



# CISSP EXAM CRAM

## THE COMPLETE COURSE

### DOMAIN 3

Security Architecture  
and Engineering

## Exam Outline

- 3.1** Research, implement and **manage engineering processes** using secure design principles
- 3.2** Understand the fundamental concepts of **security models** (*Biba, Star Model, Bell-LaPadula*)
- 3.3** **Select controls** based upon systems security requirements
- 3.4** Understand **security capabilities** of information systems (*TPM, encryption/decryption*)
- 3.5** Assess and **mitigate the vulnerabilities** of security architectures, designs, and solution elements

## Exam Outline

- 3.6 Select and determine **cryptographic solutions**
- 3.7 Understand methods of **cryptanalytic attacks**
- 3.8 Apply security principles to site and facility **design**
- 3.9 Design site and facility **security controls**

*What is actually NEW in 2021 release?*

# WHAT'S NEW IN DOMAIN 3?

## 3.1 Research, implement and manage engineering processes using secure design principles

- Threat Modeling
  - Least privilege
  - Defense in depth
  - Secure defaults
  - Fail securely
  - Separation of Duties
  - Keep it simple
  - Zero Trust
  - Privacy by design
  - Trust but verify
  - Shared responsibility
- NEW! included here
- 

# WHAT'S NEW IN DOMAIN 3?

## 3.6 Select and determine **cryptographic solutions**

- Quantum

*Relevant and expanded versus  
what is in the official study guide*

# WHAT'S NEW IN DOMAIN 3?

## 3.7 Understand methods of cryptanalytic attacks

- Brute force
- Ciphertext only
- Known plaintext
- Frequency analysis
- Chosen ciphertext
- Implementation attacks
- Side-channel
- Fault injection
- Timing
- Man-in-the-Middle (MITM)
- Pass the hash
- Kerberos exploitation
- Ransomware

*covered in "Attacks and Countermeasures"*

# SECURE DESIGN PRINCIPLES

*taken from NIST SP 800-160*

## Secure Defaults

default configuration reflects a restrictive and conservative enforcement of security policy.

## Fail Securely

indicates that components should fail in a state that denies rather than grants access.

## Trust but verify

depended on an initial authentication process to gain access to the internal “secured” environment then relied on generic access control methods.

*Due to changes in threat landscape, no longer considered sufficient*

# 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**



# Privacy by Design

The 7 principles  
from the IAPP

Making privacy an integral part of every system, technology, policy, and design process.

1. **Proactive** and not a reactive approach
2. Privacy as the **Default setting**
3. Privacy must be **embedded** in the design
4. Privacy should be a **positive-sum approach** and not a zero-sum approach
5. End to end full lifecycle **data protection**
6. **Visibility** and **transparency**
7. Keep privacy **user-centric**



Applying these principles in implementing a layered defense as part of a zero trust strategy ensures privacy.

# SECURE DESIGN PRINCIPLES

## Keep it Simple

Complexity is the worst enemy of security.

**Best-in-suite** over best-in-breed solutions are one approach used to simplify defense in-depth. Simplicity also helps to avoid configuration mistakes.

Enables organizations to move forward, improving **incrementally**, rather than demanding perfection.

Fresh application of the classic 'Kiss' principle

**CISSP**

**EXAM**

**CRAM**

**ATTACKS AND  
COUNTER MEASURES**



# COMPARE CLOUD MODELS & SERVICES

**PRIVATE**

**HYBRID**

**PUBLIC**

**IAAS**

**PAAS**

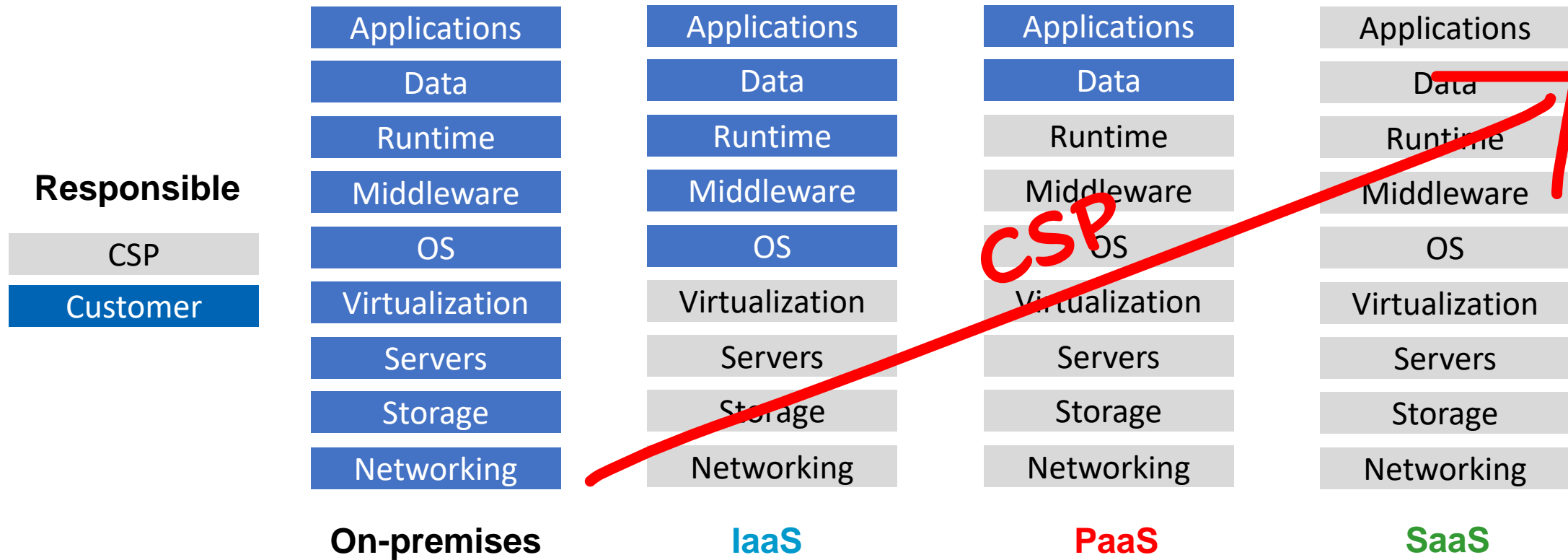
**SAAS**

# COMPARE CLOUD MODELS & SERVICES

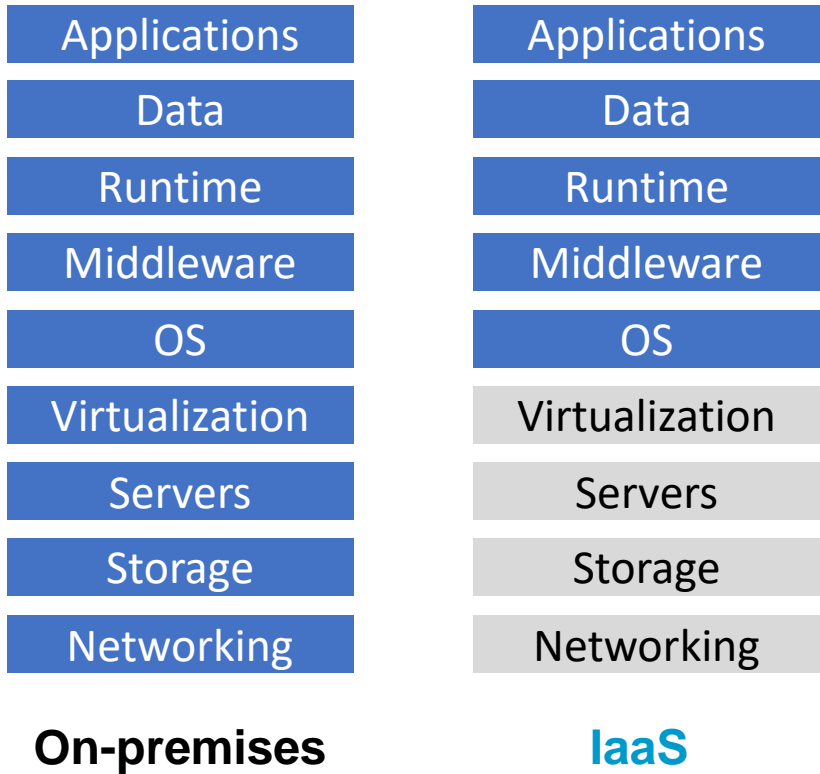
## **SHARED RESPONSIBILITY MODEL**

# SHARED RESPONSIBILITY MODEL

100% YOURS



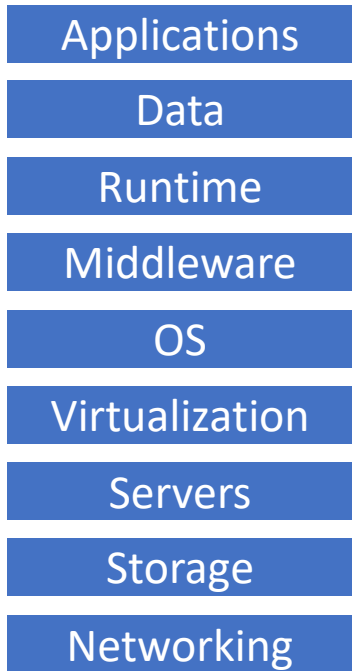
# CLOUD MODELS & SERVICES - IAAS



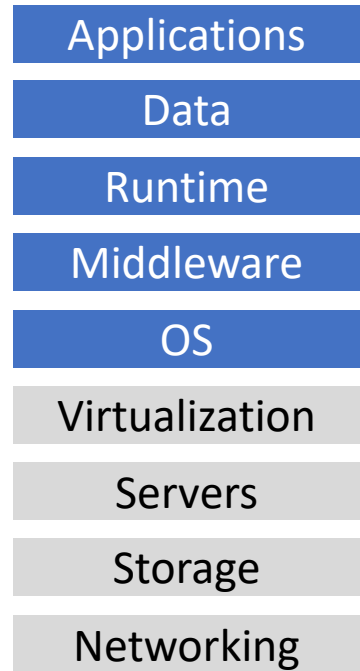
**CSP provides** building blocks, like networking, storage and compute

