isep

École d'ingénieurs du numérique

Cybersecurity – II.2317 Lecture #1 – 09/10/23

Security Vulnerabilities, Threats, and Countermeasures

An Overview of Cybersecurity

Nouredine TAMANI – nouredine.tamani@isep.fr

What is cybersecurity?

- Definition 1 (source: Wikipedia)

  “**Computer security**, **cybersecurity** or **information technology security** (**IT security**) is the protection of computer systems and networks from the theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.”

- Definition 2 (source: Cisco)

  “**Cybersecurity** is the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes.”

Domains of the cybersecurity

Cybersecurity: 2 aspects and many domains

- Technical aspect: how to design and implement a cybersecurity policy?
  - Detect vulnerabilities
  - Design a security solution
  - Implement a security solution
  - Etc.

→ Courses II.2317 is aimed at introducing the technical aspects of the cybersecurity

- Management aspect: how to govern cybersecurity in an organization?
  - Security Policy definition
  - Management of changes
  - Risk management
  - BCP: Business Continuity Plan
  - Disaster recovery
  - Etc.

→Courses II.3519 considers more the management aspects than the technical aspects
Courses II.3524 about security in software engineering

Domains of Cybersecurity

- Network security
- Data and Database security
- Operating system security
- Application security
- Device and Mobile Device Management
- User authentication and Privileged Account Management
- Information Security Management
- Cryptology
- Etc.

What Law says? (1/3)

- The law punishes fraudulent activities on Information System
- Intrude a system may be pursued and is punishable regarding the law
- An attempt to access or to maintain fraudulently inside « data automated treatment systems » is law punishable
- French « Code Pénal » Rappel de la Loi (loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique ou Art 323-1 à 323-7 du CP)
  - « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni d'un an d'emprisonnement et de 15 000 euros d'amende »
  - « Lorsqu'il en résulte soit la suppression ou la modification de données continues dans le système, soit une altération du fonctionnement de ce système, la peine est de deux ans d'emprisonnement et de 30 000 euros d'amende.

Source: Jacky Lemée Cybersecurity courses

What Law says? (2/3)

- CHAPITRE III- Des atteintes aux systèmes de traitement automatisé de données
- **Article 323-2**: **Altering IS functions**
  - Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de trois ans d'emprisonnement et de 45 000 € d’amende.
- **Article 323-3: Introducing or altering data**
  - Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de trois ans d'emprisonnement et de 45 000 € d’amende.

Source: Jacky Lemée Cybersecurity courses

What Law says? (3/3)

- CHAPITRE III- Des atteintes aux systèmes de traitement automatisé de données
- **Art. 323-3-1: Be aware that possessing tools allowing such infractions may be pursued**
  - Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.
- **Article 323-4: Punishment increases when damage is issued from collaboration**
  - La participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou de plusieurs des infractions prévues par les articles 323-1 à 323-3 est punie des peines prévues pour l'infraction elle- même ou pour l'infraction la plus sévèrement réprimée.

Source: Jacky Lemée Cybersecurity courses

Objective - Consider ISS as a service for businesses

- **Security is an information system quality, among others.**
  - Security isn't an end by itself
  - But security contributes to establish customers and employees TRUST
- **Security must be presented as a returned service and not felt by actors like a constraint**
  - Security must be accepted by each of the concerned actors
  - Every security rule or recommendation must be accompanied
  - Its justification in order not to be rejected or by-passed
- **Laws and regulations are in the ISS scope**
  - IS conformity to laws and regulations must be shown as services for the trades/business.

Source: Jacky Lemée Cybersecurity courses

Objective- ISS as a risk management process

- **No 100% level of security ... but a calculated risk**
  - Security process analyses the risks
  - This means that risks are mastered
  - Un-mastered risks must be identified and accepted by involved IS owners.
  - Risk analysis purpose.
- **Risks are environment dependent and evolve during time**
  - Each company, organization, application has its specific stakes
  - IS becomes more and more risky exposed
    - accessible (to customers, partners, suppliers ...),
    - scattered between components, geographical sites, organizations (outsourcing, cloud computing ...)
    - vulnerable to new threats

Source: Jacky Lemée Cybersecurity courses

Objective- ISS: Processes and Policies

- How can we proceed, knowing that absolute security doesn’t exist ?
- Knowing that there isn’t universal solution to tackle security.
  - *“**Security is not a product ; it’s a process.** You can’t just add it to a system after the fact. It’s vital to understand the real threats to a system, design a **security policy** commensurate with those threats, and build in appropriate security countermeasures.”* Bruce Schneier, Secret and lies.
- **To be efficient the security approach must be supported by an action will, which means a POLICY**
  - To be applicable and applied by all company IS actors, the security policy must be promulgated by the highest hierarchy level

Source: Jacky Lemée Cybersecurity courses

Outline

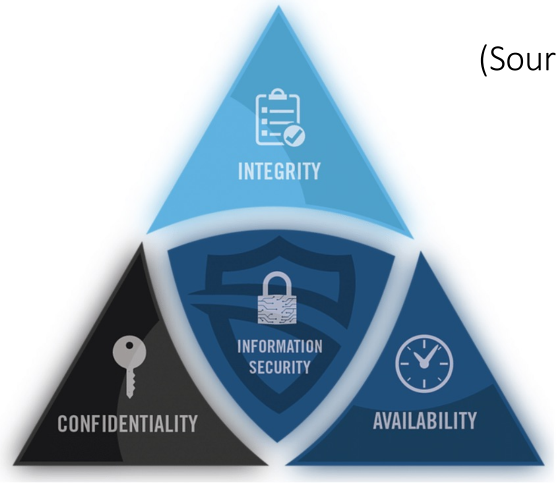
- Security Objectives: CIA Triad
- Security Concept: AAA
- Protection mechanisms / Protection controls
- Evaluate and Apply Security Governance Principles
- Threat Modeling Concepts and Methodologies
- Security Control Frameworks

CIA Triad

Confidentiality, Integrity and Availability

Security Objectives: CIA Triad

- Concept CIA Triad: Confidentiality, Integrity, and Availability



(Source: https://www.cloudskope.com/post/using-the-cia-for-better-data-security)

Figure 1. Information security with CIA triangle

- Security controls are typically evaluated on how well they address these 3 core information security tenets
- Complete security solution should adequately address each of these tenets
- Vulnerabilities and risks are also evaluated based on the threat they pose against one or more of the CIA Triad principles
- Symmetrical concepts: DAD for Disclosure, Alteration, Destruction

CIA: Confidentiality – definition

- Confidentiality ensures the protection of the secrecy of data, objects, or resources
- No one other than the intended recipient of a message receives it or can read it
- Only authorized users to access and interact with resources,
- But it prevents unauthorized users from doing so => disclosure

CIA: Confidentiality – risks and countermeasures

- Attacks on confidentiality:
  - capturing network traffic and stealing password files, social engineering, port scanning, shoulder surfing, eavesdropping, sniffing, escalation of privileges, etc.
- Unauthorized disclosure of sensitive or confidential information can also the result of human error, oversight, or ineptitude
- Events that lead to confidentiality breaches:
  - Failing to properly encrypt a transmission,
  - Failing to fully authenticate a remote system before transferring data,
  - Leaving open otherwise secured access points,
  - Accessing malicious code that opens a back door,
  - Misrouted faxes, documents left on printers,
  - Walking away from an access terminal while data is displayed on the monitor,
  - Actions of an end user or a system administrator,
  - An oversight in a security policy or a misconfigured security control.

CIA: Confidentiality – risks and countermeasures

- Countermeasures can help ensure confidentiality:
  - Encryption,
  - Network traffic padding:
    - adding additional data in the network traffic to make it more difficult to identify the sender, receiver, and/or the data being transmitted
  - Strict access control,
  - Rigorous authentication procedures,
  - Data classification:
    - Secret, confidential, private, public, etc.
  - Extensive personnel training.

CIA: Confidentiality – related concepts (1/2)

- **Sensitivity:** refers to the quality of information, which could cause harm or damage if disclosed.
- **Discretion:** is an act of decision where an operator can influence or control disclosure in order to minimize harm or damage.
- **Criticality:** the level to which information is mission critical. The higher the level of criticality, the more likely the need to maintain the confidentiality of the information.
- **Concealment:** is the act of hiding or preventing disclosure: a means of cover, obfuscation, or distraction.

  → A related concept: **security through obscurity**, which is the concept of attempting to gain protection through hiding, silence, or secrecy.

