SECURITY+ EXAM CRAM

THE COMPLETE COURSE

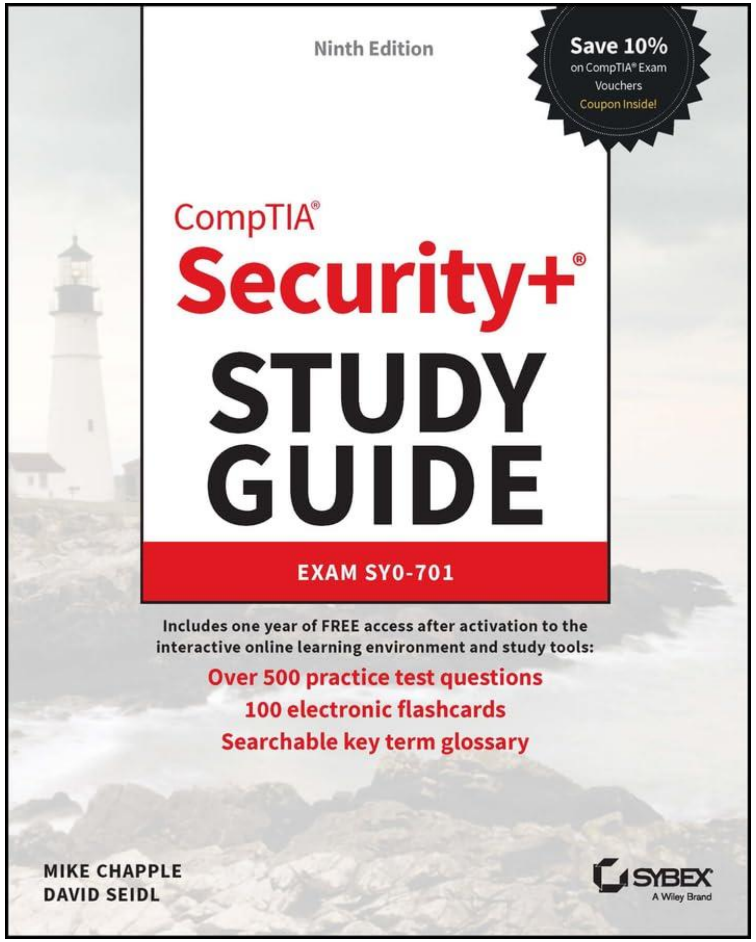
2024 EDITION

DOMAIN 1

Coverage of every topic in the official exam syllabus!

with **Pete Zerger** vCISO, CISSP, MVP

Covers **SY0-701**



Ninth Edition

Save 10% on CompTIA® Exam Vouchers Coupon Inside!

CompTIA® Security+® STUDY GUIDE

EXAM SY0-701

Includes one year of FREE access after activation to the interactive online learning environment and study tools:

Over 500 practice test questions
100 electronic flashcards
Searchable key term glossary

MIKE CHAPPLE
DAVID SEIDL

SYBEX A Wiley Brand

SECURITY+

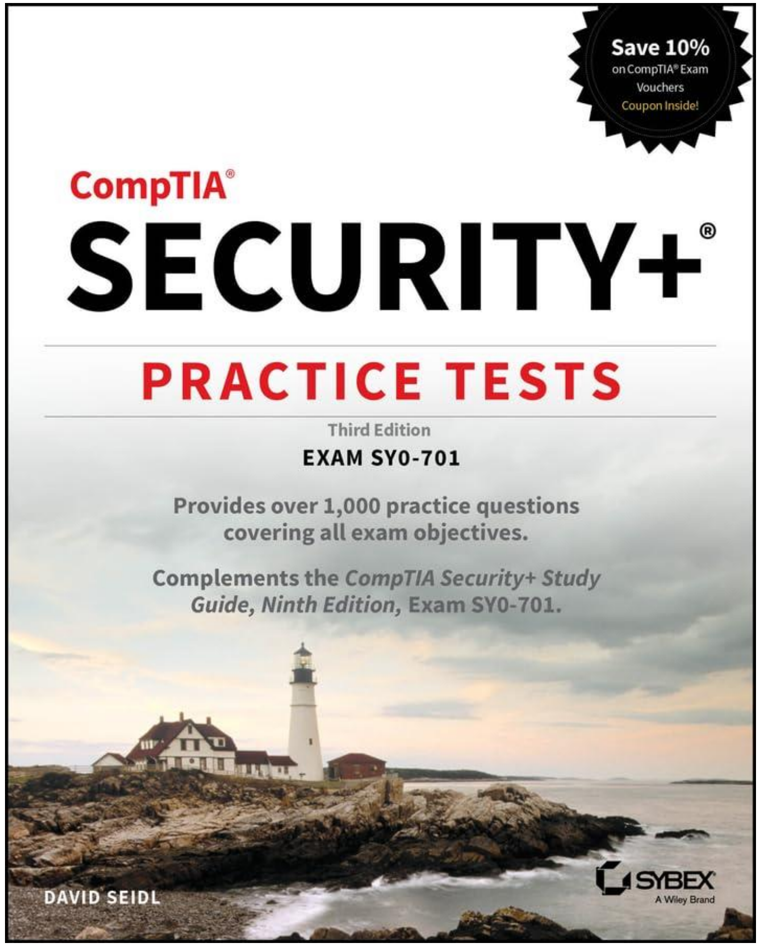
EXAM STUDY GUIDE

& PRACTICE TESTS BUNDLE

500 practice questions

100 flashcards

2 practice exams



Save 10% on CompTIA® Exam Vouchers Coupon Inside!

CompTIA®

SECURITY+®

PRACTICE TESTS

Third Edition

EXAM SY0-701

Provides over 1,000 practice questions covering all exam objectives.

Complements the *CompTIA Security+ Study Guide, Ninth Edition*, Exam SY0-701.

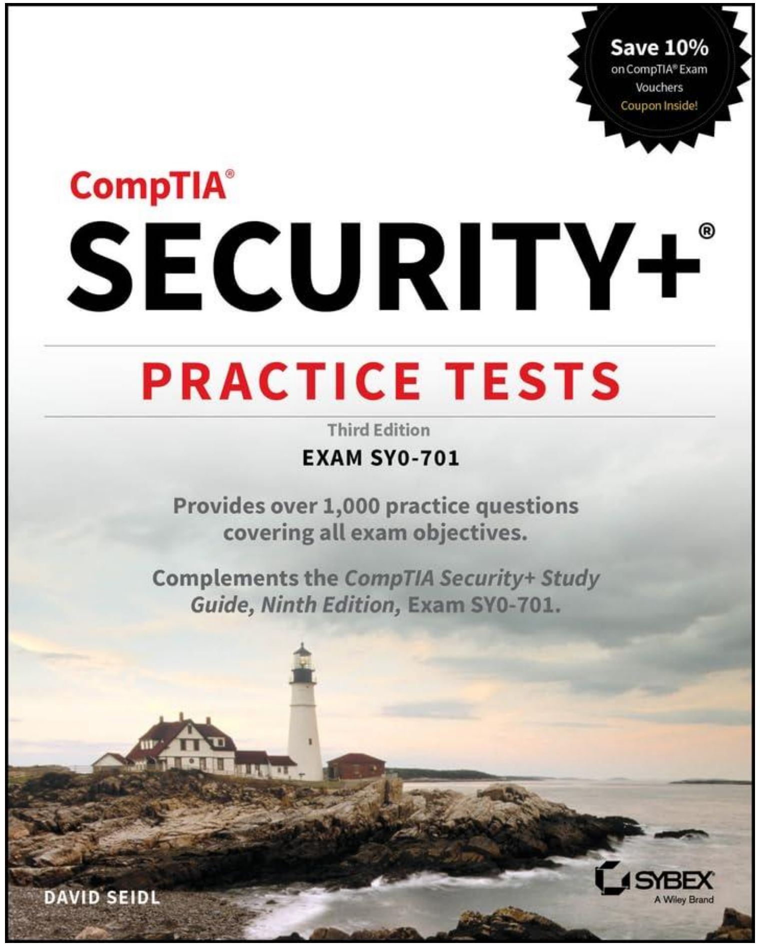
DAVID SEIDL

SYBEX A Wiley Brand

SECURITY+ EXAM STUDY GUIDE & PRACTICE TESTS BUNDLE

1000 practice questions

2 practice exams



Save 10% on CompTIA® Exam Vouchers Coupon Inside!

CompTIA®

SECURITY+®

PRACTICE TESTS

Third Edition

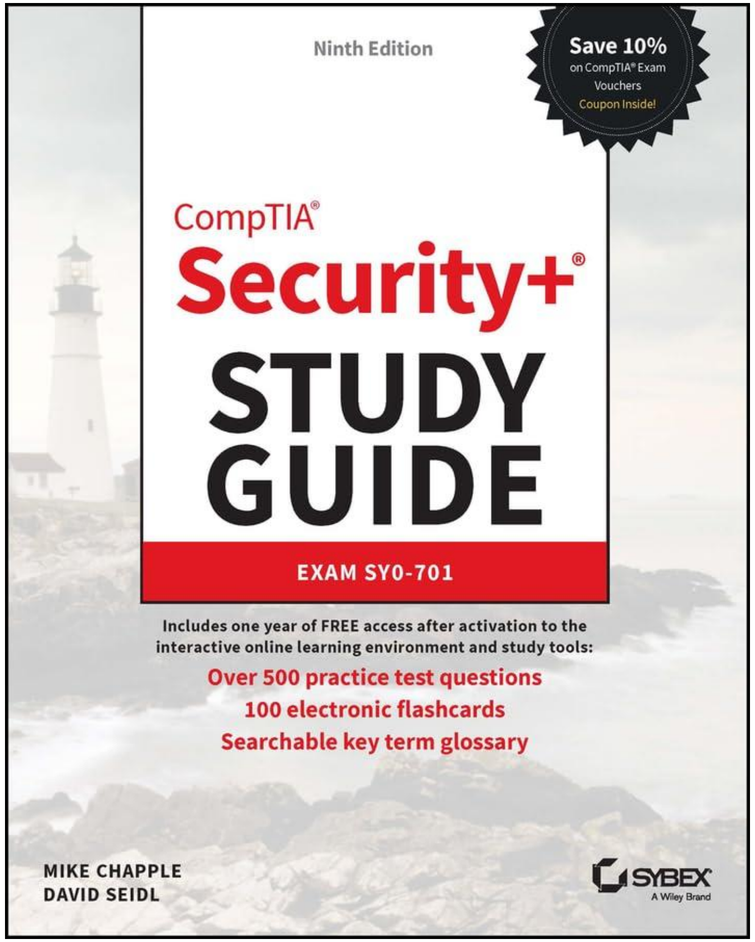
EXAM SY0-701

Provides over 1,000 practice questions covering all exam objectives.

Complements the *CompTIA Security+ Study Guide, Ninth Edition,* Exam SY0-701.

DAVID SEIDL

SYBEX A Wiley Brand



Ninth Edition

Save 10% on CompTIA® Exam Vouchers Coupon Inside!

