Introduction

INFORMATICS AND ORGANIZATIONAL SECURITY

Security ?

```
88b .d8888.  .d88b.   .o88b. d888888b d88888b d8888
   88'  YP .8P  Y8. d8P  Y8   `88'   88         88
   `8bo.   88    88 8P         88    88ooooo    88
     `Y8b. 88    88 8b         88    88         88
   db   8D `8b  d8' Y8b  d8   .88.   88.        88
   `8888Y'  `Y88P'   `Y88P' Y888888P Y88888P    YP
```

```
{1}--Venom
{2}--sqlmap
{3}--Shellnoob
--commix
--FTP Auto Bypass
-jboss-autopwn
Blind SQL Automatic Injection And Exploit
uteforce the Android Passcode given the hash
mla SQL injection Scanner

To Main Menu
```

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 which compromise 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

Source: https://www.verificient.com/

ISO 27001 – Clean Desk Policy

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 atributes

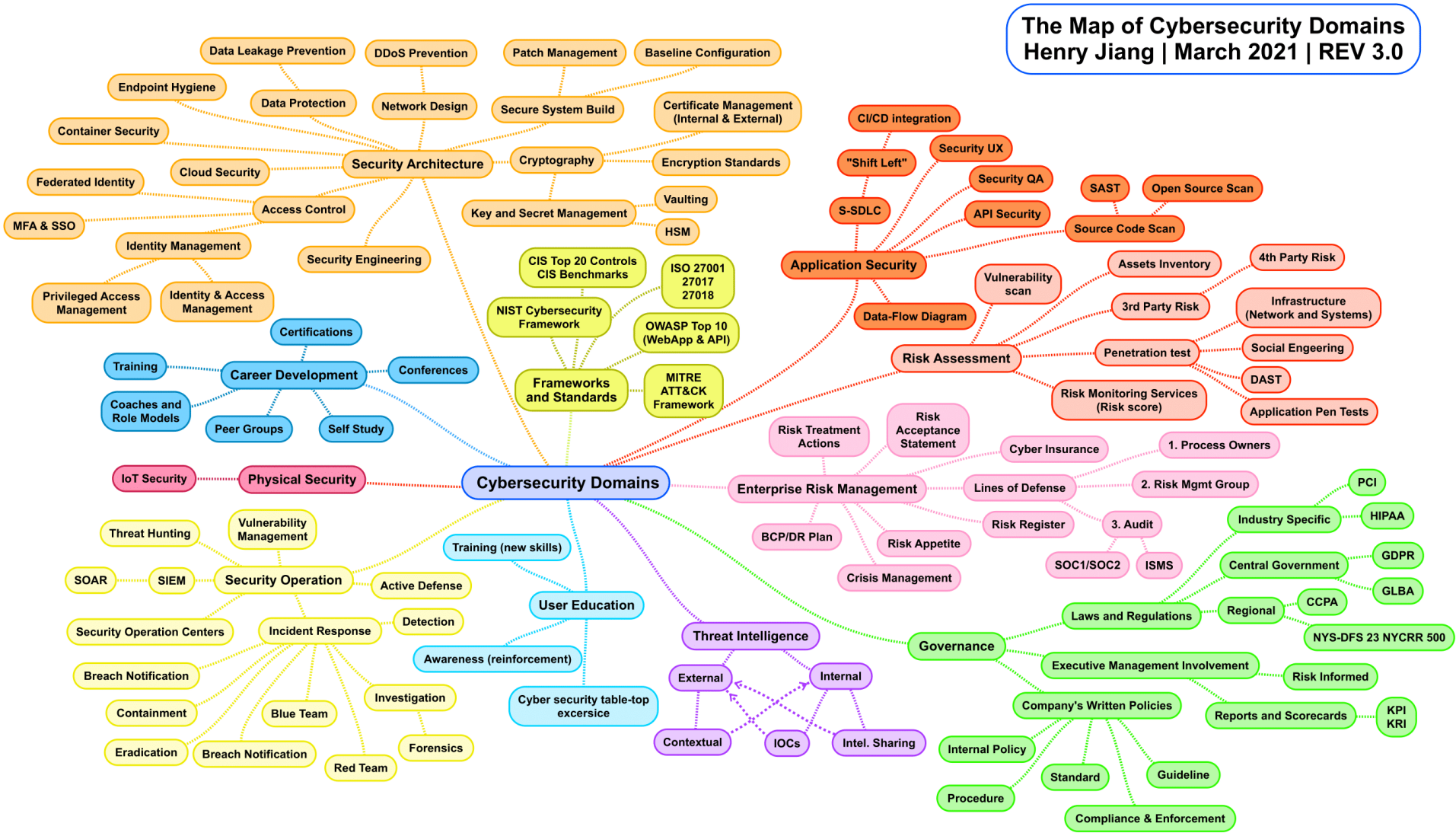
- Faults, Errors, behavior

Identify the risk for the solution to be modified

- Exposition to possible attackers
- Incentives one may have to modify it
- Identify potential actos (Threats)