CIA: Confidentiality – related concepts (2/2)

- **Secrecy:** is the act of keeping something a secret or preventing the disclosure of information.
- **Privacy:** keeping information confidential that is personally identifiable or that might cause harm, embarrassment, or disgrace to someone if revealed.
- **Seclusion:** involves storing something in an out-of-the-way location. This location can also provide strict access controls.
- **Isolation:** is the act of keeping something separated from others.

CIA: Integrity – definition

- Integrity is the concept of protecting the reliability and correctness of data
- It prevents unauthorized alterations of data.
  - It ensures that data remains correct, unaltered, and preserved.
- Confidentiality and integrity depend on each other:
  - Without object integrity confidentiality cannot be maintained
- Integrity can be examined from 3 perspectives:
  - Preventing unauthorized subjects from making modifications
  - Preventing authorized subjects from making unauthorized modifications, such as mistakes
  - Maintaining the internal and external consistency of objects:
    - their data is a correct and true reflection of the real world and
    - any relationship with any object is valid, consistent, and verifiable

CIA: Integrity – risks and countermeasures

- Numerous attacks focus on the violation of integrity:
  - Viruses, logic bombs, unauthorized access, errors in coding and applications, malicious modification, intentional replacement, and system back doors.
  - As with confidentiality, human error, oversight, or ineptitude
- Events that lead to integrity breaches:
  - Modifying or deleting files
  - Entering invalid data
  - Altering configurations
  - Including errors in commands, codes, and scripts
  - Introducing a virus
  - Executing malicious code such as a Trojan horse

CIA: Integrity – risks and countermeasures

- Integrity violations can occur because of the actions of any user:
  - Administrators
  - An oversight in a security policy
  - A misconfigured security control
- Countermeasures can ensure integrity against possible threats:
  - Strict access control,
  - Rigorous authentication procedures,
  - Intrusion detection systems,
  - Object/data encryption, hash total verifications
  - Interface restrictions, input/function checks,
  - Extensive personnel training.

CIA: Integrity – related concepts

- **Accuracy**: Being correct and precise
- **Truthfulness**: Being a true reflection of reality
- **Authenticity**: Being authentic or genuine
- **Validity**: Being factually or logically sound
- **Nonrepudiation**: Not being able to deny having performed an action or activity or being able to verify the origin of a communication or event
- **Accountability**: Being responsible or obligated for actions and results
- **Responsibility**: Being in charge or having control over something or someone
- **Completeness**: Having all needed and necessary components or parts
- **Comprehensiveness**: Being complete in scope; the full inclusion of all needed elements

CIA: Availability – definition

- Availability: authorized subjects (user, software, etc.) are granted timely and uninterrupted access to objects (data, file, service, device, etc.)
  - Availability includes efficient uninterrupted access to objects
  - Prevention of denial-of-service (DoS) attacks
- Availability requires supporting infrastructure (network services, communications, etc.) to be:
  - Functional
  - Allows authorized users to gain authorized access
- Requirements to maintain Availability on a system:
  - Controls to ensure authorized access,
  - An acceptable level of performance,
  - Quickly handle interruptions,
  - Provide for redundancy,
  - Maintain reliable backups,
  - Prevent data loss or destruction.

CIA: Availability – risks and countermeasures

- Events that lead to Availability interruptions:
  - Device failure => Destruction,
  - Software errors,
  - Environmental issues (heat, static, flooding, power loss, and so on) => Destruction
  - DoS attacks,
  - Object destruction,
  - Communication interruptions.
- Events caused by human error, oversight, or ineptitude:
  - Human intervention,
  - Accidentally deleting files,
  - Overutilizing a hardware or software component,
  - Under-allocating resources and mislabeling or incorrectly classifying objects.
  - Administrators: an oversight in a security policy or a misconfigured security control.

CIA: Availability – risks and countermeasures

- Countermeasures:
  - Designing intermediary delivery systems properly, using access controls effectively,
  - Monitoring performance and network traffic, using firewalls and routers to prevent DoS attacks,
  - Implementing redundancy for critical systems,
  - Maintaining and testing backup systems.
  - Train the personnel
  - Use of fault tolerance features at the various levels of access/storage/security

    → the goal of eliminating single points of failure to maintain availability of critical systems.

CIA: Availability – related concepts

- Availability depends on both integrity and confidentiality:
  - Without integrity and confidentiality, availability cannot be maintained
- **Usability**:

  The state of being easy to use or learn or being able to be understood and controlled by a subject,
- **Accessibility**:

  The assurance that the widest range of subjects can interact with a resource regardless of their capabilities or limitations
- **Timeliness**:

  Being prompt, on time, within a reasonable time frame, or providing low-latency response.

Recommendations (1/2)

- Unfortunately, in the real world, general concepts and best practices don’t get the job done
- The management team and security team must work together to prioritize an organization’s security needs
- This includes:
  - Establishing a budget and spending plan,
  - Allocating expertise and hours,
  - Focusing the information technology (IT) and security staff efforts.

Recommendations (2/2)

- Prioritize the security requirements of the organization:
  - Establishing priorities is a challenge
  - A possible solution is to start with prioritizing: confidentiality, integrity, and availability
- This establishes a pattern that can be replicated from concept through:
  - Design, architecture, deployment, and maintenance.

Other security concepts: AAA

- Concept AAA: **authentication**, **authorization**, and **accounting**
- Refers to 5 elements: **identification**, **authentication**, **authorization**, **auditing**, and **accounting** :
- **Identification**: Claiming to be an identity when attempting to access a secured area or system
- **Authentication**: Proving that you are that identity
- **Authorization**: Defining the permissions (i.e., allow/grant and/or deny) of a resource and object access for a specific identity
- **Auditing**: Recording a log of the events and activities related to the system and subjects
- **Accounting** (aka **accountability**): Reviewing log files to check for compliance and violations in order to hold subjects accountable for their actions

Other security concepts: AAA

- Although AAA is typically referenced in relation to authentication systems, it is a foundational concept for security
- Missing any of these five elements can result in an incomplete security mechanism

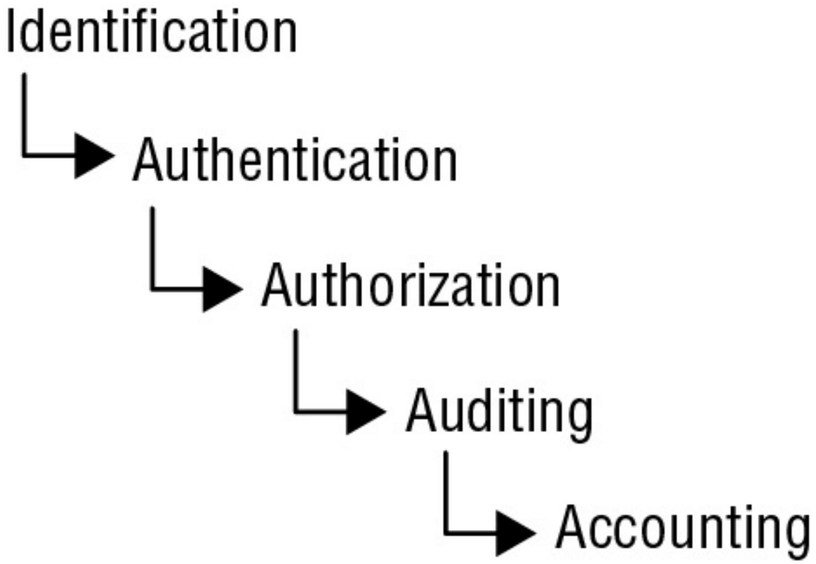


Figure 2. The five elements of AAA services.

I4A: Identification

- **Identification** is the process by which a subject professes an identity
- A subject must provide an identity to a system to start the process of authentication, authorization, and accountability (AAA):
  - Typing in a username
  - Swiping a smart card
  - Waving a proximity device
  - Speaking a phrase
  - Positioning your face, hand, or finger for a camera or scanning device
- Providing a process ID number also represents the identification process
- Without an identity, a system has no way to correlate an authentication factor with the subject

I4A: Identification

- Once a subject has been identified, the identity is accountable for any further actions by that subject
- A subject’s identity is typically labeled as public information
- The identity must be proven (authentication) or verified (ensuring nonrepudiation) before access to controlled resources is allowed (verifying authorization)
- That process is authentication

I4A: Authentication

- **Authentication**: the process of verifying or testing that the claimed identity is valid is authentication
- Authentication requires the subject to provide additional information that corresponds to the identity they are claiming
- The most common form of authentication is using a password

  → this includes the password variations of personal identification numbers (PINs) and passphrases.
- Authentication verifies the identity of the subject by comparing one or more factors against the database of valid identities (user accounts)

I4A: Authentication

- The authentication factor used to verify identity is typically labeled as, or considered to be, private information
- **Level of security of a system**: The capability of the subject and system to maintain the secrecy of the authentication factors for identities
- Insecure authentication system: If the process of illegitimately obtaining and using the authentication factor of a target user is relatively easy
- If that process is relatively difficult, then the authentication system is reasonably secure.

