

Introduction

Informatics and Communications Security

Security

Subject focused on the predictability of systems, processes, environments...

▷ Across all aspects of the life cycle:

- ♦ Planning
- ♦ Development
- ♦ Execution
- ♦ Processes
- ♦ People
- ♦ Clients and supply chain
- ♦ Mechanisms
- ♦ Standards and laws
- ♦ Intellectual Property

Security: Planning

Design of a solution complying with some requirements under a normative context

▷ Without flaws

- ♦ All operation states are the ones predicted
- ♦ There are no additional states escaping the expected logic
 - Even if forced transitions are used

▷ Under the scope of a normative context

- ♦ Specific for each activity or sector
- ♦ Ex: ISO 27001, ISO 27007, ISO 37001

Security: Development

**Implement a solution complying with the design,
without other operation modes**

- ▷ Without bugs compromising the correct execution
 - ◆ No crashes
 - ◆ Without invalid or unexpected results
 - ◆ With the correct execution times
 - ◆ With adequate resource consumption
 - ◆ Without information leaks

- ▷ Software:
 - ◆ Requires careful implementation
 - ◆ Requires tests to obtain an implementation with the expected... and only the expected behavior

Security: Execution

Code executes as it was written, with all predicted processes

- ▷ Environment is controlled, cannot be manipulated or observed
- ▷ Without the existence of anomalous behavior, introduced by environmental aspects
 - ◆ Such as: storage speed, RAM amount, trusted communications

Security: people and partners

Staff behavior cannot have a negative impact to the solution

- ▷ Norms are in place to regulate what actions are expected
- ▷ Staff is trained to distinguish correct from incorrect behavior
- ▷ Staff has the correct incentives to behave adequately
- ▷ When staff is compromised, or deviate, actions have limited impact

