Justin Ciocoi

Feb 4, 2024

CSCI 400 Textbook Notes

Chapter 1: Overview of Computer Security

1.1: Computer Security Concepts

- First, we should define computer security and related term in a more concrete sense so that we can understand the verbiage used throughout the text
- **Computer Security** includes measures and controls which ensure the confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored and communicated
- This includes three key objectives which live at the heart of computer security
  - **Confidentiality**, which includes two related ideas
    - **Data Confidentiality**, which assures that private or confidential information is not made available to unauthorized individuals
    - **Privacy**, which assures that individuals can control what information of theirs may be collected and stored and how that information can be used by third parties
  - **Integrity**, which also covers two related ideas
    - **Data Integrity**, which ensures that data and programs are only altered in a specified and authorized manner
    - **System Integrity**, which assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system
  - **Availability**, which assures that systems work promptly and service is not denied to authorized users
- While these three concepts paint a fairly broad picture of computer security, many in the field think additional concepts should be used in order to present a more complete picture of the topic

- Two of the most commonly included concepts are
    - **Authenticity**, which is the property of being genuine, verifiable, and trusted, which can provide confidence in the validity of a transmission, message, or message originator
    - **Accountability**, also referred to as non-repudiability, which allows messages or transmissions to be traced back to an original source
- Levels of impact of security breaches
    - **Low**, which can be expected to have a limited adverse affect on the organization
    - **Moderate**, which can be expected to have a serious adverse affect on the organization
    - **High**, which can be expected to have a severe adverse effect on the organization
- When implementing secure computer systems, there a variety of challenges that must be overcome
    - Computer security is not as simple as it might appear to the novice given the fairly straightforward requirements but complex implementations
    - In designing secure systems, all possible attacks have to be considered
    - Because of point two, many procedures used to provide security are counterintuitive
    - Different security measures should be implemented at different places, both in the hardware and the memory of a computer system
    - Secret information is often required for computer security, which thus raises question about how securely that information can be kept secret
    - Computer security is a constantly evolving battle of wits between the attacker and the security designer
    - There is a natural tendency to perceive little benefit from security investment until a data breach occurs
    - Security requires constant monitoring
    - Security is often an afterthought in the design process rather than being in the forefront of designers brain throughout the process
    - Many users see security measures as an impediment to efficient and user-friendly operation of a system

- This figure displays a fundamental model for computer security

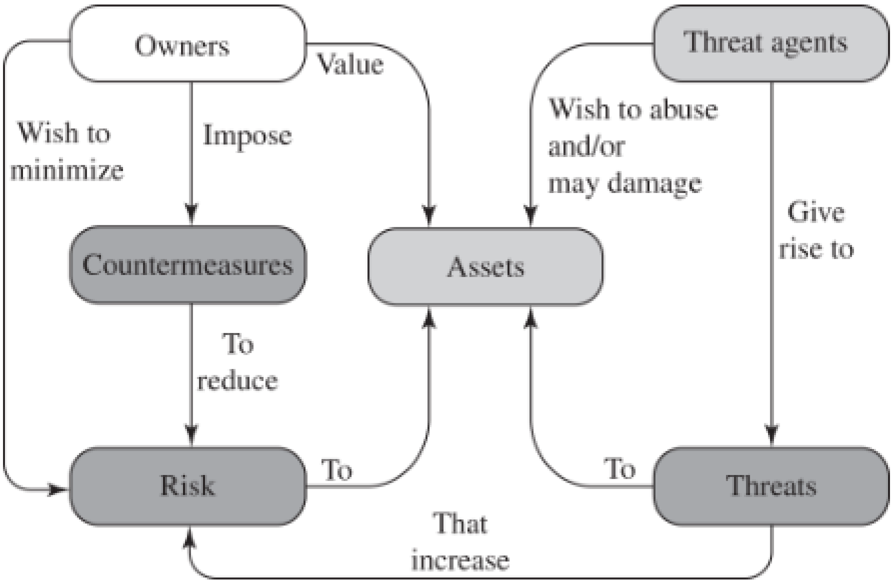


Figure 1.2 Security Concepts and Relationships

- There exist certain vulnerabilities in any computer system as follow
    - **Corruption** may occur such that incorrect information is given or incorrect actions are taken by a system
    - **Leaking** may occur such that an unauthorized user is granted access to information to which they should not have access
    - **Unavailability** may occur such that the use of the system can become impractical or even impossible
- In the execution of an attack on a computer system, the attack can be categorized into one of two types
    - **Active Attacks** which aim to alter system resources or affect their operation in some way
    - **Passive Attacks** which aim to learn or make use of information from the system while not affecting system resources
- Additionally, attacks can be categorized by their origin
    - **Insider Attacks** come from an individual within an organization, typically through the misuse of granted authorizations