CompTIA®

Security+®

STUDY GUIDE

EXAM SY0-701

Includes one year of FREE access after activation to the interactive online learning environment and study tools:

Over 500 practice test questions

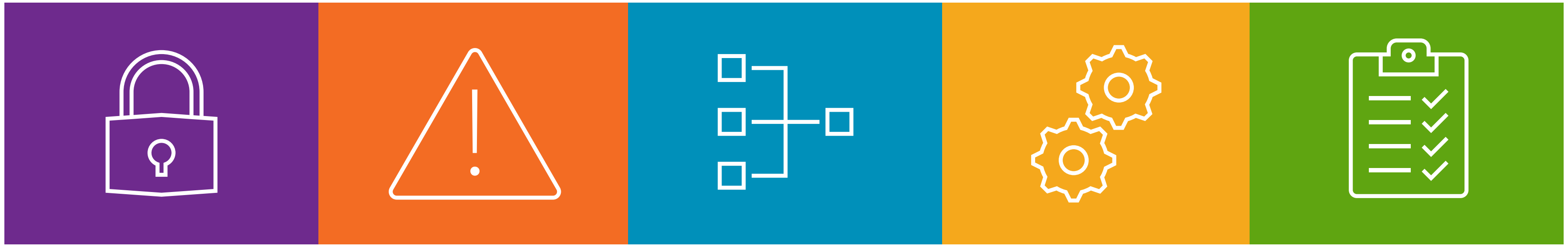
100 electronic flashcards

Searchable key term glossary

MIKE CHAPPLE
DAVID SEIDL

SYBEX A Wiley Brand

Links in video description



- 1.0 General Security Concepts

line-for-line review of the official exam syllabus!

1.0 GENERAL SECURITY CONCEPTS

1.1 Compare and contrast various types of security controls

- **Categories**
  - Technical
  - Managerial
  - Operational
  - Physical

- **Control Types**
  - Preventive
  - Deterrent
  - Detective
  - Corrective
  - Compensating
  - Directive

You should know some examples of each for the exam.

Controls can fit into multiple types based on context.

CATEGORIES OF SECURITY CONTROLS

Technical

Hardware or software mechanisms used to manage access to resources and systems and provide protection for those resources and systems.

Physical

Security mechanisms focused on providing protection to the facility and real-world objects.

Managerial

Policies and procedures, administrative controls defined by an organizations security policy.

Use planning and assessment methods to review the organization's ability to reduce and manage risk.

Operational

Help ensure that the day-to-day operations of an organization comply with their overall security. Primarily implemented and executed by people instead of systems.

CATEGORIES OF SECURITY CONTROLS EXAMPLES

Technical

Encryption

Smart cards

Passwords

Biometrics

Access control lists (ACLs)

Firewalls, routers

IDS/IPS

Physical

Guards

Fences

Lights

Motion detectors

Guard dogs

Video cameras

Alarms

Laptop locks

Managerial

Policies

Procedures

Hiring practices

Background checks

Data classification

Security training

Risk assessments

Vulnerability assessments

Operational

Awareness training

Configuration management

Media protection

CATEGORIES OF SECURITY CONTROLS

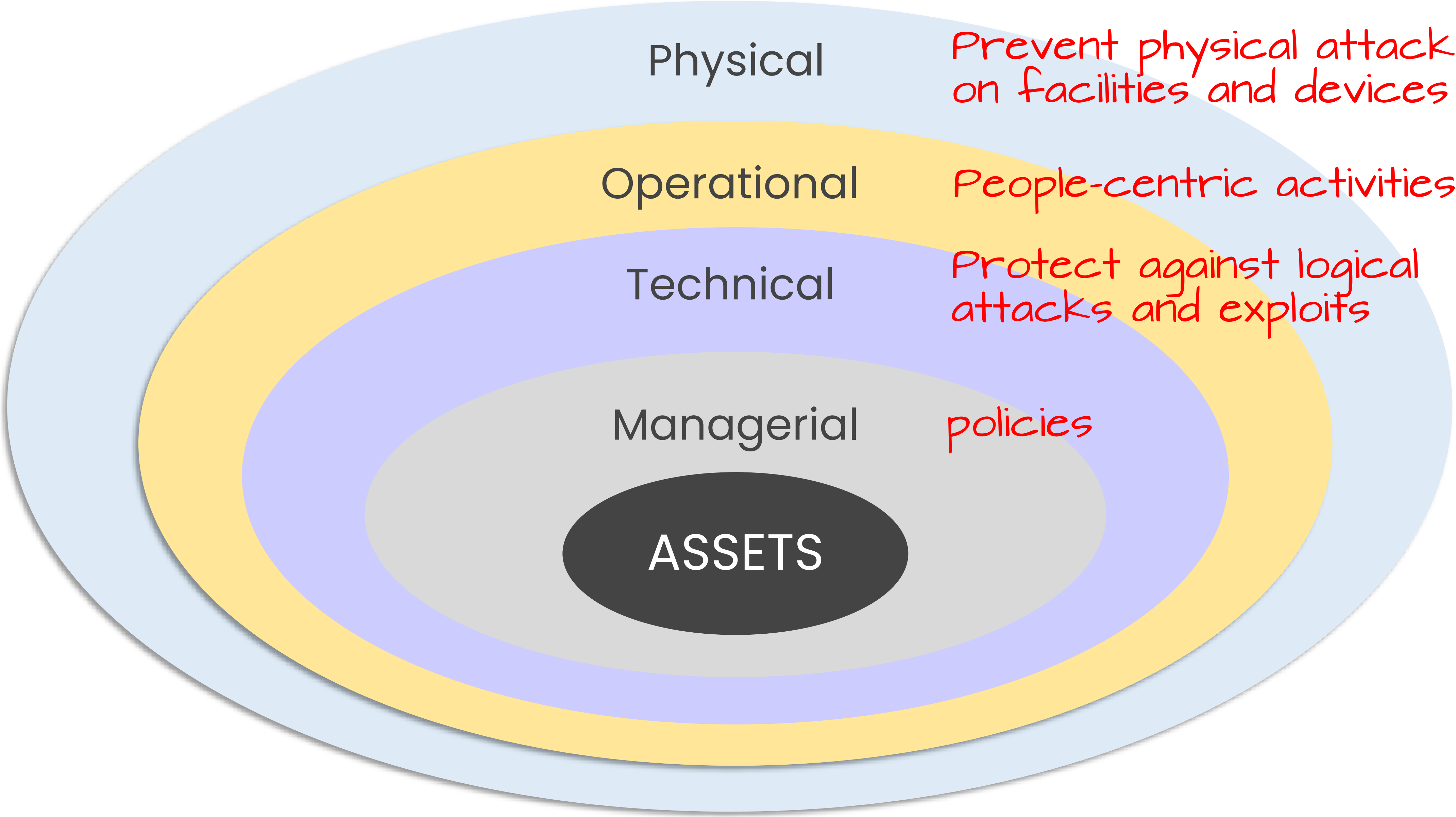
Technical → Technology (HW and SW)

Physical → Tangible (touchable)

Managerial → Policy (and policy implementation)

Operational → People (doing stuff)

SECURITY CONTROLS



Prevent physical attacks on facilities and devices

People-centric activities

Protect against logical attacks and exploits

policies

Security Controls

Security measures for countering and minimizing loss or unavailability of services or apps due to vulnerabilities

Security Controls

The terms **safeguards** and **countermeasures** may seem to be used interchangeably

Security Controls

safeguards are **proactive** (reduce likelihood of occurrence)

countermeasures are **reactive** (reduce impact after occurrence)

Control Types

Deterrent. Deployed to discourage violation of security policies.

Preventive. Deployed to thwart or stop unwanted or unauthorized activity from occurring.

Detective. Deployed to discover or detect unwanted or unauthorized activity.

Compensating. Provides options to other existing controls to aid in enforcement of security policies.

Control Types

Corrective. modifies the environment to return systems to normal after an unwanted or unauthorized activity has occurred.

Directive. direct, confine, or control the actions of subjects to force or encourage compliance with security policies.

CONTROL TYPES EXAMPLES

Preventive

deployed to stop unwanted or unauthorized activity from occurring,

EXAMPLES: fences, locks, biometrics, mantraps, alarm systems, job rotation, data classification, penetration testing, access control methods

Deterrent

deployed to discourage the violation of security policies. A deterrent control picks up where prevention leaves off.

EXAMPLES: locks, fences, security badges, security guards, lighting, security cameras, trespass or intrusion alarms, separation of duties, security policies, and security awareness training

CONTROL TYPES

Detective

deployed to discover unwanted or unauthorized activity. Often are after-the-fact controls rather than real-time controls.

EXAMPLES: security guards, guard dogs, motion detectors, job rotation, mandatory vacations, audit trails, intrusion detection systems, violation reports, honey pots, and incident investigations

Directive

direct, confine, or control the actions of subjects to force or encourage compliance with security policies..

EXAMPLES: policies, procedures, standards, guidelines, physical signage, verbal instructions, contracts and agreements

CONTROL TYPES

Corrective

deployed to restore systems to normal after an unwanted or unauthorized activity has occurred. minimal capability to respond to access violations.

EXAMPLES: backups and restores, patching, antivirus/antimalware, forensic analysis, disciplinary action

Compensating

deployed to provide options to other existing controls to aid in the enforcement and support of a security policy.

EXAMPLES: security policy, personnel supervision, monitoring, and work task procedures

CONTROL OVERLAP

One control, multiple types/functions

A single security control can be identified as multiple types, depending on the context of the situation

Overlapping Functions

Security controls are designed to work together, and their functions often overlap.

EXAMPLE: a security camera system is both **deterrent** (deterring unwanted entry) and **detective** (recording potential security incidents for later review).

Context Matters

The classification of a control can depend on how it's implemented and the specific risk it's addressing.

EXAMPLE: an access control list can be primarily **preventive** if it blocks unauthorized access or **detective** if it mainly logs access for later investigation.

CONTROL OVERLAP

One control, multiple types/functions

A single security control can be identified as multiple types, depending on the context of the situation

Focus on keywords

Exams often use specific words or phrases to hint at the control type.

EXAMPLES

Deterrent: "warning," "sign," "visibility," "perception"

Preventive: "access control," "authentication," "firewall," "encryption"

Directive: "policy," "procedure," "standard," "guideline"

Detective: "monitoring," "audit," "logging," "alert"

Corrective: "backup," "restore," "incident response," "patching"

Compensating: "alternative," "backup," "redundancy"

1.0 GENERAL SECURITY CONCEPTS

1.2 Summarize fundamental security concepts

- **Confidentiality, Integrity, and Availability (CIA)**
- **Non-repudiation**
- **Authentication, Authorization, and Accounting (AAA)**
  - Authenticating people
  - Authenticating systems
  - Authorization models
- **Gap analysis**
- **Zero Trust**
  - Control Plane
    - Adaptive identity
    - Threat scope reduction
    - Policy-driven access control
    - Policy Administrator
    - Policy Engine
  - Data Plane
    - Implicit trust zones
    - Subject/System
    - Policy Enforcement Point
- **Physical security**
  - Bollards
  - Access control vestibule
  - Fencing
  - Video surveillance
  - Security guard
  - Access badge
  - Lighting
  - Sensors
    - Infrared
    - Pressure
    - Microwave
    - Ultrasonic
- **Deception and disruption technology**
  - Honeypot
  - Honeynet
  - Honeyfile
  - Honeytoken

Security controls

DOMAIN 1: SECURITY & RISK MANAGEMENT

KNOW CIA BY HEART!