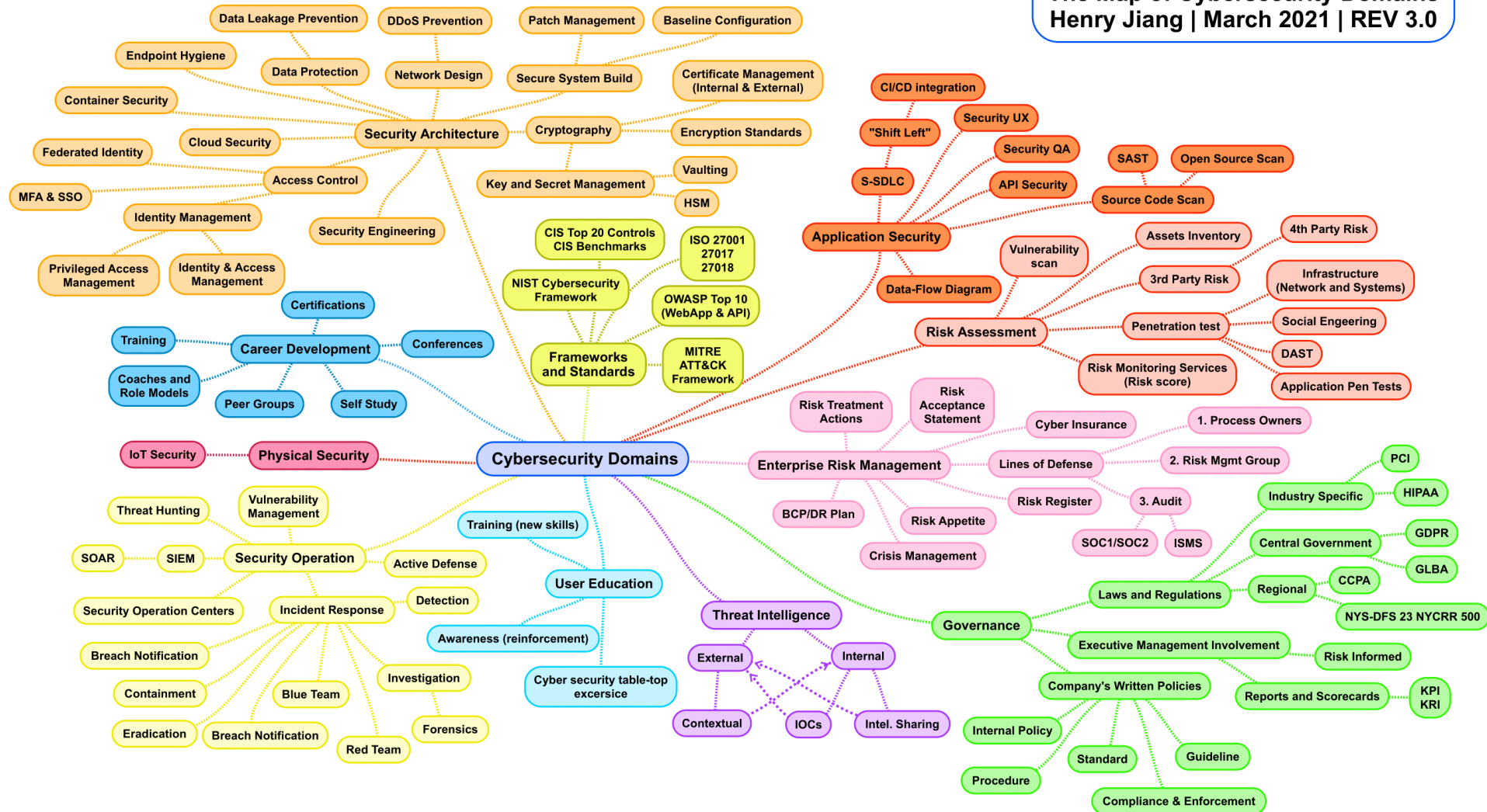
Security: Analysis and Auditing

What is the actual behavior of the solution?

- ▷ Identify deviations from the expected attributes
 - ♦ Faults, errors, behavior
- ▷ Identify the risk for the solution to be modified
 - ♦ Exposition to possible attackers
 - ♦ Incentives one may have to modify it
 - ♦ Identify potential actors (threats)
- ▷ Identify the impact of the deviations
 - ♦ Total loss of data? Denial of Service? Increase Operation Cost?

