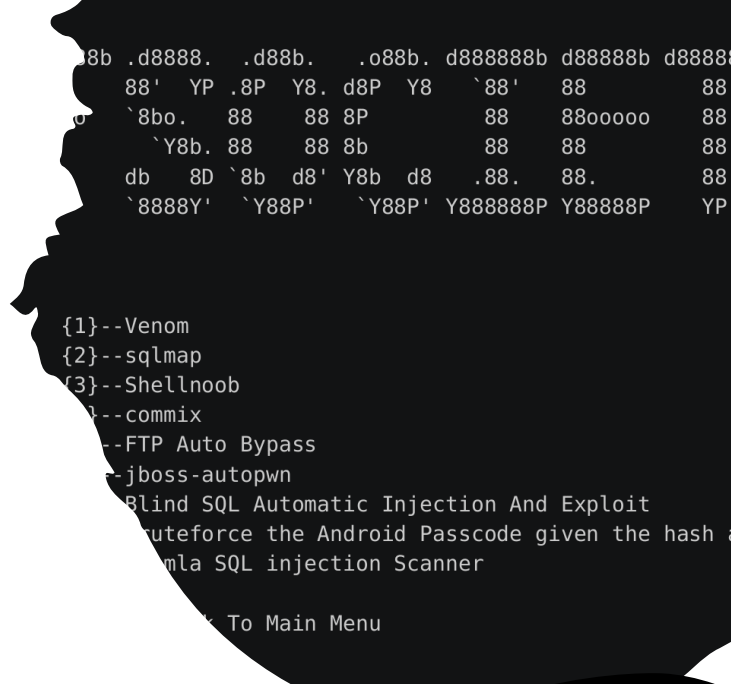


Introduction to cybersecurity

SIO

deti universidade de aveiro
departamento de eletrónica,
telecomunicações e informática

Is this Cybersecurity ?



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

- Across all aspects of a (business, system, organization) life cycle:
 - Planning
 - Development
 - Execution and operations
 - Processes
 - Human resources and clients
 - Supply Chain
 - Mechanisms and Controls
 - Standards, Compliance and Laws, ...



Areas in Cyber

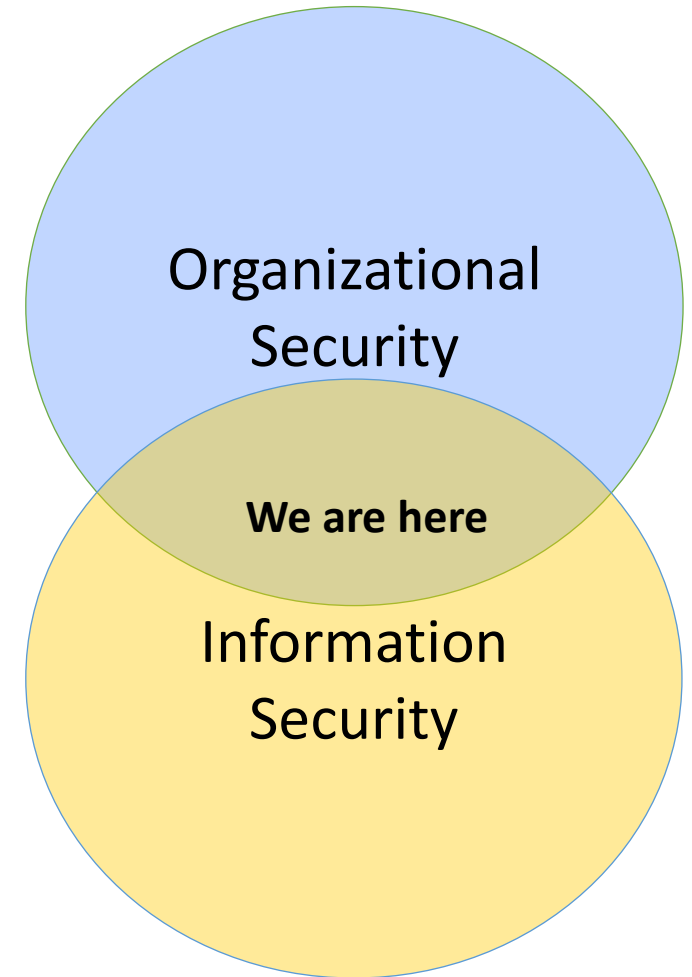
The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.1



Security Domains or Areas

Security is scoped into domains with many overlaps

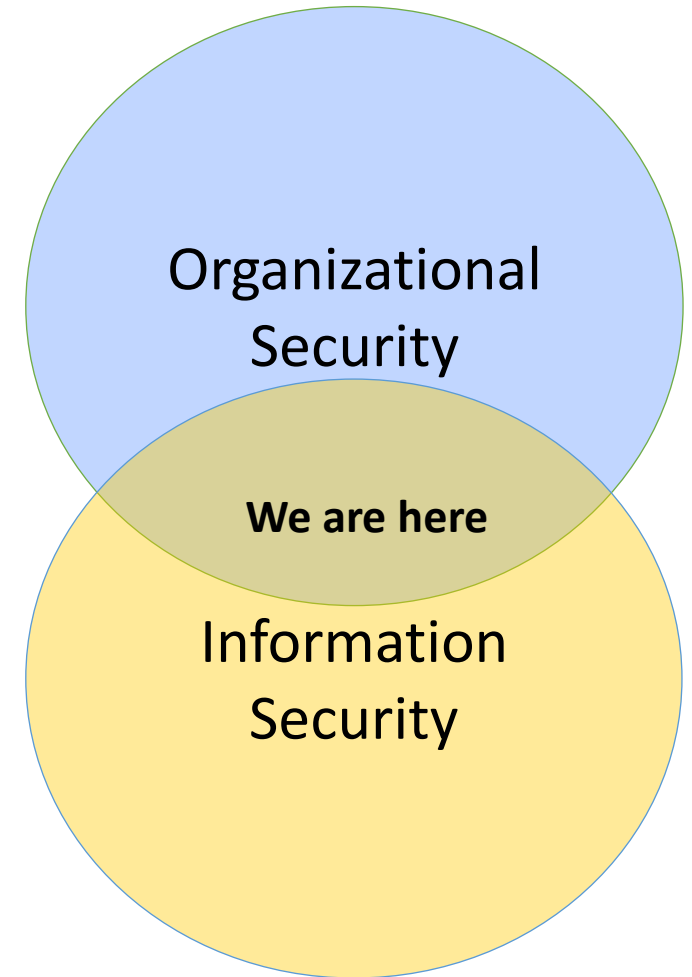
- **Organizational Security**
- Physical Security
- **Information Security**
- System Security
- Operacional Security
- Secure Development