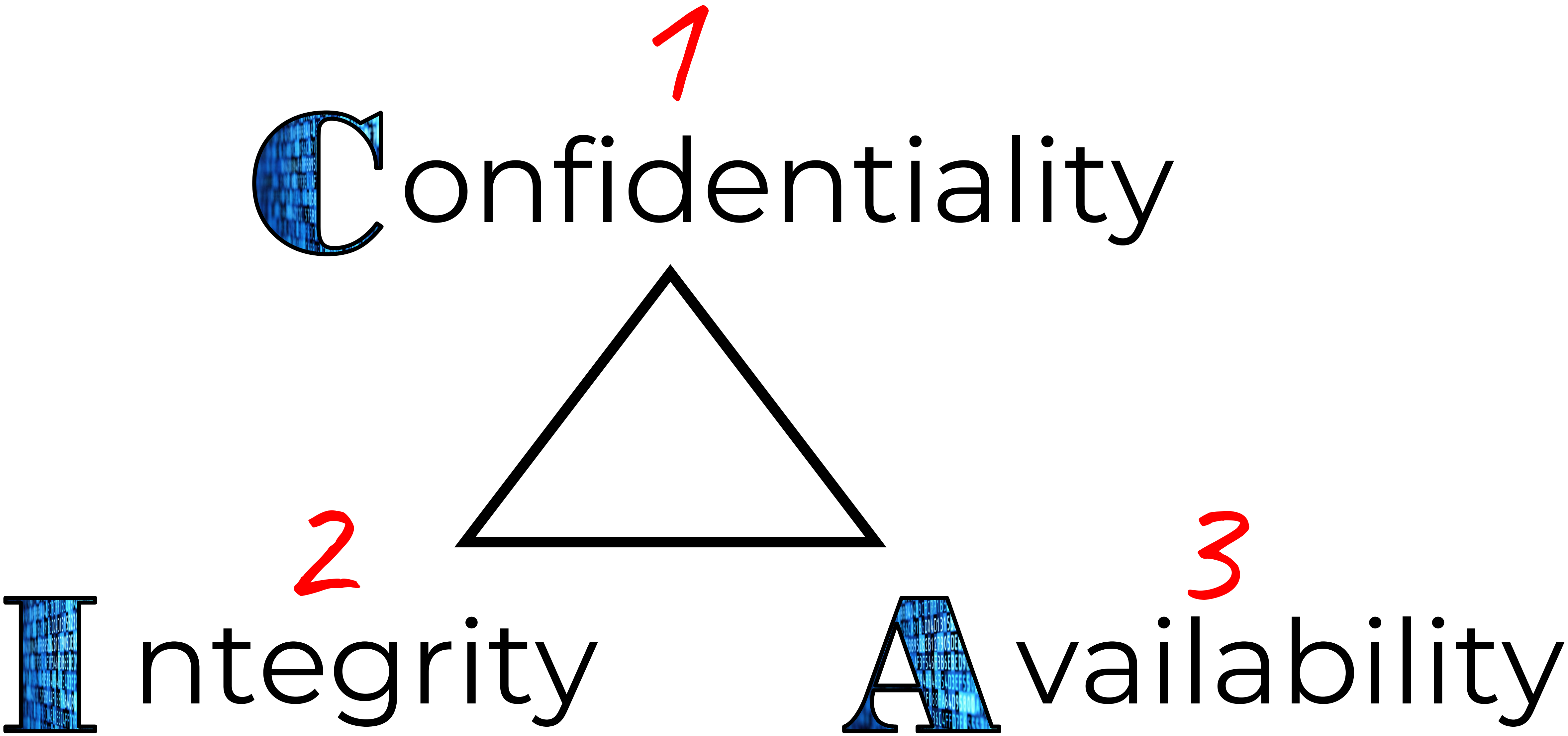
DOMAIN 1: SECURITY & RISK MANAGEMENT

Confidentiality

Integrity

Availability

DOMAIN 1: SECURITY & RISK MANAGEMENT



1

Confidentiality

2

Integrity

3

Availability

Confidentiality

Access controls help ensure that only authorized subjects can access objects

Integrity

Ensures that data or system configurations are not modified without authorization

Availability

Authorized requests for objects must be granted to subjects within a reasonable amount of time

NON-REPUDIATION

Non-repudiation is **the guarantee that no one can deny a transaction.**

Methods to provide non-repudiation

Digital Signatures prove that a digital message or document was not modified—intentionally or unintentionally—from the time it was signed.

based on asymmetric cryptography (a public/private key pair)

the digital equivalent of a handwritten signature or stamped seal.

provides non-repudiation in a publicly verifiable manner.

Non-repudiation is the ability to defeat/counter a false rejection or refusal of an obligation **with irrefutable evidence**.

REMEMBER: shared accounts/identities prevent non-repudiation!

AAA

Several protocols provide **authentication**, **authorization**, and **accounting** services.

Authentication

user/service proves identity with some type of credentials, such as a username and password.

Authorization

authenticated users are granted access to resources based on the roles and/or permissions assigned to their identity.

Accounting

methods that track user activity and records these activity in logs.

Tracks user activity and resource access as part of the audit trail

IDENTIFICATION AND AUTHENTICATION

Identification

Subjects claim an identity, and identification can be as simple as a username for a user.

Authentication

Subjects prove their identity by providing authentication credentials such as the matching password for a username.

AUTHORIZATION AND ACCOUNTABILITY

Authorization

after authentication

After authenticating subjects, systems authorize access to objects based on their proven identity.

Accountability

provides proof

Auditing logs and audit trails record events including the identity of the subject that performed an action.

identification + authentication + auditing = ACCOUNTABILITY

MAINTAINING ACCOUNTABILITY

Why is accountability important?

is maintained for individual subjects using auditing.

logs record user activities and users can be held accountable for their logged actions.

HOW THIS HELPS

directly promotes good user behavior and compliance with the organization's security policy.

Provides an audit trail for investigation if needed

MAINTAINING ACCOUNTABILITY

But it’s not only for people…

In modern enterprises, systems and devices have identities as well!

EXAMPLES:

In the cloud, **VMs have a managed identity** (managed by platform) used to access resources, such as data.

Client devices have machine identities in mobile device management (MDM) platforms.

DOMAIN 1.2: AUTHORIZATION MODELS

Non-discretionary Access Control

Enables the enforcement of system-wide restrictions that override object-specific access control. RBAC is considered non-discretionary

Discretionary Access Control (DAC)

Use-based, user-centric

A key characteristic of the Discretionary Access Control (DAC) model is that every object has an owner, and the owner can grant or deny access to any other subject.

Example: New Technology File System (NTFS)

Role Based Access Control (RBAC)

A key characteristic is the use of roles or groups. Instead of assigning permissions directly to users, user accounts are placed in roles and administrators assign privileges to the roles. Typically mapped to job roles.

Rule-based access control

A key characteristic is that it applies global rules that apply to all subjects. Rules within this model are sometimes referred to as **restrictions** or **filters**.

EXAMPLE: a firewall uses rules that allow or block traffic to all users equally.

MADATORY ACCESS CONTROL

"

> A key point about the **MAC model** is that every object and every subject has one or more labels. These labels are predefined, and the system determines access based on assigned labels.

EXAMPLE: in military security, data owner does not set access

ATTRIBUTE-BASED ACCESS CONTROL

access is restricted based on an attribute on the account, such as department, location, or functional designation.

For example, admins may require user accounts have the Legal department attribute to view contracts

SUBJECTS AND OBJECTS IN ACCESS CONTROL

Subjects | A user, group, or service accessing resources, known as objects.

Objects | Resources, such as files, folders, shares, and printers, accessed by subjects

These come up often in discussions of access control, so you should be familiar for the exam

The authorization model determines how a system grants users access to files and other resources.

GAP ANALYSIS

All auditors should have independence, but attestations from external auditors carry more weight (higher confidence)

A common task performed on a recurring basis, and often in preparation for external audits is the **gap analysis**.

Auditors will follow a standard (often ISO 27001) and then compare standard requirements to the org's current operations.

Deficiencies versus the standard will be captured in the audit report as gaps, sometimes called **control gaps**.

Control gap

a discrepancy between the security measures an organization should have in place versus controls actually in place.

The outcome of an audit is an **attestation**, which is a formal statement made by the auditor on controls and processes in place.

ZERO TRUST

Zero Trust

An approach to security architecture in which no entity is trusted by default

Based on three principles:

1) Assume breach
2) Verify explicitly
3) Least privilege access

Has largely replaced **trust but verify** and its network perimeter strategy.

Supported by **defense in depth**, that advises a layered approach to security.

Zero Trust Security

addresses the limitations of the legacy network perimeter-based security model.

treats user identity as the control plane

assumes compromise / breach in verifying every request. no entity is trusted by default

VERIFY **IDENTITY**

MANAGE **DEVICES**

MANAGE **APPS**

PROTECT **DATA**

ACCESS POLICY ENFORCEMENT

Policy Enforcement Point

responsible for enabling, monitoring, and terminating connections between a subject (such as a user or device) and an enterprise resource.

acts as the gateway that enforces access control policies.

when an access request occurs, the PEP evaluates the request against predefined policies and applies the necessary controls.

For example, PEP might enforce Multi-Factor Authentication (MFA) for access requests from unexpected locations. Dynamic based on conditions/context

Policy Decision Point

is where access decisions are made based on various factors such as user identity, device health, and risk assessment.

evaluates the context of an access request and decides whether it should be allowed, denied, or subjected to additional controls.

considers the **5 W's** (who, what, when, where, and why)

In short, the **PEP enforces policies** at the connection level, while the **PDP makes access decisions** based on contextual information.

ACCESS POLICY ENFORCEMENT

The key elements of **Zero Trust Network Architecture**:

Control Plane

- ✓ Adaptive Identity
- ✓ Threat Scope Reduction
- ✓ Policy-Driven Access Control
- ✓ Policy Administrator
- ✓ Policy Engine

Drives the policy-based decision logic for zero trust

Data Plane

- ✓ Implicit Trust Zones
- ✓ Subject/System
- ✓ Policy Enforcement Point

Enforces the decisions defined in control plane

Described in **NIST SP 800-207**

ZERO TRUST CONTROL PLANE

Adaptive Identity

changes the way that the system asks a user to authenticate based on context of the request. EXAMPLES: location, device, app, risk

Threat Scope Reduction

an end goal of ZTNA, which is to decrease risks to the organization.

Policy-Driven Access Control

controls based upon a user's identity rather than simply their system's location. EXAMPLE: Conditional Access in MSFT Entra ID

Policy Administrator (PA)

PA + PE = Policy Decision Point (PDP)

responsible for communicating the decisions made by the policy engine.