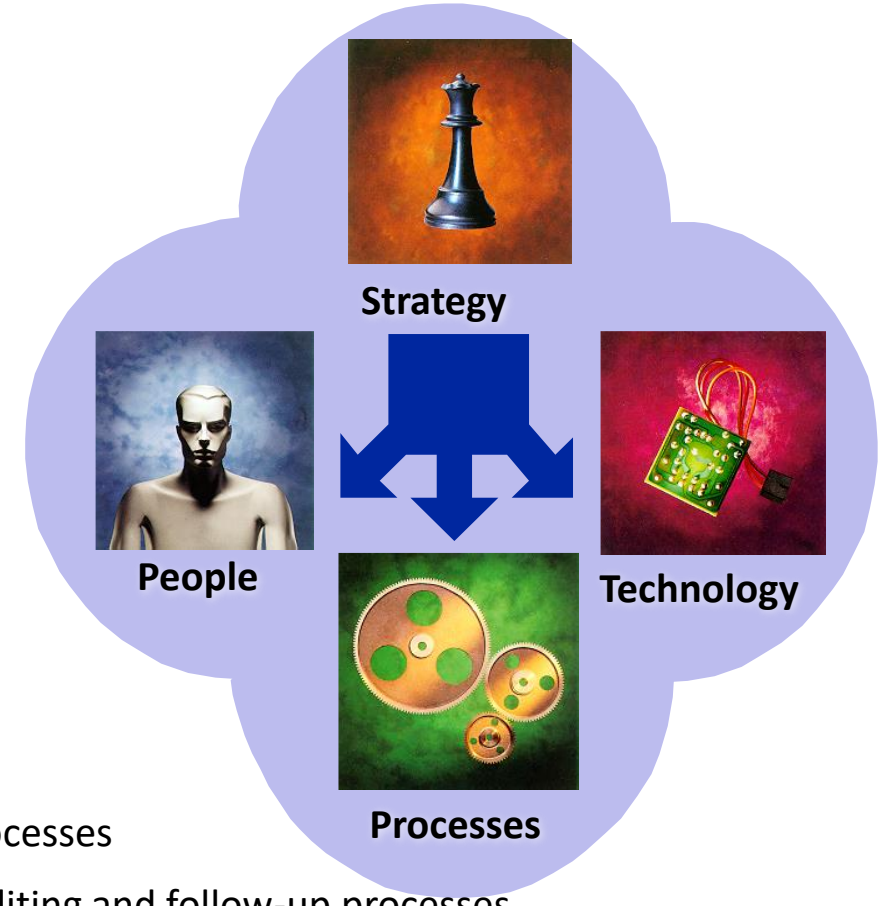
Identify the impact of the deviations

- Total loss of data? Denial of Service? Increase Operation Cost?


The Map of Cybersecurity Domains
Henry Jiang | March 2021 | REV 3.0
Cybersecurity Domains
Security Architecture
Data Leakage Prevention
DDoS Prevention
Patch Management
Baseline Configuration
Endpoint Hygiene
Data Protection
Network Design
Secure System Build
Certificate Management (Internal & External)
Container Security
Cloud Security
Cryptography
Encryption Standards
Federated Identity
Access Control
Key and Secret Management
Vaulting
MFA & SSO
HSM
Identity Management
Security Engineering
Privileged Access Management
Identity & Access Management
Application Security
CI/CD integration
Security UX
"Shift Left"
Security QA
S-SDLC
API Security
SAST
Open Source Scan
Source Code Scan
Data-Flow Diagram
Risk Assessment
Vulnerability scan
Assets Inventory
4th Party Risk
3rd Party Risk
Infrastructure (Network and Systems)
Penetration test
Social Engeering
DAST
Risk Monitoring Services (Risk score)
Application Pen Tests
Frameworks and Standards
CIS Top 20 Controls
CIS Benchmarks
ISO 27001
27017
27018
NIST Cybersecurity Framework
OWASP Top 10 (WebApp & API)
MITRE ATT&CK Framework
Career Development
Certifications
Training
Conferences
Coaches and Role Models
Peer Groups
Self Study
Enterprise Risk Management
Risk Treatment Actions
Risk Acceptance Statement
Cyber Insurance
1. Process Owners
Lines of Defense
2. Risk Mgmt Group
Risk Register
3. Audit
BCP/DR Plan
Risk Appetite
SOC1/SOC2
ISMS
Crisis Management
Physical Security
IoT Security
Security Operation
Threat Hunting
Vulnerability Management
SOAR
SIEM
Active Defense
Security Operation Centers
Incident Response
Detection
Breach Notification
Containment
Blue Team
Investigation
Eradication
Breach Notification
Red Team
Forensics
User Education
Training (new skills)
Awareness (reinforcement)
Cyber security table-top excersice
Threat Intelligence
External
Internal
Contextual
IOCs
Intel. Sharing
Governance
Laws and Regulations
Industry Specific
PCI
HIPAA
Central Government
GDPR
GLBA
Regional
CCPA
NYS-DFS 23 NYCRR 500
Executive Management Involvement
Risk Informed
Company's Written Policies
Reports and Scorecards
KPI
KRI
Internal Policy
Standard
Guideline
Procedure
Compliance & Enforcement