**CSP manages** staff, HW, and datacenter

# CLOUD MODELS & SERVICES - IAAS



**On-premises**



**IaaS**



Azure Virtual  
Machines



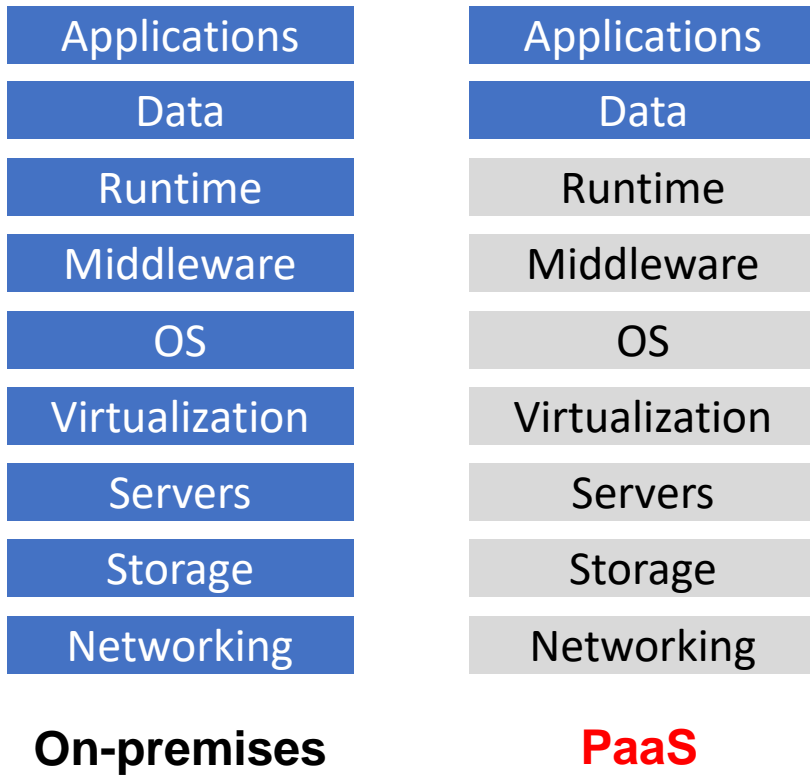
Amazon EC2



GCP Compute  
Engine



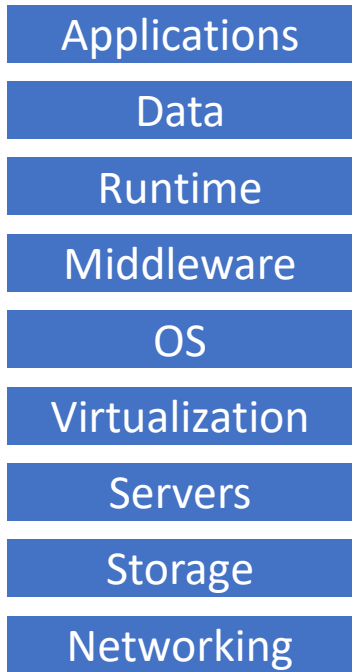
# CLOUD MODELS & SERVICES - PAAS



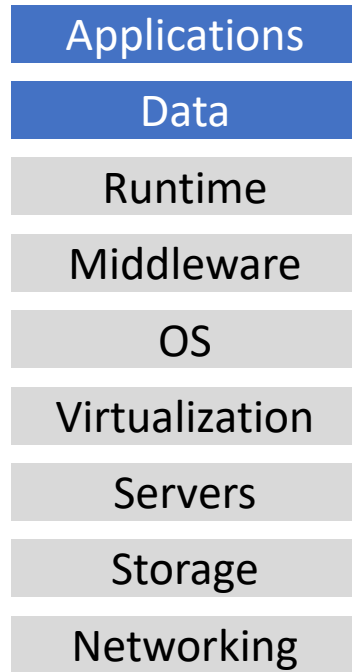
**Customer is responsible** for deployment and management of apps

**CSP manages** provisioning, configuration, hardware, and OS

# CLOUD MODELS & SERVICES - PAAS



**On-premises**



**PaaS**



Azure SQL  
Database



API  
Management



Azure App  
Service

# HOW

is SERVERLESS

# DIFFERENT

from PAAS in terms of

# RESPONSIBILITY?

function-as-a  
service (FaaS)



# PaaS

# Serverless

**More control** over deployment environment

Application **has to be configured** to auto-scale

Application takes **a while to spin up**

Devs have to write code

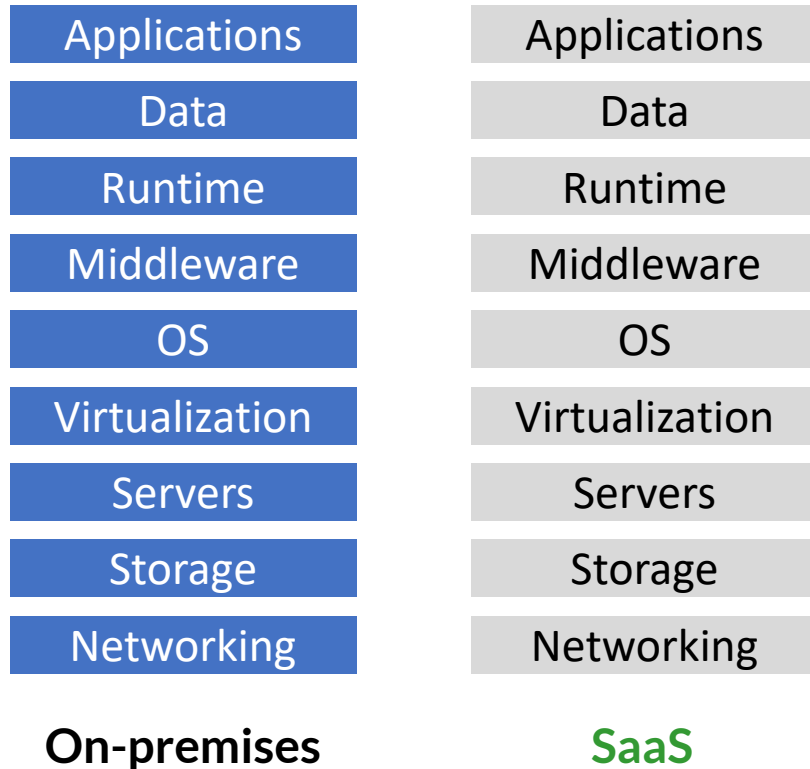
No server management

**Less control** over deployment environment

Application scales **automatically**

Application code only **executes when invoked**

# CLOUD MODELS & SERVICES - SAAS



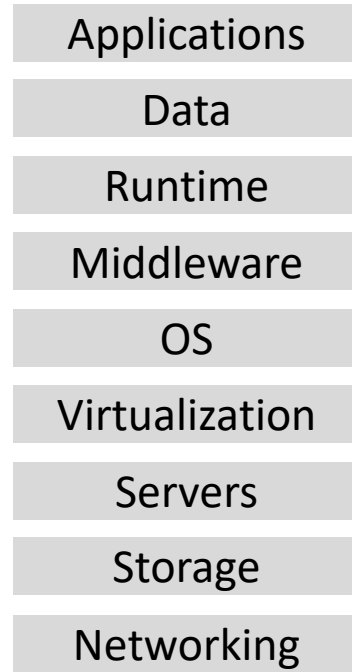
Customer just **configures features**.

**CSP is responsible for** management, operation, and service availability.

# CLOUD MODELS & SERVICES - SAAS



On-premises



SaaS



# CLOUD MODELS

**Describe the differences between Public, Private and Hybrid cloud models**

Describe  
**Public Cloud**

Everything runs on your  
**cloud provider's hardware.**

# CLOUD MODELS

**Describe the differences between Public, Private and Hybrid cloud models**

Describe  
Public Cloud

Advantages include **scalability**, **agility**, **pay-as-you-go**, no **maintenance**, and **low skills**



# CLOUD MODELS

**Describe the differences between Public, Private and Hybrid cloud models**

Describe  
Private Cloud

A cloud environment **in your own datacenter**

# CLOUD MODELS

**Describe the differences between Public, Private and Hybrid cloud models**

Describe  
Private Cloud

Advantages include **legacy support, control, and compliance**

# CLOUD MODELS

**Describe the differences between Public, Private and Hybrid cloud models**

Describe  
**Hybrid Cloud**

**Combines public and private clouds**, allowing you to run your apps in the right location

# CLOUD MODELS

**Describe the differences between Public, Private and Hybrid cloud models**

Describe  
**Hybrid Cloud**

Advantages include **flexibility** in legacy, compliance, and scalability scenarios

# CLOUD ACCESS SECURITY BROKER

## WHAT IS A CASB?

---

A cloud access security broker (CASB) is a security policy enforcement solution that may be installed on-premises or in the cloud.

shadow IT

What is **post-quantum cryptography**?

The development of **new kinds of cryptographic approaches** that can be implemented using today's conventional computers.

...but will be impervious (resistant) to attacks from tomorrow's quantum computers.

*Which algorithms are susceptible?*

*Which algorithms are resistant?*

# POST-QUANTUM CRYPTOGRAPHY

How well do current encryption algorithms hold up to the power of quantum computing?

## SYMMETRIC

Shared Key

*bulk encryption (fast)*

Holds up fairly well to quantum computing



## ASYMMETRIC

Public Key Cryptography

*key exchange, digital signatures*

Quantum poses more immediate threats here



# POST-QUANTUM CRYPTOGRAPHY

How well do current encryption algorithms hold up to the power of quantum computing?

**SYMMETRIC**

Shared Key

*bulk encryption (fast)*

**Grover's algorithm** shows that a quantum computer speeds up these attacks to effectively **halve the key length**.

This would mean that a **256-bit key** is as strong against a **quantum** computer as a 128-bit key is against a conventional computer.



Doubling key length from 128 to 256 does not make the key twice as strong, it makes it  **$2^{128}$  times as strong**.



# POST-QUANTUM CRYPTOGRAPHY

How well do current encryption algorithms hold up to the power of quantum computing?

## ASYMMETRIC

Public Key Cryptography

key exchange,  
digital signatures

**Shor's algorithm** can easily break all of the commonly used public-key algorithms based on both factoring and the discrete logarithm problem



This means **RSA** is vulnerable



This means **Elliptic Curve** is vulnerable



However, **Lattice** offers some resistance!



Doubling the key length increases the difficulty to break by a **factor of eight**. *That's not a sustainable advantage.*

How well do current encryption algorithms hold up to the power of quantum computing?

## QUICK NOTES ON **LATTICE**



However, **Lattice** offers some resistance!

Based on different types of problems: the **shortest vector problem** and the **closest vector problem**

Potentially enables us to replace essentially all of our currently endangered schemes

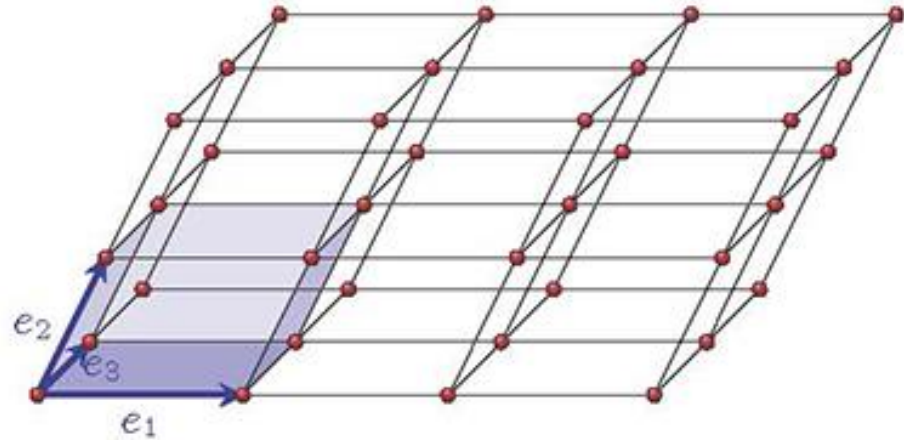
Lattice-based cryptographic schemes make up the lion's share of scientific publications on post-quantum cryptography



Research, selection, and standards development is ongoing

What exactly is a **lattice**?

a 3-dimensional array of  
regularly spaced points



## FOR THE EXAM

---

If you see a question asking for which types of public key (asymmetric) algorithms are “quantum resistant”, the answer is:

LATTICE

# CRYPTOGRAPHY

## Code

Cryptographic systems of symbols that operate on words or phrases and are sometimes secret but **don't always** provide confidentiality.

## Cipher

*always secret!*

Ciphers, are **always** meant to hide the true meaning of a message.

# CRYPTOGRAPHY – TYPES OF CIPHERS

## Stream cipher

is a **symmetric key cipher** where plaintext digits are combined with a pseudorandom **cipher** digit **stream** (keystream). In a **stream cipher**, each plaintext digit is encrypted one at a time with the corresponding digit of the keystream, to give a digit of the **ciphertext stream**.

## Block cipher

is a **method of encrypting text** (to produce **ciphertext**) 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.

## Substitution

use the encryption algorithm to replace each character or bit of the plaintext message with a different character. *Julius Caesar developed one of the earliest ciphers of this type now known as the “Caesar cipher”.*

# CRYPTOGRAPHY – TYPES OF CIPHERS

## Transposition

uses an encryption algorithm to rearrange the letters of a plaintext message, forming the ciphertext message.

**Initialization vector (IV)** *cryptographic version of a random number* is a random bit string (a nonce) that is XORed with the message, reducing predictability and repeatability.

Size of the IV varies by algorithm but is normally the same length as the block size of the cipher or as large as the encryption key.

## Caesar, Vigenère, One-time Pad

Three very similar stream ciphers. The main difference between these ciphers is **key length**.