I4A: Authentication

- **Identification** and authentication are often used together as a single two-step process
- Providing an identity is the first step and providing the authentication factors is the second step
- In some systems, it may seem as you are providing only one element and gaining access such as when keying in an ID code or a PIN:
  - However, either the identification is handled by another means (physical location), or authentication is assumed by your ability to access the system physically.
  - Both identification and authentication take place, but you might not be as aware of them as when you manually type in both a name and a password.

I4A: Authentication

- A subject can provide several types of authentication:
  - Something you know (e.g., passwords, PINs),
  - Something you have (e.g., keys, tokens, smart cards),
  - Something you are (e.g., biometrics, such as fingerprints, iris, or voice recognition),…
- Each authentication technique or factor has its unique benefits and drawbacks.
- (authentication will be studied in a dedicated lecture)

I4A: Authorization

- **Authorization** ensures that the requested activity or access to an object is possible given the rights and privileges assigned to the authenticated identity
- Once a subject is authenticated, access must be authorized
- In most cases, the system evaluates an access control matrix that compares the subject, the object, and the intended activity
  - If the specific action is allowed, the subject is authorized
  - If the specific action is not allowed, the subject is not authorized
- Just because a subject has been identified and authenticated (logged on) does not mean:
  - They have been authorized to perform any function or
  - Access all resources within the controlled environment

I4A: Authorization

- Example: It is possible for a subject to be logged onto a network but to be blocked from accessing a file or printing to a printer
- Identification and authentication are all-or-nothing aspects of access control
- Authorization has a wide range of variations between all or nothing for each object within the environment:
  - A user may be able to read a file but not delete it,
  - Print a document but not alter the print queue,
  - Log on to a system but not access any resources.
- Authorization is usually defined using one of the models of access control:
  - Discretionary Access Control (DAC),
  - Mandatory Access Control (MAC),
  - Role Based Access Control (RBAC or role-BAC).

I4A: Auditing

- **Auditing**, or monitoring, is the programmatic means by which a subject’s actions are tracked and recorded
- It is also the process by which unauthorized or abnormal activities are detected on a system
- Auditing is recording activities:
  - Subject and its objects
  - Core system functions that maintain the operating environment and the security mechanisms
- System crashes may indicate faulty programs, corrupt drivers, or intrusion attempts
- The event logs leading up to a crash can often be used to discover the reason a system failed

I4A: Auditing

- Log files provide an audit trail for re-creating the history of an event, intrusion, or system failure
- Auditing is needed to detect:
  - Malicious actions by subjects
  - Attempted intrusions
  - System failures
- Auditing is needed to:
  - Reconstruct events
  - Provide evidence for prosecution
  - Produce problem reports and analysis
- Auditing is usually a native feature of operating systems and most applications and services:
  - Configuring the system to record information about specific types of events is straightforward

I4A: Auditing

- Monitoring is part of what is needed for audits, and audit logs are part of a monitoring system, but the two terms have different meanings
- Monitoring is a type of watching, while auditing is a recording of the information into a record or file
- It is possible to monitor without auditing:
  - We can't audit without some form of monitoring,
  - These terms are often used interchangeably is some scientific literature

I4A: Accountability

- An organization’s security policy can be properly enforced only if accountability is maintained
- Effective accountability relies on the ability to prove a subject’s identity and track their activities
- Accountability is established by linking a human to activities:
  - **Online identity** through the security services and mechanisms of auditing, authorization, authentication, and identification
- Human accountability ultimately dependents on the strength of the authentication process:
  - Without a strong authentication process, there is a doubt that the human associated with a specific user account was the actual entity controlling that user account when the undesired action took place

I4A: Accountability

- To have viable accountability:
  - We may need to be able to support security decisions and their implementation in a court of law,
  - If an organization is unable to legally support its security efforts, then it will be unable to hold a human accountable for actions linked to a user account,
  - With only a password as authentication, there is significant room for doubt.
- Passwords are the least secure form of authentication
  - Dozens of different methods available to compromise them
- to reduce the risk of compromising an authentication process, we can use multifactor authentication:
  - Password, smartcard, and fingerprint scan in combination

Control mechanisms

Protection mechanisms / Protection controls

Protection mechanisms / Protection controls

- Protection mechanisms:
  - Layering / level of access
  - Abstraction
  - Data hiding
  - Encryption
- Not all *security controls* must have them
- But many controls offer their protection for confidentiality, integrity, and availability using these mechanisms

Protection mechanism: Layering

- Layering, aka defense in depth, is the use of multiple controls in a series
- Using layers in a series rather than in parallel is important:
  - Performing in a series means to perform one after the other in a linear way,
  - Each attack will be scanned, evaluated, or mitigated by every security control,
  - Failure of a single security control does not render the entire solution ineffective,
  - If security controls were implemented in parallel, a threat could pass through a single checkpoint that did not address its malicious activity.
- Serial configurations are very narrow but very deep, whereas parallel configurations are very wide but very shallow
- Parallel systems are useful in distributed computing applications,
  - Parallelism is not often a useful concept in the realm of security.

Protection mechanism: Layering

- **Example: physical entrances to buildings.**
  - A parallel configuration is used for shopping malls,
  - A series configuration would most likely be used in a bank or an airport,
- Layering also includes the fact that networks comprise several separate entities:
  - Each with its own unique security controls and vulnerabilities
- In an effective security solution, there is a synergy between all networked systems that creates a single security front
- Using separate security systems creates a layered security solution

Protection mechanism: Abstraction

- **Abstraction** consists in:
  - Putting similar elements into groups, classes, or roles that are assigned security controls, restrictions, or permissions as a collective
  - Classifying objects or assigning roles to subjects
- The definition of object and subject types
  - (it is like a data structure used to define a template for a class of entities)
- Abstraction is used to define:
  - What types of data an object can contain,
  - What types of functions can be performed on or by that object,
  - What capabilities that object has.
- Abstraction simplifies security by enabling the user to assign security controls to a group of objects collected by type or function

Protection mechanism: Data hiding

- Data hiding is exactly what it sounds like:
  - Preventing data from being discovered or accessed by a subject
  - Positioning data in a logical storage compartment that is not accessible or seen by the subject
- Forms of data hiding include:
  - Keeping a database from being accessed by unauthorized visitors
  - Restricting a subject at a lower classification level from accessing data at a higher classification level
  - Preventing an application from accessing hardware directly is also a form of data hiding

Protection mechanism: Data hiding

- Do not confuse with the term security through obscurity:
  - Data hiding is the act of intentionally positioning data so that it is not viewable or accessible to an unauthorized subject
  - Security through obscurity is the idea of not informing a subject about an object being present
- Security through obscurity does not implement any form of protection
  - It is instead an attempt to hope something important is not discovered by keeping knowledge of it a secret
- Examples:
  - When a programmer is aware of a flaw in their software code, but they release the product anyway hoping that no one discovers the issue and exploits it
  - When you hide the SSID of your WIFI Access Point

Protection mechanism: Encryption

- Encryption is the art and science of hiding the meaning or intent of a communication from unintended recipients
- Encryption can take many forms and be applied to every type of electronic communication
- Encryption is an important element in security controls, especially regarding the transmission of data between systems
- There are various strengths of encryption, each of which is designed and/or appropriate for a specific use or purpose
- Encryption is discussed in a dedicated lecture about “Cryptology”

Evaluate and Apply Security Governance Principles

Security Governance

Security Management Planning

Organizational Processes

Organizational Roles and responsibilities

Security Governance

- **Security governance** is the collection of practices related to supporting, defining, and directing the security efforts of an organization
- Security governance principles are often closely related to (and often intertwined) with corporate and IT governance
- The common goal of governance is to maintain business processes while striving toward growth and resiliency
- Some aspects of governance are imposed on organizations:
  - →due to legislative and regulatory compliance needs
  - →imposed by industry guidelines or license requirements

Security Governance

- All forms of governance, including security governance, must be assessed and verified from time to time
- Governance compliance issues often vary from industry to industry and from country to country
- The organization should be given the direction, guidance, and tools to provide sufficient oversight and management:
  - Address threats and risks with a focus on eliminating downtime and keeping potential loss or damage to a minimum.