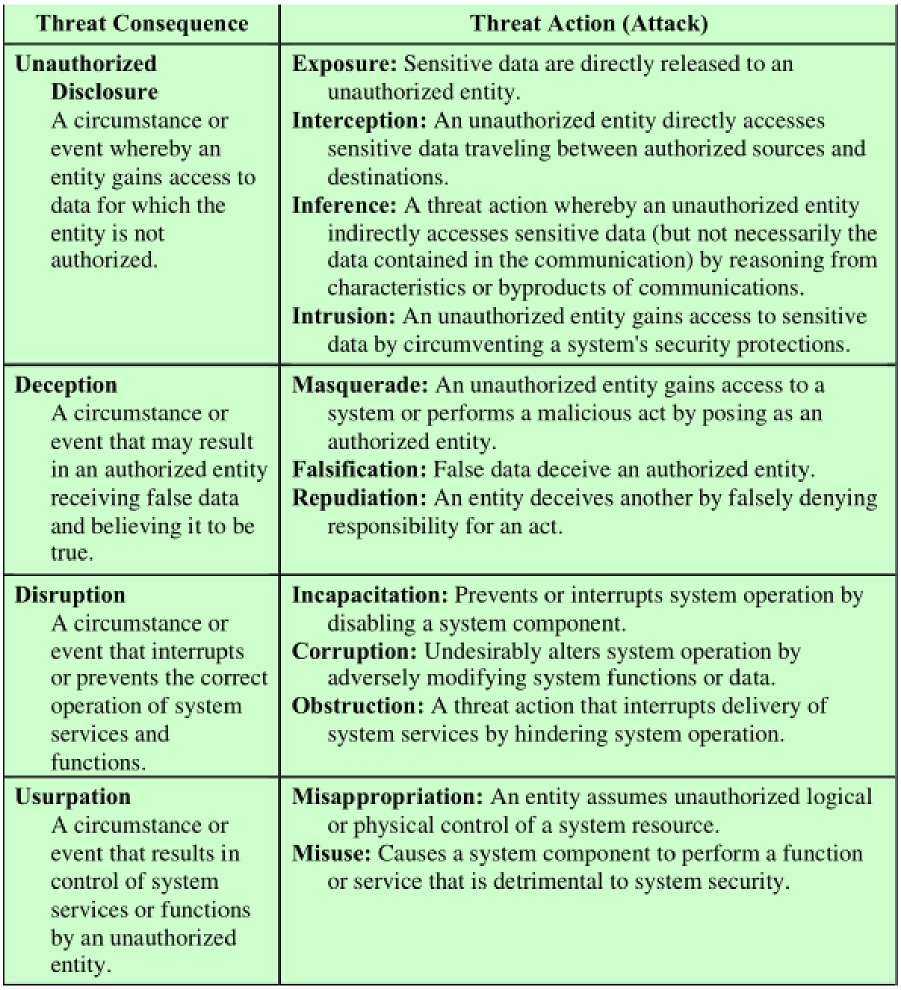
- **Outsider Attacks** come from an individual outside of an organization and is usually conducted over the internet

1.2: Threats, Attacks, and Assets

- **Unauthorized Disclosure** is a threat to confidentiality and can be brought about by the following types of attacks
  - **Exposure** which releases sensitive information to outsiders
    - This can be done either deliberately or unintentionally
  - **Interception** which often happens in the form of packet sniffing can allow an attacker to discern information on its way from one point to another
  - **Inference** which attackers can use to observe system traffic and using certain assumptions discern specific information
  - **Intrusion** where an adversary gains unauthorized access to sensitive data through overcoming access control measures
- **Deception** is a threat to either system integrity or data integrity , and is brought about through the following types of attacks
  - **Masquerade** where an unauthorized user can pose as an authorized user in order to gain access to system information or resources
  - **Falsification** in which an adversary can alter or replace valid data, and introduce false data into a file or database
  - **Repudiation** such that a user is able to deny sending or possessing certain sensitive information
- **Disruption** is a threat to availability or system integrity, and is brought about by the following types of attacks y
  - **Incapacitation** which renders a system incapacitated
  - **Corruption** where system software can operate in malicious or unexpected ways
  - **Obstruction** where certain resources needed by a system, such as communication links, are obstructed rendering a system unavailable
- **Usurpation** is a threat to system integrity and is brought about by the following types of attacks