Dimensions to consider

- Selection
- Training
- Awareness
- Organization of security



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

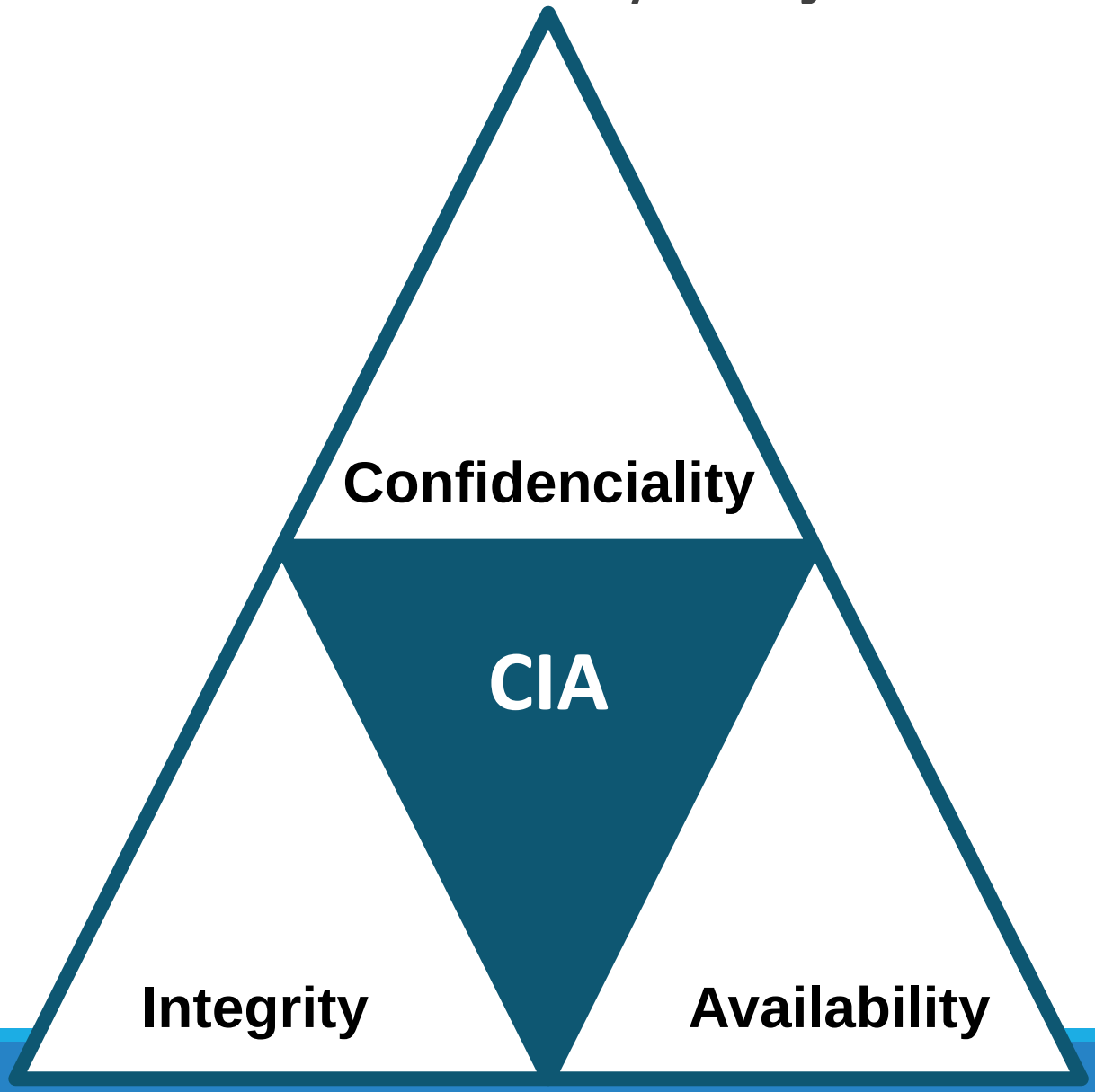
Offensive: focus on exploiting predictability

- 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 personel
- Training

Information Security

Integrity: Information remains unchanged

- Can be applied to behavior of devices and services

Measures:

- Identity control (hashes)
- Backups
- Access Controls
- Robust Storage Devices
- Data verification processes

Information Security

<u>Availability</u>: Information is available to target entities

- Can be applied to service 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

- bad sectors in disks
- failure of power supplies
- 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
- Vandalism
  - Interference with the normal system behavior without any benefit for the attacker

Core Concepts

1. **Domains**
2. **Policies**
3. **Mechanisms**
4. **Controls**

Security Domains

A set of entities sharing similar security attributes

Allow managing security in a aggregated manner

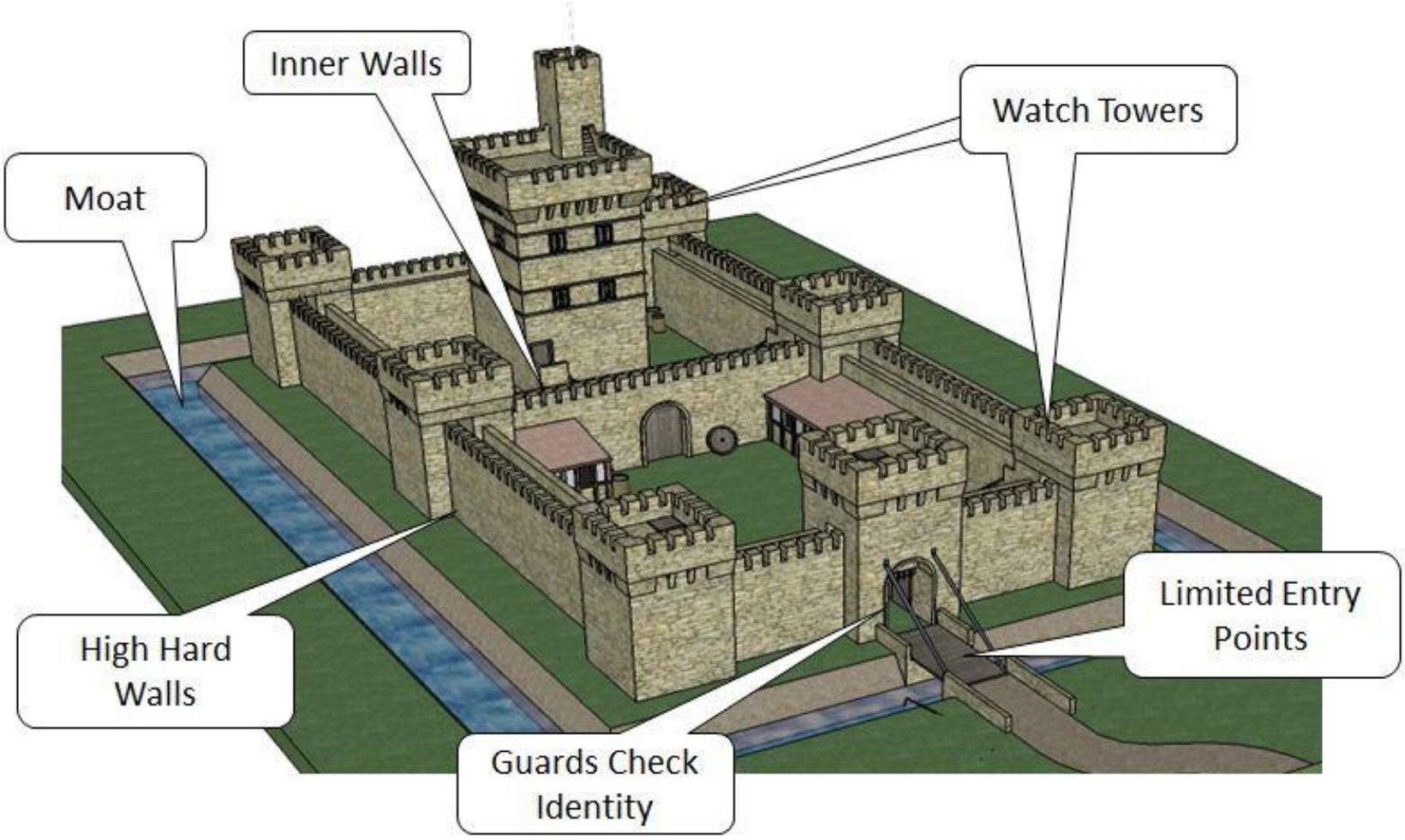
- Management will set the attributes of the domain
- Entities are added do the domain and will get the “group” attributes