Security Governance

- **Ultimately, security governance is the implementation of a security solution and a management method that are tightly interconnected**
- Security is not and should not be treated as an IT issue only:
  - Security affects every aspect of an organization
  - No longer just something the IT staff can handle on their own

    → Security is a business operations issue
- Security is an organizational process, not just something the IT geeks do behind the scenes

Security management planning: definition

- Security management planning ensures proper creation, implementation, and enforcement of a security policy.
- It aligns the security functions to the strategy, goals, mission, and objectives of the organization
- Two possible approaches to tackle security management planning:
  - **The top-down approach**
  - **The bottom-up approach**

Security management planning: approaches

- The top-down approach:
  - **Upper, or senior, management** is responsible for initiating and defining policies for the organization,
  - It is the responsibility of **middle management** to flesh out the security policy into standards, baselines, guidelines, and procedures,
  - The **operational managers** or security professionals must then implement the configurations prescribed in the security management documentation,
  - Finally, the **end users** must comply with all the security policies of the organization.
- The bottom-up approach:
  - The IT staff makes security decisions directly without input from senior management,
  - The bottom-up approach is rarely used in organizations,
  - It is considered problematic in the IT industry.

Security management planning: rules

- Security management is a responsibility of upper management, not of the IT staff
- Security management is considered an issue of business operations rather than IT administration
- The team or department responsible for security within an organization should be autonomous
- The information security (InfoSec) team should be led by a designated chief information security officer (CISO)
- CISO must report directly to senior management

Security management planning: Plans

A security management planning team should develop three types of plans, as shown in Figure 3.

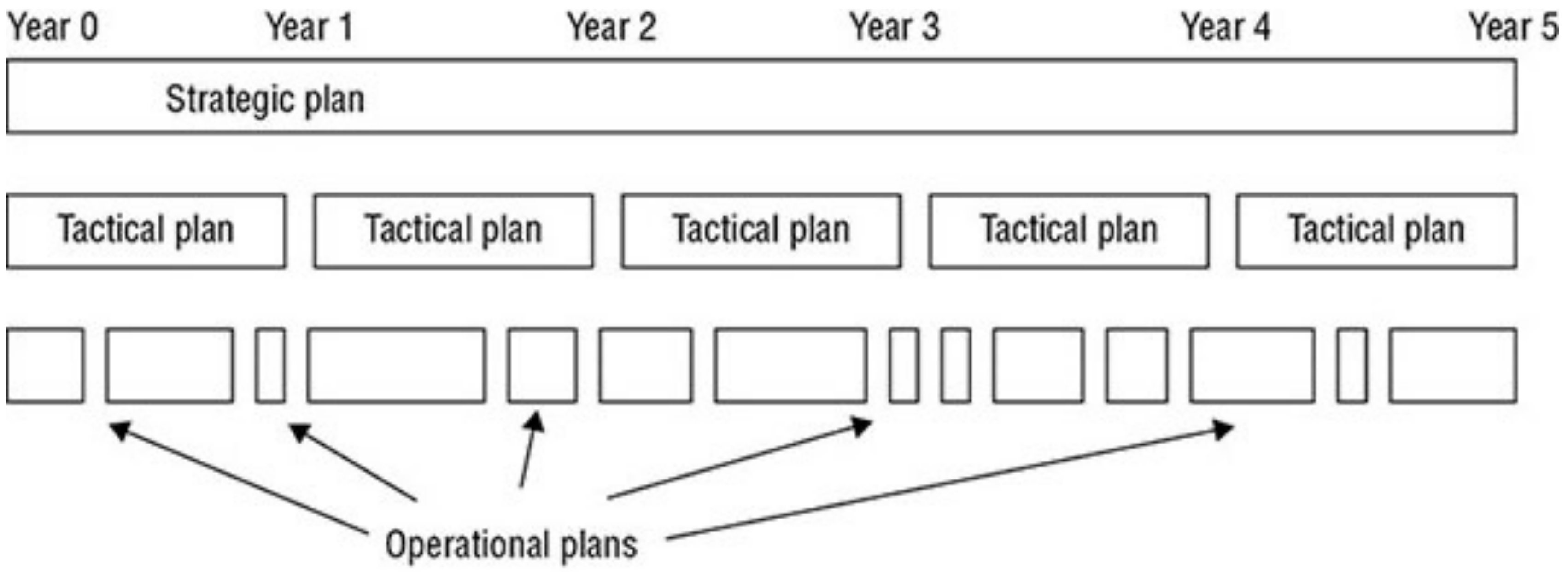


Figure 3. Strategic, tactical, and operational plan timeline comparison

Security management planning: Strategic Plan

Strategic Plan

- A strategic plan is a long-term stable plan
- It defines the organization's security purpose
- It also helps understand security functions and align it to the goals, mission, and objectives of the organization
- It's useful for about 5 years if it is maintained and updated annually
- It serves as the planning horizon:
  - Long-term goals and visions for the future are discussed in a strategic plan
  - A strategic plan should include a risk assessment

Security management planning: Tactical Plan

Tactical Plan:

- The tactical plan is a midterm plan developed to:
  - Provide more details on accomplishing the goals set forth in the strategic plan,
  - Can be crafted ad hoc based upon unpredicted events.
- It is typically useful for about a year and often prescribes and schedules the tasks necessary to accomplish organizational goals
- **Examples:**
  - Project plans, acquisition plans, hiring plans, budget plans, maintenance plans, support plans, and system development plans.

Security management planning: Operational Plan

Operational Plan:

- An operational plan is a short-term
- Operational plans must be updated often (such as monthly or quarterly) to retain compliance with tactical plans
- Operational plans spell out how to accomplish the various goals of the organization
  - Resource allotments, budgetary requirements, staffing assignments, scheduling, and step-by-step or implementation procedures.
- Operational plans also include details on how the implementation processes follow the organization's security policy

Organizational Processes: Change Management

- Two additional examples of organizational processes that are essential to strong security governance are:
  - change control/change management
  - data classification.
- The goal of change management:
  - Ensure that any change does not lead to reduced or compromised security
  - Making it possible to roll back any change to a previous secured state
  - It can be implemented on any system despite the level of security
  - It improves the security of an environment by protecting implemented security from unintentional, tangential, or affected reductions in security
  - Make all changes subject to detailed documentation and auditing and thus able to be reviewed and scrutinized by management.

Organizational Processes: Change Management

- Change management should be used to oversee alterations to every aspect of a system:
  - Hardware configuration
  - Operating system (OS)
  - Application software
- Change management should be included in design, development, testing, evaluation, implementation, distribution, evolution, growth, ongoing operation, and modification.
- It requires a detailed inventory of every component and configuration
- It also requires the collection and maintenance of complete documentation for every system component

Organizational Processes: Change Management

- An example of a change management process is a parallel run:
  - A type of new system deployment testing where the new system and the old system are run in parallel
  - Each major or significant user process is performed on each system simultaneously
  - Ensure that the new system supports all required business functionality that the old system supported or provided

Organizational Roles and Responsibilities

- A security role is the part an individual plays in the overall scheme of security implementation and administration within an organization
- Security roles are not necessarily prescribed in job descriptions because they are not always distinct or static
- 6 roles are presented in the logical order in which they appear in a secured environment:
  - Senior Manager
  - Security Professional
  - Data Owner
  - Data Custodian
  - User
  - Auditor

Organizational Roles and Responsibilities: Senior Manager

- **Senior Manager:**
  - The organizational owner (senior manager) role is assigned to the person:
    - Who is responsible for the security maintained by an organization and
    - Whos should be most concerned about the protection of its assets.
  - All activities must be approved by and signed off on by the senior manager before they can be carried out
  - It indicates the accepted ownership of the implemented security within the organization
  - The senior manager is the person who:
    - Held liable for the overall success or failure of a security solution and
    - Is responsible for exercising due care and due diligence in establishing security for an organization.
  - Even though senior managers are ultimately responsible for security, they rarely implement security solutions

Organizational Roles and Responsibilities: Security Professional

- **Security Professional (**IS/IT function role)**:**
  - Information security (InfoSec) officer, or computer incident response team (CIRT) role is assigned to a trained and experienced network, systems, and security engineer:
  - Functional responsibility for security: writing the security policy and implementing it
  - The security professional role is often filled by a team that is responsible for designing and implementing security solutions based on the approved security policy
  - Security professionals are not decision makers: they are implementer
  - All decisions must be left to the senior manager

Organizational Roles and Responsibilities: Data Owner

- **Data Owner:**
  - The data owner role is assigned to the person who is responsible for classifying information for placement and protection within the security solution
  - The data owner is typically a high-level manager who is ultimately responsible for data protection
  - The data owner usually delegates the responsibility of the actual data management tasks to a data custodian

Organizational Roles and Responsibilities: Data Custodian

- **Data Custodian:**
  - This role is assigned to the user who is responsible for implementing the prescribed protection defined by the security policy and senior management
  - The data custodian performs all activities necessary to provide adequate protection for the CIA Triad of data:
    - Performing and testing backups,
    - Validating data integrity,
    - Deploying security solutions,
    - Managing data storage based on classification.