Security Domains

Organizational Security (ISO 27001)

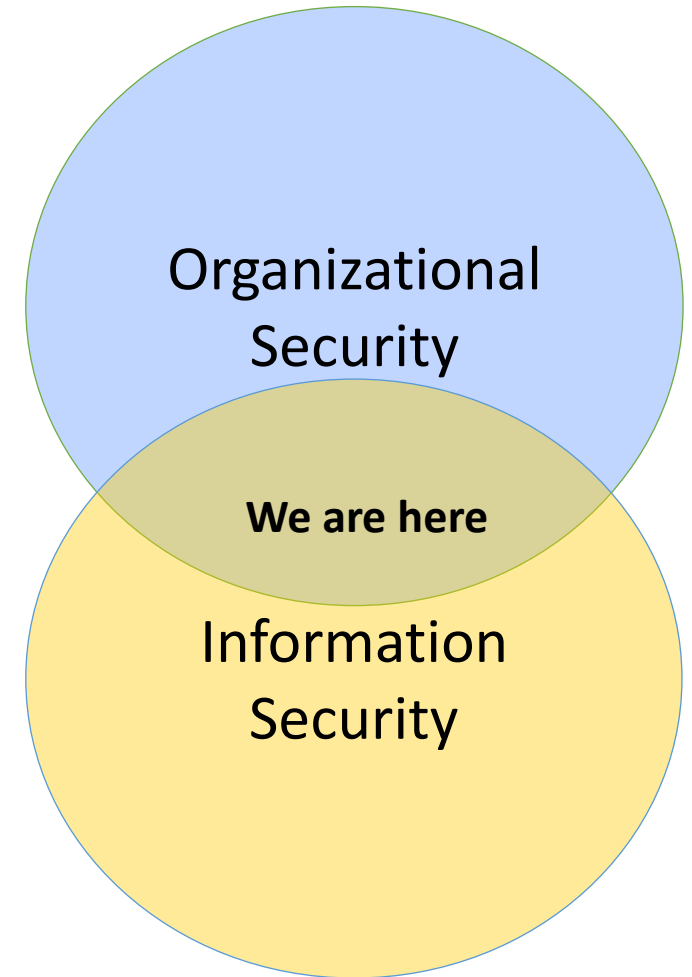
- Measures to **protect data** (electronic and otherwise) collected, held, and processed,
- and to protect its **computer systems, devices, infrastructure, computing environment, information and data stored** and all **other relevant equipment**
- from damage and **threats** whether internal, external, **deliberate, or accidental.**



Security Domains

Information Security (ISO 27001)

- preservation of **confidentiality, integrity, and availability** (CIA) of information.
- **Confidentiality:** Ensuring that information is accessed only by authorized individuals.
- **Integrity:** Maintaining the accuracy and completeness of information.
- **Availability:** Ensuring that information is accessible when needed by authorized users.



Information Security Objectives

- **Confidentiality:** Ensuring that information is accessed only by authorized individuals.
- **Measures:**
 - Encrypt information
 - Use access passwords (strong)
 - Use Identity Management and Authentication systems
 - Doors, Strong walls
 - Security personel
 - Training

Information Security Objectives

- **Integrity:** Maintaining the accuracy and completeness of information.

- **Measures:**
 - Identity control (hashes)
 - Backups
 - Access controls
 - Robust storage devices
 - Data verification processes

Information Security Objectives

- **Availability:** Ensuring that information is accessible when needed by authorized users.