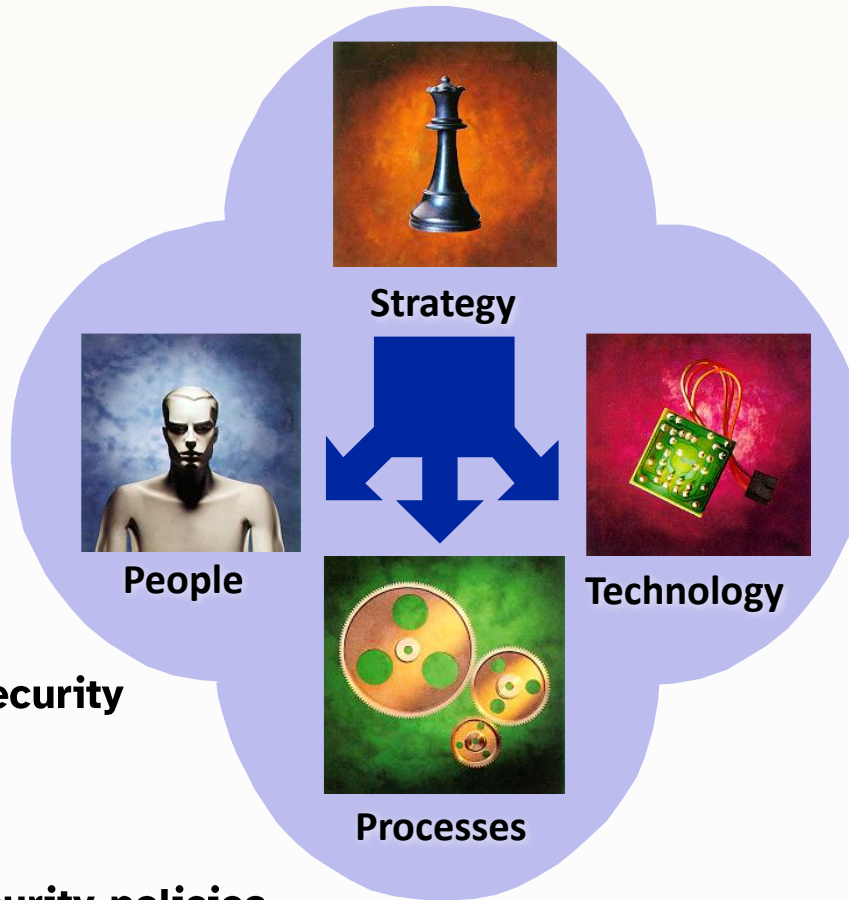
The Map of Cybersecurity Domains

Henry Jiang | March 2021 | REV 3.0



Dimensions to consider

- Selection
- Training
- Awareness
- Organization of security



- Vulnerability scanning
- Firewalls
- Authentication
- Access Control
- Cryptography
- Digital Signatures
- Public key certification
- etc...

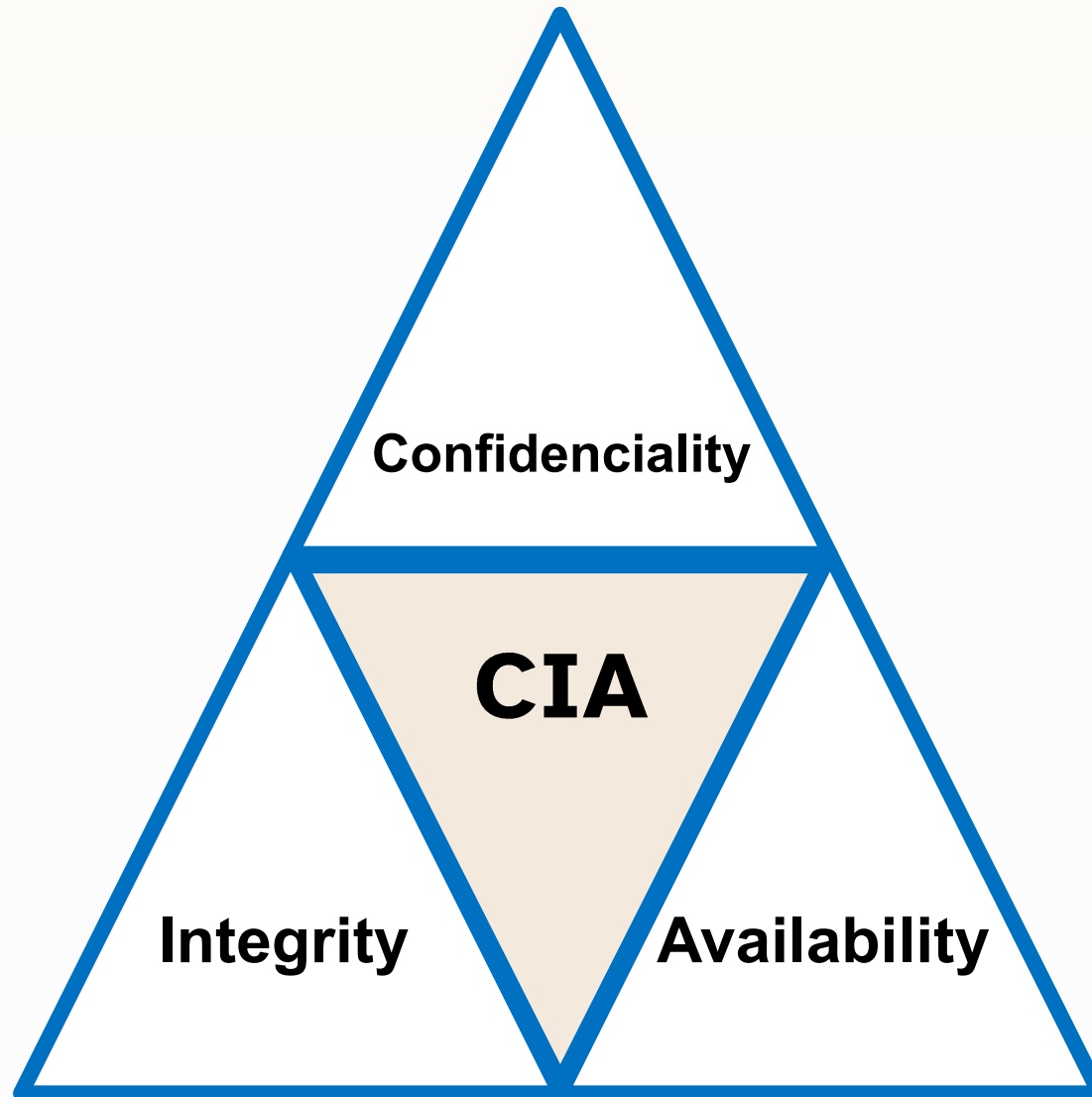
- Security policies
- Security administration processes
- Continued evolution of auditing and follow-up processes