Organizational Roles and Responsibilities: User

- User:
  - The user (end user or operator) role is assigned to any person who has access to the secured system
  - Users have only enough access to perform the tasks necessary for their job position (the principle of least privilege)
  - Users are responsible for understanding and upholding the security policy of an organization:
    - Following prescribed operational procedures
    - Operating within defined security parameters

Organizational Roles and Responsibilities: Auditor

- Auditor:
  - An auditor is responsible for reviewing and verifying that the security policy is properly implemented, and the derived security solutions are adequate
  - The auditor produces compliance and effectiveness reports that are reviewed by the senior manager
  - Issues discovered through these reports are transformed into new directives
  - These directives are assigned by the senior manager to security professionals or data custodians
  - The auditor is listed as the final role because the auditor needs a source of activity (users/operators working in an environment) to audit or monitor

Security Control Frameworks

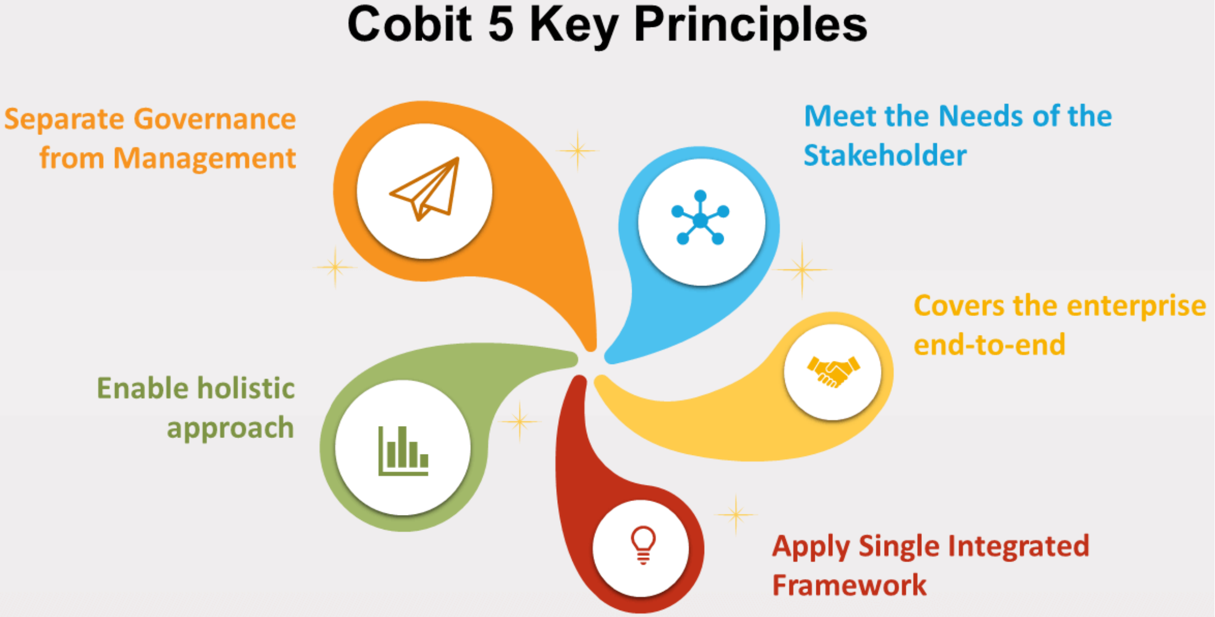
Standards and Guidelines for IT security

Security Control Frameworks

- Defines the structure of the security solution desired by the organization
- Several options for security concept infrastructure, but COBIT is the more widely used
- COBIT: **C**ontrol **Ob**jectives for **I**nformation and Related **T**echnology (COBIT)
- COBIT is a documented set of best IT security practices crafted by the Information Systems Audit and Control Association (ISACA)
- It prescribes goals and requirements for security controls
- It encourages the mapping of IT security ideals to business objectives

Security Control Frameworks

- COBIT 5 is based on 5 key principles for governance and management of enterprise IT:
  - **Principle 1**: Meeting Stakeholder Needs
  - **Principle 2**: Covering the Enterprise End-to-End
  - **Principle 3**: Applying a Single, Integrated Framework
  - **Principle 4**: Enabling a Holistic Approach
  - **Principle 5**: Separating Governance From Management

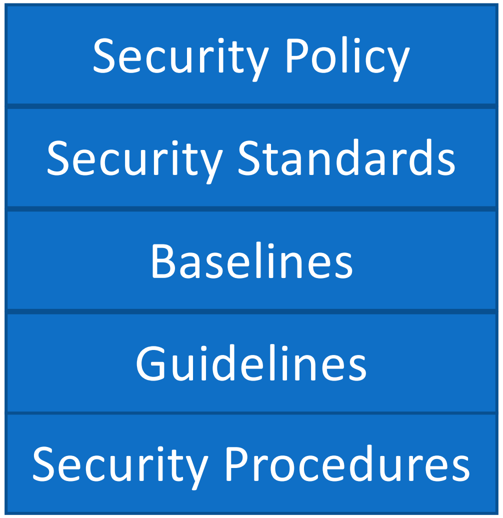

Cobit 5 Key Principles
Separate Governance from Management
Meet the Needs of the Stakeholder
Covers the enterprise end-to-end
Enable holistic approach
Apply Single Integrated Framework

Security Control Frameworks

- COBIT is used:
  - To plan the IT security of an organization
  - Guideline for auditors.
- For more details on COBIT: visit the ISACA website (www.isaca.org)
- There are many other standards and guidelines for IT security: (lecture)
  - **Open-Source Security Testing Methodology Manual (OSSTMM)** (www.isecom.org/research/)
  - **ISO/IEC 27002** (which replaced ISO 17799) (https://www.iso.org/standard/54533.html):
    - An international standard that can be the basis of implementing organizational security and related management practices
  - **Information Technology Infrastructure Library (ITIL)** (www.itlibrary.org):
    - Initially crafted by the British government, ITIL is a set of recommended best practices for core IT security and operational processes and
    - Often used as a starting point for the crafting of a customized IT security solution

Develop, Document, and Implement Security Policy

- Formalized process of implementing security
  - Reduce the likelihood of a security failure
  - Reduce the chaos and complexity of designing and implementing security solutions for IT infrastructures
- Format: a hierarchical organization of documentation
  - Each level focuses on a specific type or category of information and issues
- Objective: produce a solid and reliable security infrastructure



Security Policy

Security Standards

Baselines

Guidelines

Security Procedures

Security formalization: Security Policy

- The top of the formalization
- It defines:
  - The scope of security needed by the organization,
  - Discusses the assets that require protection,
  - The extent to which security solutions should go to provide the necessary protection.,
  - Relevant terminology

  ➔ Main security objectives and outlines the security framework of an organization
- Identifies the major functional areas of data processing
- Strategic plan for implementing security

Security formalization: Security Policy

- The security policy is used to:
  - Assign responsibilities,
  - Define roles,
  - Specify audit requirements,
  - Outline enforcement processes,
  - Indicate compliance requirements,
  - Define acceptable risk levels.
- This document is used as the <u>proof that senior management</u> has exercised <u>due care</u> in protecting itself against intrusion, attack, and disaster.
- Security policies are compulsory

Security formalization: Security Policy

- A system-specific security policy:
  - Focuses on individual systems or types of systems,
  - Prescribes approved hardware and software,
  - Outlines methods for locking down a system, and even
  - Mandates firewall or other specific security controls.
- In addition, there are 3 categories of security policies:
  - Regulatory: industry or legal standards, regulation to be compliance with.
  - Advisory: senior management’s desires for security and compliance within an organization.
  - Informative: information or knowledge (support, research, or background information) about a specific subject

