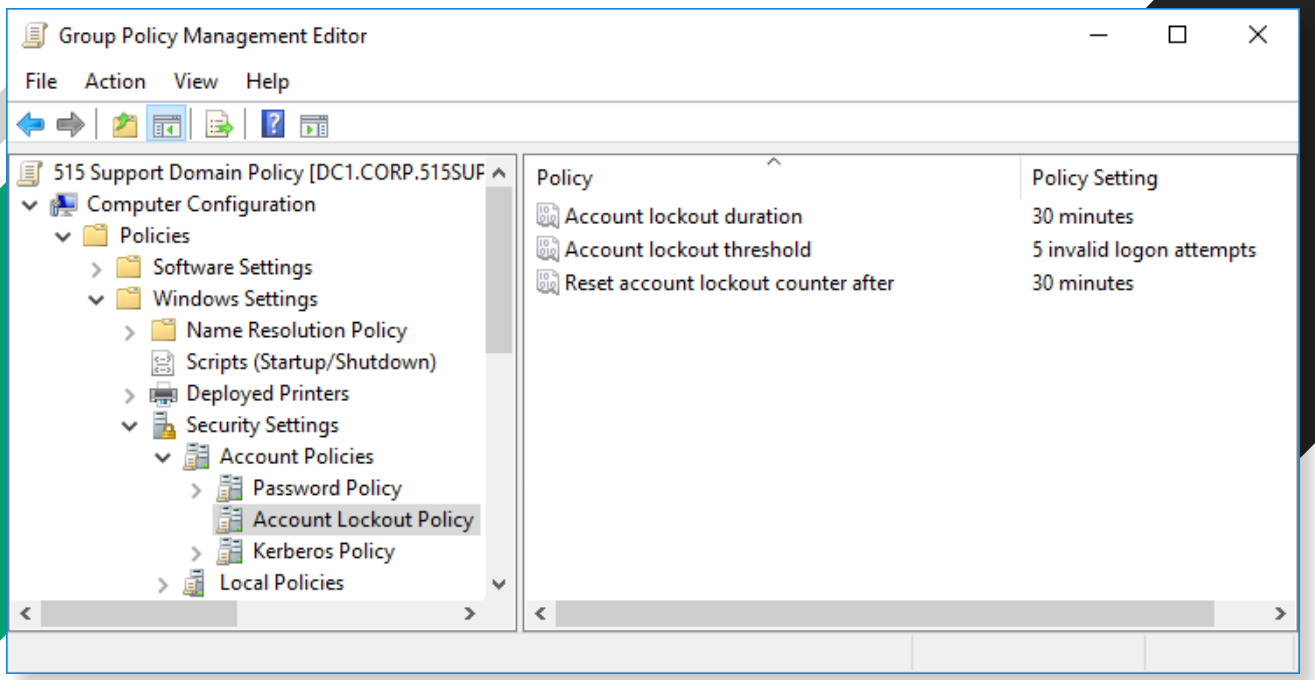
Geofencing Refers To Accepting Or Rejecting Access Requests Based On Location.

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



4.8 Privileged Access Management

A privileged account is one that can make significant configuration changes to a host, such as installing software or disabling a firewall or other security system. Privileged accounts also have the right to manage network appliances, application servers, and databases.

Privileged Access Management (PAM) refers to policies, procedures and technical controls to prevent compromise of privileged accounts.

It is a good idea to restrict the number of administrative accounts as much as possible. The more accounts there are, the more likely it is that one of them will be compromised. On the other hand, you do not want administrators to share accounts or to use default accounts, as that compromises accountability.

To protect privileged account credentials, it is important not to sign in on untrusted workstations. A **secure administrative workstation (SAW)** is a computer with a very low attack surface running the minimum possible apps.

Traditional administrator accounts have standing permissions. **Just-in-time (JIT)** permissions means that an account's elevated privileges are not assigned at log-in. Instead, the permissions must be explicitly requested and are only granted for a limited period. This is referred to as zero standing privileges (ZSP).

There are three main models for implementing this

- **Temporary Elevation -** Means that the account gains administrative rights for a limited period. The User Account Control (UAC) feature of Windows and the sudo command in Linux use this concept.
- **Password Vaulting/Brokering -** The privileged account must be "checked out" from a repository and is made available for a limited amount of time. The administrator must log a justification for using the privileges.
- **Ephemeral Credentials -** Means the system generates or enables an account to use to perform the administrative task and then destroys or disables it once the task has been performed. Temporary or ephemeral membership of security groups or roles can serve a similar purpose.

4.9 Local, Network & Remote Authentication

This involves a complex architecture of components but the following three scenarios are typical:

Windows Authentication

- **Windows local sign-in --** the Local Security Authority (LSA) compares the submitted credential to a hash stored in the Security Accounts Manager (SAM) database.
- **Windows network sign-in --** the LSA can pass the credentials for authentication to a network service either Kerberos or NT LAN Manager (NTLM) authentication.
- **Remote sign-in --** if the user's device is not connected to the local network, authentication can take place over some type of virtual private network (VPN) or web portal.