Perspectives

Security has multiple intertwined perspectives

- ▷ Defensive: focus on maintaining predictability
- ▷ Offensive: focus on exploiting predictability
 - ♦ May have malicious/criminal intent
 - ♦ May have the purpose of validating the solution (Red Teams)
- ▷ Other:
 - ♦ Reverse Engineering: Recovery of design from built products
 - ♦ Forensics: extract information and reconstruct previous events
 - ♦ Disaster Recovery: minimize the impact of attacks
 - ♦ Auditing: validate the solution complies with some set of requirements

Information Security Objectives



Information Security Objectives

Confidentiality: Information may only be accessed by a restricted group of entities

▷ Measures:

- ◆ Encrypt information
- ◆ Use access passwords (strong)
- ◆ Use identity management and authentication systems
- ◆ Doors, strong walls
- ◆ Security personnel
- ◆ Training

Information Security

Integrity: Information remains unchanged

- ▷ Can be applied to devices and services
- ▷ Measures:
 - ◆ Integrity control (hashes)
 - ◆ Backups
 - ◆ Access controls
 - ◆ Robust storage devices
 - ◆ Data verification processes

Information Security

Availability: Information is available to target entities

- ▷ Can be applied to devices and devices
- ▷ Measures:
 - ◆ Backups
 - ◆ Disaster recovery plans
 - ◆ Redundancy
 - ◆ Virtualization
 - ◆ Monitoring

Information Security - Others

▷ Privacy: how personal information is handled

- ♦ Acquired
- ♦ Processed
- ♦ Stored
- ♦ Shared
- ♦ Deleted

▷ Measures:

- ♦ Access control
- ♦ Transparent processes
- ♦ Ciphers
- ♦ Integrity and authenticity controls
- ♦ Logs

Security objectives (1/3)

▷ Defense against catastrophic events

- ♦ Natural phenomena
- ♦ Abnormal temperature, lightning, thunder, flooding, radiation, ...

▷ Degradation of computer hardware

- ♦ Failure of power supplies
- ♦ Bad sectors in disks
- ♦ Bit errors in RAM cells or SSD, etc.

Security objectives (2/3)

▷ Defense against ordinary faults / failures

- ♦ Power outages
- ♦ Systems' internal failures
 - Linux Kernel panic, Windows blue screen, OS X panic
 - Deadlocks
 - Abnormal resource usage
- ♦ Software faults / communication faults...