**Caesar** shift cipher uses a key of length one

**Vigenère** cipher uses a longer key (usually a word or sentence),

**One-time pad** uses a key that is as long as the message itself. ←

# ONE-TIME PAD SUCCESS FACTORS

## To be successful...

For a **one-time pad** to be successful, the key must be  
Generated randomly without any known pattern.  
At least as long as the message to be encrypted.

## AND

The pads must be protected against physical disclosure  
Each pad must be used only one time and then discarded

ALL these must be true!



# CONCEPT: ZERO-KNOWLEDGE PROOF

**Zero-knowledge proof** is a communication concept.

A specific type of information is exchanged, but no real data is transferred, as with digital signatures and digital certificates.

## MORE SIMPLY

It enables one to prove knowledge of a fact to another individual without revealing the fact itself.

# CONCEPT: SPLIT KNOWLEGE

“

**Split knowledge** means that the information or privilege required to perform an operation is divided among **multiple users**.

This ensures that no single person has sufficient privileges to compromise the security of the environment.

# CONCEPT: WORK FUNCTION (WORK FACTOR)

**Work function**, or **work factor**, is a way to measure the strength of a cryptography system by measuring the effort in terms of cost and/ or time to **decrypt messages**.

Usually, the time and effort required to perform a complete brute-force attack against an encryption system is what a work function rating represents.

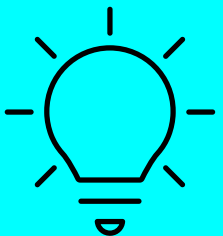
The security and protection offered by a cryptosystem is directly proportional to value of its work function/factor.

*The time and effort required to break a protective measure*

# IMPORTANCE OF KEY SECURITY

**Cryptographic keys** provide the necessary element of secrecy to a cryptosystem.

Modern cryptosystems utilize keys that are **at least 128 bits long** to provide adequate security.



This will change as technologies evolve and emerge (like quantum computing)

# CONCEPT: SYMMETRIC vs ASYMMETRIC

**Symmetric**

*faster*

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

**Asymmetric**

*stronger*

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

# CONFIDENTIALITY, INTEGRITY & NONREPUDIATION

## Confidentiality

is one of the major goals of cryptography. It protects the secrecy of data while it is both at rest and in transit.

## Integrity

provides the recipient of a message with the assurance that **data was not altered** (intentionally or unintentionally) between the time it was created and the time it was accessed.

## Nonrepudiation

provides undeniable proof that the sender of a message actually authored it. It prevents the sender from subsequently denying that they sent the original message.

# DES (AND 3DES) MODES

**Electronic Codebook Mode (ECB).** Simplest & least secure mode. Processes 64-bit blocks, encrypts block with the chosen key. If same block encountered multiple times, **same encrypted block is produced**, making it easy to break.

**Cipher Block Chaining (CBC).** Each block of unencrypted text is **XORed** with the block of ciphertext immediately preceding. Decryption process simply decrypts ciphertext and reverses the XOR operation.

**Cipher Feedback (CFB).** Is the streaming version of CBC. Works on data in real time, using memory buffers of same block size. When buffer is full, data is encrypted and transmitted. *Uses chaining, so errors propagate.*

**Output Feedback (OFB).** Operates similar to CFB, but XORs the plain text with a seed value. No chaining function, so errors do not propagate.

**Counter (CTR).** Uses an **incrementing counter instead of a seed.** Errors do not propagate.

# XOR CIPHER

The **Exclusive-OR** option (**XOR**, also known as **binary addition**) is used heavily in cryptology, sounds more complicated than it actually is: a function of flipping bits in a simple, systematic fashion.

Original Value	Key Value	Cipher Value
1	1	0
1	0	1
0	1	1
0	0	0

binary values match = 0, otherwise cipher value is 1



# KEY CLUSTERING

---

A Weakness in cryptography where a plain-text message generates identical ciphertext messages using the same algorithm but using different keys.

# 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!*

# EXAMPLE: 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



# 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.

# CRYPTOGRAPHIC SALTS

## SALTS

Cryptographic

Attackers may use **rainbow tables** of precomputed values 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 SIGNATURE STANDARD

**DSS**

Digital Signature  
Standard

The Digital Signature Standard uses the SHA-1, SHA-2, and SHA-3 **message digest** functions...

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

Digital Signature Algorithm (DSA)

Rivest, Shamir, Adleman (RSA) algorithm

Elliptic Curve DSA (ECDSA) algorithm.

# PUBLIC KEY INFRASTRUCTURE

PKI

Public Key  
Infrastructure

**Certificate authorities (CAs)** generate **digital certificates** containing the public keys of system users.

Users then **distribute certificates** to people with whom they want to communicate.

Certificate recipients **verify a certificate** using the CA's public key.

*certs used for web, network, and some email security*

# SECURING TRAFFIC

## Email

Standards for encrypted messages include **S/MIME** protocol and **Pretty Good Privacy (PGP)**.

## Web

The de facto standard for secure web traffic is the use of HTTP over **Transport Layer Security (TLS)**, largely replacing the older **SSL**.

## Network

**IPsec** protocol standard provides a common framework for encrypting network traffic and is built into many common operating systems.



# IPSEC BASICS

## IPsec

A security architecture framework that supports **secure communication over IP**.

Establishes a secure channel in either **transport mode** or **tunnel mode**.

Can be used to establish direct communication **between computers** or over a **VPN connection**

Uses two protocols: **Authentication Header (AH)** and **Encapsulating Security Payload (ESP)**

# COMMON CRYPTOGRAPHIC ATTACKS

**Brute-force attacks** are attempts to randomly find the correct cryptographic key. Known plaintext, chosen ciphertext, and chosen plaintext attacks require the attacker to have some extra information in addition to the ciphertext.

**Meet-in-the-middle attack** exploits protocols that use two rounds of encryption.

**Man-in-the-middle attack** fools both parties into communicating with the attacker instead of directly with each other.

**Birthday attack** is an attempt to find collisions in hash functions.

**Replay attack** is an attempt to reuse authentication requests.

# DIGITAL RIGHTS MANAGEMENT

## DRM


Digital Rights  
Management

Allow content owners to **enforce restrictions** on the use of their content by others.

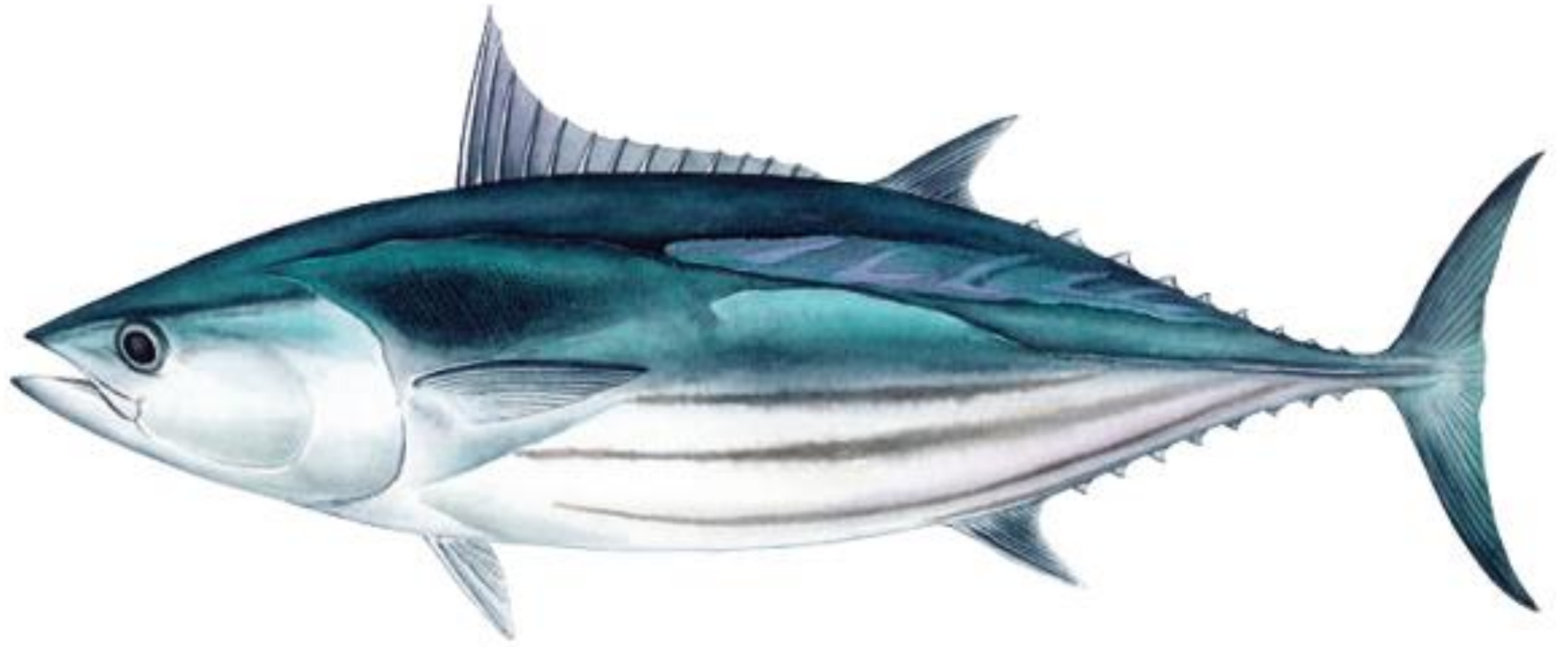
Commonly protect entertainment content, such as music, movies, and e-books

Occasionally found in the enterprise, protecting sensitive information stored in documents.

# CRYPTOGRAPHY – SYMMETRIC ALGORITHMS



NAME	TYPE	Algorithm Type	Block Size (bits)	Key Size (bits)	Strength
AES	Symmetric	Block cipher	128	128, 192, 256	Strong
Blowfish	Symmetric		64	32-448 key bit	
DES	Symmetric	Block cipher	64	56 bit	Very weak
3DES	Symmetric	Block cipher	64	112 or 168 bit	Moderate
IDEA	Symmetric		64	128	
RC2	Symmetric		64	128	
RC4	Symmetric	Stream cipher	Streaming	128	
RC5	Symmetric	RSA Block mode cipher	32, 64, 128	0 – 2,040 bit	Very Strong
Skipjack	Symmetric		64	80	
Twofish	Symmetric		128	1-256	



This is a skipjack

# CRYPTOGRAPHY – SYMMETRIC ALGORITHMS

NAME	TYPE	Algorithm Type	Block Size (bits)	Key Size (bits)	Strength
AES	Symmetric	Block cipher	128	128, 192, 256	Strong
Blowfish	Symmetric		64	32-448 key bit	
DES	Symmetric	Block cipher	64	56 bit	Very weak
3DES	Symmetric	Block cipher	64	112 or 168 bit	Moderate
IDEA	Symmetric		64	128	
RC2	Symmetric		64	128	
RC4	Symmetric	Stream cipher	Streaming	128	
RC5	Symmetric	RSA block mode cipher	32, 64, 128	0 – 2,040 bit	Strong
RC6	Symmetric	RSA block mode cipher	128	128, 192, 256 - 2,2040	Very Strong
Skipjack	Symmetric		64	80	
Twofish	Symmetric		128	1-256	

x 2

# CRYPTOGRAPHY

## Hash Algorithms

**MD\***

*Message Digest*

NAME	TYPE	HASH VALUE LENGTH	STILL IN USE?	REPLACED BY
HMAC	Hash	Variable	Yes	-
HAVAL	Hash	128, 160, 192, 224, 256	No	
MD2	Hash	128	No	MD6, et. Al.
MD4	Hash	128	No	MD6, et. Al.
MD5	Hash	128	No	MD6, et. Al.
SHA-1	Hash	160	No	SHA-2
SHA-224*	Hash	224	Yes	-
SHA-256*	Hash	256	Yes	-
SHA-384*	Hash	384	Yes	-
SHA-512*	Hash	512	Yes	-