Behavior and interactions are homogenous inside the domain

Domains can be organized in a flat of hierarchical manner

Interactions between domains are usually controlled

Security Domains



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

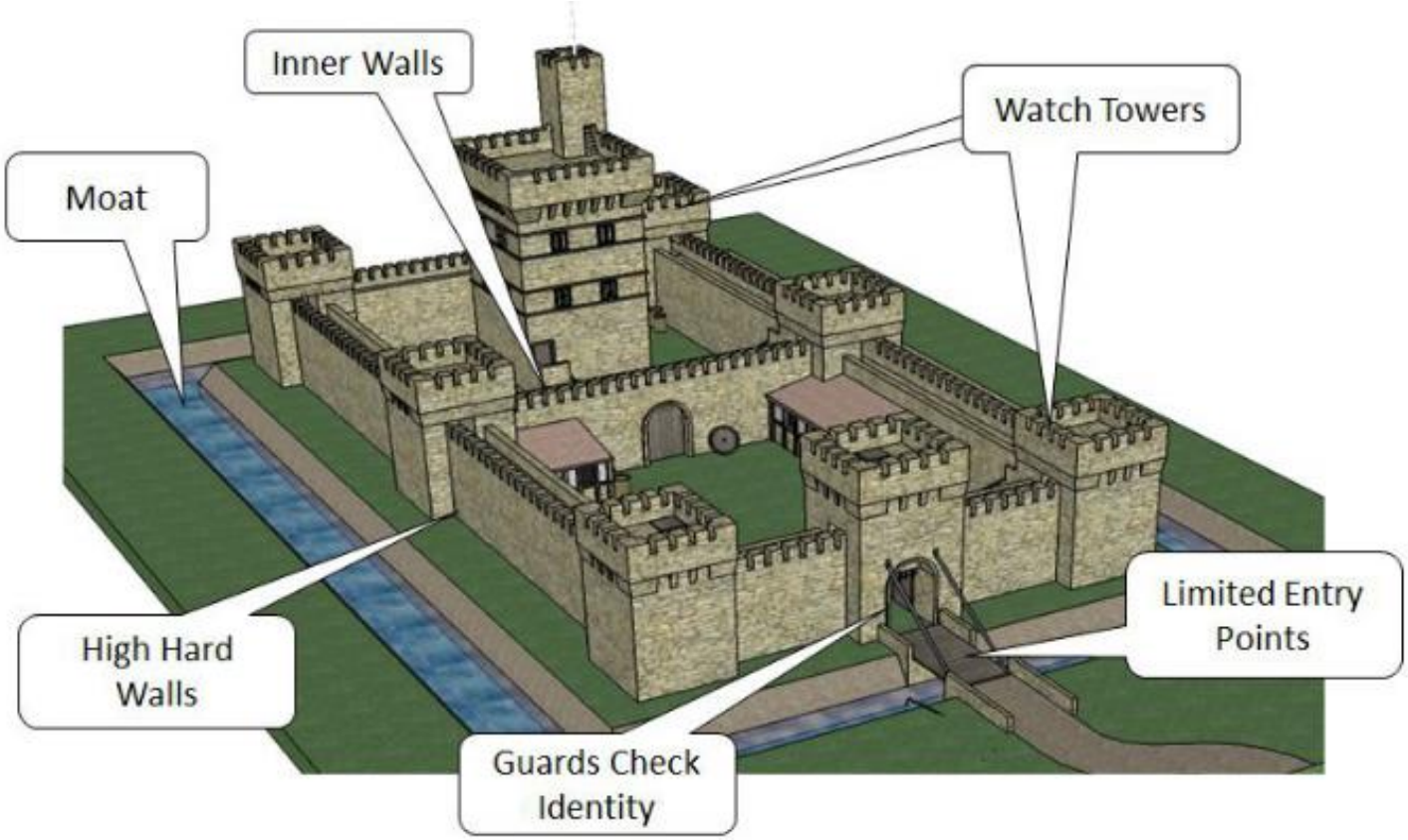
- Policies define, at a higher level, what needs to be done or exist
- Mechanisms are used to deploy policies