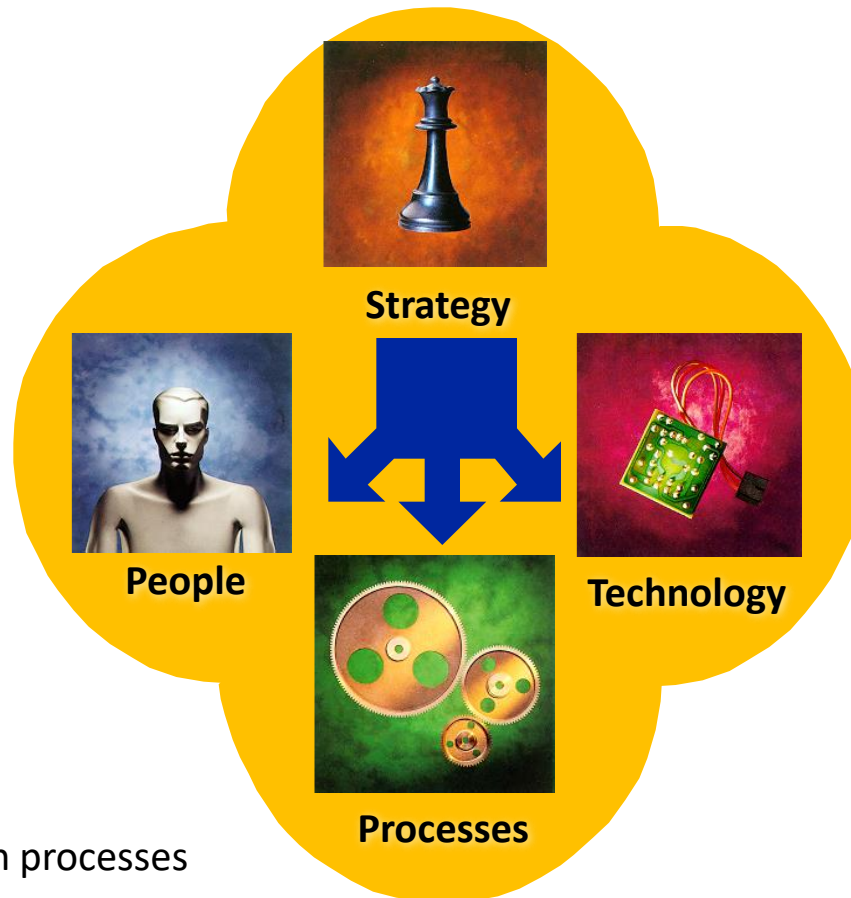
- **Measures:**
 - Backups
 - Disaster recovery plans
 - Redundancy
 - Virtualization
 - Monitoring

How can we use security in an organization?

With a strategy following the organizational dimensions

- Selection
- Training
- Awareness
- Organization of security

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



- Vulnerability scanning
- Firewalls
- Authentication
- Access Control
- Cryptography
- Digital Signatures
- Certification authorities
- Certification hierarchies
- etc...

Pitfalls

Pushing one dimensions without the other weakens the security posture

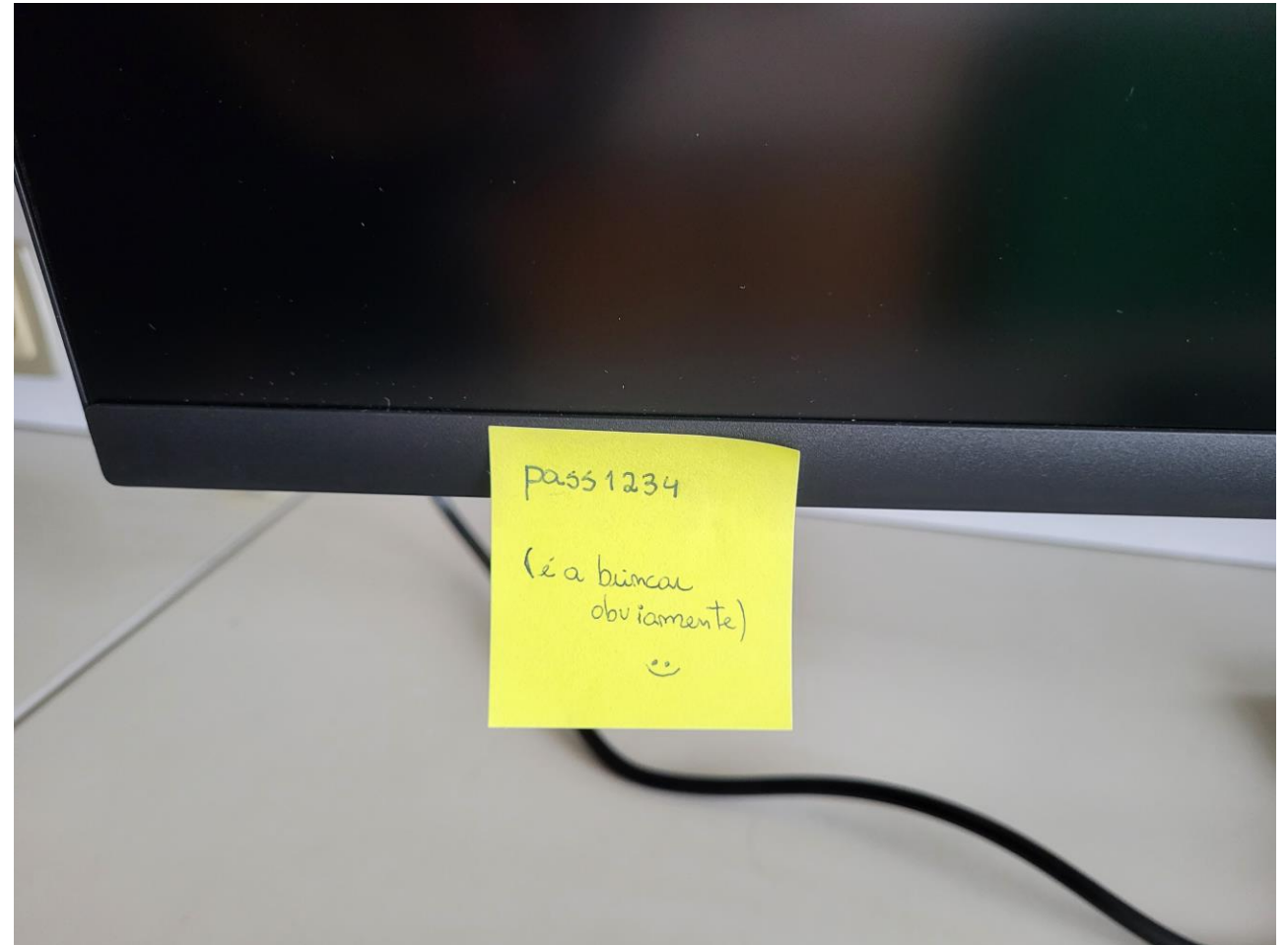
- What may have failed?
 - Technology?
 - Processes?
 - People?
 - Strategy?
- Walls, firewalls, processes... everything bypassed