# CRYPTOGRAPHY

## Hash Algorithms

**MD\***

*Message Digest*

NAME	TYPE	HASH VALUE LENGTH	STILL IN USE?	REPLACED BY
HMAC	Hash	Variable	Yes	-
HAVAL	Hash	128, 160, 192, 224, 256	No	
MD2	Hash	128	No	MD6, et. Al.
MD4	Hash	128	No	MD6, et. Al.
MD5	Hash	128	No	MD6, et. Al.
SHA-1	Hash	160	No	SHA-2
SHA-224*	Hash	224	Yes	-
SHA-256*	Hash	256	Yes	-
SHA-384*	Hash	384	Yes	-
SHA-512*	Hash	512	Yes	-



# CRYPTOGRAPHY

## Hash Algorithms

**MD\***

*Message Digest*

NAME	TYPE	HASH VALUE LENGTH	STILL IN USE?	REPLACED BY
HMAC	Hash	Variable	Yes	-
HAVAL	Hash	128, 160, 192, 224, 256	No	
MD2	Hash	128	NO	MD6, et. Al.
MD4	Hash	128	NO	MD6, et. Al.
MD5	Hash	128	NO	MD6, et. Al.
SHA-1	Hash	160	No	SHA-2
SHA-224*	Hash	224	Yes	-
SHA-256*	Hash	256	Yes	-
SHA-384*	Hash	384	Yes	-
SHA-512*	Hash	512	Yes	-

# CRYPTOGRAPHY

## Hash Algorithms

**SHA\***

Secure Hash  
Algorithm

NAME	TYPE	HASH VALUE LENGTH	STILL IN USE?	REPLACED BY
HMAC	Hash	Variable	Yes	-
HAVAL	Hash	128, 160, 192, 224, 256	No	
MD2	Hash	128	No	MD6, et. Al.
MD4	Hash	128	No	MD6, et. Al.
MD5	Hash	128	No	MD6, et. Al.
SHA-1	Hash	160	No	SHA-2
SHA-224*	Hash	224	Yes	-
SHA-256*	Hash	256	Yes	-
SHA-384*	Hash	384	Yes	-
SHA-512*	Hash	512	Yes	-

# CRYPTOGRAPHY

## Hash Algorithms

**SHA\***

Secure Hash  
Algorithm

NAME	TYPE	HASH VALUE LENGTH	STILL IN USE?	REPLACED BY
HMAC	Hash	Variable	Yes	-
HAVAL	Hash	128, 160, 192, 224, 256	No	
MD2	Hash	128	No	MD6, et. Al.
MD4	Hash	128	No	MD6, et. Al.
MD5	Hash	128	No	MD6, et. Al.
SHA-1	Hash	160	No	SHA-2
SHA-224*	Hash	224	Yes	-
SHA-256*	Hash	256	Yes	-
SHA-384*	Hash	384	Yes	-
SHA-512*	Hash	512	Yes	-

# CRYPTOGRAPHY

## Hash Algorithms

*\*SHA-2 variants*

NAME	TYPE	HASH VALUE LENGTH	STILL IN USE?	REPLACED BY
HMAC	Hash	Variable	Yes	-
HAVAL	Hash	128, 160, 192, 224, 256	No	
MD2	Hash	128	No	MD6, et. Al.
MD4	Hash	128	No	MD6, et. Al.
MD5	Hash	128	No	MD6, et. Al.
SHA-1	Hash	160	No	SHA-2
SHA-224*	Hash	224	Yes	-
SHA-256*	Hash	256	Yes	-
SHA-384*	Hash	384	Yes	-
SHA-512*	Hash	512	Yes	-

# CRYPTOGRAPHY

## Hash Algorithms

**SHA\***

Secure Hash  
Algorithm

NAME	TYPE	HASH VALUE LENGTH	STILL IN USE?	REPLACED BY
HMAC	Hash	Variable	Yes	-
HAVAL	Hash	128, 160, 192, 224, 256	No	
MD2	Hash	128	No	MD6, et. al.
MD4	Hash	128	No	MD6, et. al.
MD5	Hash	128	No	MD6, et. al.
SHA-1	Hash	160	NO	SHA-2
SHA-224*	Hash	224	YES	-
SHA-256*	Hash	256	YES	-
SHA-384*	Hash	384	YES	-
SHA-512*	Hash	512	YES	-

# THE THREE MAJOR PUBLIC KEY CRYPTOSYSTEMS

## RSA

is the most famous public key cryptosystem; it was developed by **Rivest, Shamir, and Adleman** in 1977. It depends on the difficulty of factoring the product of prime numbers.

## El Gamal

is an extension of the Diffie-Hellman key exchange algorithm that depends on modular arithmetic. *(less common than RSA in last several years)*

## Elliptic curve

Algorithm depends on the elliptic curve discrete logarithm problem and provides **more security** than other algorithms when both are used with keys of the same length.

---

# DIGITAL SIGNATURES

## Digital signatures

Rely on **public key cryptography** and **hashing functions**

DS algorithms suitable for use in FIPS 186-4 (the Digital Signature Standard) must use **SHA-2** hashing functions

Three currently approved encryption algorithms:

- Digital Signature Algorithm (DSA), as specified in FIPS 186-4
- Rivest, Shamir, Adleman (RSA), specified in ANSI X9.31
- Elliptic Curve DSA (ECDSA), specified in ANSI X9.62

# CRYPTOGRAPHY – ASYMMETRIC ALGORITHMS

Name	Type	Algorithm Type	Size	Strength	Replaced By
RSA	Asymmetric	Key transport	512	Strong	-
Diffie-Hellman	Asymmetric	Key exchange	-	Moderate	El Gamal
El Gamal	Asymmetric	Key exchange	-	Very Strong	-
ECC	Asymmetric	Elliptic Curve	Variable (smaller key size due to EC, 160-bit EC key = 1025 RSA)	Very Strong	-



# WHAT IS A SECURITY MODEL?

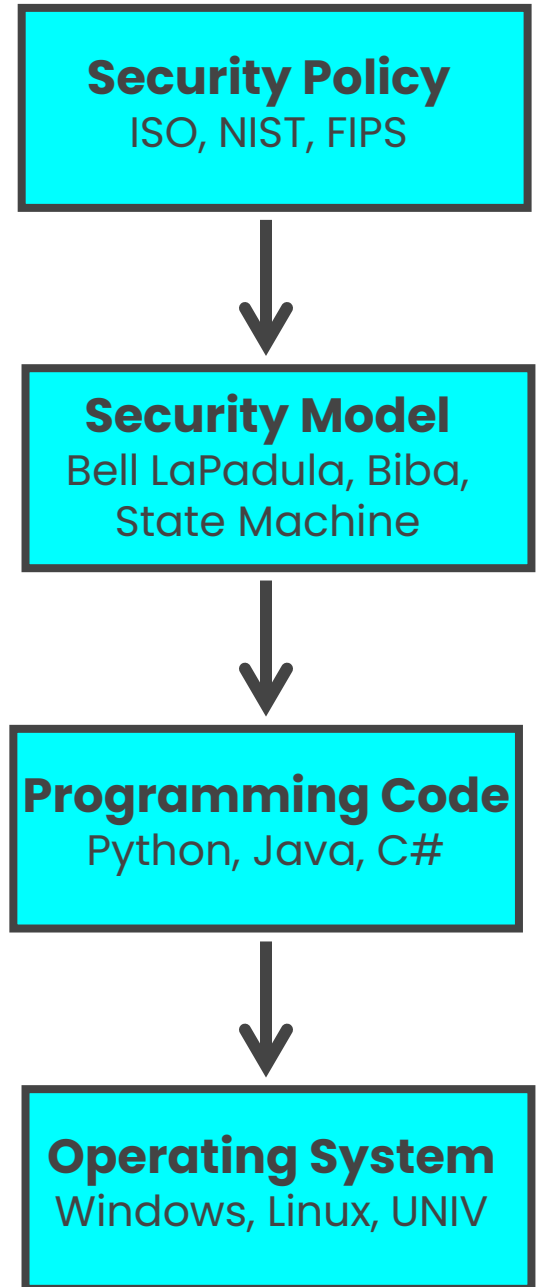
Security models are used to determine how security will be implemented, what subjects can access the system, and what objects they will have access to.

They are a way to formalize security policy.

Typically implemented by enforcing integrity, confidentiality, or other controls.

Each of these models lays out broad guidelines and is not specific in nature.

It is up to the developer to decide how these models will be used and integrated into specific designs.



# WHAT IS THE PURPOSE OF A **Security Model?**

---

Provides a way for designers to map abstract statements into a security policy

# WHAT IS THE PURPOSE OF A **Security Model?**

---

Determines how security will be implemented, what **subjects** can access the system, and what **objects** they will have access to.

# STATE MACHINE MODEL

## State Machine Model

Describes a system that is always secure **no matter what state it is in.**

Based on the computer science definition of a finite state machine (FSM).

A **state** is a **snapshot of a system** at a specific moment in time. All state transitions must be evaluated.

If each possible state transition results in another secure state, the system can be called a **secure state machine.**

# INFORMATION FLOW MODEL

## Information Flow Model

Focuses on the flow of information

Information flow models are based on a state machine model

**Biba** and **Bell-LaPadula** are both information flow models

Bell-LaPadula preventing information flow from a high security level to a low security level.

Biba focuses on flow from low to high security level

# NON-INTERFERENCE MODEL

## Non- Interference Model

is loosely based on the information flow model.

is concerned with how actions of a subject at a higher security level affect the system state or the actions of a subject at a lower security level.

ensures that the actions of different objects and subjects aren't seen by (and don't interfere with) other objects and subjects on the same system.

# LATTICE-BASED MODEL

based on the interaction between any combination of:

**objects** (such as resources, computers, and applications) and

**subjects** (such as individuals, groups or organizations).

Lattice-based models are used to define the levels of security that an object may have and that a subject may have access to.

# SECURITY MODELS

Three properties that will be mentioned repeatedly when talking about security models.

## **Simple security property**

Describes rules for **read**

## **Star \* security property**

Describes rules for **write**

## **Invocation property**

Rules around invocations (calls), such as to subjects



# SECURITY MODELS

## Integrity

### **Biba**

No read down, no write up

### **Clark-Wilson**

Access control triple

### **Goguen-Meseguer**

THE noninterference model

### **Sutherland**

preventing interference  
(information flow and SMM)

## Confidentiality

 government (DoD)

### **Bell-LaPadula**

No read up, no write down

### **Brewer and Nash**

aka "Chinese Wall"

### **Take Grant**

Employs a "directed graph"

# Bell LaPadula

Lattice-based

State machine model enforces **confidentiality**

Uses mandatory access control (mac) to enforce the DoD multilevel security policy ← government!