Generic security mechanisms

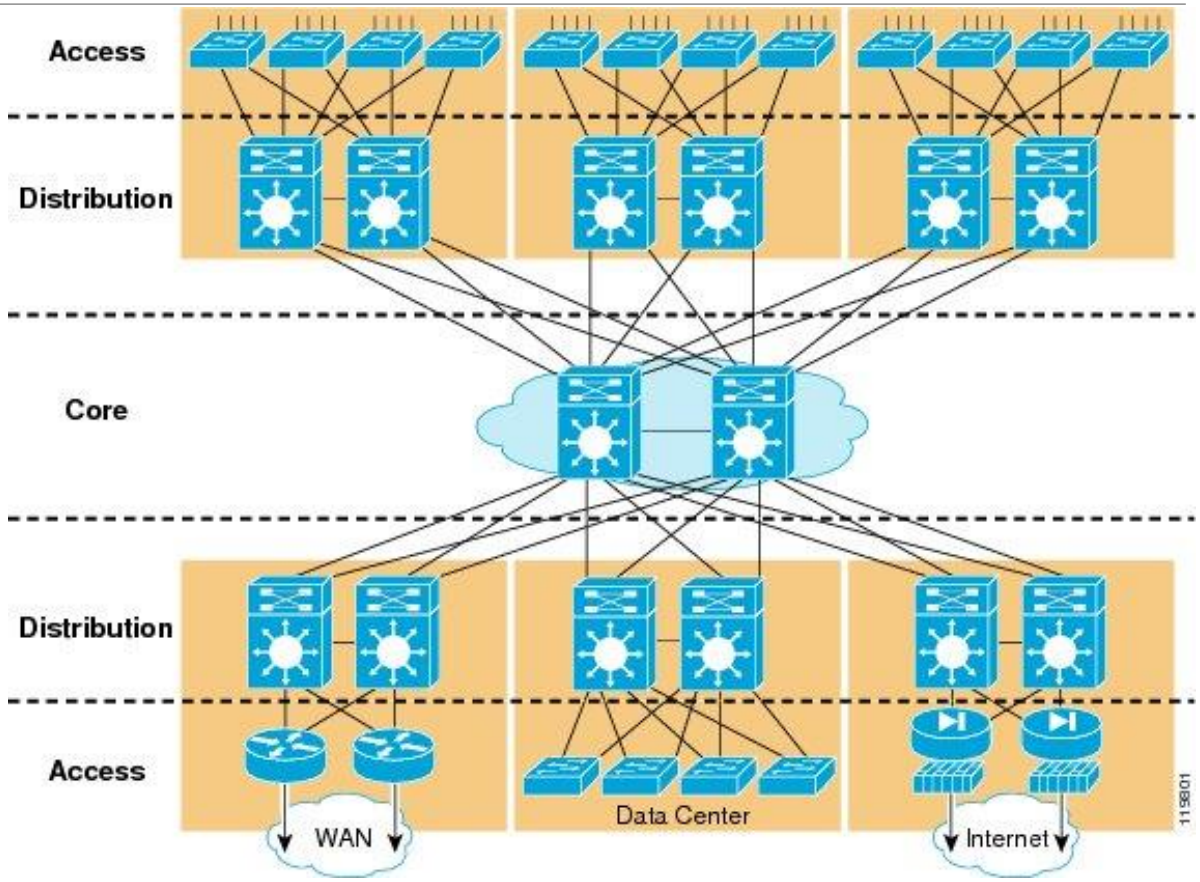
- Confinement (Sandboxing)
- Authentication
- Access control
- Privileged Execution
- Filtering
- Logging
- Auditing
- Cryptographic algorithms
- Cryptographic protocols

Security mechanisms

Policy: Movement between domains is restricted
Mechanisms: Doors, guards, passwords, objects/documents



Policy: systems must be resilient
Mechanisms: equipments and links are doubled, arquitecture



Source: CISCO

Security Controls

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

Controls include policies and mechanisms, but also:

- Standards and Loaws
- Processes
- Policies
- Mechanisms
- Techniques

Controls are explicitly stated and can be auditable

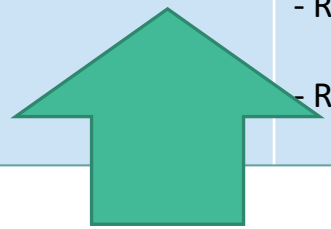
- E.g.: ISO 27001 defines 114 controls in 14 groups
  - … asset management, physical security, incidente management…

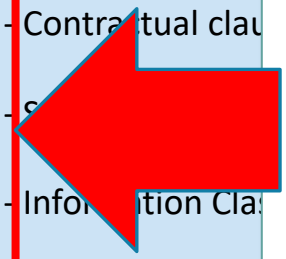
Types of Security Controls

	Prevention	Detection	Correction
Physical	- Fences - Gates - Locks	- CCTV	- Repair Locks - Repair Windows - Redeploy access cards
Technical	- Firewall - Authentication - Antivirus	- 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

Types of Security Controls

	Prevention	Detection	Correction
Physical	- Fences - Gates - Locks	- CCTV	- Repair Locks - Repair Windows
Technical	- Firewall - Authentication - Antivirus		
Administrative	- Contra tual clau - S - Infor tion Cla		





Green: in relation to na event

Red: in relation to it's nature

Practical Security

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

Realistic Prevention

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

Security in computing systems: Complex problems

Computers can do much damage in a short time frame

- Computers manage huge amounts of information
- Process and communicate with very high speed