Pitfalls

Pushing one dimensions without the other

- When it works and there is a security culture



Security objectives

1/3 – Intrinsic and unavoidable aspects

- 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 – Unpredictable ordinary failures

- 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

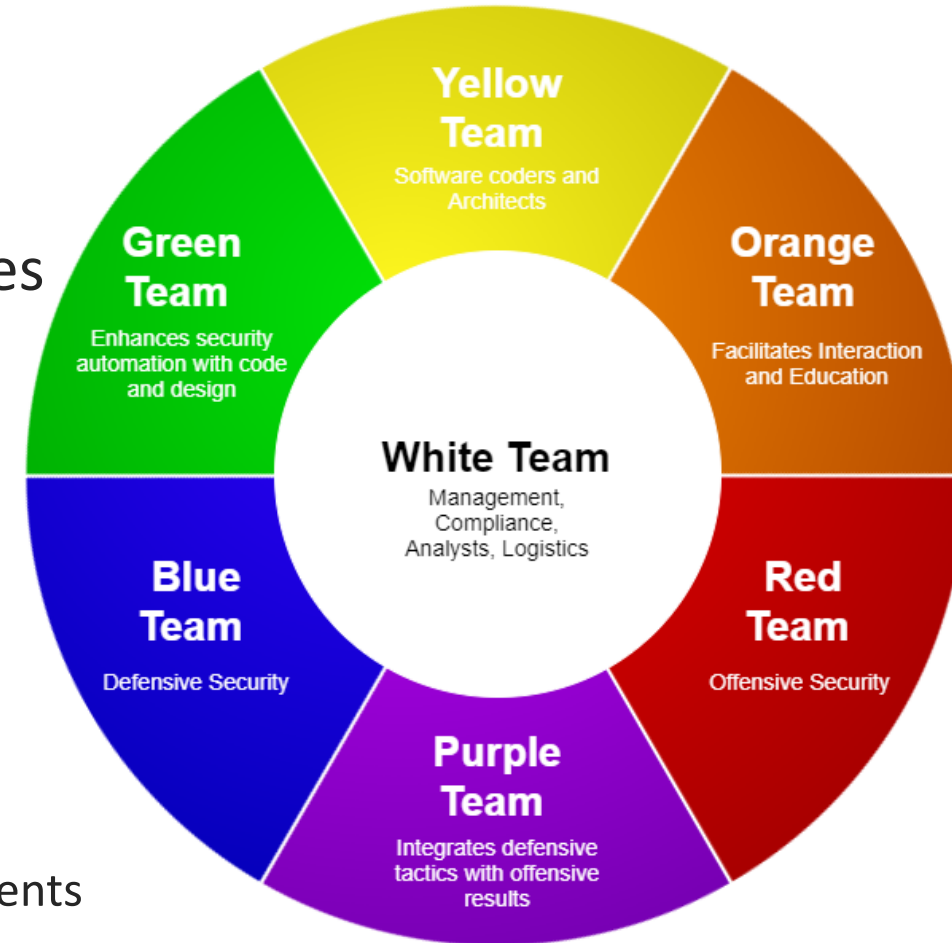
3/3 – Threats

- Defense against non-authorized activities (adversaries)
 - Initiated by someone “from outside”, “from inside” or “through a supplier”
- Types of non-authorized activities:
 - Information access
 - Information alteration
 - Resource usage
 - CPU, memory, print, network, wallets, etc...
 - Denial of Service
 - Vandalism
 - Interference with the normal system behavior without any benefit for the attacker

Security Perspectives

Which type of approaches

- Defensive tasks: focus on maintaining predictability and building layers
 - Deployment of Firewalls, Backups, Alert systems
 - Creation of processes and compliance
- Offensive: focus on exploiting vulnerabilities in entities
 - 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