### **Simple security property**

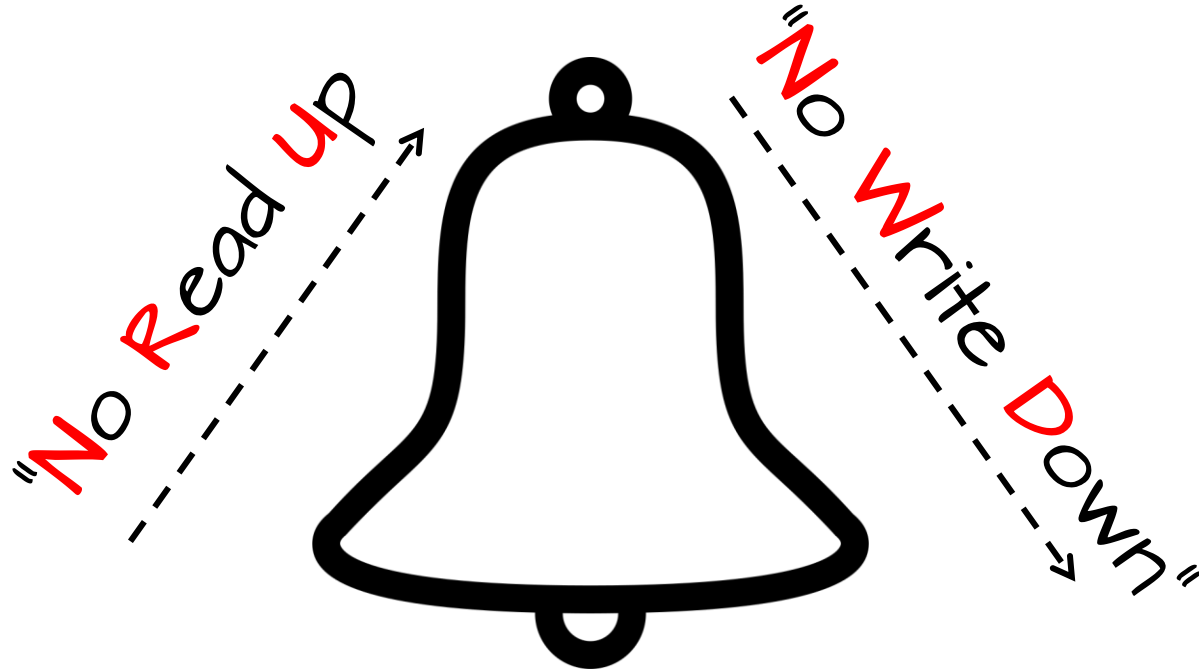
subject cannot read data at a higher level of classification. "no read up"

### **Star \* security property**

subject cannot write info to lower level of classification  
"no write down"

# SECURITY MODELS

## Bell LaPadula

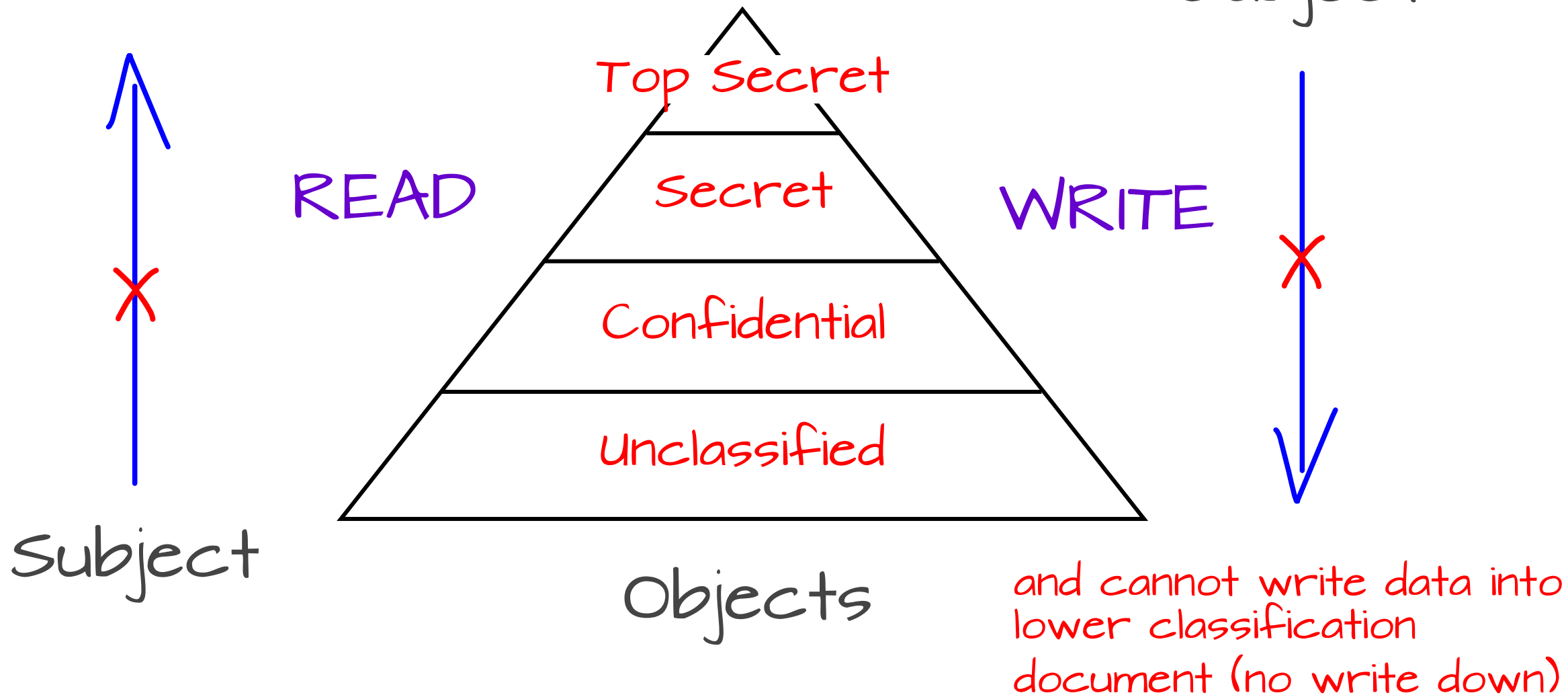


Mnemonic: "No Running under Nets With Dingos"

# Bell LaPadula

User cannot read higher  
classifications (no read up)

Subject



# Biba

A lattice-based model developed to address concerns of **integrity**.

**Simple integrity property**—subject at one level of integrity is not permitted to read an object of lower integrity. "no read down"

**Star \* integrity property**—object at one level of integrity is not allowed to write to object of higher integrity. "no write up"

**Invocation property**—prohibits a subject at one level of integrity from invoking a subject at a higher level of integrity.

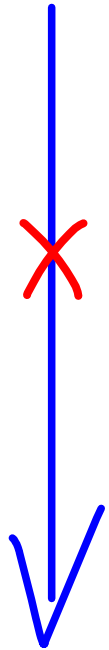
**SIMPLE** property = **READ**

**STAR** property = **WRITE**

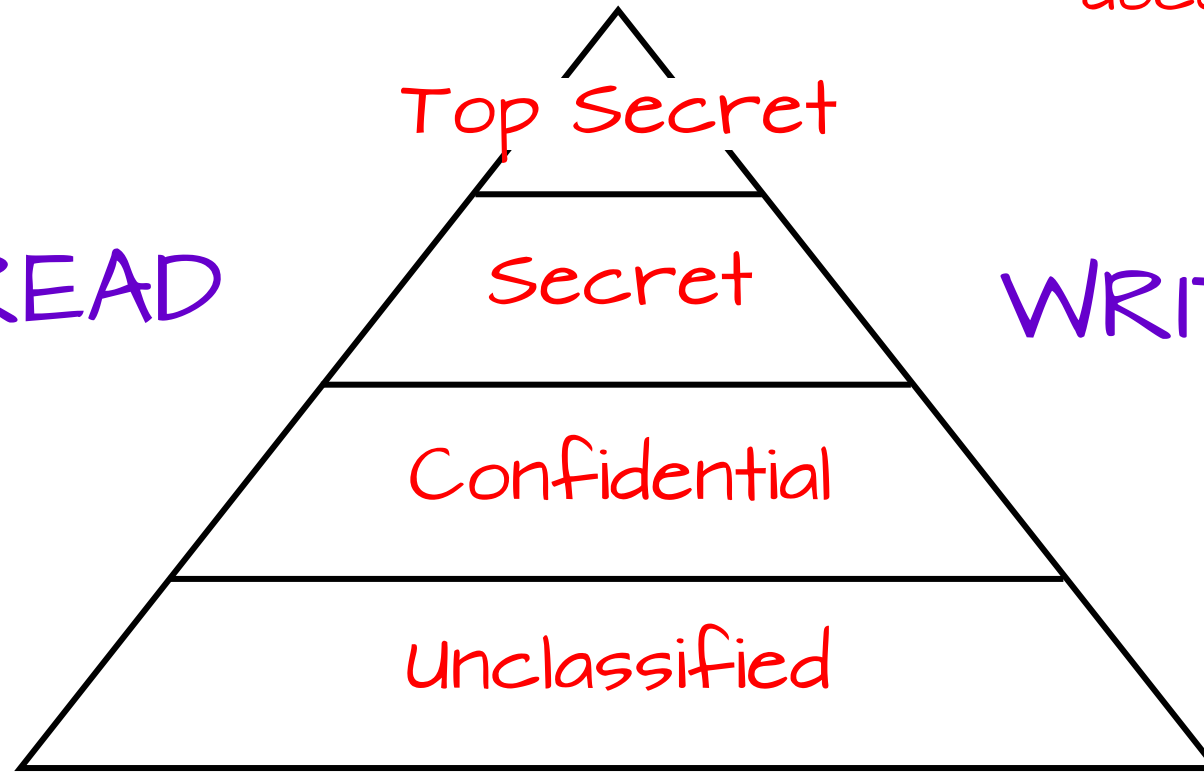
# Biba

and cannot write data  
into higher classification  
document (no write up)

Subject



READ



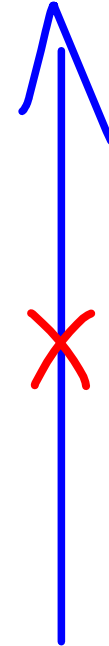
Top Secret

Secret

Confidential

Unclassified

WRITE



User cannot read lower  
classifications (no read down)

Objects

Subject

# Clark-Wilson

uses security **labels** to grant access to objects.

**constrained data item (CDI)** —is any data item whose integrity is **protected** by the security model.

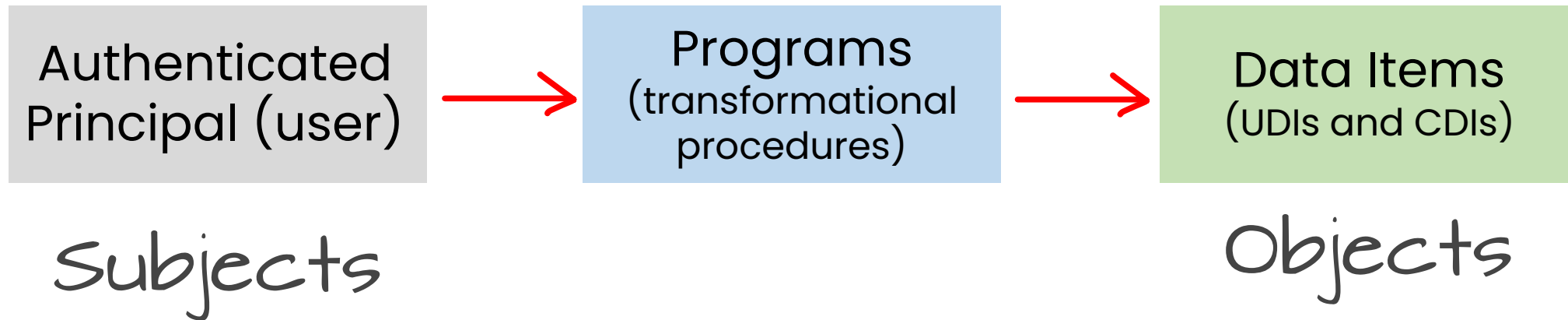
**unconstrained data item (UDI)** —is any data item that is not controlled by the security model.

**integrity verification procedure (IVP)** —is a procedure that scans data items and confirms their integrity.

**Transformation procedures (TPs)** —are the only procedures that are **allowed to modify a CDI**.

# Clark-Wilson

What is the **access control triple(triplet)**?



The relationship between an authenticated principal (i.e., user) and a set of programs (i.e., TPs) that operate on a set of data items (e.g., UDIs and CDIs).



# DOMAIN 3: SECURITY MODELS

## Take Grant Model

another **confidentiality-based** model that supports **four basic operations**: take, grant, create, and revoke.

## Brewer and Nash Model

also called the "Chinese Wall model". It was developed to prevent conflict of interest (COI) problems. (**confidentiality-based**)

## Graham-Denning model

This model uses a formal set of protection rules for which each object has an owner and a controller.

It is focused on the **secure creation** and **deletion** of both **subjects** and **objects**.

A collection of **eight primary protection rules** or actions that define the boundaries of certain secure actions.

### “Eight rules” of Graham-Denning

Securely **create** an **object**.