The number of weaknesses is always growing

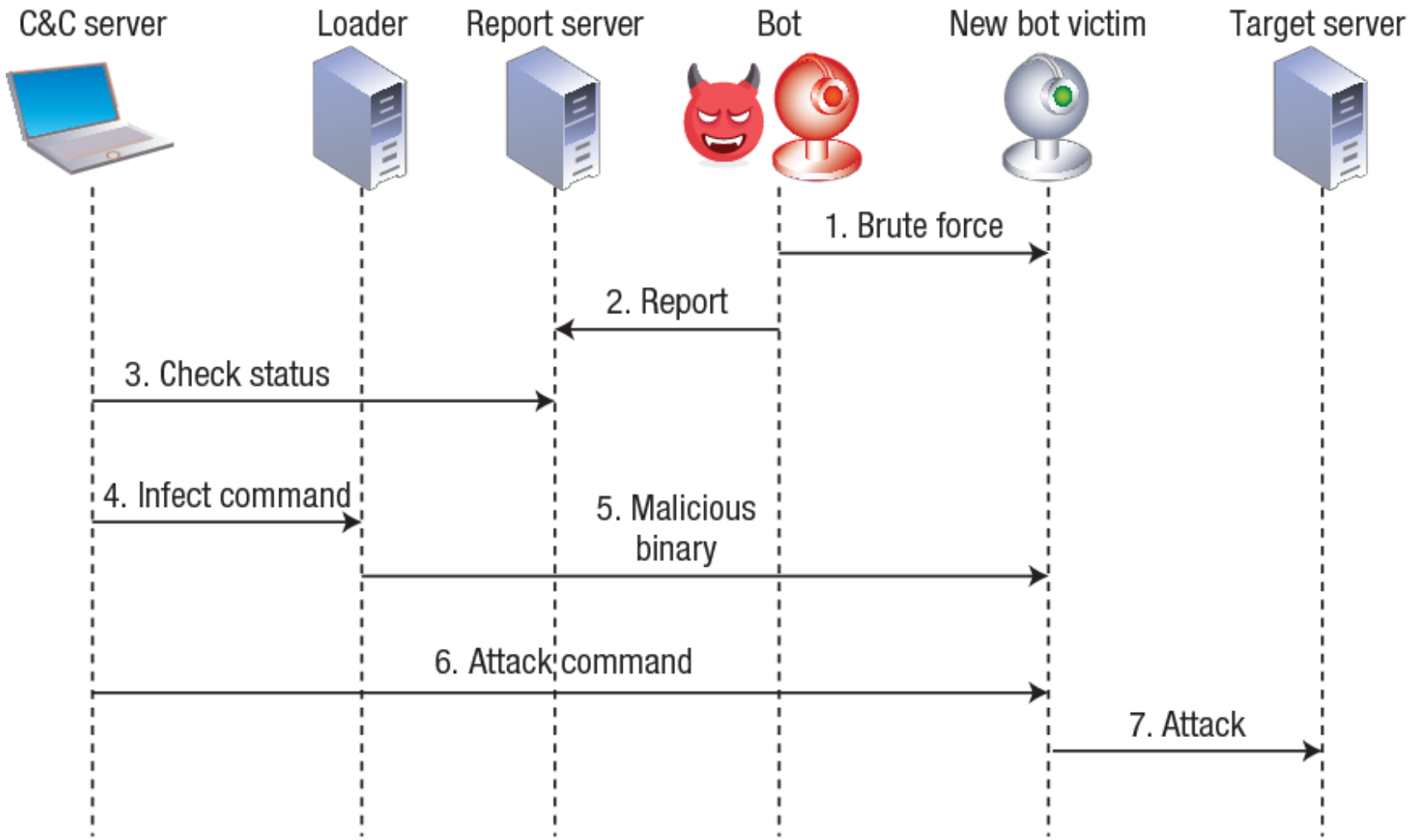
- Due to the increased complexity
- Due to every reducing time-to-market, or cost

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.
Mirai causes a distributed denial of service (DDoS) to a set of target servers by constantly propagating to weakly configured Internet of Things (IoT) devices.

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

Security in computing systems: Complex problems

Users are mostly unaware of the risks

- They do not know the problems,
- ... the impact
- ... the good practices
- .... nor the solutions

Users are mostly careless

- Because they take risks
- Do not care (Do not have/identify any responsability
- Do not estimate the risk correctly

Main vulnerability sources

Hostile applications or bugs in applications

- Rootkits: Insert elements in the operating system
- Worms: Software programs controlled by an attacker
- Virus: Pieces of code that infect other files (ex, macros)

Users

- Ignorant or careless
  - telnet vs. ssh, IMAP vs. IMAPS, HTTP vs HTTPS
  - False sense of security (I have an anti-virus, so I'm protected!)
- Hostile

Defective administration

- Default configuration is seldom the most secure
- Security restriction vs flexible operation
- Exceptions to individuals

Communication over uncontrolled/unknown network links

- Public hotspots, campus networks, hostile governments

Security policies for distributed systems (some)

Must encompass several hosts and networks

Security Domains

- Definition of the set of hosts and networks of the domain
- Definition of the set of accepted/authorized users
- Definition of the set of accepted/not accepted activities

Security Gateways

- Definition of the set of allowed in-out interactions

Security Controls

- Define the points for future auditing

Perimeter Defense

(minimal defense, frequently not sufficient)

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

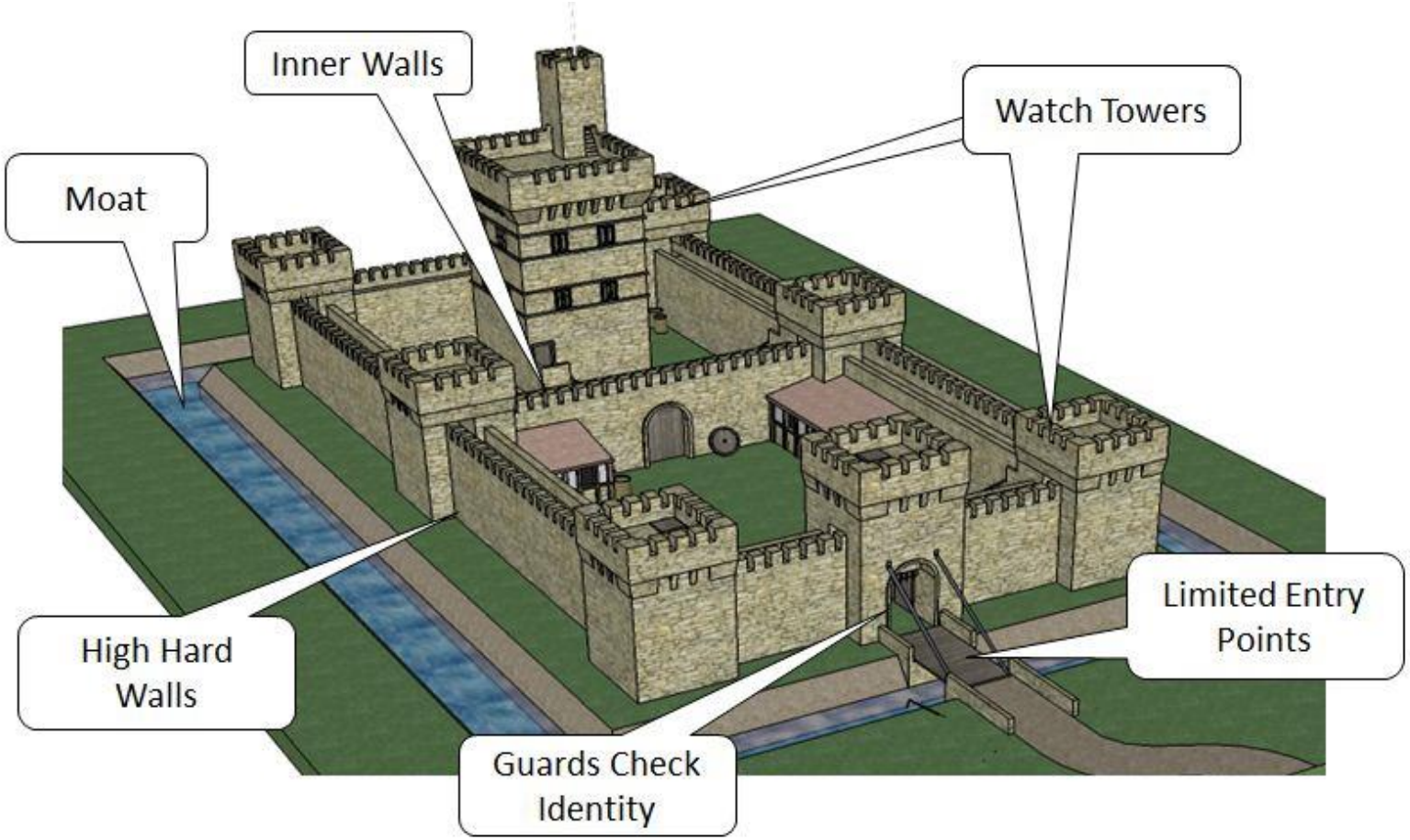
Used domestic scenarios or small offices