Policy Engine (PE)

EXAMPLE: MSFT Entra ID (Azure Active Directory)

decides whether to grant access to a resource for a given subject.

ZERO TRUST DATA PLANE

Implicit Trust Zones

part of traditional security approach in which firewalls and other security devices formed a perimeter. Systems belonging to the org were placed inside this boundary.

Subject/System

A **subject** is a user who wishes to access a resource.

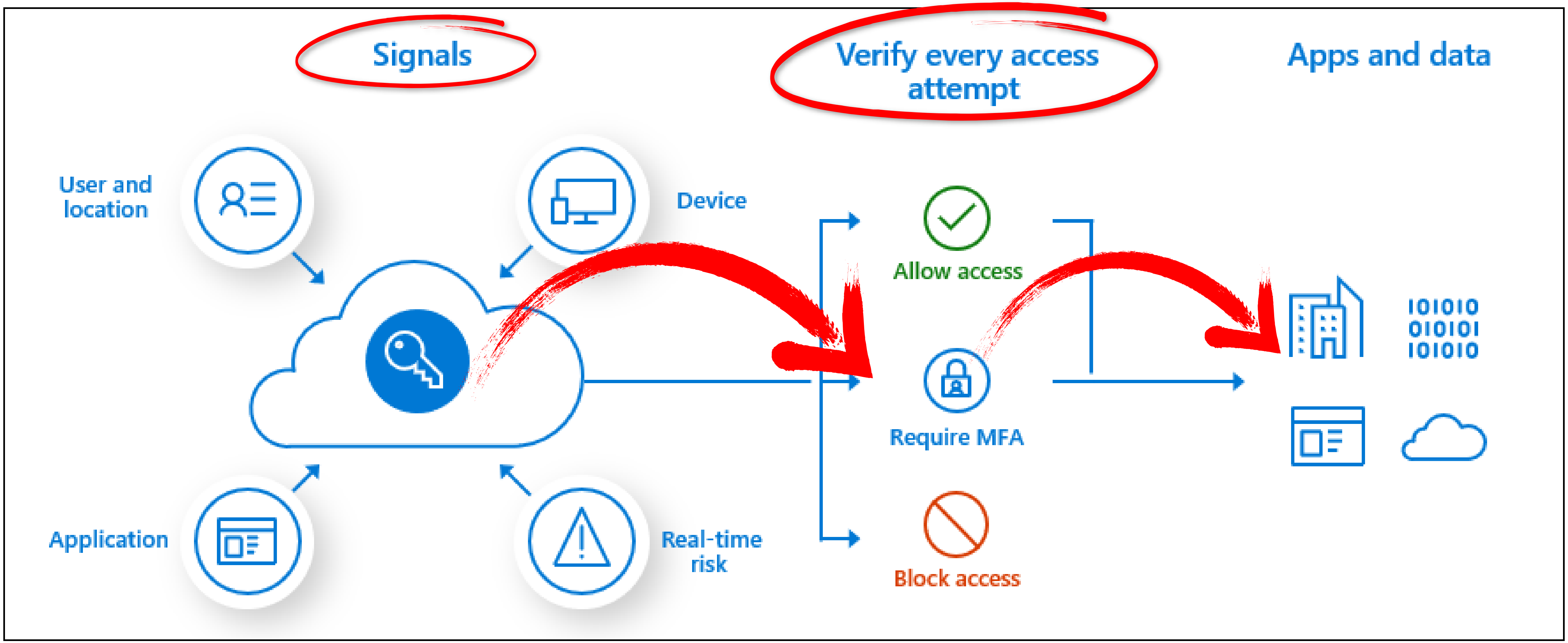
A **system** is a non-human entity, often the device used by the user, to access the resource.

Policy Enforcement Point

when a user or system requests access to a resource, the PEP evaluates it against predefined policies and applies the necessary controls.

EXAMPLE: MSFT Entra ID (Azure Active Directory)

CONDITIONAL ACCESS enforcing "conditions of access"

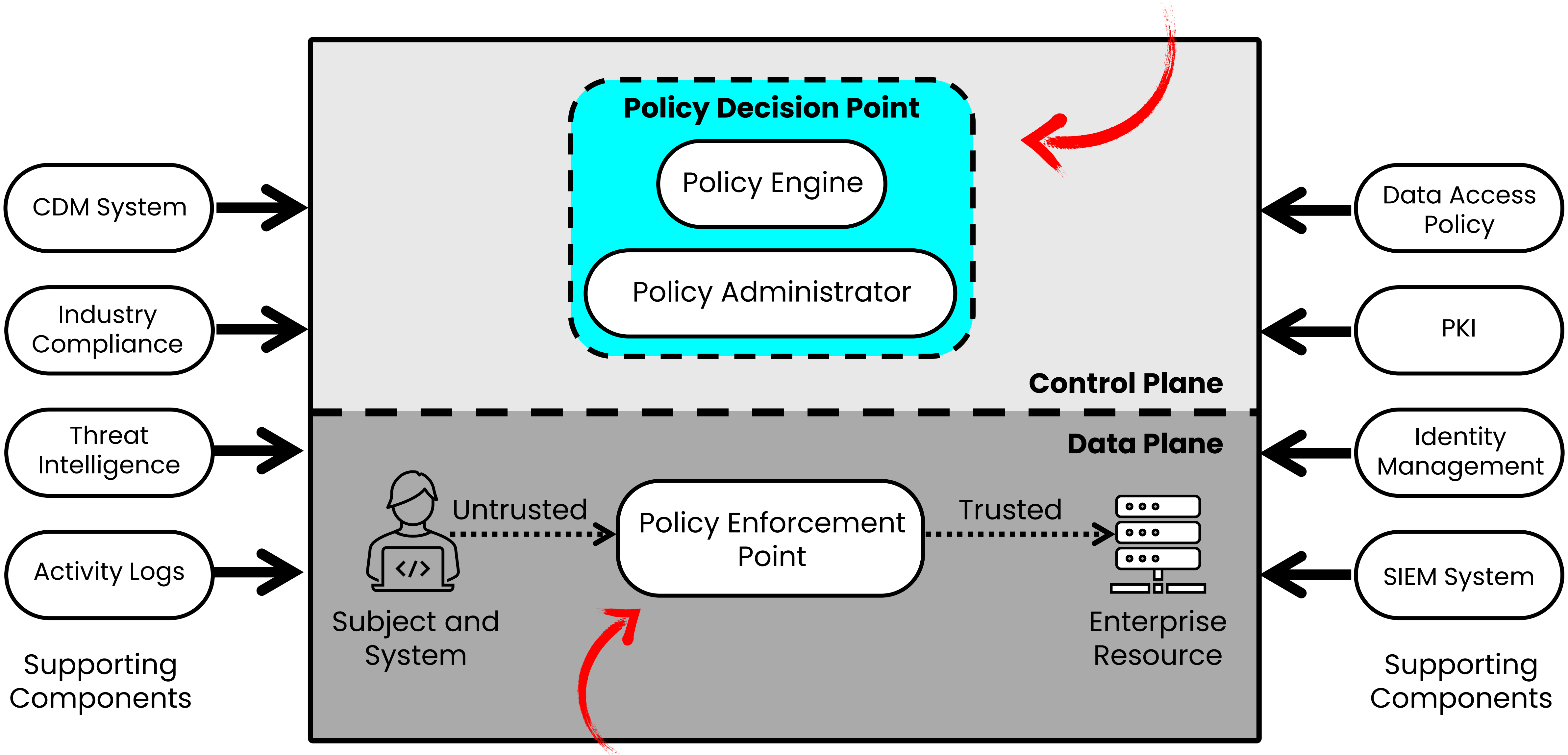


signal > decision > enforcement

image credit: Microsoft

Zero Trust

(logical diagram)



Where security controls are applied

DEMO

A quick tour of Conditional Access

EXAMPLE FOR CONTEXT - The Security+ exam is vendor-agnostic.

PHYSICAL SECURITY

There is no security without physical security

Without control over the **physical environment**, no amount of administrative or technical/logical access controls can provide adequate security.

If a malicious person can gain physical access to your facility or equipment, they can do just about anything they want, from destruction to disclosure and alteration.

BOLLARD

bollard

A short, sturdy vertical post, usually made of concrete, steel, or other heavy-duty materials.

They can be fixed in place or retractable.

Act as physical barriers, preventing vehicles from forcibly entering a restricted area.

Delineate pedestrian areas, parking lots, and sensitive zones to minimize accidental damage

Primarily used to control traffic flow and protect buildings or areas from vehicle-based attacks.

ACCESS CONTROL VESTIBULE

Previously called a mantrap

Access control vestibule

A physical security system comprising a small space with two interlocking doors.

Only one door can be opened at a time.

Designed to strictly control access to highly secure areas by allowing only one person at a time to pass through.

Protects against

Tailgating (slipping in on someone else's badge)

Piggybacking (like tailgating, but with bad intent)

Unauthorized entry of any kind

FENCES

Efficacy of fences by height

3-4 feet

deters the casual trespasser

6-7 feet

too difficult to climb easily

may block vision (providing additional security)

8-feet *(topped with barbed wire)*

will deter determined intruders

Fence is a DETERRENT control

PIDAS is a DETECTIVE control

EXPENSIVE and may generate false positives

PIDAS (**p**erimeter **i**ntrusion **d**etection and **a**ssessment **s**ystem) will detect someone attempting to climb a fence.

FENCES

Efficacy of fences by height

3-4 feet

deters the casual trespasser

6-7 feet

too difficult to climb easily

may block vision (providing additional security)

8-feet *(topped with barbed wire)*

will deter determined intruders

Fence is a DETERRENT control

PIDAS is a DETECTIVE control

To augment fences some orgs may erect stronger barricades, or zig-zag paths to prevent a vehicle from ramming a gate.

PHYSICAL SECURITY

Can you see how each may also serve to deter potential attacks?

Video surveillance

Detective control

Cameras and closed-circuit television (CCTV) systems provide video surveillance and reliable proof of a person's identity and activity.

Many cameras include motion and object detection capabilities.

Security guards

Preventive control

a preventive physical security control, and they can prevent unauthorized personnel from entering a secure area.

can recognize people and compare an individual's picture ID for people they don't recognize.

Access badges

Preventive control

can electronically unlock a door and help prevent unauthorized personnel from entering a secure area.

LIGHTING

Deterrent control

When planning lighting, think about **location**, **efficiency** and **protection**.

Location

installing lights at all the entrances and exits to a building can deter attackers from trying to break in.

Efficiency

a combination of automation, light dimmers, and motion sensors to save on electricity costs without sacrificing security.

automatically turn on at dusk, automatically turn off at dawn.

Protection

protect the lights. If an attacker can remove the light bulbs, it defeats the control.

either place the lights high enough so that they can't be reached or protect them with a metal cage.