Securely **create** a **subject**.

Securely **delete** an **object**.

Securely **delete** a **subject**.

Securely provide the **read** access right.

Securely provide the **grant** access right.

Securely provide the **delete** access right.

Securely provide the **transfer** access right.

# DOMAIN 3: SECURITY MODES

## Dedicated Mode

Security clearance that permits **access** to **ALL** info processed by system, **approval** for **ALL** info processed by system, **valid need-to-know** for **ALL** info processed by system.

## Multilevel Mode

Can process information at different levels even when all system users **do not have the required security clearance** to access all information processed by the system.

## System High Mode

Each user must have valid security clearance, access approval for **ALL** info processed by system, and valid **need-to-know for at least **SOME**** info on the system. Offers most granular control over resources and users of these models.

## Compartmented Mode

**Goes one step further than System High.** Each user must have valid security clearance, access approval for **ALL INFO** processed by system, but requires valid need-to-know for **ALL INFO** they will have access to on the system.

## DOMAIN 3: TRUSTED COMPUTING BASE

**TCB** is a **combination of hardware, software and controls** that work together to form a “trusted base” to enforce your security policy

Is a subset of the complete information system. Is the only portion that can be trusted to adhere to and enforce your security policy

**Security perimeter** is an **imaginary boundary** that separates TCB from the rest of the system

TCB must create secure channels (aka “**trusted paths**”) to communicate with the rest of the system

Protects users (aka subjects) from compromise as a result of TCB interchange

# REFERENCE MONITOR & SECURITY KERNEL

**Reference monitor** *enforces access control*

is the logical part of the TCB that confirms whether a subject has the **right to use a resource** prior to granting access.

**Security kernel** *implements access control*

is the collection of the TCB components that implement the functionality of the reference monitor.

## Common Criteria (ISO-IEC 15408)

The Common Criteria enable an **objective evaluation** to validate that a particular product or system satisfies a defined set of security requirements.

## TCSEC (Trusted Computer System Evaluation Criteria)

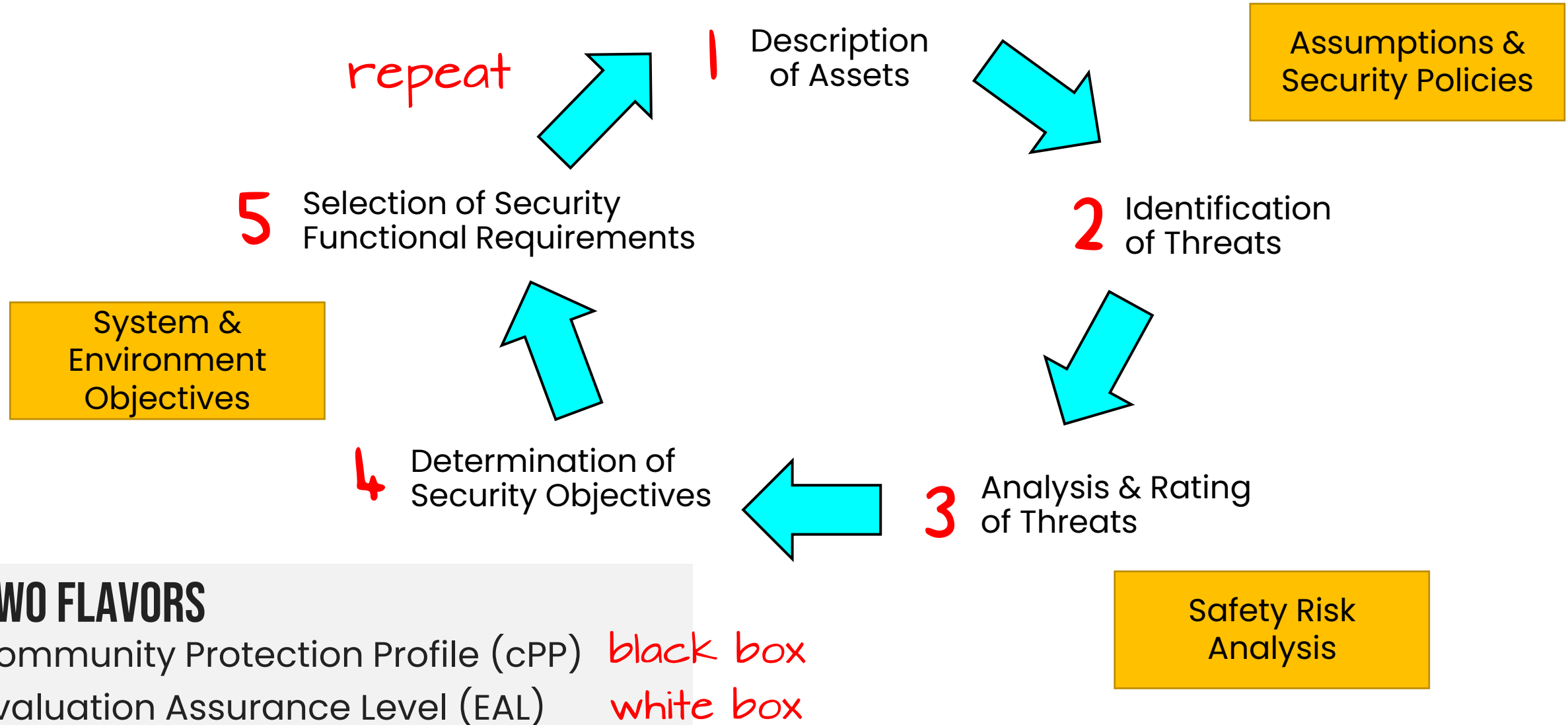
A structured set of criteria for evaluating computer security within products and systems.

## ITSEC (Information Technology Security Evaluation Criteria)

The ITSEC represents an initial attempt to create security evaluation criteria in Europe. TSEC uses two scales to rate functionality and assurance.

*CC Has replaced or superseded both ITCSEC and ITSEC.*

# DOMAIN 3: COMMON CRITERIA (ISO-IEC 15408)



# DOMAIN 3: TSCSEC, ITSEC, and COMMON CRITERIA

## Comparison of security evaluation standards

TCSEC	ITSEC	CC description	
D	F-D+E0	EAL0, EAL1	Minimal/no protection
C1	F-C1+E1	EAL2	Discretionary security mechanisms
C2	F-C2+E2	EAL3	Controlled access protection
B1	F-B1+E3	EAL4	Labeled security protection
B2	F-B2+E4	EAL5	Structured security protection
B3	F-B3+E5	EAL6	Security domains
A1	F-B3+E6	EAL7	Verified security design



## DOMAIN 3: COVERT CHANNELS

### Covert Channels

A method that is used to pass information over a path that is **not normally used** for communication.

Because it's not normally used, it may not be protected by the system's normal security controls.

**Two types:** **covert timing** channel and **covert storage** channel

hard to detect because it's outside normal comm channels

## Trusted Platform Module

A **chip** that resides on the motherboard of the device.

Multi-purpose, like 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

# DOMAIN 3: TYPES OF ACCESS CONTROL

## **Mandatory Access Control**

Enforces an access policy that is **determined by the system**, not the object owner. Relies on **classification labels** that are representative of security domains and realms.

## **Discretionary Access Control**

Permits the **owner or creator** of an object to control and define its accessibility, because the owner has full control by default.

## **Non-discretionary Access Control**

Enables the enforcement of system-wide restrictions that override **object-specific** access control.

## **Rule-based Access Control**

Defines specific functions for access to requested objects. Commonly found in firewall systems.

# ROLE-BASED ACCESS CONTROL


---

Uses a well-defined collection of **named job roles** to endow each one with specific permissions, thereby seeking to ensure that users who occupy such roles can access what they need to get their jobs done.

# DOMAIN 3: MAC MODEL CLASSIFICATIONS

## Hierarchical environment

Various classification labels are assigned in an **ordered structure** from low security to medium security to high security.



## Compartmentalized environment

Requires specific **security clearances** over compartments or domains instead of objects.

## Hybrid environment

Contains levels with compartments that are isolated from the rest of the security domain. Combines both **hierarchical and compartmentalized** environments so that security levels have subcompartments.



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.

# SECURITY MODELS, DESIGN, AND CAPABILITIES

## Certification

The **technical evaluation** of each part of a computer system to assess its concordance with security standards

*agreement, alignment*

## Accreditation

The **process of formal acceptance** of a certified configuration from a designated authority.

# SECURITY MODELS, DESIGN, AND CAPABILITIES

## Open system

are designed using industry standards and are usually **easy to integrate** with other open systems

## Closed system

are generally proprietary hardware and/or software. Their specifications are not **normally published**, and they are usually **harder to integrate** with other systems.



# ENSURE CONFIDENTIALITY, INTEGRITY, AVAILABILITY

## Techniques for ensuring CIA...

**Confinement** restricts a process to reading from and writing to certain memory locations.

**Bounds** are the limits of memory a process cannot exceed when reading or writing.

**Isolation** is the mode a process runs in when it is confined through the use of memory bounds.

# FACTORS OF AUTHENTICATION



MFA

Something you **know** (pin or password)

# FACTORS OF AUTHENTICATION



MFA

Something you **know** (pin or password)

Something you **have** (trusted device)

# FACTORS OF AUTHENTICATION



MFA

Something you **know** (pin or password)

Something you **have** (trusted device)

Something you **are** (biometric)

# AUTHENTICATION & AUTHORIZATION



AuthN and  
AuthZ

**Authentication (AuthN)** is the process of proving that you are who you say you are.

# AUTHENTICATION & AUTHORIZATION



AuthN and  
AuthZ

*Identity*

**Authentication (AuthN)** is the process of proving that you are who you say you are.

**Authorization (AuthZ)** is the act of granting an authenticated party permission to do something.

*Access*

# AUTHENTICATION & AUTHORIZATION



AuthN and  
AuthZ

**Permissions, rights, and privileges** are then granted to users based on their proven identity.

If user has rights to a resource, they are granted **authorization**.

# AUTHENTICATION & AUTHORIZATION



AuthN and  
AuthZ

**Permissions, rights, and privileges** are then granted to users based on their proven identity.

If user has rights to a resource, they are granted **authorization**.

Authentication can be achieved with both **symmetric** and **asymmetric** cryptosystems.



# MULTITASKING AND MULTITHREADING

## Multitasking

simultaneous execution of more than one application on a computer and is managed by the operating system.

## Multithreading

Permits multiple concurrent tasks to be performed within a single process.

# MULTIPROCESSING AND MULTIPROGRAMMING

## Multiprocessing

The use of more than one processor to increase computing power.

## Multiprogramming

Similar to multitasking but takes place on mainframe systems and requires specific programming.

# SINGLE-STATE AND MULTISTATE PROCESSORS

“

**Single-state** processors are capable of operating at only one security level at a time, whereas **multistate** can simultaneously operate at **multiple security levels**.

# PROCESSOR OPERATING MODES

## User

Applications operate in a limited instruction set environment known as user mode

## Privileged

Controlled operations are performed in privileged mode, also known as **system** mode, **kernel** mode, and **supervisory** mode.

# Memory Types

### **Read-only Memory (ROM).**

Read-only. Contents **burned in at factory**.

### **RAM.**

Static RAM (SRAM) uses flip-flops, dynamic RAM (DRAM) uses capacitors

### **PROM.**

Programmable chip similar to ROM, with several sub-types (described here).

### **EPROM.**

**Erasing, Clearing** (overwriting w/ unclassified data).

# Memory Types

There are two main subcategories of EPROM, which are UVEEPROM and EEPROM

### **Ultraviolet EPROM (UVEEPROM)**

chips have a small window that, when illuminated with a special ultraviolet light, erases contents.

### **Electronically Erasable PROM (EEPROM)**

uses electric voltages delivered to the pins of the chip to force erasure. (*a more flexible alternative to UVEEPROM*)

**Flash Memory.** Derivative concept from EEPROM.

nonvolatile, can be electronically erased and rewritten.