Linux Authentication -Local user account names are stored in **/etc/passwd**. When a user logs in to a local interactive shell, the password is checked against a hash stored in /etc/shadow.

A pluggable authentication module (PAM) is a package for enabling different authentication providers.

Single Sign-On (SSO) - This system allows the user to authenticate once to a local device and be authenticated to compatible application servers without having to enter credentials again.

In Windows, SSO is provided by the Kerberos framework.

4.10 Kerberos Authentication & Authorization

Kerberos is a single sign-on network authentication and authorization protocol used on many networks notably as implemented by Microsoft's Active Directory (AD) service.

Kerberos Authentication - This protocol is made up of 3 parts

- KDC (Authentication Service)
- Principal
- Application Server

SECTION 5 -

SECURE ENTERPRISE NETWORK ARCHITECTURE

5.1 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.

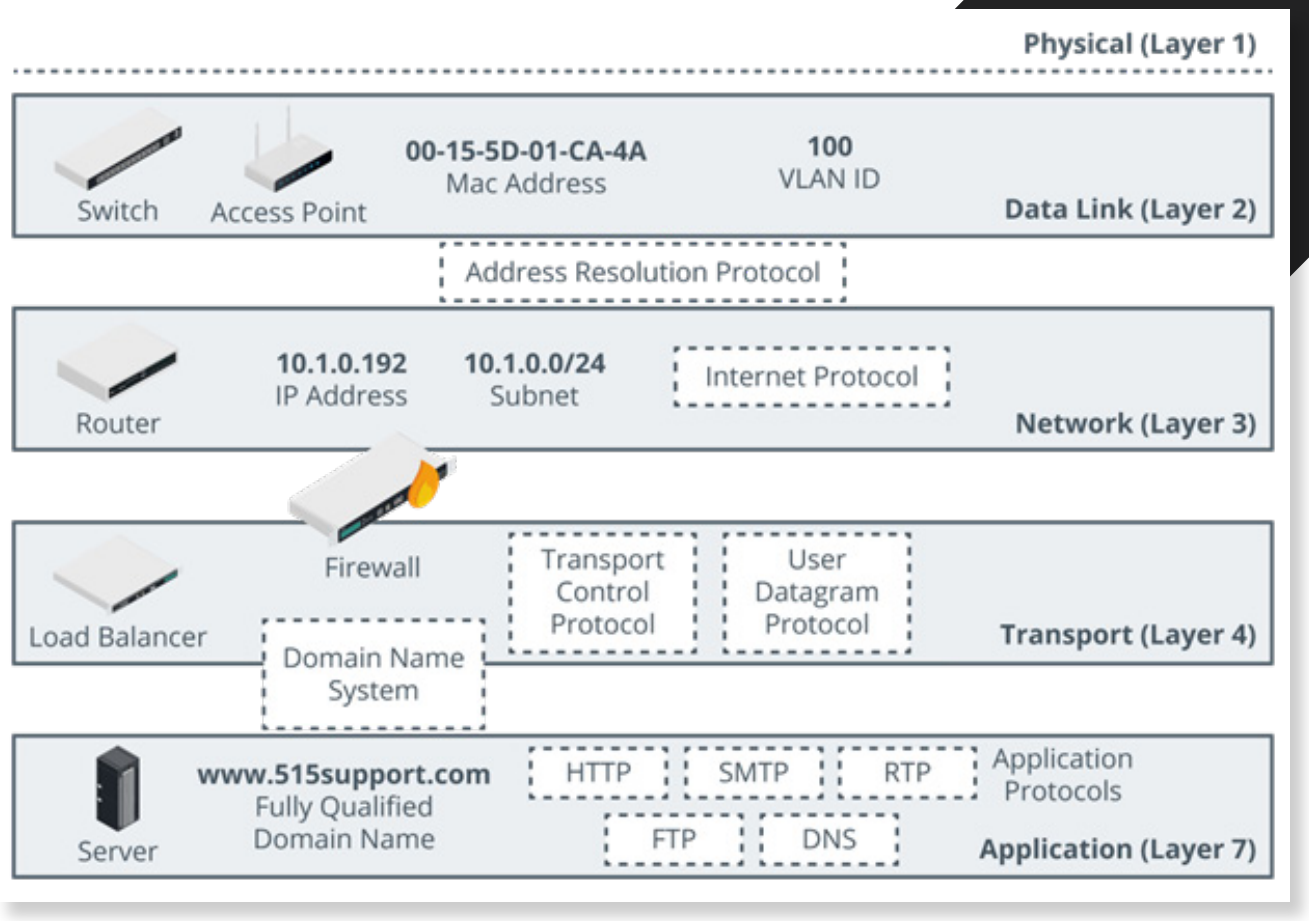
Load balancers - distribute traffic between network segments or servers to optimize performance. They work at layer 4 of the OSI model or higher

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.



5.2 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.