Security formalization: Security Standards

- Standards define compulsory requirements for the homogenous use of hardware, software, technology, and security controls
- They provide a course of action by which technology and procedures are uniformly implemented throughout an organization
- Tactical documents that define steps to accomplish the goals and overall direction defined by security policies

Security formalization: Baselines

- A baseline defines a minimum level of security that every system throughout the organization must meet
- A baseline is a more operationally focused form of a standard
- goals of a security policy + requirements of the standards => rules against which to implement and compare IT systems
  - All systems not complying with the baseline should be taken out of production until they can be brought up to the baseline

Security formalization: Baselines

- Baselines are usually system specific and often refer to an industry or government standard:
  - Trusted Computer System Evaluation Criteria (TCSEC)
  - Information Technology Security Evaluation and Criteria (ITSEC)
  - NIST (National Institute of Standards and Technology) standards → USA
  - ANSSI (Agence Nationale de la Sécurité des Système d'Information) → France

Security formalization: Guidelines

- A guideline:
  - Offers recommendations on how standards and baselines are implemented,
  - Serves as an operational guide for both security professionals and users.
- Guidelines are flexible:
  - Can be customized for each unique system or condition and
  - Can be used in the creation of new procedures.
- They state which security mechanisms should be deployed
  - Instead of prescribing a specific product or control and detailing configuration settings
- They are not compulsory

Security formalization: Security Procedures

- A procedure or Standard Operating Procedure (SOP):
  - Detailed, step-by-step, how-to document
  - Describes the exact actions necessary to implement a specific security mechanism, control, or solution
- A procedure discuss the entire system deployment operation or focus on a single product or aspect (device, software, etc.)
- In most cases, procedures are system and software specific
- They must be updated as the hardware and software of a system evolve
- <u>The purpose of a procedure is to ensure the integrity of business processes</u>

Security formalization: Security Procedures

- Following a detailed procedure ➔ all activities follow policies, standards, and guidelines
- Procedures help ensure standardization of security across all systems
- Policies, standards, baselines, guidelines, and procedures should not be developed as an afterthought at the urging of a consultant or auditor
- These documents should be used and updated frequently
- Without planning, design, structure, and oversight provided by these documents, no environment will remain secure

Security formalization: Security Procedures

- Common mistake: develop a single document containing aspects of all these elements
- At the top of the formalization security policy documentation structure there are fewer documents

  → They contain general broad discussions of overview and goals
- There are more documents further down the formalization structure (guidelines and procedures)

  → They contain details specific to a limited number of systems, networks, divisions, and areas

Security Framework: some recommendations

- Keeping these documents as separate entities
- Not all users need to know the security standards, baselines, guidelines, and procedures for all security classification levels
- When changes occur, it is easier to update and redistribute only the affected material
- A security policy should not be an afterthought but a key part of establishing an organization

Security Framework: some recommendations

- The dependencies among the components: policies, standards, guidelines, and procedures
- The inverted pyramid is used to convey the volume or size of each of these documents

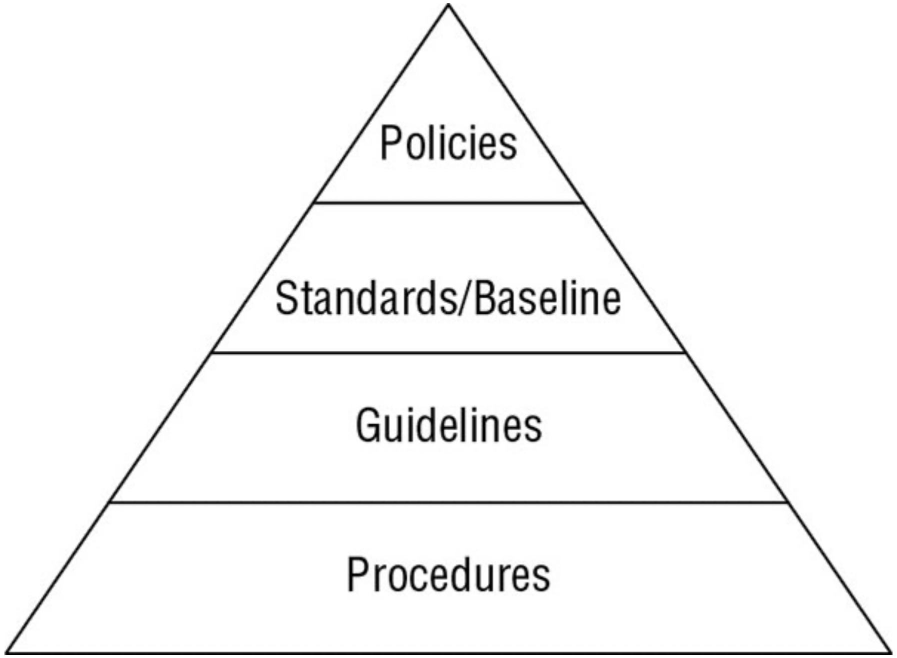


FIGURE 4 The comparative relationships of security policy components.

Threat Modeling Concepts and Methodologies

- Threat modeling is the security process where potential threats are identified, categorized, and analyzed
- Threat modeling can be performed:
  - Proactive measure during design and development,
  - Reactive measure once a product has been deployed.
- In either case, the process identifies:
  - Potential harm,
  - Probability of occurrence,
  - Priority of concern,
  - Means to eradicate or reduce the threat.
- Threat modeling isn’t meant to be a single event

Threat Modeling Concepts and Methodologies

- Threat modeling attempts to reduce vulnerabilities and reduce the impact of any vulnerabilities that remain
- It begins early in the design process of a system and continue throughout its lifecycle:
  - Microsoft uses a Security Development Lifecycle (SDL) process to implement security at each stage of a product's development
- "Secure by Design, Secure by Default, Secure in Deployment and Communication" (SD3+C)
- This process has two goals:
  - To reduce the number of security-related design and coding defects
  - To reduce the severity of any remaining defects
- The overall result is reduced risk

Threat Modeling Concepts and Methodologies

Proactive approach or a defensive approach **:**

- It takes place during the early stages of systems development
- It is based on predicting threats and designing specific defenses during the coding and crafting process
- Integrated security solutions are more cost effective and more successful than those shoehorned in later
- Unfortunately, not all threats can be predicted during the design phase

Threat Modeling Concepts and Methodologies

Reactive approach:

- It takes place after a product has been created and deployed
- This deployment could be in a test or laboratory environment or to the general marketplace
- This type of threat modeling is also known as the adversarial approach
- The core concept behind *ethical hacking, penetration testing, source code review, and fuzz testing*
- Benefits: finding flaws and threats
- Inconvenient: additional effort in coding to add in new countermeasures

Threat Modeling Concepts and Methodologies

Identifying Threats:

- There’s an almost infinite possibility of threats,
- It’s important to use a structured approach to accurately identify relevant threats
- Example: some organizations use one or more of the following 3 approaches:
  - Focused on Assets
  - Focused on Attackers
  - Focused on Software

Threat Modeling Concepts and Methodologies

Identifying Threats – Focus on Assets:

- Uses asset valuation results and attempts to identify threats to the valuable assets
- If the asset hosts data:

  Access controls can be evaluated to identify threats that can bypass authentication or authorization mechanisms

Threat Modeling Concepts and Methodologies

Identifying Threats – Focus on Attackers:

- Identifying potential attackers and the threats they represent based on the attacker's goals
- An organization can then use this knowledge to identify and protect its relevant assets
- Challenge of this approach: new attackers can appear that weren't previously considered a threat

Threat Modeling Concepts and Methodologies

Identifying Threats – Focus on Software:

- If an organization develops software, it can consider potential threats against the software
- Some organizations develop their own software (Web site for example)
- Fancy web pages drive more traffic, but they also require more sophisticated programming and present additional threats.