Core Concepts

1. Security Domains

2. Security Policies

3. Security Mechanisms

4. Security Controls

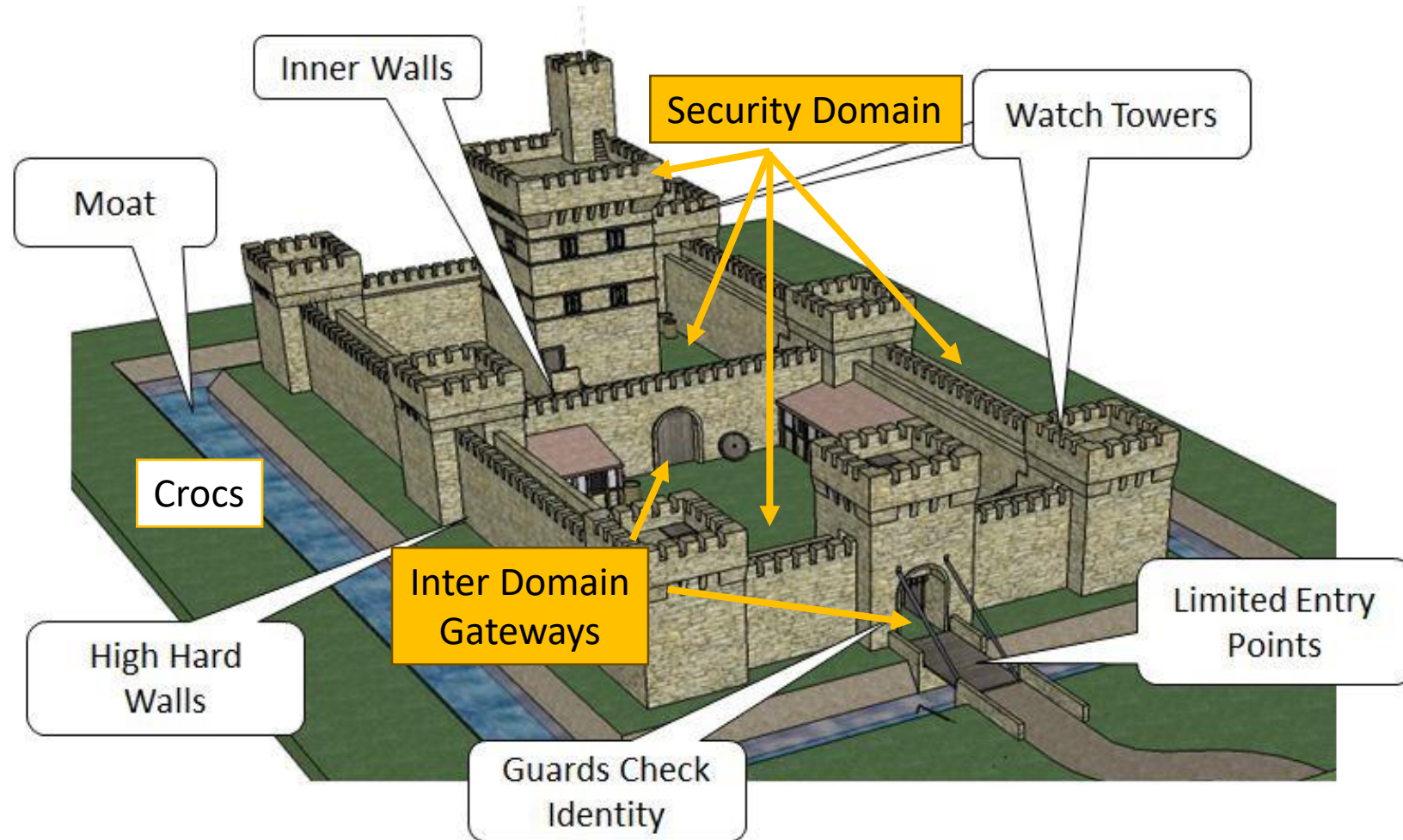
Security Domains

A system or subsystem that is under the authority of a single trusted authority. Security domains may be organized (eg, hierarchically) to form larger domains.

- Allow managing security in an aggregated manner
 - Management will set the attributes of the domain
 - Entities are added do the domain and will get the “group” attributes
- Behavior and interactions are ruled by homogeneous rules inside the domain
- Domains can be organized in a flat of hierarchical manner
 - Flat: Domains do not overlap but have frontiers, and exist at the same abstraction level
 - Hierarchical: Domains have different levels of abstraction (Organization -> devices -> Servers -> ServerA)
- Interactions between domains are usually controlled
 - With gateways that limit, change or log interactions

Security Domains

Popular application of security domains circa year 1500



Security policies

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

- Define the power of each subject
 - Least privilege principle: each subject should only have the privileges required for the fulfillment of his 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

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

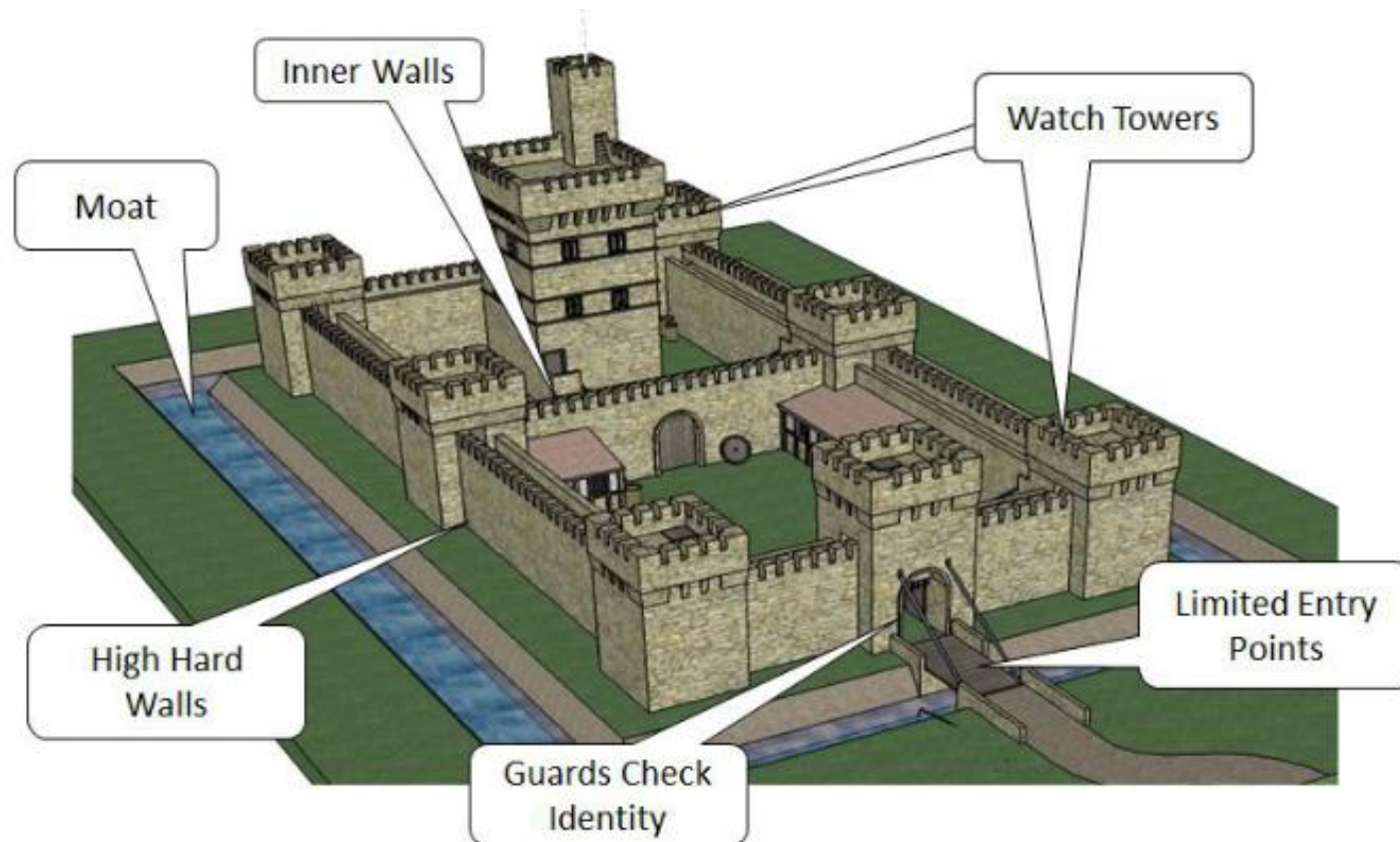
- Define what are legal and illegal activities
 - **Forbid list model**: Some activities are denied, the rest are allowed
 - **Permit list model**: Some activities are allowed, the rest is forbidden