SENSORS

Infrared

detects heat signatures in the form of infrared radiation emitted by people, animals, or objects.

integrated into security cameras and alarm systems to improve detection capabilities

Pressure

designed to detect changes in pressure on a surface or in a specific area, such as a person walking on a floor or stepping on a mat.

used in access control systems to ensure that only authorized individuals can enter

Microwave

uses microwave technology to detect movement within a specific area.

often used with other types of sensors to reduce false alarms

Ultrasonic

emits high-frequency sound waves and measure the time it takes for the sound waves to bounce back after hitting an object or surface.

commonly used in parking assistance, robotic navigation, and intrusion detection

DECEPTION AND DISRUPTION

Honeypot

A group of honeypots is called a honeynet.

Lure bad people into doing bad things. Lets you watch them.

Only ENTICE, not ENTRAP. You are not allowed to let them download items with “Enticement”.

For example, allowing download of a fake payroll file would be entrapment.

Goal is to **distract** from real assets and **isolate** in a padded cell until you can track them down.

DECEPTION AND DISRUPTION

Honeyfile

a decoy file deceptively named so it attracts the attention of an attacker.

Honeytoken

a fake record inserted into a database to detect data theft.

These are all intended to deceive attackers and disrupt attackers, divert them from live networks and allow observation.

1.0 GENERAL SECURITY CONCEPTS

1.3 Explain the importance of change management processes and the impact to security.

WHAT do these solve for? Why do we use them?

- **Business processes impacting security operation**
  - Approval process
  - Ownership
  - Stakeholders
  - Impact analysis
  - Test results
  - Backout plan
  - Maintenance window
  - Standard operating procedure

- **Technical implications**
  - Allow lists/deny lists
  - Restricted activities
  - Downtime
  - Service restart
  - Application restart
  - Legacy applications
  - Dependencies

- **Documentation**
  - Updating diagrams
  - Updating policies/procedures
- **Version control**

Configuration & Change Management

Can prevent security related incidents and outages

Configuration Management

ensures that systems are configured similarly, configurations are known and documented. Ensures true 'current state' is known to all

Baselining ensures that systems are deployed with a common baseline or starting point, and imaging is a common baselining method.

Change Management

the policy outlining the procedures for processing changes

helps reduce risk associated with changes, including outages or weakened security from unauthorized changes.

Requires changes to be requested, approved, tested, and documented.

Change Management vs Change Control

Change Control

refers to the process of evaluating a change request within an organization and deciding if it should go ahead.

requests are sent to the **Change Advisory Board (CAB)** to ensure that it is beneficial to the company.

Change Management

policy that details how changes will be processed in an organization

Guidance on the process

Change Control

process of evaluating a change request to decide if it should be implemented

The process in action

BUSINESS PROCESSES impacting security operation

A change management program should address important business process issues, including:

Approval process: ensures that every proposed change is properly reviewed and cleared by management before it takes place. Ensure alignment across teams

Ownership: clearly defines who is responsible for each change by designating a primary owner who will be the key decisionmaker and sponsor of the change.

Stakeholder analysis: identifies all the individuals and groups within the organization and outside the organization that might be affected by the change.

Enables team to contact and coordinate with all relevant stakeholders

Impact analysis: review of potential impacts of a change, including side effects.

Ensures team considers impact to systems and stakeholders

Testing: confirms that the change will work as expected by validating it in a test environment before production rollout.

Test results should be captured in the change approval request

BUSINESS PROCESSES impacting security operation

A change management program should address important business process issues, including:

Backout plan: provides detailed step-by-step sequence that the team should follow to roll back if the change goes wrong.

Ensures systems can be quickly restored to an operational state

Maintenance windows: Standing window of time during which changes can be implemented that minimizes impact to business, often outside of business hours.

For critical services, may be defined in customer contracts

REMEMBER: Any change that affects system or data exposure may impact security!

These elements together can define a **standard operating procedure** for change management.

TECHNICAL IMPLICATIONS

There are several technical implications that should be considered as part of the change management process.

- ☑ Allow lists/deny lists
- ☑ Restricted activities
- ☑ Downtime
- ☑ Application restarts
- ☑ Legacy applications
- ☑ Dependencies

WHY?

To avoid service disruptions and security vulnerabilities

TECHNICAL IMPLICATIONS

There are several technical implications that should be considered as part of the change management process.

Allow lists/deny lists

firewall rules, application allow/deny lists, and access control lists (ACLs) may need to be updated.

Restricted activities

some activities may need to be restricted, such as data updates during database replication/migration.

Downtime

some changes may cause service interruption, resulting in direct impact to the business.

This is where our 'maintenance window' comes into play

TECHNICAL IMPLICATIONS

There are several technical implications that should be considered as part of the change management process.

Application restarts
putting controls around risky activities, such as application and service restarts.

Legacy applications use case for private or hybrid cloud
modifications to legacy apps that may not support some changes, such as component/service version updates.

Dependencies
tracking dependencies between systems and services to identify downstream effects of current and future changes.

DOCUMENTATION

The process of documentation current state of and changes to the operating environment.

Provides team members with a repository of information about the way that systems and applications are designed and configured.

Serves as a reference for current and future team members

Change management processes should ensure that changes are not closed out until all documentation and diagrams are updated.

It is a continuous process across new deployments and changes

Documentation applies not only to environment, but to policies and procedures that direct operation and support of the environment.

Provides benefits to IT and security operations, BC/DR, incident response, and future design and planning iterations.

DOCUMENTATION

The process of documentation current state of and changes to the operating environment.

Provides team members with a repository of information about the way that systems and applications are designed and configured.

Serves as a reference for current and future team members

Change management processes should ensure that changes are not closed out until all documentation and diagrams are updated.

It is a continuous process across new deployments and changes

Documentation applies not only to environment, but to policies and procedures that direct operation and support of the environment.

⚠ You cannot fully secure a system or service for which you do not have a true picture of current state!

VERSION CONTROL

A formal process used to track the current versions of software code and system/application configurations.

Most organizations use a formal **version control system** that is integrated into their software development processes.

For most orgs, this is some platform based on Git.

Developers modify the code and check it into a version control system that identifies conflicts in their changes with those made by other devs.

It also tracks the current dev, test, and production versions of code.

Code for different environments is tracked in Git using code 'branches'

FOR THE EXAM: Focus on the functions of version control, not on any specific version control system.

1.0 GENERAL SECURITY CONCEPTS

1.4 Explain the importance of using appropriate cryptographic solutions.

- **Public key infrastructure (PKI)**
  - Public key
  - Private key
  - Key escrow
- **Encryption**
  - Level
    - Full-disk
    - Partition
    - File
    - Volume
    - Database
    - Record
  - Transport/communication
  - Asymmetric
  - Symmetric
  - Key exchange
  - Algorithms
  - Key length
- **Tools**
  - Trusted Platform Module (TPM)
  - Hardware security module (HSM)
  - Key management system
  - Secure enclave
- **Obfuscation**
  - Steganography
  - Tokenization
  - Data masking
- **Hashing**
- **Salting**
- **Digital signatures**
- **Key stretching**
- **Blockchain**
- **Open public ledger**
- **Certificates**
  - Certificate authorities
  - Certificate revocation lists (CRLs)
  - Online Certificate Status Protocol (OCSP)
  - Self-signed
  - Third-party
  - Root of trust
  - Certificate signing request (CSR) generation
  - Wildcard

PUBLIC KEY INFRASTRUCTURE (PKI)

CONCEPTS

Key management

management of cryptographic keys in a cryptosystem.

Operational considerations include dealing with the generation, exchange, storage, use, crypto-shredding (destruction) and replacement of keys.

Design considerations include cryptographic protocol design, key servers, user procedures, and other relevant protocols.

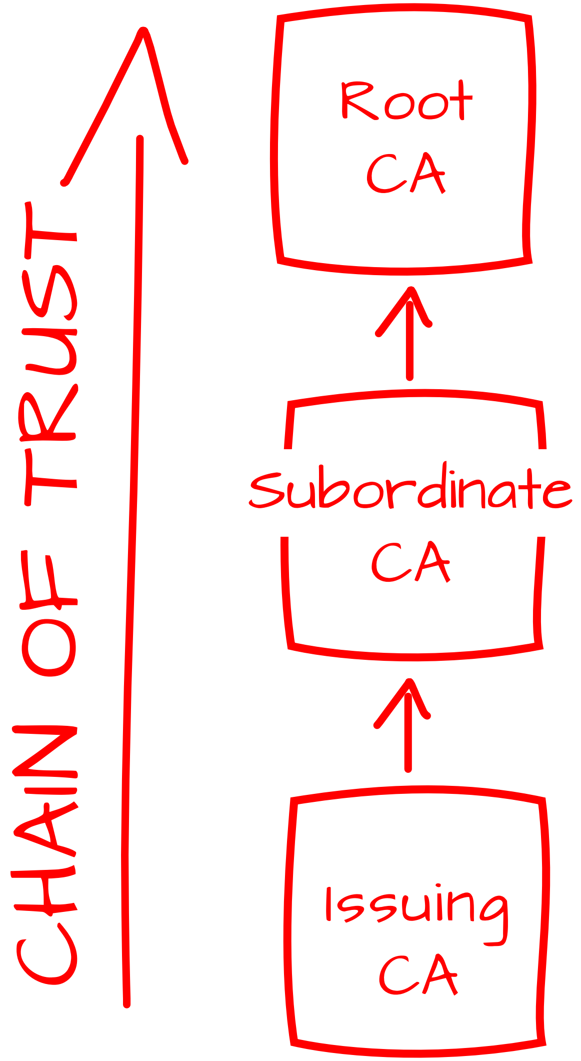
Certificate authority (CA)

Certification Authorities create digital certificates and own the policies.

PKI hierarchy can include a single CA that serves as root and issuing CA, but this is not recommended.

Also called a 'certification authority' by some vendors

PUBLIC KEY INFRASTRUCTURE (PKI) CONCEPTS



CHAIN OF TRUST

Root CA

Subordinate CA

Issuing CA

Usually maintained in an offline state

Issues certs to new subordinate CAs

Also called a Policy CA or Intermediate CA

Issues certs to new issuing CAs

Certificates for clients, servers, devices, websites, etc. issued from here

Can be consolidated to fewer servers, creating a 1 or 2-level hierarchy.

PUBLIC KEY INFRASTRUCTURE (PKI)

CONCEPTS

Certificate revocation list (CRL)

Contains information about any certificates that have been revoked due to compromises to the certificate or PKI hierarchy.

CRL of issuing CA contains info on revocation of certs it has issued

CAs are required to publish CRLs, but it's up to certificate consumers if they check these lists and how they respond if a certificate has been revoked.

Each CRL is published to a file, that the client must download to check, which can grow large over time

PUBLIC KEY INFRASTRUCTURE (PKI) CONCEPTS

Online Certificate Status Protocol (OCSP)

Offers a faster way to check a certificate's status compared to downloading a CRL.

With OCSP, the consumer of a certificate can submit a request to the issuing CA to obtain the status of a specific certificate.

Certificate signing request (CSR)

Records identifying information for a person or device that owns a private key as well as information on the corresponding public key.

It is the message that's sent to the CA in order to get a digital certificate created.