# SECURITY ISSUES WITH STORAGE

**Primary storage** is the same as memory.

**Secondary storage** consists of magnetic, flash, and optical media that must be first read into primary memory before the CPU can use the data.

**Random access storage** devices can be read at any point

**Sequential access storage** devices require scanning through all the data physically stored before the desired location.

# SECURITY ISSUES WITH STORAGE

**Three main security issues** surrounding secondary storage devices:

1. **Removable media** can be used to steal data
2. Access controls and encryption must be applied to protect data
3. Data can remain on the media even after file deletion or media formatting.



# SECURITY RISKS OF INPUT & OUTPUT DEVICES

“

Subject to **eavesdropping and tapping**, used to smuggle data out of an organization, or used to create unauthorized, insecure points of entry into an organization's systems and networks.

# THE PURPOSE OF FIRMWARE

## THE PURPOSE OF FIRMWARE

---

Software stored on a ROM chip, containing basic **instructions** needed to start a computer. Also used to provide operating instructions in peripheral devices such as printers

# VULNERABILITIES, THREATS, & COUNTERMEASURES

## Process isolation

ensures that individual processes can access only their own data.

## Layering

creates different realms of security within a process and limits communication between them.

## Abstraction

creates "black-box" interfaces for programmers to use without requiring knowledge of an algorithms or device's inner workings.

## Data hiding

prevents information from being read from a different security level. Hardware segmentation enforces process isolation with physical controls.

# THE ROLE OF SECURITY POLICY

## THE ROLE OF SECURITY POLICY

---

The role is to **inform and guide** the **design, development, implementation, testing, and maintenance** of some particular system.

# VULNERABILITIES, THREATS, & COUNTERMEASURES

## **Cloud computing**

the concept of computing where processing and storage are performed elsewhere over a network connection rather than locally. (Azure, Amazon, GCP)

Sensitive & confidential data can be at risk IF the cloud provider and their personnel might not adhere to the same security standards as your organization.

# HYPERVISORS

## Hypervisor

The hypervisor, also known as a virtual machine monitor (VMM), is the component of virtualization that **creates, manages, and operates** the virtual machines (VMs).

### Type I hypervisor

A native or bare-metal hypervisor. In this configuration, there is no host OS; instead, the **hypervisor installs directly** onto the hardware where the host OS would normally reside.

### Type II hypervisor

A **hosted hypervisor**. In this configuration, a standard regular OS is present on the hardware, and the hypervisor is then installed as another software application.

# CLOUD ACCESS SECURITY BROKER

## WHAT IS A CASB?

---

A **cloud access security broker (CASB)** is a **security policy enforcement** solution that may be installed on-premises or in the cloud.

shadow IT

# Security-aas

---

A cloud provider concept in which security is provided to an organization through or by an online entity.



# SMART DEVICES

## Smart devices

---

Mobile devices that offer customization options, typically through installing apps, and may use on-device or in-the-cloud artificial intelligence (AI) processing.

# INTERNET OF THINGS

## Internet of Things

---

A class of devices connected to the internet in order to provide automation, remote control, or AI processing in a home or business setting

# MOBILE DEVICE AND MOBILE APP SECURITY

## Mobile device security

the range of potential security options or features that may be available for a mobile device. security features include full device encryption, remote wiping, lockout, screen locks, GPS, application control, etc.

## Understand mobile application security

the applications and functions used on a mobile device need to be secured. Related concepts include key management, credential management, authentication, geotagging, encryption, application whitelisting, and transitive trust/authentication.

## Bring your own device (BYOD)

is a **policy** that allows employees to use their own personal mobile devices to work to access business information and resources. May improve employee morale and job satisfaction, but it increases security risks to the organization.

# EMBEDDED SYSTEMS & STATIC ENVIRONMENTS

## Embedded system

is typically designed around a limited set of **specific functions** in relation to the larger product of which it's a component.

## Static environments

are applications, OSs, hardware sets, or networks that are configured for a **specific** need, capability, or **function**, and then set to remain unaltered.

**Both need security management.** These techniques may include network segmentation, security layers, application firewalls, manual updates, firmware version control, wrappers, and control redundancy and diversity.

# PRIVILEGE & ACCOUNTABILITY

## **Principle of least privilege**

ensures that only a minimum number of processes are authorized to run in supervisory mode.

## **Separation of privilege**

increases the granularity of secure operations.

**Accountability** ensures that an audit trail exists to trace operations back to their source.

# COMMON FLAWS & VULNERABILITIES

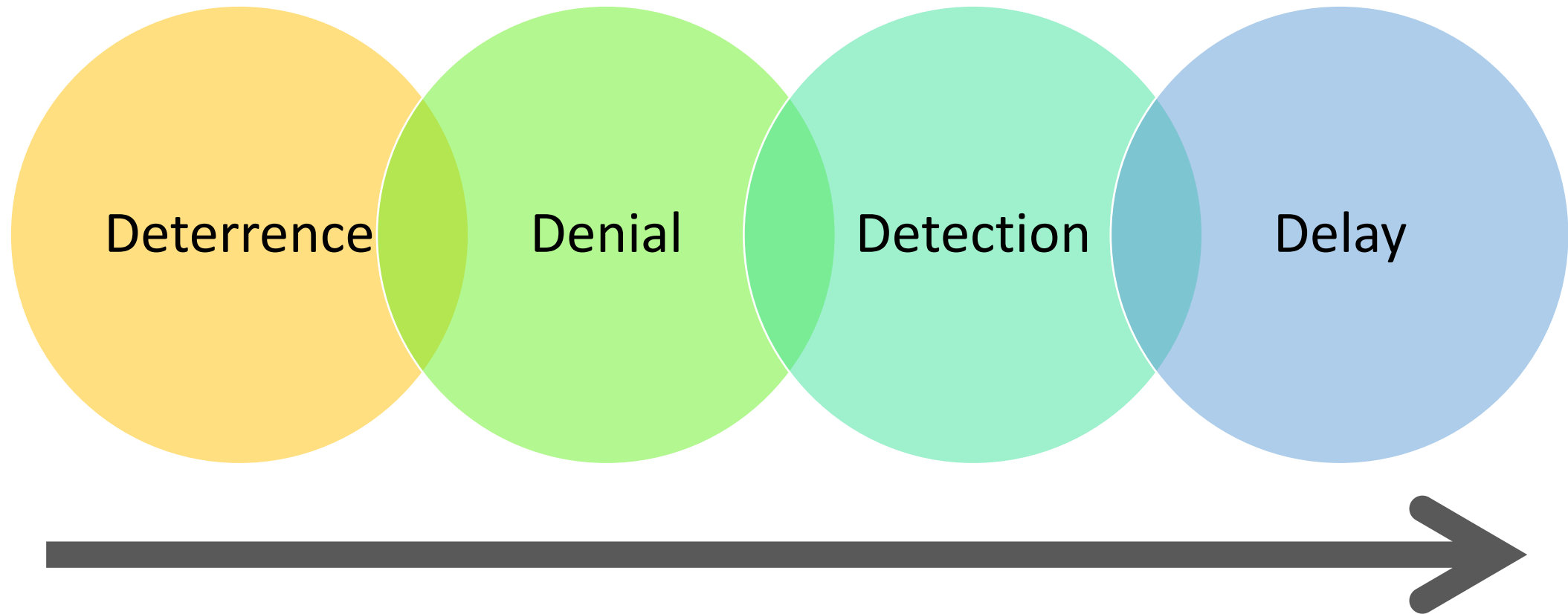
## Buffer overflow

occurs when the programmer fails to **check the size of input data** prior to writing the data into a specific memory location.

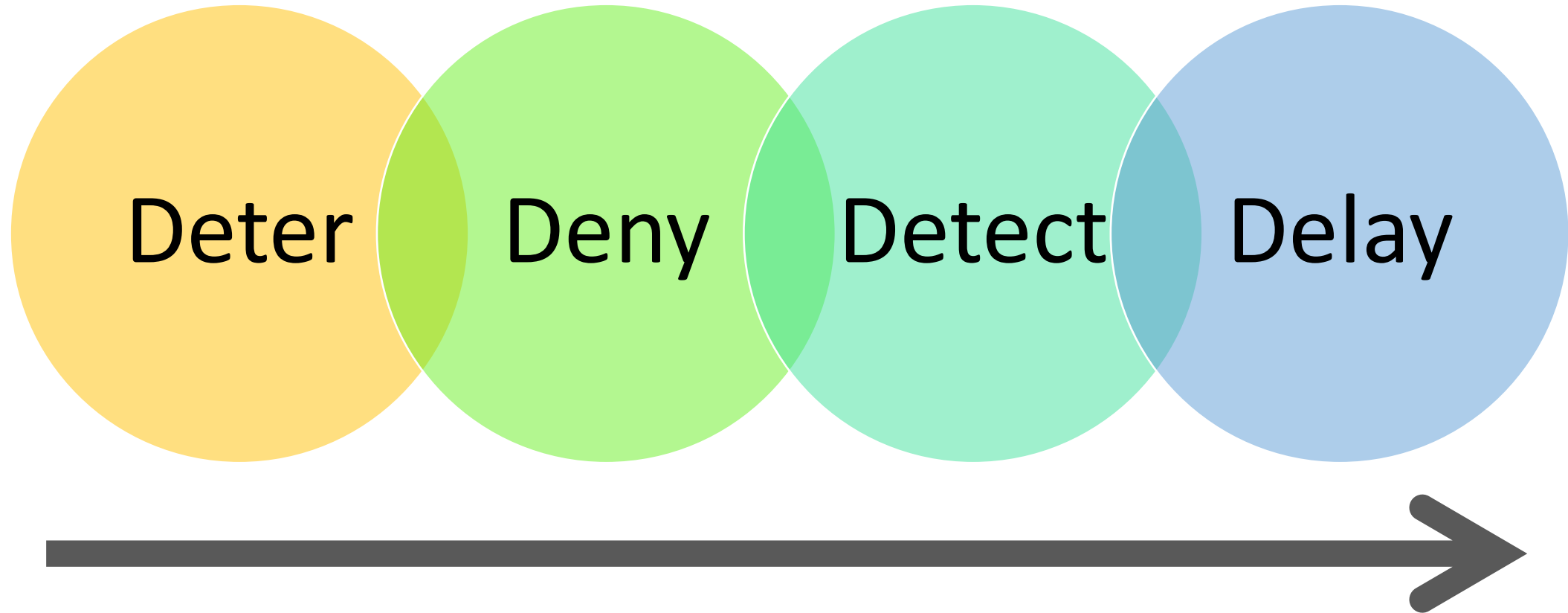
In addition to buffer overflows, programmers can leave **back doors** and **privileged programs** on a system after it is deployed.

Even well-written systems can be susceptible to **time-of-check-to-time-of-use (TOCTTOU)** attacks. Any state change presents an opportunity for an attacker to compromise a system.