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

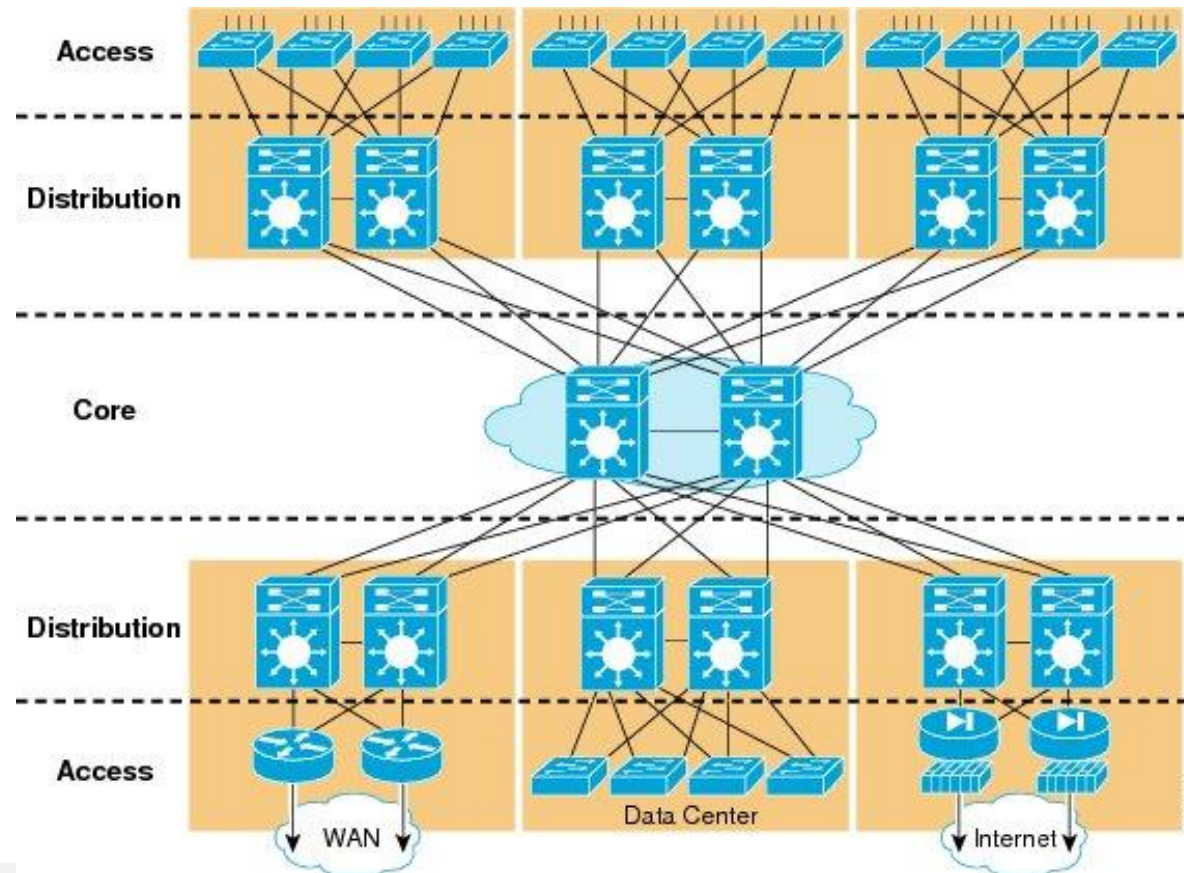
Security Mechanisms

- **Policy:** Movement between domains is restricted
- **Mechanisms:** Doors, guards, passwords, objects/documents, training, salary



Security Mechanisms

- **Policy:** systems must be resilient to arbitrary failures of one component
- **Mechanisms:** equipment and links are doubled, protocols are developed



Security Controls

A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability

- 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, incident management...