- **Misappropriation** in which resources are incorrectly allocated such as in a distributed denial of service (DDOS) attack
- **Misuse** which can occur either through malicious logic or through a hacker whom has gained unauthorized access to a system

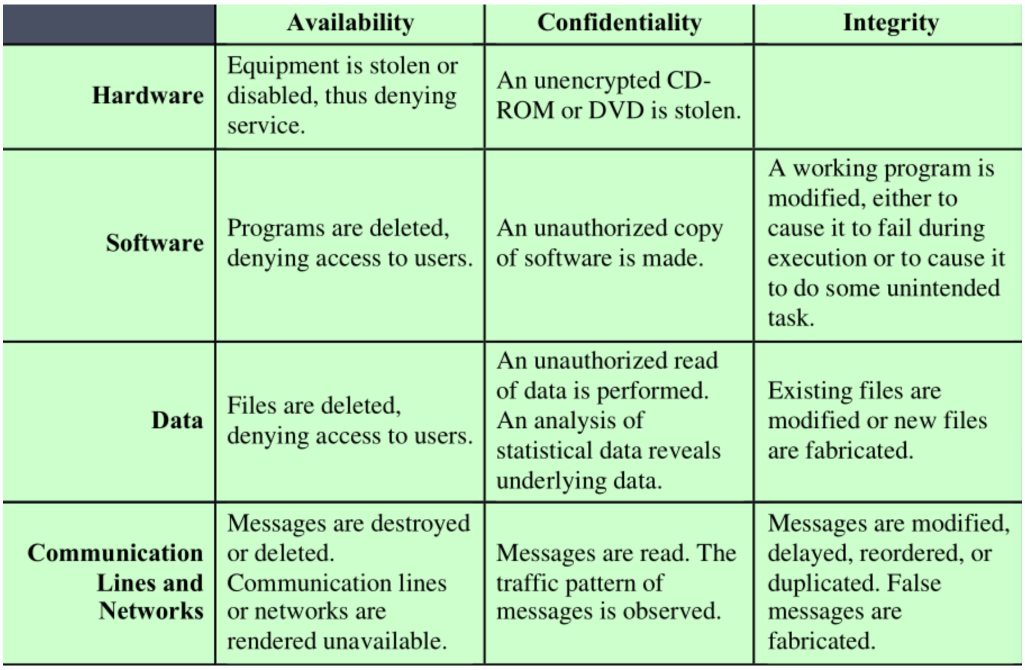
- The below table briefly explains the above types of threats



Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	**Exposure:** Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.
Disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**Incapacitation:** Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.
Usurpation A circumstance or event that results in control of system services or functions by an unauthorized entity.	**Misappropriation:** An entity assumes unauthorized logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.

- In any computer system, the systems **assets** can be broadly categorized as hardware, software, data, and communication lines/networks

- The below table shows the assets and the different ways threats can affect these assets



	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service.	An unencrypted CD-ROM or DVD is stolen.	
Software	Programs are deleted, denying access to users.	An unauthorized copy of software is made.	A working program is modified, either to cause it to fail during execution or to cause it to do some unintended task.
Data	Files are deleted, denying access to users.	An unauthorized read of data is performed. An analysis of statistical data reveals underlying data.	Existing files are modified or new files are fabricated.
Communication Lines and Networks	Messages are destroyed or deleted. Communication lines or networks are rendered unavailable.	Messages are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

- Network attacks, or attacks on communication lines and networks, can be classified as either *active* or *passive*
  - A passive attack attempts to make use of information from the system but does not affect system resources
  - An active attack attempts to alter system resources or affect their operation
- Passive attacks are very difficult to detect because they do not involve any alteration of the data and thus require far more intensive monitoring to detect
  - Thus, the emphasis in dealing with these attacks is often prevention rather then detection due to the large cost of detecting passive attacks
- Here are some examples of **passive attacks**
  - **Release of Message Contents** where a file which is transferred and should be kept confidential is not, allowing an eavesdropper access to any sensitive information transmitted
  - **Traffic Analysis** allows attackers to track activity over a network or communication link and, given certain assumptions, use pattern recognition to gain knowledge of transmission type or purpose
- **Active attacks** can be broadly categorized into four types
  - **Replay** involves capturing a certain transmission unit which is used in access control to later "replay" or reproduce the transmission unit in order to gain unauthorized access

  - **Masquerade** attacks take place when one entity pretends to be a different entity
  - **Modification of Messages** is fairly self explanatory and can change messages used in access control for sensitive information
  - **Denial of Service** prevents or inhibits the normal use of communication networks