Limitations

- Too simple
- Doesn’t protect against internal attackers
  - Previously trusted users
  - Attackers that acquired internal access

Defense in Depth

(with flaws, but better)



Defense in Depth

Protection against internal and external attackers

- From the Internet
- Users
- Other organization

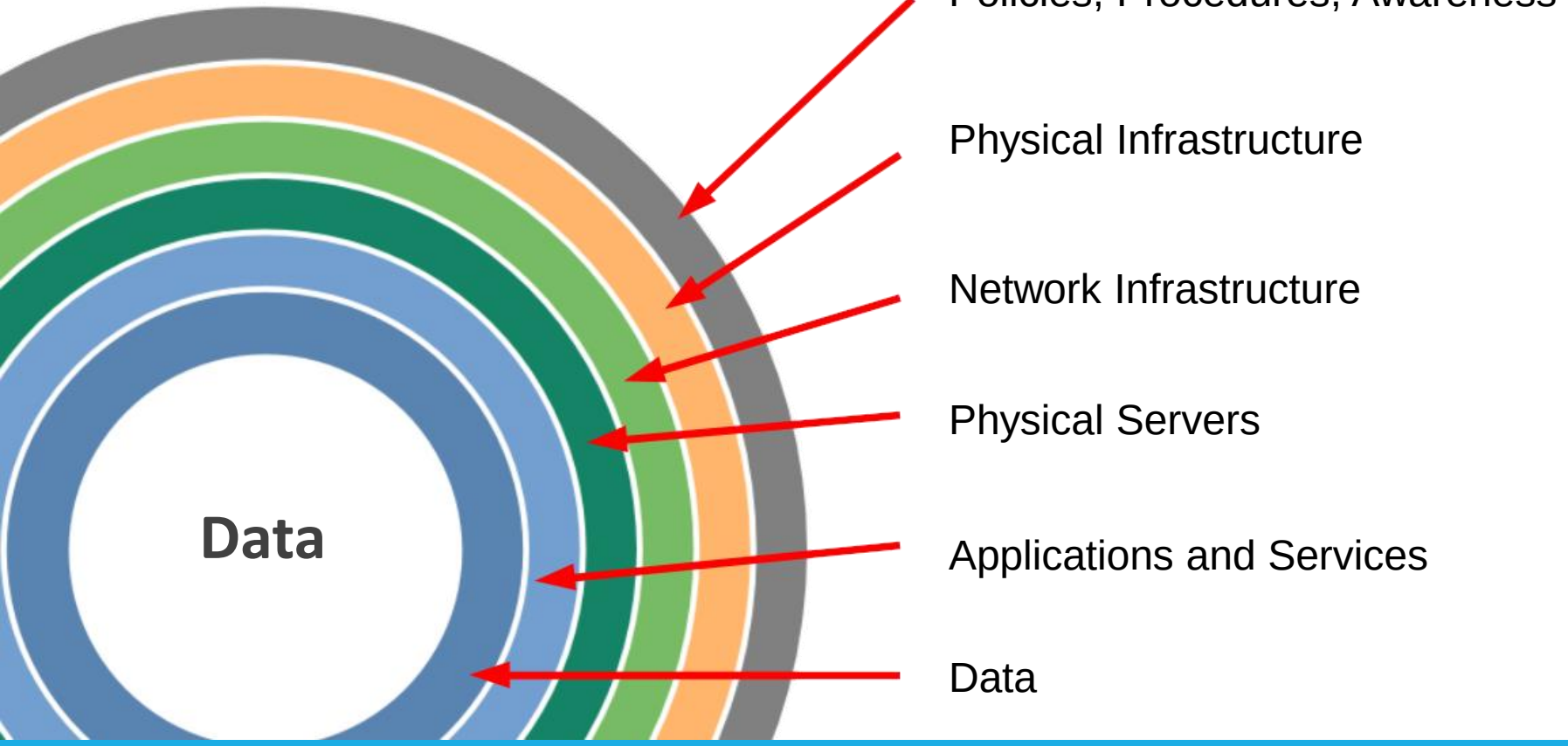
Assumes well defined domains across the organization

- 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

Defense in Depth



Defense in Depth

Trusted Operating Systems

- Security levels, certification
- Secure execution environments for servers
- Sand-boxing / virtual machines

Firewalls & Security Appliances

- Traffic control between networks
- Monitoring (traffic load, etc.)