Types of Security Controls

	Prevention	Detection	Correction
Physical	<ul style="list-style-type: none">- Fences- Gates- Locks	<ul style="list-style-type: none">- CCTV	<ul style="list-style-type: none">- Repair Locks- Repair Windows- Redeploy access cards
Technical	<ul style="list-style-type: none">- Firewall- Authentication- Antivirus	<ul style="list-style-type: none">- Intrusion Detection Systems- Alarms- Honeypots	<ul style="list-style-type: none">- Vulnerability patching- Reboot Systems- Redeploy VMs- Remove Virus
Administrative	<ul style="list-style-type: none">- Contractual clauses- Separation of Duties- Information Classification	<ul style="list-style-type: none">- Review Access Matrixes- Audits	<ul style="list-style-type: none">- Implement a business continuity plan- Implement an incident response plan

Practical security

Key concept: Realistic Prevention

- Consider that **perfect security is impossible!**
- Focus on the **most probable events** for the **most relevant assets**
 - 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
 - Security mechanisms must cost less than the asset it protects
- Consider all domains and entities
 - A single breach can be escalated to a more serious situation

Practical security

Key concept: Realistic Prevention

- Consider the impact of an attack
 - Under the light of CIA and other potential impact areas (e.g., brand or legal)
- Consider the cost and recover time
 - Data, 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 assuming that everything else failed

Security in computing systems

Complex problems

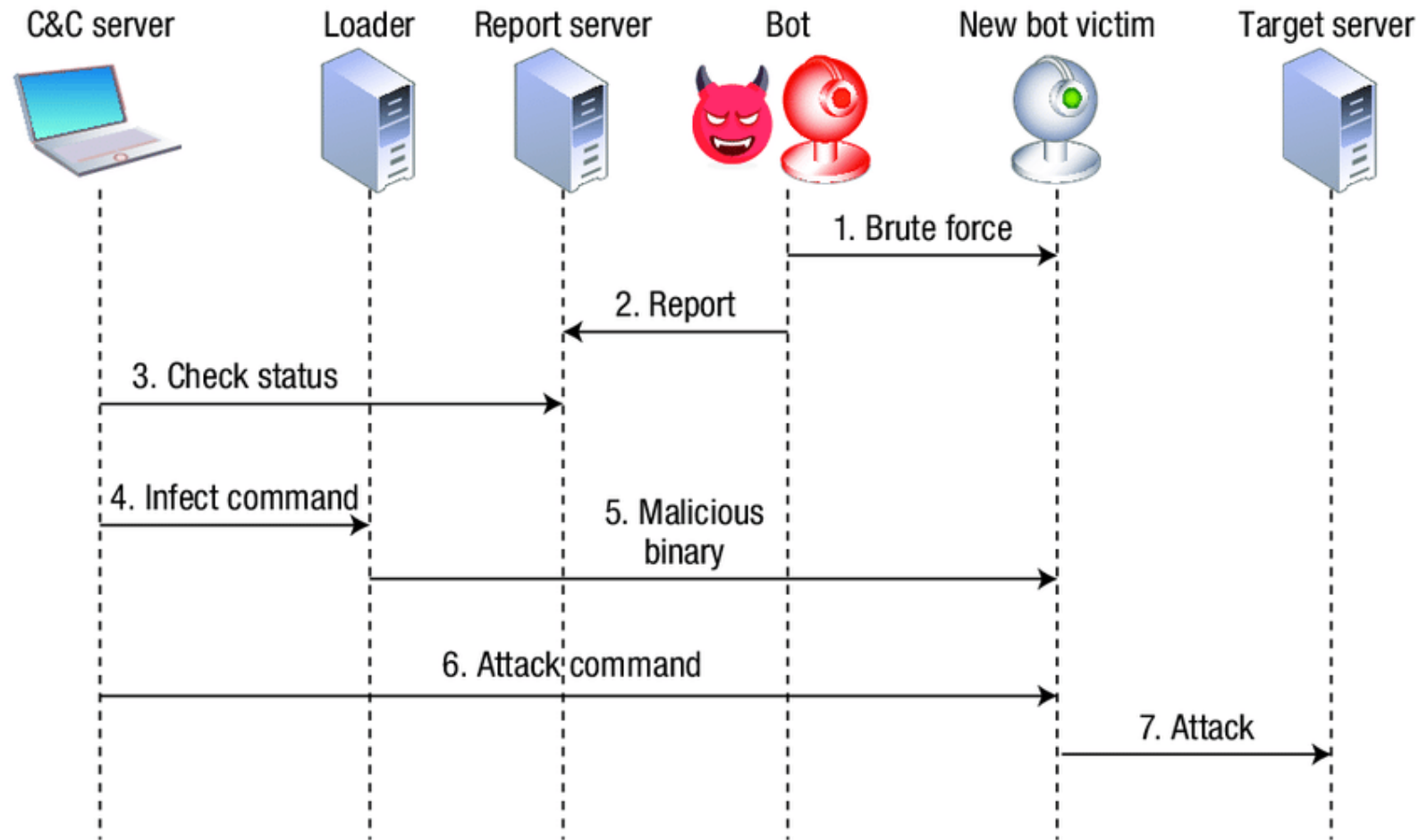
- Computers can do much damage in short time frames
 - Computers manage huge amounts of information
 - Process and communicate with very high speed

- The number of weaknesses **is always growing**
 - Due to the increased complexity
 - Due to every reducing time-to-market, or cost

Security in computing systems

Complex problems

- Networks allow **novel attack** mechanisms
 - “Anonymous” attacks from any place in the planet
 - Fast spread across geographical boundaries
 - Exploitation of insecure hosts and applications
- Attackers can build **complex attack chains**
 - First exploration
 - Lateral movement
 - Exfiltration
 - Check: <https://attack.mitre.org/matrices/enterprise/>



Mirai botnet operation and communication

Causes Distributed Denial of Service (DDoS) attacks to a set of services, by constantly propagating to weakly configured IoT Devices. Observe that victims are used to conduct further attacks to other victims

source: Koliass, Constantinos et al. "DDoS in the IoT: Mirai and Other Botnets." Computer 50 (2017): 80-84.