CN (common name)

the Fully Qualified Domain Name (FQDN) of the entity (e.g. web server)

PUBLIC KEY INFRASTRUCTURE (PKI) CONCEPTS

Online vs. offline CA. Online CA is always running, offline CA is kept offline except for specific issuance and renewal operations.

Offline is best practice for your root CA.

Stapling. a method used with OCSP, which allows a web server to provide information on the validity of its own certificate.

Done by the web server essentially downloading the OCSP response from the certificate vendor in advance and providing it to browsers.

Pinning. a method designed to mitigate the use of fraudulent certificates.

Once a public key or certificate has been seen for a specific host, that key or certificate is pinned to the host.

Should a different key or certificate be seen for that host, that might indicate an issue with a fraudulent certificate.

PUBLIC KEY INFRASTRUCTURE (PKI)

CONCEPTS

Certificate chaining

Refers to the fact that certificates are handled by a chain of trust.

You purchase a digital certificate from a certificate authority (CA), so you trust that CA's certificate.

In turn, that CA trusts a root certificate.

Trust model

A model of how different certificate authorities trust each other and how their clients will trust certificates from other certification authorities.

The four main types of trust models that are used with PKI are bridge, hierarchical, hybrid, and mesh.

PUBLIC KEY INFRASTRUCTURE (PKI)

Key escrow

Addresses the possibility that a cryptographic key may be lost.

The concern is usually with symmetric keys or with the private key in asymmetric cryptography.

If that occurs, then there is no way to get the key back, and the user cannot decrypt messages.

Organizations establish key escrows to enable recovery of lost keys.

CERTIFICATE FORMATS

X.509 certificate formats and descriptions

FORMAT	EXT	PRI KEY	DESCRIPTION
Distinguished encoding rules	DER	NO	Secure remote access (Linux and network)
Privacy enhanced mail	PEM	YES	Secure copy to Linux/Unix
Personal information exchange	PFX	YES	Supports storage of all certificates in path
Base64-encoded	CER	NO	Storage of a single certificate.
PKCS#12 standard	P12	YES	Supports storage of all certificates in path
Cryptographic Message Syntax Standard	P7B	NO	Supports storage of all certificates in path. KCS #12 is the successor to Microsoft's "PFX“.

EXT = File extension **PRI KEY** = File includes private key?

Certificates are not whole without the private key!

TYPES OF CERTIFICATES

User

Used to represent a user's digital identity.

In most cases, a user certificate is mapped back to a user account.

Root

This is the "root of trust"

A trust anchor in a PKI environment is the root certificate from which the whole chain of trust is derived; this is the root CA.

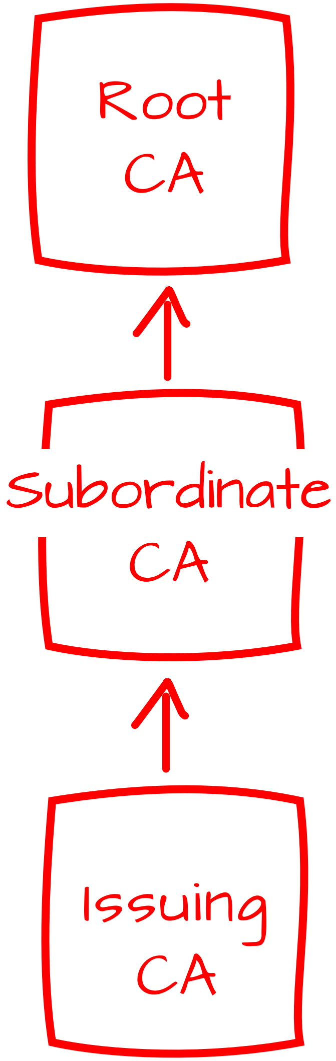
Domain validation

A Domain-Validated (DV) certificate is an X.509 certificate that proves the ownership of a domain name.

Extended validation

Extended validation certificates provide a higher level of trust in identifying the entity that is using the certificate.

Commonly used in the financial services sector.



ROOT OF TRUST

Think of the certificate of root CA as "root of trust"

In a PKI, the root certificate serves as the trust anchor, as it is the most trusted component of the system.

Your org's root certificate will be deployed to your org's devices to the list of trusted certificate authorities.

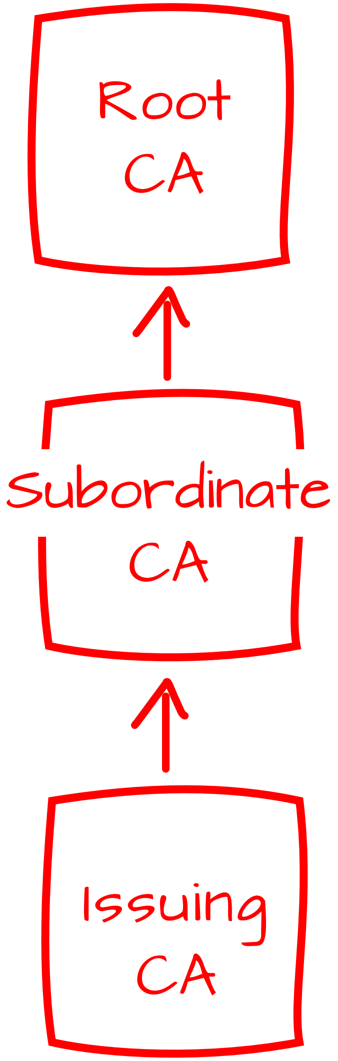
Your CA's root certificate is generally only known and trusted within your organization

For external customer-facing use cases

For resources accessed externally, you will buy a certificate from a trusted third party.

e.g. Digicert, Entrust, GlobalSign, GoDaddy

Root certificates from widely trusted sources are pre-installed on most devices (computers, phones, etc.)



SECURITY+ EXAM CRAM

THE COMPLETE COURSE

DEMO

Certificates, certificate authority & root of trust

INSIDE CLOUD AND SECURITY

TYPES OF CERTIFICATES

Wildcard

Supports multiple FQDNs in the same domain

Can be used for a domain and a subdomain. For example:

In the **contoso.com** domain, there are two servers called **web** and **mail**.

The wildcard certificate is *.contoso.com and, when installed, it would work for the Fully Qualified Domain Names (FQDNs) for both of these.

A wildcard can be used for multiple servers in the same domain, saving costs.

Code signing

Provides proof of content integrity

When code is distributed over the Internet, it is essential that users can trust that it was actually produced by the claimed sender.

An attacker would like to produce a fake device driver or web component (actually malware) that is claimed to be from some legitimate software vendor.

Using a code signing certificate to digitally sign the code mitigates this danger.

TYPES OF CERTIFICATES

Self-signed

A self-signed certificate is issued by the same entity that is using it. However, it does not have a CRL and cannot be validated or trusted.

It is the cheapest form of internal certificates and can be placed on multiple servers.

Machine/computer

A computer or machine certificate is used to identify a computer within a domain.

Email

Allow users to digitally sign their emails to verify their identity through the attestation of a trusted third party known as a certificate authority (CA).

Allow users to encrypt the entire contents (messages, attachments, etc.)

Third-party

A certificate issued by a widely trusted external provider such as GoDaddy or Digicert.

Preferred for TLS on public-facing services, such as company website.

TYPES OF CERTIFICATES

Subject alternative name (SAN)

an extension to the X. 509 specification that allows users to specify additional host names for a single SSL certificate.

Is standard practice for SSL certificates, and it's on its way to replacing the use of the common name.

You can also insert other information into a SAN certificate, such as an IP address.

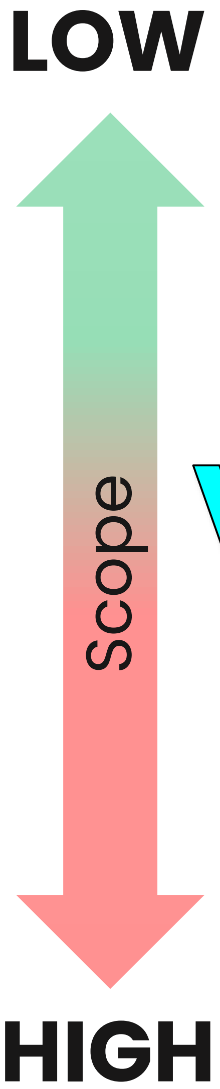
Enables support for FQDNs from multiple domains in a single certificate.

Expiration

certificates are valid for a limited period from the date of issuance, as specified on the certificate.

Current industry guidance on maximum certificate lifetime from widely trusted issuing authorities (like Digicert) is currently 1 year (398 days).

LEVEL (SCOPE) OF ENCRYPTION



File Encryption

operates at the individual file level, meaning files could have unique encryption keys.

Useful for files containing sensitive info

e.g. financial info, PHI, PII

Volume Encryption

encryption targets a specific partition or volume within the physical drive.

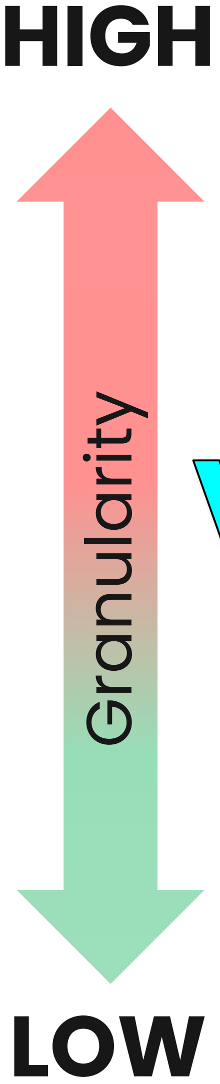
Useful when different volumes need varying levels of protection. data volume vs system volume

Disk Encryption

automatically encrypts data when it is written to or read from the entire disk.

Bitlocker on Windows, dm-crypt on Linux.

LEVEL (SCOPE) OF ENCRYPTION



File Encryption

operates at the individual file level, meaning files could have unique encryption keys.

Useful for files containing sensitive info

e.g. financial info, PHI, PII

Volume Encryption

encryption targets a specific partition or volume within the physical drive.

Useful when different volumes need varying levels of protection. data volume vs system volume

Disk Encryption

automatically encrypts data when it is written to or read from the entire disk.

Bitlocker on Windows, dm-crypt on Linux.

VOLUME VS PARTITION

Partition

It represents a distinct section of storage on a disk.

In Windows, the C drive is typically a primary partition

Is a distinct PHYSICAL section of storage

Volume

Represents a logical division of a storage device.

Represents a single accessible storage area.

Can span multiple partitions or disks.

Assembles one or more partitions into a unified storage area

DRIVE ENCRYPTION

FDE

Full Disk Encryption

Full Disk Encryption is built into the Windows operating system.

Bitlocker is an implementation of FDE.

Bitlocker protects disks, volumes, and partitions

SED

Self-Encrypting Drive

encryption on a SED that's built into the hardware of the drive itself.

anything that's written to that drive is automatically stored in encrypted form.

A good SED should follow the 'Opal Storage Specification'

PROTECTING DATA AT REST

Full Disk Encryption (FDE) "under the hood"

Trusted Platform Module (**TPM**): is on the motherboard and is used to store the encryption keys so when system boots, it can compare keys and ensure that the system has not been tampered with. A TPM is a HRoT

Hardware Root of Trust: When using certificates for FDE, they use a hardware root of trust that verifies that the keys match before the secure boot process takes place.