Threat Modeling Concepts and Methodologies

Threat Modeling: Threat Categorization

- Once threats are identified, they are categorized based on their goals or motivations
- Additionally, it's common to pair threats with vulnerabilities to identify threats
- A goal of threat modeling is to prioritize the potential threats against an organization's valuable assets
- When attempting to inventory and categorize threats, it is often helpful to use a guide or reference

Apply Threat Modeling Concepts and Methodologies

Threat Modeling: Threat Categorization STRIDE

- Microsoft developed a threat categorization scheme known as the STRIDE threat model
- STRIDE is an acronym standing for the following:
  - **Spoofing** (false identity), **Tampering** (falsify data), **Repudiation** (denying actions), **Information disclosure** (revealing confidential information), **Denial of service** (prevent an authorized action), and **Elevation of privilege** (get admin privileges for a limited user)
- STRIDE is often used in relation to assessing threats against applications or operating systems
- STRIDE is applicable to other situations:
  - Network threats
  - Host threats

Apply Threat Modeling Concepts and Methodologies: PASTA

- PASTA: Process for Attack Simulation and Threat Analysis is a 7-stage threat modeling methodology
- PASTA is a risk-centric approach that aims at selecting or developing countermeasures in relation to the value of the assets to be protected
- The following are the seven steps of PASTA:
  - Stage I: Definition of the Objectives (DO) for the Analysis of Risks
  - Stage II: Definition of the Technical Scope (DTS)
  - Stage III: Application Decomposition and Analysis (ADA)
  - Stage IV: Threat Analysis (TA)
  - Stage V: Weakness and Vulnerability Analysis (WVA)
  - Stage VI: Attack Modeling & Simulation (AMS)
  - Stage VII: Risk Analysis & Management (RAM)

Apply Threat Modeling Concepts and Methodologies: PASTA

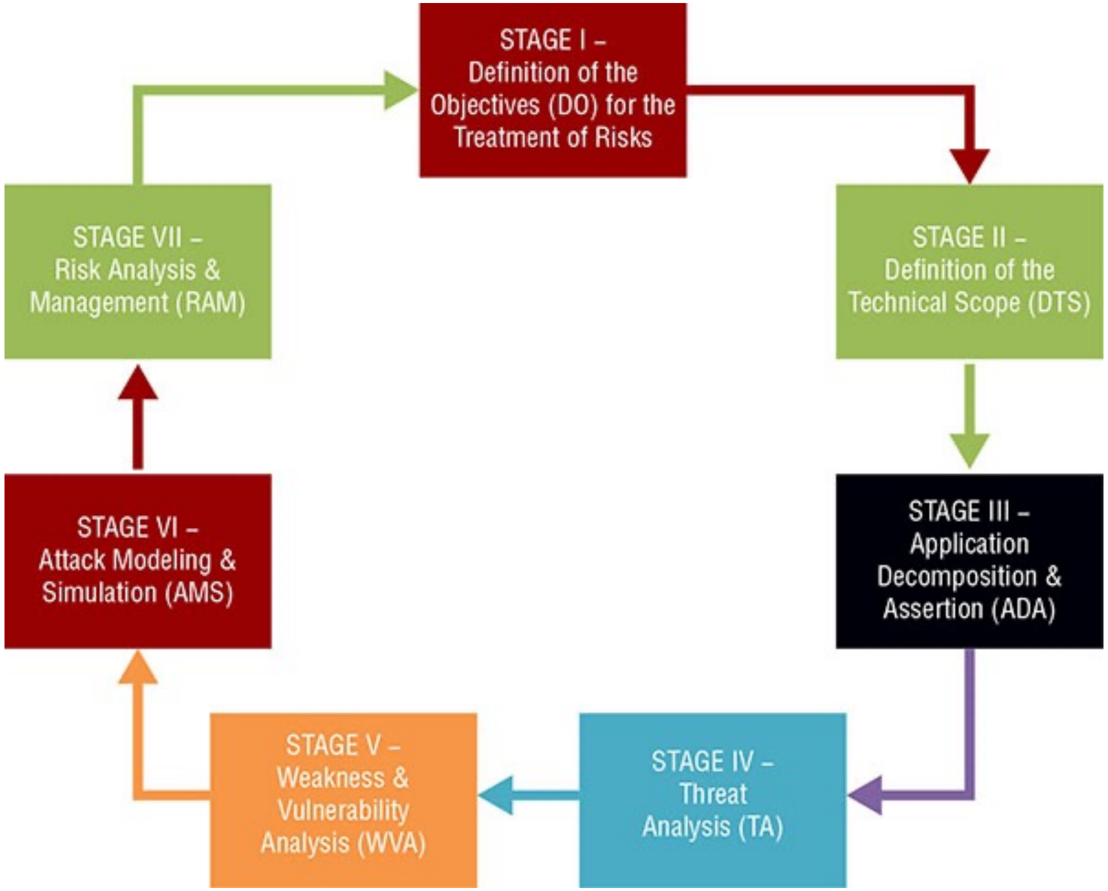

STAGE I – Definition of the Objectives (DO) for the Treatment of Risks
STAGE II – Definition of the Technical Scope (DTS)
STAGE III – Application Decomposition & Assertion (ADA)
STAGE IV – Threat Analysis (TA)
STAGE V – Weakness & Vulnerability Analysis (WVA)
STAGE VI – Attack Modeling & Simulation (AMS)
STAGE VII – Risk Analysis & Management (RAM)

FIGURE 5. An example of diagramming to reveal threat concerns.

- Each stage of PASTA has a specific list of objectives to achieve and deliverables to produce to complete the stage
- For more information on PASTA:
  - **Risk Centric Threat Modeling**: Process for Attack Simulation and Threat Analysis, first edition, by Tony UcedaVelez and Marco M. Morana.

Apply Threat Modeling Concepts and Methodologies: Trike

- Trike is another threat modeling methodology that focuses on a risk-based approach
- Trike provides:
  - A method of performing a security audit in a reliable and repeatable procedure
  - A consistent framework for communication and collaboration among security workers
- Trike is used to craft an assessment of an acceptable level of risk for each class of asset
- Acceptable level of risk is then used to determine appropriate risk response actions

Apply Threat Modeling Concepts and Methodologies: VAST

- Visual, Agile, and Simple Threat (VAST) is a threat modeling concept based on Agile project management and programming principles
- The goal of VAST is to integrate threat and risk management into an Agile programming environment on a scalable basis

Apply Threat Modeling Concepts and Methodologies

- The purpose of threat modeling methodologies is:
  - To consider the range of compromise concerns
  - To focus on the goal or end results of an attack
- Attempting to identify every specific attack method and technique is an impossible task

  → New attacks are being developed constantly

Apply Threat Modeling Concepts and Methodologies: Individual Threats

- Be Alert for Individual Threats
- Competition is often a key part of business growth:
  - Adversarial competition can increase the threat level from individuals
  - Disgruntled employees, adversaries, contractors, employees, even trusted partners
- Never assume that a consultant or contractor has the same loyalty to your organization as a long-term employee
- Don’t take employee loyalty for granted either
  - Employees who are frustrated with their working environment or feel they’ve been treated unfairly may attempt to retaliate
  - An employee experiencing financial hardship may consider unethical and illegal activities

Apply Threat Modeling Concepts and Methodologies: Diagramming

- Determining and diagramming potential attacks
- The creation of a diagram of the elements involved in a transaction along with indications of data flow and privilege boundaries (Figure 6).