Security objectives (3/3)

- ▷ Defense against non-authorized activities (adversaries)
 - ♦ Initiated by someone “from outside” or “from inside”

- ▷ Types of non-authorized activities:
 - ♦ Information access
 - ♦ Information alteration
 - ♦ Resource usage
 - CPU, memory, print, network, etc.
 - ♦ Denial of Service (DoS)
 - ♦ Vandalism
 - Interference with the normal system behavior without any benefit for the attacker

Core Concepts

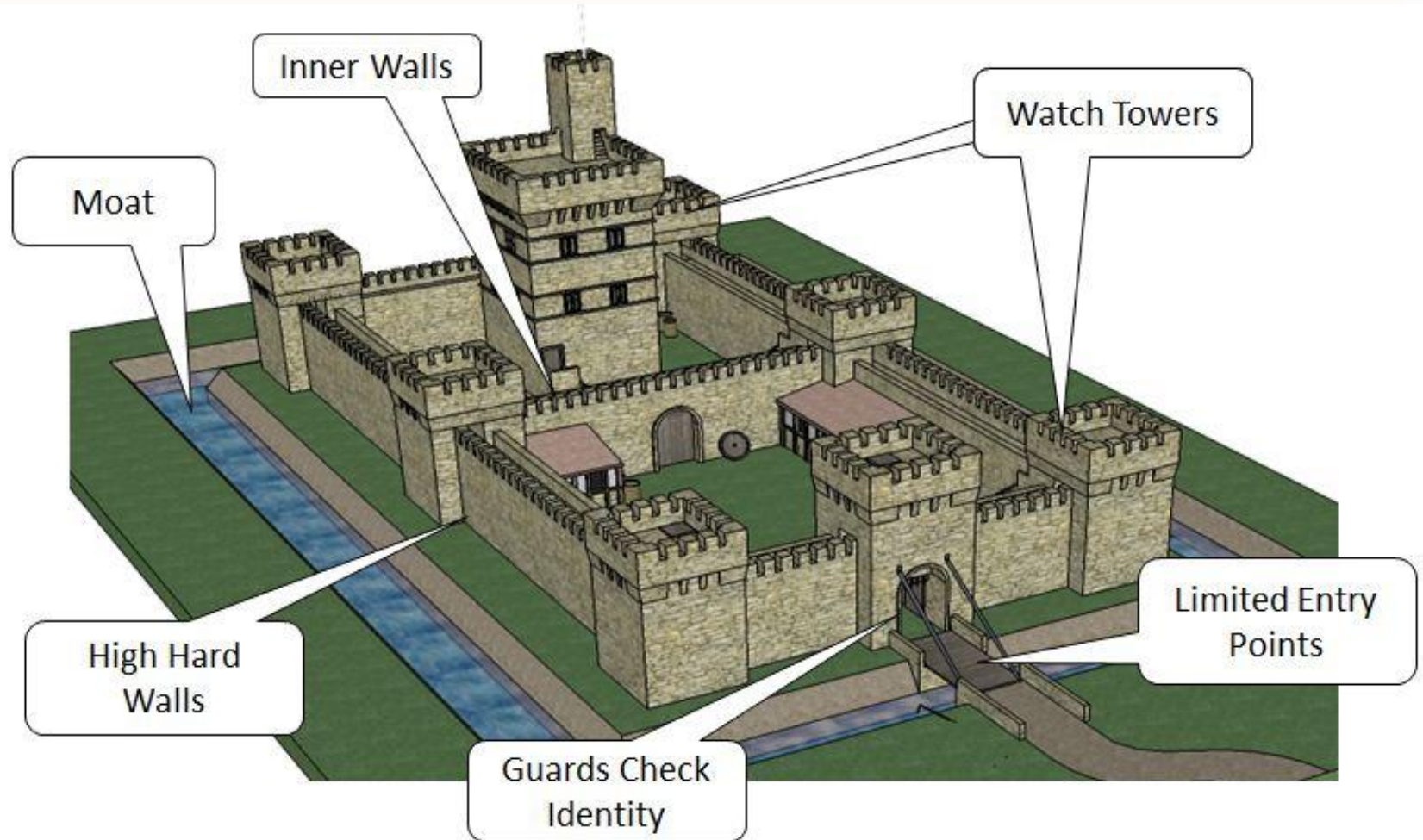
- ▷ Domains
- ▷ Policies
- ▷ Mechanisms
- ▷ Controls