Self-Encrypting Drives (SEDs)

The OPAL storage specification is the industry standard for self-encrypting drives. This is a hardware solution, and typically outperform software-based alternatives.

They don't have the same vulnerabilities as software and therefore are more secure.

SEDs are **Solid State Drives** (**SSDs**) and are purchased already set to encrypt data at rest. The encryption keys are stored on the hard drive controller.

They are immune to a cold boot attack and are compatible with all operating systems

SED is effective in protecting the data on lost or stolen devices (such as a laptop). Only the **user** and **vendor** can decrypt the data.

PROTECTING DATA AT REST

How can we encrypt different types of data **at rest**?

Cloud Storage Encryption

CSPs usually protect data at rest by automatically encrypting before persisting it to managed disks, blob storage, file, or queue storage.

Transparent data encryption (TDE)

Helps protect SQL Database and data warehouses against threat of malicious activity with real-time encryption and decryption of database, backups, and transaction log files at rest without requiring app changes.

CSP = Cloud Service Provider

TRANSPORT/COMMUNICATION

How can we encrypt different types of data **in transit**?

> “Data in transit is most often encrypted using **TLS** or **HTTPS**
>
> This is typically how a session is encrypted before a user enters the credit card details.”

While similar in function, TLS has largely replaced SSL

TRANSPORT/COMMUNICATION

Also called "data in motion"

How can we encrypt different types of data **in transit**?

> Data in transit is most often encrypted using **TLS** or **HTTPS**
>
> This is typically how a session is encrypted before a user enters the credit card details.

TLS is common for encrypting network communications, such as VPN

PROTECTING DATA IN USE / IN PROCESSING

How can we encrypt different types of data **in use**?

Data-in-use/in processing occurs when we launch an application such as Microsoft Word or Adobe Acrobat

Apps not running the data from the disk drive but running the application in random access memory (RAM).

This is volatile memory, meaning that, should you power down the computer, the contents are erased.

In some cases, data in-memory will be encrypted

Encrypting Records

Many relational databases support **row** or **column** level encryption.

Row-level encrypts an entire record, column-level encrypts specific fields within the record.

Commonly implemented within the database tier, but also possible in code of frontend applications

Database Encryption

Transparent data encryption is full database-level encryption (database files, logs, backups)

Requires no changes in application and comes with virtually no performance impact

Offered on most relational database management (RDBMS) platforms, like MSSQL, MySQL, and PostgreSQL

CONCEPT: SYMMETRIC vs ASYMMETRIC

Symmetric

Relies on the use of a **shared secret key**. Lacks support for scalability, easy key distribution, and nonrepudiation

Asymmetric

Public-private key pairs for communication between parties. Supports scalability, easy key distribution, and nonrepudiation

ASYMMETRIC KEY TYPES

Public keys are shared among communicating parties.

Private keys are kept secret.

DATA

To encrypt a message: use the recipient's public key.

To decrypt a message: use your own private key.

DIGITAL SIGNATURE

To sign a message: use your own private key.

To validate a signature: use the sender's public key.

each party has both a private key and public key!

COMMON USES

How are different algorithm types used?

Symmetric

Typically used for bulk encryption / encrypting large amounts of data.

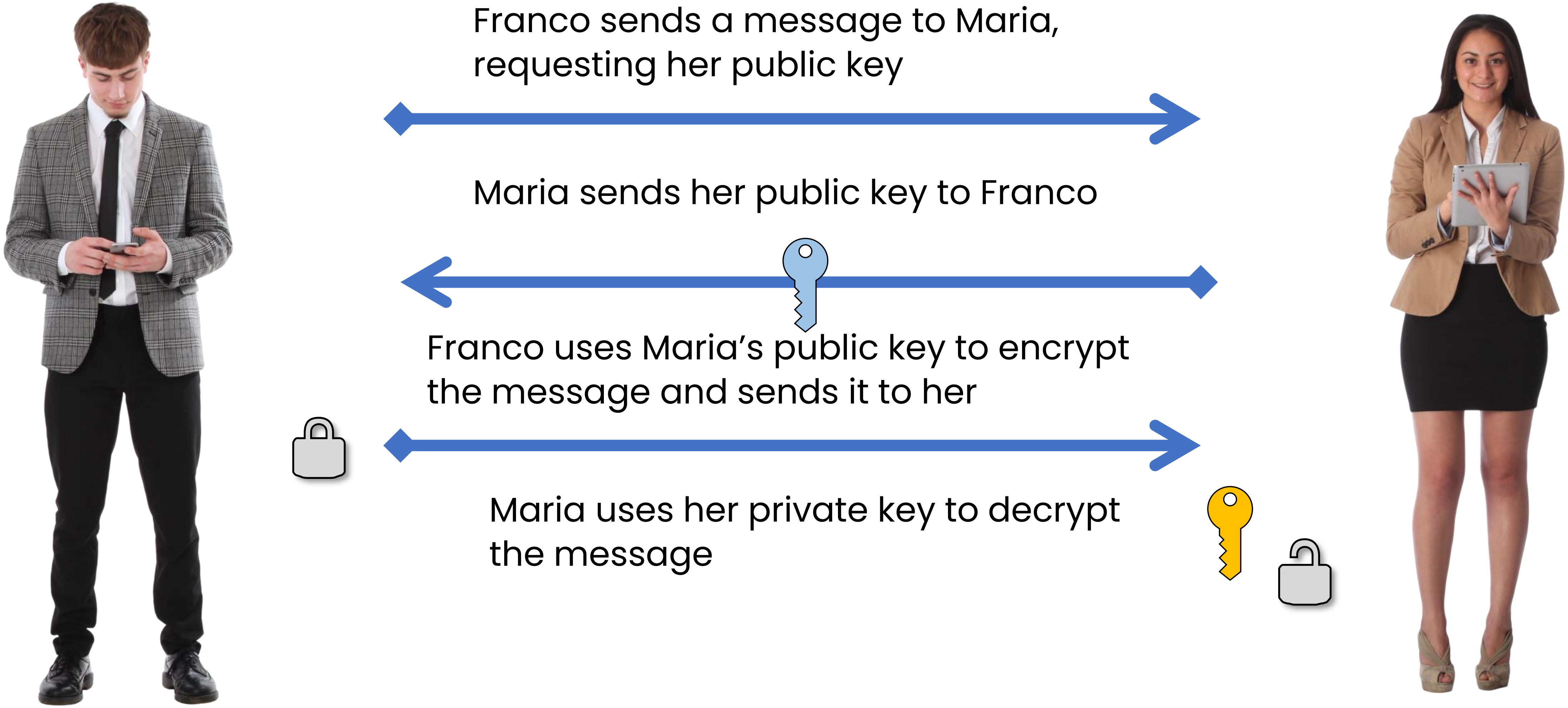
Asymmetric

Distribution of symmetric bulk encryption keys (shared key)

Identity authentication via digital signatures and certificates

Non-repudiation services and key agreement

KEY EXCHANGE IN ASYMMETRIC CRYPTOGRAPHY



Franco sends a message to Maria, requesting her public key

Maria sends her public key to Franco

Franco uses Maria’s public key to encrypt the message and sends it to her

Maria uses her private key to decrypt the message

Common symmetric encryption algorithms

AES (Advanced Encryption Standard): The current industry gold standard. Highly efficient and widely implemented.

It offers various key lengths (128, 192, 256 bits), providing flexibility in security levels.

3DES (Triple DES): A variation of DES applying encryption three times.

Being phased out and replaced by AES

Twofish: A finalist in the competition to select AES, known for its flexibility and security.

Blowfish: Predecessor to Twofish, also known for its strength and speed.

Symmetric algorithms are used for bulk data encryption

1.4 ENCRYPTION ALGORITHMS

Common asymmetric encryption algorithms

RSA (Rivest–Shamir–Adleman): One of the oldest and most widely used asymmetric algorithms.

Often used for key exchange and digital signatures. Its security relies on the difficulty of factoring large prime numbers.

ECC (Elliptic Curve Cryptography): A more modern approach using elliptic curves.

Offers similar security levels to RSA but with smaller key sizes, making it suitable for resource-constrained environments.

Diffie-Hellman: Primarily a key exchange protocol, allowing two parties to establish a shared secret key over an insecure channel.

ElGamal: An algorithm based on the difficulty of the discrete logarithm problem. Used for encryption and digital signatures.

COMMON USES OF ALGORITHMS

How are different algorithm types used?

Symmetric Example: AES256

Typically used for bulk encryption / encrypting large amounts of data.

Asymmetric Example: RSA, DH, ECC

Distribution of symmetric bulk encryption keys (shared key)

Identity authentication via digital signatures and certificates

Non-repudiation services and key agreement

TYPES OF CIPHERS

Stream cipher

is a symmetric key **cipher** where plaintext digits are combined with a pseudorandom **cipher digit stream** (keystream).

each **plaintext** digit is encrypted one at a time with the corresponding digit of the keystream, to create a digit of the **ciphertext** stream.

Block cipher

is a method of encrypting text in which a cryptographic key and algorithm are applied to a block of data (for example, 64 contiguous bits) at once as a group rather than to one bit at a time.

Considered to be more secure than stream ciphers

TYPES OF CIPHERS

Substitution cipher

uses the encryption algorithm to replace each character or bit of the plaintext message with a different character.

Examples include Caesar cipher, Vigenère cipher

Transposition cipher

rearranges order of plaintext letters according to a specific rule.

the message itself is left unchanged, just the order is scrambled.

Examples include Rail Fence and Columnar Transposition

CRYPTOGRAPHIC KEY LENGTH

An effective means to increase the strength of an algorithm is by increasing its **key length**

The relationship between key length and work factor is **exponential**.

A small increase in key length leads to a significant increase in the amount of work required to break the encryption.

EXAMPLES

Asymmetric

RSA (Rivest-Shamir-Adleman), the primary public key cryptography algorithm used on the Internet.

It supports key sizes of 1024, 2048, and 4096 bits.

NIST recommends minimum key length of 2048

CRYPTOGRAPHIC KEY LENGTH

An effective means to increase the strength of an algorithm is by increasing its **key length**

The relationship between key length and work factor is **exponential**.

A small increase in key length leads to a significant increase in the amount of work required to break the encryption.

EXAMPLES

Symmetric

Advanced Encryption Standard (AES) is the go-to algorithm for the US Federal gov't.

It supports key sizes of 128, 192, and 256 bits.

256-bit key is recommended for quantum resistance

CRYPTOGRAPHIC KEY LENGTH

An effective means to increase the strength of an algorithm is by increasing its **key length**

The relationship between key length and work factor is **exponential**.

A small increase in key length leads to a significant increase in the amount of work required to break the encryption.

Doubling key length from 128 to 256 does not make the key twice as strong.

It makes it 2^{128} times as strong!

Static versus Ephemeral Keys

The two primary categories of asymmetric keys are **static** and **ephemeral**.