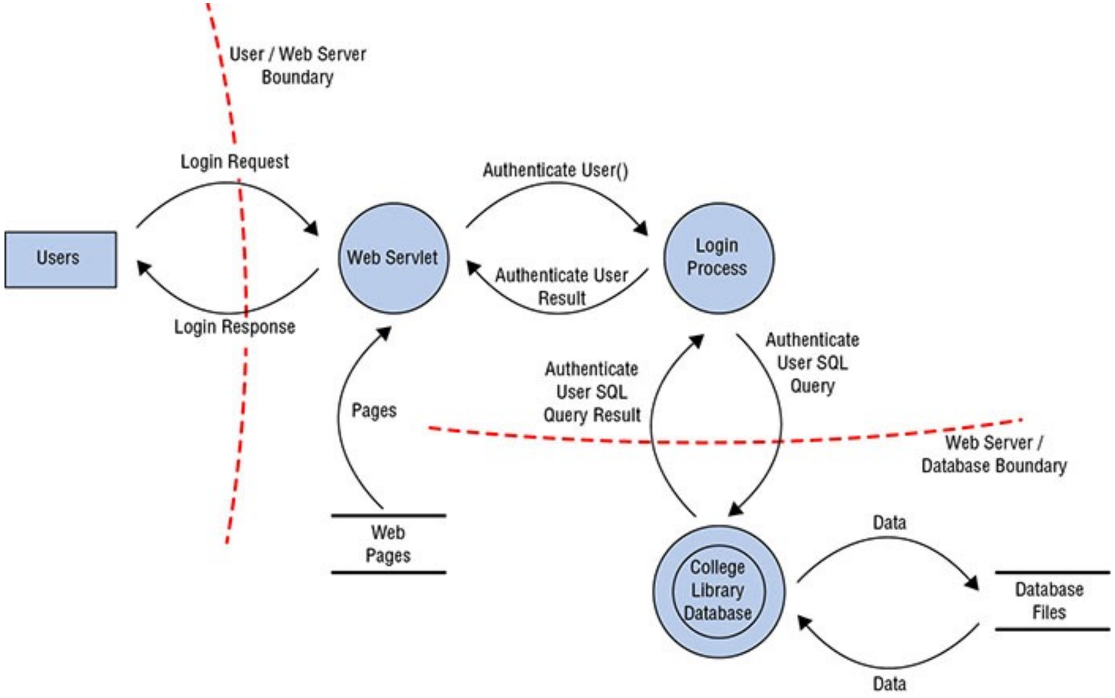


FIGURE 6. An example of diagramming to reveal threat concerns

Apply Threat Modeling Concepts and Methodologies: Diagramming

- Figure 6 an example of a data flow diagram that shows:
  - Each major component of a system,
  - The boundaries between security zones,
  - The potential flow or movement of information and data.
- It is possible to examine each point where a compromise could occur
- Such data flow diagrams are useful in gaining a better understanding of:
  - The relationships of resources,
  - Movements of data through a visual representation.

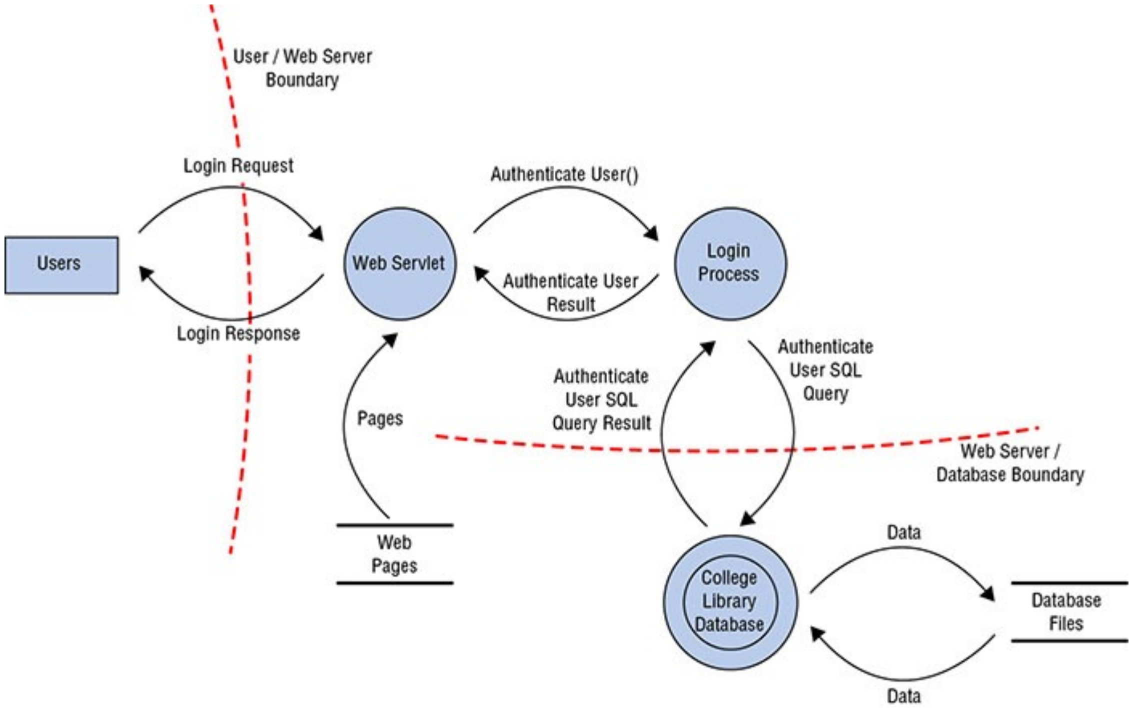


FIGURE 6. An example of diagramming to reveal threat concerns

Apply Threat Modeling Concepts and Methodologies: Diagramming

- Once a diagram has been crafted, identify all the technologies involved:
  - Operating systems, applications (network service and client based), and protocols
- Be specific as to the version numbers and update/patch level in use
- Next, identify attacks that could be targeted at each element of the diagram
- All forms of attacks should be considered: logical/technical, physical, and social
- This process will quickly lead you into the next phase of threat modeling:

→ Reduction Analysis

Apply Threat Modeling Concepts and Methodologies: Reduction Analysis

- **Reduction analysis** is also known as decomposing the application, system, or environment
- **Objectives**: understanding the logic of the product and its interactions with external elements
- **Divide and conquer principle:** an entire environment needs to be divided into smaller containers or compartments (subroutines, modules, objects, protocols, departments, tasks, and networks)
- Each identified sub-element should be evaluated to understand inputs, processing, security, data management, storage, and outputs

Apply Threat Modeling Concepts and Methodologies: Reduction Analysis

- In the decomposition process, you must identify five key concepts:
  - Trust Boundaries: Any location where the level of trust or security changes
  - Data Flow Paths: The movement of data between locations
  - Input Points: Locations where external input is received
  - Privileged Operations: Any activity that requires greater privileges than of a standard user account or process, typically required to make system changes or alter security
  - Details about Security Stance and Approach: The declaration of the security policy, security foundations, and security assumptions

Apply Threat Modeling Concepts and Methodologies: Prioritization and Response

- Fully document the threats to define:
  - Means
  - Target
  - Consequences of a threat
  - Techniques required to implement an exploitation
  - List of potential countermeasures and safeguards
- After documentation, rank or rate the threats
- This can be accomplished using a wide range of techniques, such as:
  - Probability × Damage Potential ranking
  - High/medium/low rating
  - DREAD system

Apply Threat Modeling Concepts and Methodologies: Prioritization and Response

- The ranking technique of **Probability × Damage Potential**:
  - Produces a risk severity number on a scale of 1 to 100, with 100 the most severe risk possible
  - These rankings can be somewhat arbitrary and subjective
  - But since the same person or team will be assigning the numbers for their own organization the assessment values are accurate on a relative basis

Apply Threat Modeling Concepts and Methodologies: Prioritization and Response

- The **high/medium/low** rating process is even simpler:
  - Each threat is assigned one of these three priority labels
  - Those given the high-priority label need to be addressed immediately
  - Those given the medium-priority label should be addressed eventually, but they don’t require immediate action
  - Those given the low-priority level might be addressed, but they could be deemed optional if they require too much effort or expense

Apply Threat Modeling Concepts and Methodologies: Prioritization and Response

- The **DREAD** rating system is designed to provide a flexible rating that is based on the answers to 5 questions about each threat:
  - **Damage potential**: How severe is the damage likely to be if the threat is realized?
  - **Reproducibility**: How complicated is it for attackers to reproduce the exploit?
  - **Exploitability**: How hard is it to perform the attack?
  - **Affected users**: How many users are likely to be affected by the attack (as a percentage)?
  - **Discoverability**: How hard is it for an attacker to discover the weakness?

Apply Threat Modeling Concepts and Methodologies: Prioritization and Response

DREAD (count.):

- By asking these and potentially additional customized questions:
  - Assigning H/M/L or 3/2/1 values to the answers,
  - Then we can establish a detailed threat prioritization.
- Response options should include:
  - Adjusting software architecture,
  - Altering operations and processes,
  - Implementing defensive and detective components.

Further reading

- https://www.ssi.gouv.fr/en/publications/:
  - Dozens of free publications in all domains of cybersecurity from ANSSI (in English)
  - Compliance with the French/EU regulation in the matter
- https://www.enisa.europa.eu/publications
  - Numerous free publications in all domains of cybersecurity from ENISA (in English)
  - Compliance with the EU regulation in the matter
- Mike Chapple, James Michael Stewart, Darril Gibson. **(ISC)2 CISSP® Certified Information Systems Security Professional**. Official Study Guide. Eighth Edition. O'Reilly Media, Inc. 2020.
- Elad Elrom. **The Blockchain Developer. A Practical Guide for Designing, Implementing, Publishing, Testing, and Securing Distributed Blockchain-based Projects**. ISBN 978-1-4842-4846-1e-ISBN 978-1-4842-4847-8. https://doi.org/10.1007/978-1-4842-4847-8 © Elad Elrom 2019
- https://www.cse.wustl.edu/~jain/cse571-07/ftp/ids/#sec2