Security Domains

A set of entities sharing similar security attributes

- ▷ Allow managing security in an aggregated manner
 - ♦ Management will set the attributes of the domain
 - ♦ Entities are added to the domain and will get the “group” attributes
- ▷ Behavior and interactions are homogenous inside the domain
- ▷ Domains can be organized in a flat or hierarchical manner
- ▷ Interactions between domains are usually controlled

Security Domains



Security Policies (1/3)

Set of guidelines related to security, that rule over a domain

- ▷ Organization will contain multiple policies
 - ◆ Applicable to each specific domain
 - ◆ They may overlap and have different scopes/abstraction levels
- ▷ The multiple policies must be coherent
- ▷ Examples
 - ◆ Users can only access web services
 - ◆ Subjects must be authenticated in order to enter the domain
 - ◆ Walls must be made of concrete
 - ◆ Communications must be encrypted

Security Policies (2/3)

- ▷ Define the power of each subject
 - ♦ Least privilege principle: each subject should only have the privileges required for the fulfillment of their duties
- ▷ Define security procedures
 - ♦ Who does what in which circumstances
- ▷ Define the minimum security requirements of a domain
 - ♦ Security levels, security Groups
 - ♦ Required authorization
 - And the related minimum authentication requirements (strong/weak, single/multifactor, remote/face-to-face)

Security Policies (3/3)

- ▷ Define defense strategies and fight back tactics
 - ◆ Defensive architecture
 - ◆ Monitoring of critical activities or attack signs
 - ◆ Reaction against attacks or other abnormal scenarios

- ▷ Define what are legal and illegal activities
 - ◆ **Forbid list model:** Some activities are denied, the rest are allowed
 - ◆ **Permit list model:** Some activities are allowed, the rest is forbidden