Static Keys

RSA uses static keys.

Static keys are semi-permanent and stay the same over a long period of time.

A certificate includes an embedded public key matched to a private key. This key pair is valid for the lifetime of a certificate.

Certificates have expiration dates and systems continue to use these keys until the certificate expires. 1-2 years is a common certificate lifetime

A **certification authority (CA)** can validate a certificates static key with a **certificate revocation list (CRL)** or using the **Online Certificate Status Protocol (OCSP)**.

Static versus Ephemeral Keys

The two primary categories of asymmetric keys are **static** and **ephemeral**.

Ephemeral Keys

Ephemeral keys have very short lifetimes and are re-created for each session.

An ephemeral key pair includes a private ephemeral key and a public ephemeral key.

Systems use these key pairs for a single session and then discard them.

Some versions of Diffie-Hellman use ephemeral keys.

1.4 TOOLS

Trusted Platform Module

TPM

A chip that resides on the motherboard of the device.

Multi-purpose, for storage and management of keys used for full disk encryption (FDE) solutions.

Provides the operating system with access to keys, but prevents drive removal and data access

TPM is also leveraged by the secure OS boot process

Hardware Security Module (HSM)

a physical computing device that safeguards and manages digital keys, performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions.

Like a TPM, but are often removable or external devices

Hardware Root of Trust

A line of defense against executing unauthorized firmware on a system

And when certificates are used in FDE, they use a hardware root of trust for key storage.

It verifies that the keys match before the secure boot process takes place

Trusted platform module (TPM) and **Hardware Security Module (HSM)** are both implementations of **HRoT**

Key Management System (KMS)

E.G. Azure Key Vault, AWS KMS, GCP Cloud KMS Vault

CSPs offer a cloud service for centralized secure storage and access for application secrets called a vault.

A secret is anything that you want to control access to, such as **API keys**, **passwords**, **certificates**, **tokens**, or **cryptographic keys.**

Service will typically offer programmatic access via API to support DevOps and continuous integration/continuous deployment (CI/CD)

Access control at vault instance-level and to secrets stored within.

Secrets and keys can generally be protected either by software or by FIPS 140-2 Level 2 validated HSMs.

TOOLS

Secure Enclave

provides a secure and isolated area within a system or application for processing sensitive data.

uses hardware-based security mechanisms to create an isolated trusted execution environment

allows sensitive data to be processed and stored securely, even in a potentially insecure computing environment.

Also called "Trusted Execution Environment"

OBFUSCATION

Privacy enhancing technologies

Steganography

a computer file, message, image, or video is concealed within another file, message, image, or video.

an attacker may hide info in this way to exfiltrate sensitive company data.

OBFUSCATION

Tokenization

Stateless, stronger than encryption, keys not local

where meaningful data is replaced with a token that is generated randomly, and the original data is held in a vault.

Pseudo-nymization

Reversal requires access to another data source

de-identification procedure in which personally identifiable information (PII) fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.

OBFUSCATION

Anonymization

process of removing all relevant data so that it is impossible to identify original subject or person.

Only effective if you do NOT need the identity data!

Data minimization

only necessary data required to fulfill the specific purpose should be collected

Collect "the minimum amount" to meet the stated purpose and manage retention to meet regulations

Data masking

when only partial data is left in a data field.

for example, a credit card may be shown as

**** **** **** 1234

Commonly implemented within the database tier, but also possible in code of frontend applications

HASHING VS ENCRYPTION

How is hashing different from encryption?

Encryption

Encryption is a two-way function; what is encrypted can be decrypted with the proper key.

Hashing

no way to reverse if properly designed

a one-way function that scrambles plain text to produce a unique message digest.

Common uses of hashing

Verification of digital signatures

Generation of pseudo-random numbers

Integrity services (data integrity and authenticity)

File integrity monitoring, validation of data transfer

COMMON USES OF ALGORITHMS

How are different algorithm types used?

Symmetric

Example: AES256

Typically used for bulk encryption / encrypting large amounts of data.

Asymmetric

Example: RSA, DH, ECC

Distribution of symmetric bulk encryption keys (shared key)

Identity authentication via digital signatures and certificates

Non-repudiation services and key agreement

Hash functions

Verification of digital signatures

Generation of pseudo-random numbers

Integrity services (data integrity and authenticity)

HASH FUNCTION REQUIREMENTS

Good hash functions have five requirements:

1. They must allow input of any length.
2. Provide fixed-length output.
3. Make it relatively easy to compute the hash function for any input.
4. Provide one-way functionality.
5. Must be collision free.

DIFFERENCES BETWEEN ALGORITHM TYPES

Feature / Algorithm	HASH	SYMMETRIC	ASYMMETRIC
NUMBER OF KEYS	0	1	2+
RECOMMENDED KEY LENGTH (NIST)	256 bits	128 bits (more for some sensitive data types)	2048 bits
COMMON EXAMPLE	SHA	AES	RSA
SPEED	Fast	Fast	Relatively Slow
COMPLEXITY	Medium	Medium	High
EFFECT OF KEY COMPROMISE	N/A	Loss of both sender & receiver	Loss for owner of the asymmetric key only
KEY MANAGEMENT & SHARING	N/A	Challenging	Easy & Secure
EXAMPLES	SHA-224, SHA-256, SHA-384, SHA-512	AES, Blowfish, Twofish, 3DES, RC4	RSA, DSA, ECC, Diffie-Helman

Always evolving, and eventually affected by quantum computing

SALTING

SALTS

Cryptographic

Attackers may use **rainbow tables**, which contain precomputed values of cryptographic hash functions to identify commonly used passwords

A **salt** is random data that is used as an additional input to a one-way function that hashes data, a password or passphrase.

Adding salts to the passwords before hashing them reduces the effectiveness of rainbow table attacks.

Digital Signatures

Digital signatures are similar in concept to handwritten signatures on printed documents that identify individuals, but they provide more security benefits.

is an encrypted hash of a message, encrypted with the sender's private key.

in a signed email scenario, it provides three key benefits:

Authentication. This positively identifies the sender of the email.

ownership of a digital signature secret key is bound to a specific user

Non-repudiation. The sender cannot later deny sending the message.

This is sometimes required with online transactions

Integrity. provides assurances that the message has not been modified or corrupted.

Recipients know that the message was not altered in transit

These are the basics important for the Security+ exam

DIGITAL SIGNATURE STANDARD

DSS

Digital Signature Standard

The Digital Signature Standard uses the SHA-2, and SHA-3 **message digest** functions…

Works in conjunction with one of three **asymmetric encryption algorithms**:

Digital Signature Algorithm (DSA)

Rivest, Shamir, Adleman (RSA) algorithm

Elliptic Curve DSA (ECDSA) algorithm.

DSS is documented in FIPS 186-4 from NIST at https://csrc.nist.gov/publications/detail/fips/186/4/final

KEY STRETCHING

Key Length

some cipher suites are easier to crack than others.

larger keys tend to be more secure, because there are more possible key combinations

Key Stretching

processes used to take a key that may be weak and make it stronger, by making it longer and more random

a longer key has more combinations a brute force attack has to go through to crack

Quantum computing will impact this recommendation

Since 2015, NIST recommends a minimum of **2048-bit keys** for RSA. This will change over time as computing power advances.

BLOCKCHAIN

Blockchain was originally the technology that powered Bitcoin but has broader uses.

A **distributed, public ledger** that can be used to store financial, medical, or other transactions. Anyone is free to join and participate

does not use intermediaries such as banks and financial institutions.

data is "chained together" with a block of data holding both the hash for that block and the hash of the preceding block.

To create a new block on the chain: the computer that wishes to add the block solves a cryptographic puzzle and sends the solution to the other computers participating in that blockchain.

This is known as "proof of work"

BLOCKCHAIN vs OPEN PUBLIC LEDGER?

What is the difference between **blockchain** and an **open public ledger**?

Decentralization. blockchain is decentralized - it is distributed across a peer-to-peer network with no central authority.

An open public ledger can be centralized and maintained by a single entity.

Immutability. blockchain data is immutable and cryptographically secured. Once data is added to the blockchain, it is extremely difficult to alter it.

Data on a public ledger can be changed more easily.

Validation. blockchain uses consensus mechanisms like proof-of-work or proof-of-stake to validate new data added to the chain.

Public ledgers rely more on the integrity of the central authority.

Transparency. blockchain transactions can be pseudonymous for privacy.

Public ledger transactions are typically fully transparent.

Common use cases

Common scenarios for specific cryptographic choices.

Low power devices. devices often use ECC for encryption, as it uses a small key. IoT devices do not have the processing power for conventional encryption.

Low latency. Means "encryption and decryption should not take a long time". Specialized encryption hardware is a common answer in this scenario.

a VPN concentrator or encryption accelerator cards can improve efficiency

High resiliency. Use the most secure encryption algorithm practical to prevent the encryption key from being cracked by attackers.

Device, application, or service compatibility may influence decisions

Supporting confidentiality. Encryption should be implemented for exchange of any sensitive data, and in a way that ensures only authorized parties can view.

For example, connecting remote offices via IPSec VPN

Common use cases

Common scenarios for specific cryptographic choices.

Supporting integrity. two important scenarios for ensuring integrity: ensuring file data has not been tampered with, and communications are not altered in transit.

File hash to check file integrity, digital signature for email.

Supporting obfuscation. obfuscation is commonly used in source code or with data to ensure it cannot be read by anyone who steals it.

Steganography, tokenization, masking can be used to obscure data.

Supporting authentication. a single-factor username and password are not considered secure as theft of the password leads to compromise.

MFA for user authentication, certificate-based auth for devices

Supporting non-repudiation. When you digitally sign an email with your private key, you cannot deny that it was you, as there is only one private key.

Non-repudiation is important in any legally binding transaction

Limitations

Common scenarios for specific cryptographic choices.

Speed. Application and hardware must be able to keep pace with the selected encryption.

Size. If encrypting 16 bytes of data with a block cipher, the encrypted information is also 16 bytes. This overhead must be considered in resource planning

Need enough memory, storage, and network to support the result

Weak keys. Larger keys are generally stronger and thus more difficult to break.

Find balance between security, compatibility, and capacity

Time. encryption and hashing take time. Larger amounts of data and asymmetric encryption take more time than small data and symmetric encryption.

Selections need to match time constraints in transactions

Longevity. consider how long encryption algorithms selected can be used.

Older algorithms will generally be retired sooner

Limitations

Common scenarios for specific cryptographic choices.

Predictability. cryptography relies on randomization. Random number generation that can't be easily predicted is crucial for any type of cryptography.

Reuse. using the same key is commonly seen in a number of encryption mechanisms. If an attacker gains access to the key, they can decrypt data encrypted with it.

some IoT devices may not allow a key change

Entropy. a measure of the randomness or diversity of a data-generating function.

Data with full entropy is completely random with no meaningful patterns.

Resource vs security constraints. the more secure the encryption used and higher the key length, the more processing power and memory the server will need.

requires balance between algorithms and hardware selections

INSIDE CLOUD AND SECURITY

THANKS

FOR WATCHING!