Secure communications / VPNs

- Secure channels over insecure, public networks
- Secure extension of organizational networks

Defense in Depth

Authentication

- Local
- Remote (network authentication)
- Single Sign-On
- Using secrets, token, bio-metrics, device, location

Certification Authorities / PKI

- Management of public key certificates

Encryption of files and sessions

- Privacy / confidentiality of network data
- Privacy / confidentiality of long-term stored data

Defense in Depth

Intrusion detection

- Detection of forbidden / abnormal activities
- Network-Based / Host-based

Vulnerability scanners

- Scanning for problem fixing or exploitation
- Network-based / Host-based

Penetration testing

- Vulnerability assessment
- Demo penetration attempts
- Testing of installed security mechanisms
- Assessment of badly implemented security policies

Defense in Depth

Content monitoring

- Detect virus, worms and other malware

Security management

- Develop security policies
- Apply policies in a distributed manner
- Co-administration/contracting external teams

Incident response / Real time following

- Capability to detect and react to incidents in real time
- Means for fast and effect response to incidents

Zero Trust

Defense model without specific perimeters

- There is no inherent trust in entities just because they are internal
  - Actually, they 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, filtros, adaptadores, plugins

Zero Trust – Principles (NCSC)

1. **Know your architecture**
   - Users, devices, services and data
2. **Know your identities**
   - Users, devices, services and data
3. **Assess user behaviour, service and device health**
4. **Use policies to authorize requests**

Zero Trust – Principles (NCSC)

5. **Authenticate and Authorize everywhere**
   - No open APIs, or IP address based access

6. **Focus your monitoring on users, devices and services**

7. **Don’t trust any network, including your own**
   - Internal attackers should not have more rights than external attackers

8. **Choose services designed for Zero Trust**
   - Legacy services to be avoided, but can be integrated

Today – Standard users

Use the same devices for all interactions

- Talk with other users
- Access leisure services and websites
- Access critical services (eg, banks)
- Work (?)

Service and system use based on a final objective

- Buy, sell, read, listen, communicate
- No or little security considerations

No training, fearless

- Bad at predicting the risk of their actions
- Consider that security issues only happen to large entities/others
  - Think they are not relevant
- With wrong base concepts
  - “Algorithms” to generate passwords, password reuse
- With no investment in security infrastructure (except an antivirus?)
  - Trust an antivirus more than anything else
- Without disaster recovery processes

Today - Companies

Focused on a business

- The product they provide
- Financials
- Human Resources

Interact with security aspects as required

- Should comply with existing norms and regulations
  - RGPD, sector specific regulation
- May have security strategies
  - From nothing to an extreme focus in “security driven culture”
- May provide training and invest in security
- May have frequent audits
- May even have a CISO: Chief Information Security Officer

Category	Basic Organizations	Progressing Organizations	Advanced Organizations
Philosophy	Cybersecurity is a "necessary evil."	Cybersecurity must be more integrated into the business	Cybersecurity is part of the culture.
People	CISO reports to IT. Small security team with minimal skills. High burnout rate and turnover.	CISO reports to COO or other non-IT manager. Larger security team with some autonomy from IT. Remain overworked, understaffed, and under-skilled.	CISO reports to CEO and is active with the board. CISO considered a business executive. Large, well-organized staff with good work environment. Skills and staff problems persist due to the global cybersecurity skills shortage.
Process	Informal and ad-hoc. Subservient to IT.	Better coordination with IT but processes remain informal, manual, and dependent upon individual contributors.	Documented and formal with an eye toward more scale and automation.
Technology	Elementary security technologies with simple configurations. De-centralized security organization with limited coordination across functions. Focus on prevention and regulatory compliance.	More advanced use of security technologies and adoption of new tools for incident detection and security analytics.	Building an enterprise security technology architecture. Focus on incident prevention, detection, and response. Adding elements of identity management and data security to deal with cloud and mobile computing security.

Source: Enterprise Strategy Group, 2014.

Today - Nations

Focused on national sovereignty

- Acting independently or as part of strategic groups (e.g, NATO)

Have entities dedicated to cybersecurity

- Cyber Defense
  - Part of their defense forces (e.g. army)
  - Ad-hoc entities hired or shadow
- Cyber resilience of the nation entities
  - Utilities, university, companies, citizens
- Criminal Investigation

May have offensive actions against other entities

- Companies, individuals, groups, other nations
- Cold war alike, totalitarian governments, sovereignty

Today – Offensive Groups

Will conduct attacks against any other entity

- In ad-hoc or coordinated manner
- May have great amount of funds available
  - By economic groups or nations
- May act as a collective without strict coordination

Sometimes considered Advanced Persistent Threats (APT)

- Will develop attacks over the course of months or even years
- May keep control of an entity without being discovered

Motivations are many

- Hacktivism: Lulzsec, Anonymous, Antisec, (4chan?)
- Economic competition
- National Interest: APTs
- Cyberwar

Today – Criminal Groups

Frequently operate as a commercial company

- Business model
- Employees and other collaborators
- “User Support” (to help victims pay ransoms)
- Sometimes with publicity and public presence

Operate on several models

- May operate from countries which “ignore” them
  - And they will not attack systems on those countries
- For hire operations (other companies, nations)
- Directly targeting a broad user base, other companies
  - Focusing on specific areas (critical infrastructures, health, banking…)
- Provide malicious software as a service

Rich and dynamic software environment

- Software specifically developed for these activities
  - Exploring vulnerabilities in systems
  - Vulnerabilities are traded and are assets to incorporate when attacking systems
- May rely both on automated software and targeted software

Limiting factors

Cibersecurity is limited by economical, operational and logistical aspects

- All entities have limited resources

Cybersecurity deals with building and applying a strategy, with a limited budget, under a operational and legal context

http://targetedattacks.trendmicro.com/cyoa/en/