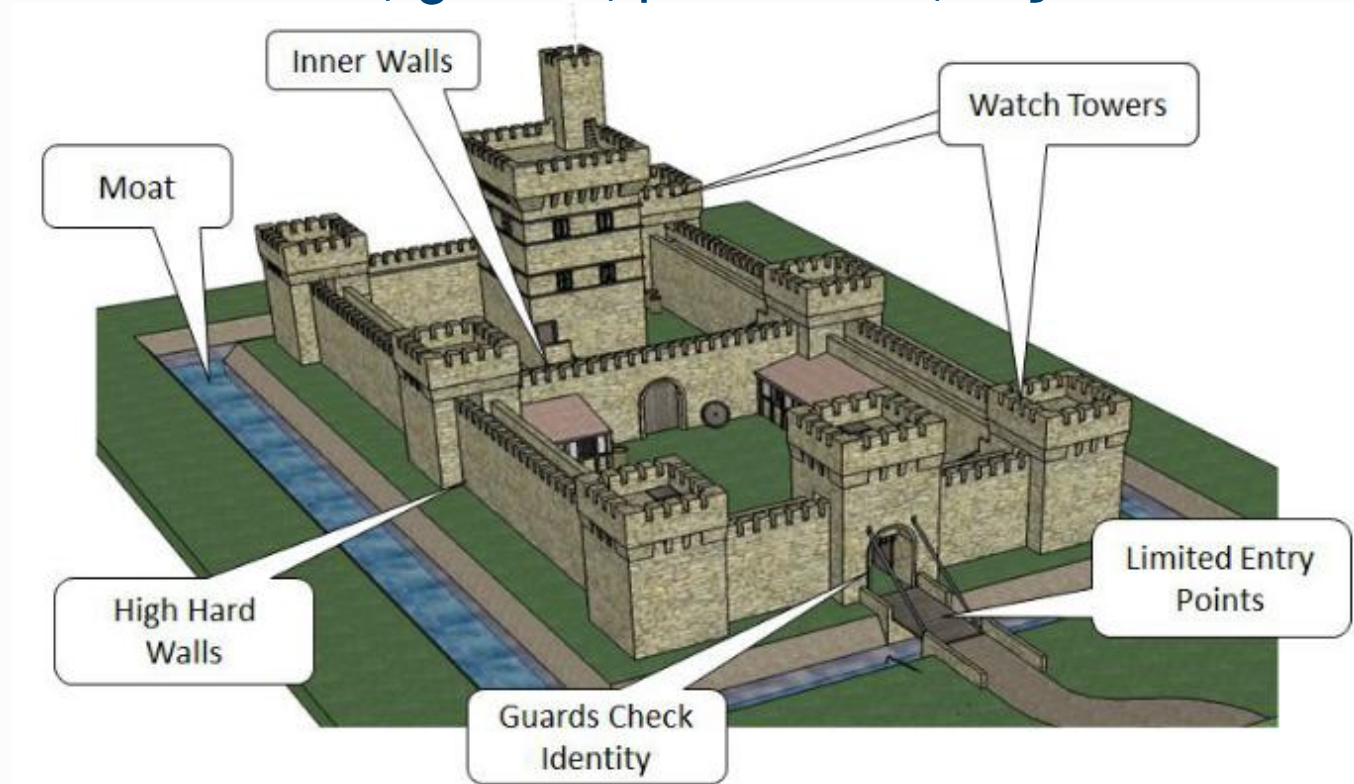
Security mechanisms

- ▷ Mechanisms implement policies
 - ◆ Policies define, at a higher level, what needs to be done or exist
 - ◆ Mechanisms are used to deploy policies
- ▷ Generic security mechanisms
 - ◆ Confinement (sandboxing)
 - ◆ Authentication
 - ◆ Access control
 - ◆ Privileged Execution
 - ◆ Filtering
 - ◆ Logging
 - ◆ Auditing
 - ◆ Cryptographic algorithms
 - ◆ Cryptographic protocols

Security mechanisms

Policy: Movement between domains is restricted

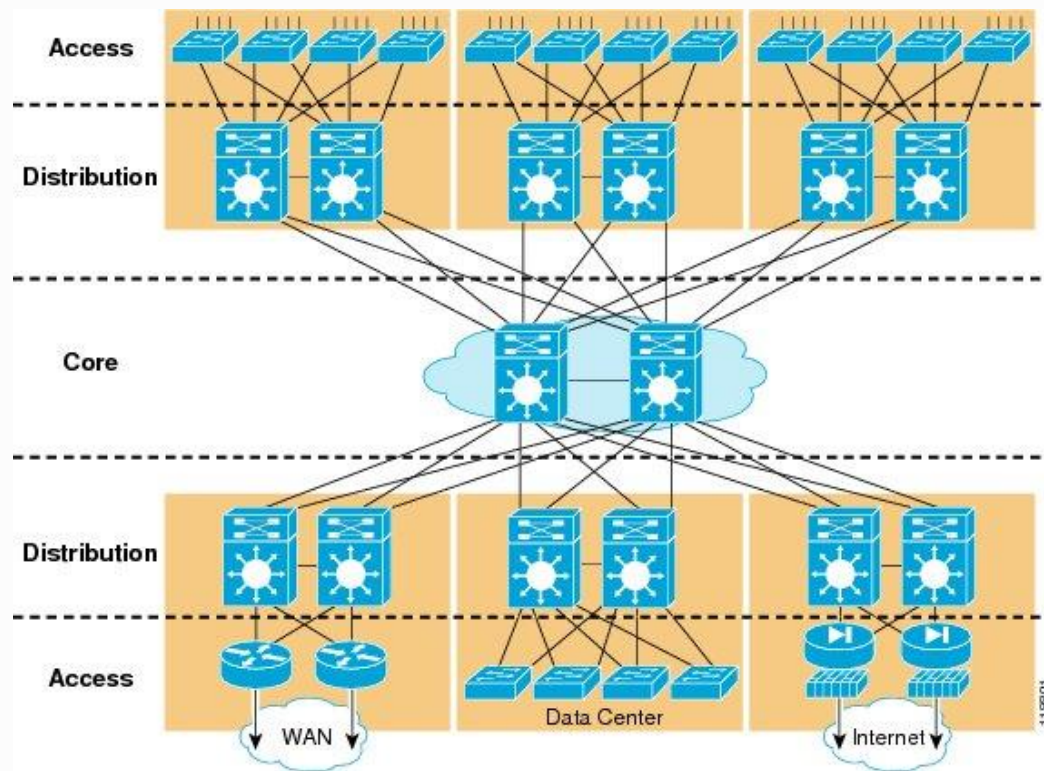
Mechanisms: Doors, guards, passwords, objects/documents