# FUNCTIONAL ORDER OF SECURITY CONTROLS

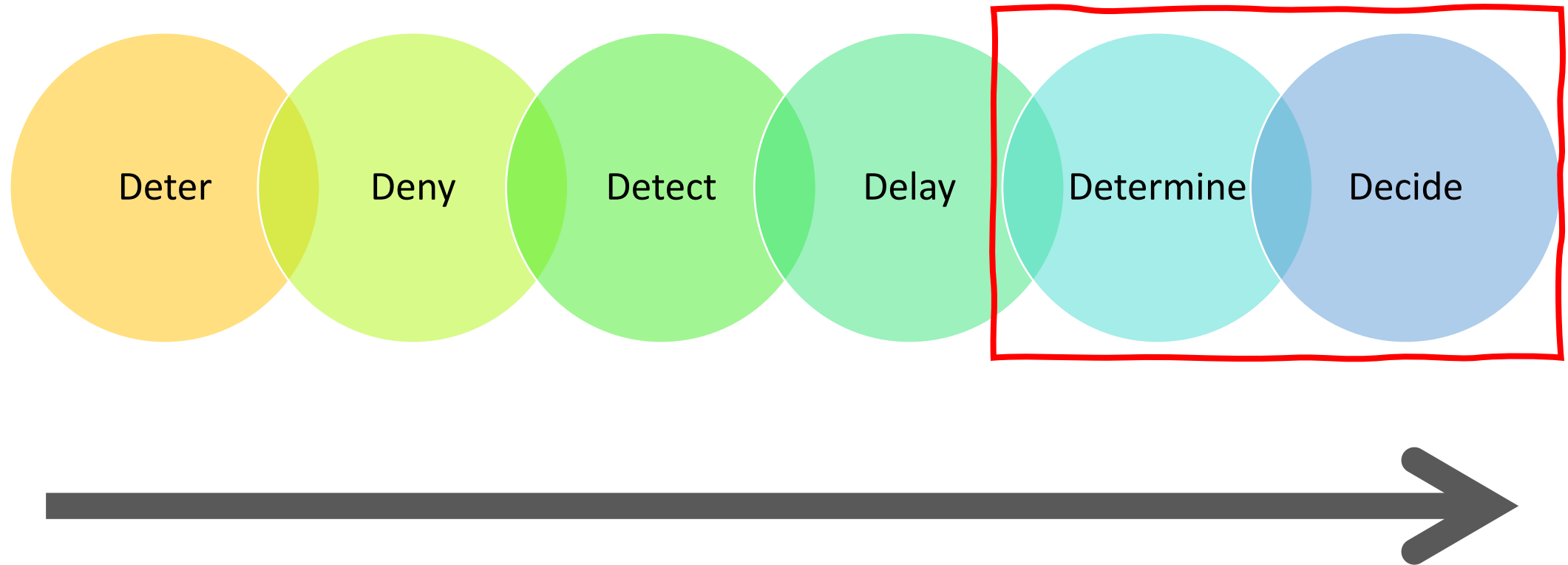


# FUNCTIONAL ORDER OF SECURITY CONTROLS





# FUNCTIONAL ORDER OF SECURITY CONTROLS



# PHYSICAL SECURITY CONTROLS

Physical security controls can be divided into three groups:

## **Administrative**

also known as management controls and include policies and procedures, like **site management, personnel controls, awareness training**, and **emergency response and procedures**.

## **Logical**

also known as technical controls and are implemented through technology like **access controls, intrusion detection, alarms, CCTV, monitoring, HVAC, power supplies**, and **fire detection and suppression**.

## **Physical**

use physical means to protect objects and includes **fencing, lighting, locks, construction materials, access control vestibules (mantraps), dogs**, and **guards**.

# PHYSICAL SECURITY REQUIREMENTS

## Know the **logical controls** for physical security

Technical controls for physical security include:

- access controls
- intrusion detection
- alarms
- CCTV and monitoring
- HVAC
- power supplies
- fire detection and suppression

# PHYSICAL SECURITY REQUIREMENTS

## **Know administrative controls for physical security**

Administrative controls for physical security include:

- facility construction
- facility selection
- site management
- personnel controls
- awareness training
- emergency response
- emergency procedure

# PHYSICAL SECURITY REQUIREMENTS

## Know the **physical controls** for physical security

Physical controls for physical security include:

- fencing
- lighting
- locks
- construction materials
- mantraps
- dogs
- guards

# PHYSICAL SECURITY REQUIREMENTS

**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.

# PHYSICAL SECURITY CONTROLS

## FENCE

**3-4 feet** – deters casual trespasser

**6-7 feet** – too hard to climb easily

**8 feet (w/ barbed wire)** – will deter intruders

## TEMP

**Humidity:** 40% – 60% ideal

**Temps:** for computers **60-75F** (15-23C), damage at 175F. Manage storage devices damaged at **100F**

## ELECTRICAL IMPACTS

**Blackout:** prolonged loss of power

**Brownout:** prolonged low voltage

**Fault:** short loss of power

**Surge:** prolonged high voltage

**Spike:** temporary high voltage

**Sag:** temporary low voltage

## LIGHTS

8 feet high with 2 feet candle power

# HUMIDITY AND STATIC ELECTRICITY

“

**Too much** humidity can cause corrosion. **Too little** humidity causes static electricity. Even on nonstatic carpet, low humidity can generate 20,000-volt static discharge!



# FIRE AND SUPPRESSION AGENTS

**Class A (ASH)** fires are **common combustibles** such as **wood, paper**, etc. This type of fire is the most common and should be extinguished with **water or soda acid**.

**Class B (BOIL)** – fires are **burning alcohol, oil**, and **other petroleum products** such as gasoline. They are extinguished with **gas or soda acid**. You should never use water to extinguish a class B fire.

**Class C (CONDUCTIVE)** – fires are **electrical fires** which are fed by electricity and may occur in equipment or wiring. Electrical fires are conductive fires, and the extinguishing agent must be non-conductive, such as **any type of gas**.

**Class D (DILYTHIUM)** – fires are **burning metals** and are extinguished with dry powder.

**Class K (KITCHEN)** – fires are **kitchen fires, such as burning oil or grease**. Wet chemicals are used to extinguish class K fires.

The three **categories of fire detection** systems include **smoke sensing**, **flame sensing**, and **heat sensing**.

# FIRE EXTINGUISHER CLASSES

Fire extinguishers and suppression agents

Class	Type	Suppression material
A	Common combustibles	Water, soda acid (a dry powder or liquid chemical)
B	Liquids	CO2, halon, soda acid
C	Electrical	CO2, halon
D	Metal	Dry powder
K	Kitchen	Wet chemicals

# VOLTAGE AND NOISE

## Electromagnetic interference

- **Common mode noise.** Generated by the difference in power between the **hot and ground** wires of a power source operating electrical equipment
- **Traverse mode noise.** Generated by a difference in power in the **hot and neutral** wires of a power source operating electrical equipment

## Radio frequency interference (RFI)

is the source of interference that is generated by electrical appliances, light sources, electrical cables and circuits, and so on.

Static Voltage	Possible Damage
40	Destruction of sensitive circuits and other components
1,000	Scrambling of monitor displays
1,500	Destruction of hard drive data
2,000	Abrupt system shutdown
4,000	Printer jam or component damage
17,000	Permanent circuit damage

# DAMAGE FROM FIRE AND FIRE SUPPRESSION

The destructive elements of a fire include smoke and heat but also the suppression medium, such as water or soda acid.

**Smoke** is damaging to most **storage devices**.

**Heat** can damage any **electronic or computer** component.

**Suppression mediums** can cause short circuits, initiate corrosion, or otherwise render equipment useless.



All of these issues must be addressed when designing a fire response system. *#1 concern is ALWAYS human safety!*

# WATER SUPPRESSION SYSTEMS

← good for areas with people + computers

**Preaction systems** use closed sprinkler heads, and the pipe is charged with compressed air instead of water. The water is held in check by an electrically-operated sprinkler valve and the compressed air.

**Wet pipe systems** are filled with water. Dry pipe systems contain compressed air until fire suppression systems are triggered, and then the pipe is filled with water; and flame activated sprinklers trigger when a predefined temperature is reached.

**Dry pipe systems** also have closed sprinkler heads: the difference is the pipes are filled with compressed air. The water is held back by a valve that remains closed as long as sufficient air pressure remains in the pipes. Often used in areas where water may freeze, such as parking garages.

**Deluge systems** are similar to dry pipes, except the sprinkler heads are open and larger than dry pipe heads. The pipes are empty at normal air pressure; the water is held back by a deluge valve.

water and electricity do not mix!

# GAS DISCHARGE SYSTEMS

Usually **more effective than water discharge systems**, but should not be used in environments where people are located, because they work by **removing oxygen from the air.**

**Halon** is effective, but bad for environment (ozone-depleting), **turns to toxic gas at 900F.** Suitable replacements include:

- FM-200 (HFC-227ea)
- CEA-410 or CEA-308
- NAF-S-III (HCFC Blend A)
- FE-13 (HCFC-23)
- Argon (IG55) or Argonite (IG01)
- Inergen (IG541)
- Aero-K

# LOCK TYPES

## **Electronic Combination Locks**

(aka Cipher lock) Something you know

## **Key Card Systems**

Something you have

## **Biometric Systems**

Something you are

## **Conventional Locks**

Easily picked / bumped & keys easily duplicated

## **Pick-and-Bump Resistant Locks**

Expensive, harder to pick & keys not easily duplicated.

# FACILITY DESIGN SPECIFICATIONS

## For the exam...



**mantrap**

Remember what **locks** can be picked and which need to be bumped

Remember how high **lights** and **fences** need to be

Know the different **physical controls** related to **entry**



# FACILITY DESIGN SPECIFICATIONS

For the exam...



**bollard**

Remember what **locks** can be picked and which need to be bumped

Remember how high **lights** and **fences** need to be

Know the different **physical controls** related to **entry**

# SITE SELECTION & FACILITY DESIGN

Know key elements in **site selection** and **facility design**.

## **For site selection**

Visibility, composition of the surrounding area, area accessibility, and the effects of natural disasters.

## **For facility design**

Understanding the level of security needed by your organization and planning for it before construction begins.

# SECURE WORK AREA DESIGN AND CONFIGURATION

Know how to design and configure **secure work areas**.

There should not be **equal access** to all locations within a facility. Areas with high-value assets require restricted access.

**Valuable and confidential assets** should be located in the heart or center of protection provided by a facility.

Centralized server or computer rooms need not be human compatible.

# THREATS TO PHYSICAL ACCESS CONTROLS

No matter which physical access control is used, a security guard or other monitoring system must be deployed to prevent:

**Abuses** of physical access control include propping open secured doors and bypassing locks or access controls.

**Masquerading** is using someone else's security ID to gain entry to a facility.

**Piggybacking** is following someone through a secured gate or doorway without being identified or authorized personally.

# SECURING A WIRING CLOSET

Know the security concerns of a **wiring closet**

This is where the networking cables for **a floor or even a whole building** are connected to essential equipment, such as patch panels, switches, routers, and backbone channels.

Most security focuses on **preventing physical unauthorized access**. If an unauthorized intruder gains access, they may steal equipment, pull/cut cables, or plant a listening device.

# PHYSICAL SECURITY REQUIREMENTS

Understand how to **handle visitors in a secure facility**.

If a facility employs **restricted areas** to control physical security, then a mechanism to handle visitors is required.

Often an **escort is assigned to visitors**, and their access and activities are monitored closely.

**Tracking actions** of outsiders when they are granted access to prevent malicious activity against the most protected assets.

# PHYSICAL SECURITY REQUIREMENTS

Understand the needs for **media storage**

Media storage facilities should be designed to securely store blank, reusable, and installation media.

**Concerns** include, theft, corruption, data remnant recovery

Media storage facility **protections** include

- locked cabinets or safes
- using a librarian/custodian
- implementing a check-in/check-out process
- using media sanitization

# EVIDENCE STORAGE

Understand the concerns for **evidence storage**

Used to retain logs, drive images, virtual machine snapshots, and other datasets for recovery, internal investigations, and forensic investigations.

**Protections** for evidence storage include:

- locked cabinets or safes
- dedicated/isolated storage facilities
- offline storage
- access restrictions and activity tracking
- hash management and encryption



# AUDIT TRAILS AND ACCESS LOGS

**Audit trails** and **access logs** are useful tools for managing for **physical access control**.

**Creation** May need to be created manually by security guards or may generated automatically with the right equipment (smartcards and certain proximity readers).

**Monitoring** You should also consider monitoring entry points with CCTV. Through CCTV, you can compare the audit trails and access logs with a visually recorded history of the events.



**Why are these important?** Such information is critical to reconstructing the events of an intrusion, breach, or attack.

# THE NEED FOR CLEAN POWER

Power supplied by electric companies is not always **consistent and clean**.

Most electronic equipment requires clean power in order to function properly and avoid damage.

A **UPS** is a type of self-charging battery that can be used to

- supply **consistent, clean power** to sensitive equipment.
- supply power for minutes or hours (depending on it's size) in the event of **power failure**