Perimeter Defense Model

Minimal defense, frequently not sufficient. The most common.

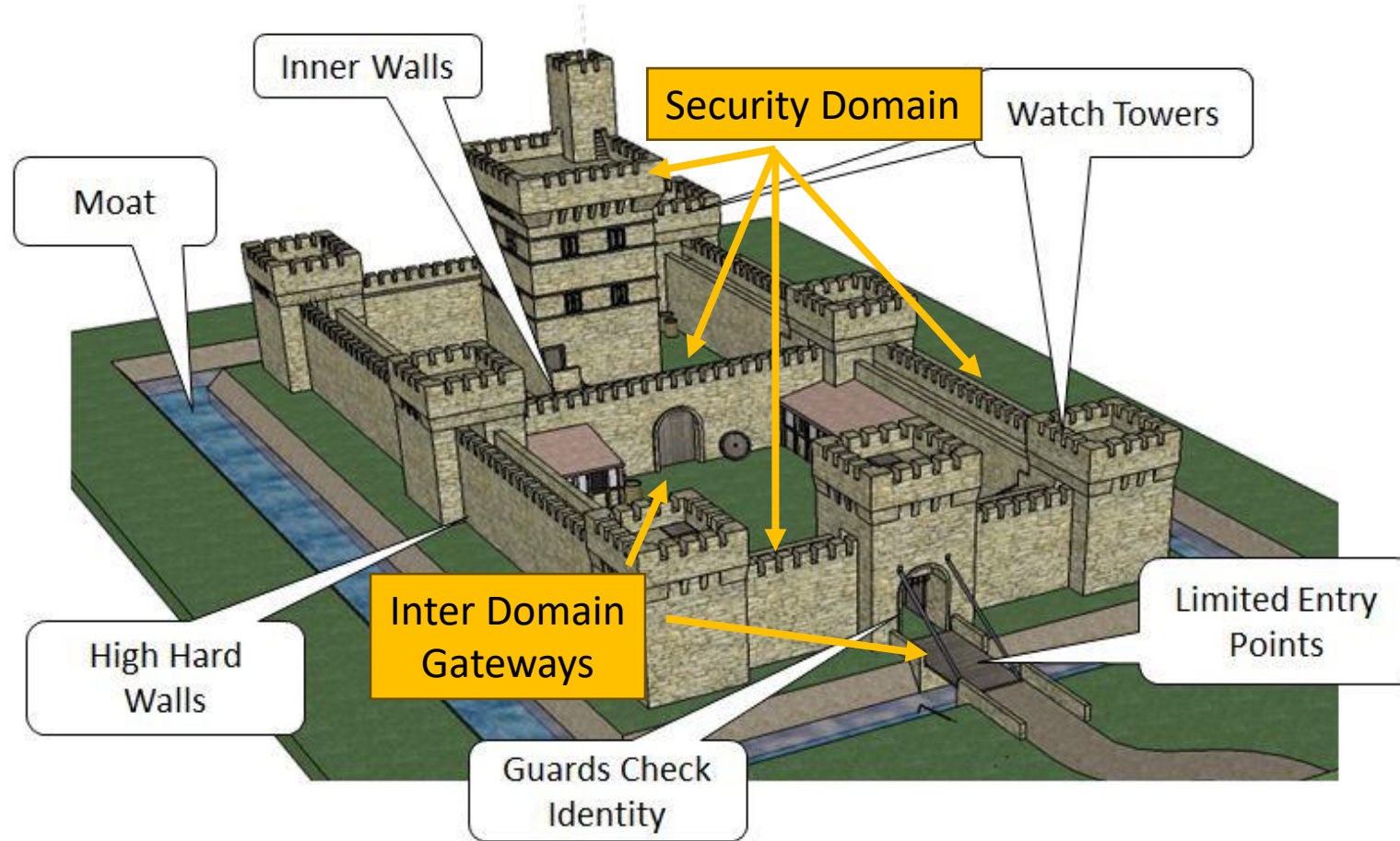


Perimeter Defense Model

- 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 Model

Layered approach with multiple domains (better)



Defense in Depth Model

- Protection against internal and external attackers
 - From the Internet
 - Users
 - Other organizations

- Assumes well-defined domains across the organization
 - Walls, doors, authentication, security personnel, ciphers, secure networks

- Limitations
 - Needs coordination between the different 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 Model

- 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
 - Requires detailed knowledge, controls and observability between all entities

- 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

In practice?

- Cybersecurity is limited by economics, operations and logistics
 - All entities have limited resources
 - Even attackers!
 - Security is a business continuity activity, it cannot prevent business
- Cybersecurity deals with building and applying a strategy
 - under an operational and legal context
 - preventing issues that may never happen
- Try this: <http://targetedattacks.trendmicro.com/cyoa/en/>