Security mechanisms

Policy: systems must be resilient

Mechanisms: equipments and links are doubled, architecture



Source: CISCO

Security Controls

**Controls are any aspect allowing to minimize risk
(protect the CIA properties)**

- ▷ Controls include policies & mechanisms, but also:
 - ♦ Standards and laws
 - ♦ Processes
 - ♦ Techniques

- ▷ Controls are explicitly stated and can be auditable
 - ♦ E.g.: ISO 27001 defines 114 controls in 14 groups
 - ... asset management, physical security, incidente management...

Types of Security Controls

	Prevention	Detection	Correction
Physical	Fences Gates Locks	CCTV	Repair Locks Repair Windows Redeploy access cards
Technical	Firewall Authentication Antivirus Encryption	Intrusion Detection Systems Alarms Honeypots	Vulnerability patching Reboot Systems Redeploy VMs Remove Virus
Administrative	Contractual clauses Separation of duties Information classification	Review access matrixes Audits	Implement a business continuity plan Implement an incident response plan

Practical Security (1/2)

Realistic Prevention

- ▷ Consider that perfect security is impossible!
- ▷ Focus on the most probable events
 - ♦ May depend on physical location, legal framework, ...
- ▷ Consider cost and profit
 - ♦ A great number of controls has a low cost
 - ♦ However, there is no upper limit on the cost of a security strategy
- ▷ Consider all domains and entities
 - ♦ A single breach can be escalated to a more serious situation

Practical Security (2/2)

▷ Consider Impact

- ◆ Under the light of CIA and other potential impact areas (e.g., brand)

▷ Consider the cost and recover time

- ◆ Monetary cost, reputation, market access

▷ Characterize attackers

- ◆ Define controls specific for those attackers
- ◆ There will always exist more resourceful attackers

▷ Consider that the system will be compromised

- ◆ Have recovery plans

Perimeter Defense

- ▷ Protection against external attackers
 - ♦ Internet
 - ♦ Foreign users
 - ♦ Other organizations
- ▷ Assumes that internal users are trusted and share the same policies
 - ♦ Friends, family, collaborators
- ▷ Used in domestic scenarios or small offices
- ▷ Limitations
 - ♦ Too simple
 - ♦ Doesn't protect against internal attackers
 - Previously trusted users
 - Attackers that acquired internal access

Defense in Depth

- ▷ Protection against internal and external attackers
 - ♦ From the Internet
 - ♦ Users
 - ♦ Other organizations
- ▷ Assumes well-defined domains across the organization
 - ♦ Walls, doors, authentication, security personell, ciphers, secure networks
- ▷ Limitations
 - ♦ Needs coordination between the diferent controls
 - May end with overlapping controls, but also with holes in the security perimeters
 - ♦ Cost
 - ♦ Requires training, changes to processes and frequent audits

Zero Trust, Zero Trust Architectures

- ▷ Defense model without specific perimeters
 - ◆ There is no inherent trust in entities just because they are internal
 - Actually, there may be no notion of internal and external
- ▷ Model recommended for new systems
 - ◆ Traditional systems should migrate to it
 - ◆ Implies the design of systems/services specific for this model
 - ◆ Legacy systems will need additional protection layers
 - Firewalls, filters, adapters, plugins