1.4: Fundamental Security Design Principles

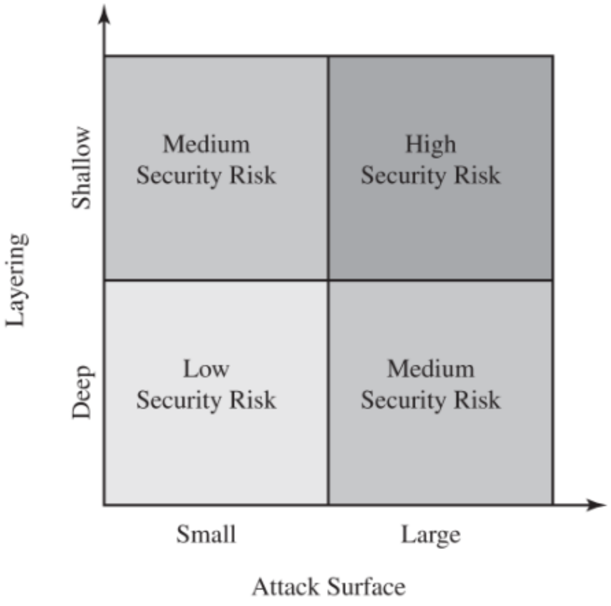
- This section will briefly discuss each of the principles outlined in [NCAE13]
- The first eight were proposed in [SALT75] and have withstood the test of time
  - **Economy of Mechanism**
    - This principle essentially states that the design of security measures, in both hardware and software, should be as small and simple as possible
    - This makes security features easier to test and verify, and will create fewer subtle weaknesses in those features
  - **Fail-Safe Default**
    - This means that access decisions should be based on permission rather than exclusion
    - This means that the default situation is a lack of access and data protection schemes identify the conditions under which access will be permitted
  - **Complete Mediation** meaning every access should be checked against the access control mechanism
  - **Open Design** meaning that the design of a security mechanism should be open and transparent rather than secret
  - **Separation of Privilege**
    - This means that multiple privilege attributes are required to achieve access to a protected resource
    - A common example of this in modern applications is multifactor user authentication
  - **Least Privilege** meaning that any action taken should grant the user the least necessary permissions in order to achieve this task

    - **Least Common Mechanism** meaning the design of the security mechanism should minimize the functions shared by different users in order to reduce the number of unintended communications
    - **Psychological Acceptability** meaning that the security mechanisms should not be so intrusive as to seriously interrupt the workflow of the user
    - **Isolation**
        - Public access systems should be isolated from critical resources to prevent disclosure or tampering
        - The files and processes of individual users should be isolated from one another except when it is explicitly desired
        - Security mechanisms should be isolated in the sense of preventing access to those mechanisms
    - **Encapsulation** which can be considered a subset of isolation based on the concept of the same name in object-oriented programming
    - **Modularity**
        - This refers to the development of security functions as separate modules as well as the use of a modular architecture for implementations
        - This allows code re-use, which is especially useful in the case of various commonly used cryptographic libraries like openSSL
        - Modular architecture also allows for more easy migration and upgradability of security features
    - **Layering** which refers to the use of multiple, overlapping protection approaches
    - **Least Astonishment** meaning that security features should respond to user inputs in a way that is least likely to astonish the user

1.5: Attack Surfaces and Attack Trees

- Examples of attack surfaces are the following
    - Open ports on outward facing Web and other servers, and code listening on those ports
    - Services available on the inside of a firewall

    - Code that process incoming data, e-mail, XML, office documents, and custom data-exchange formats
    - Interfaces, SQL, and web forms
    - An employee with access to sensitive information vulnerable to a social engineering attack
- These attack surfaces can be categorized in the following way
    - **Network Attack Surface**
        - This refers to vulnerabilities over an enterprise network, wide-are network, or Internet
        - This includes attacks like denial of service and disruption of communication links
    - **Software Attack Surface**
        - This refers to vulnerabilities in application, utility, or operating system code
        - Web server software is of particular importance here
    - **Human Attack Surface**
        - This refers to vulnerabilities created by personnel or outsiders
        - This includes social engineering attacks
    - Reducing the size of an attack surface is effective in reducing attacks, and when combined with layering can lead to an effective security mechanism
    - The relationship between layering and attack surface size is shown in the below table



- An **Attack Tree** is a branching, hierarchical data structure which represents a set of potential techniques for exploiting security vulnerabilities
- The root node is the goal of an attacker with each child node being a subgoal necessary to reach said goal
- Leaf nodes represent ways to initiate an attack
- Using attack trees is useful for effectively exploiting the publicly available information on attack patterns

1.6: Computer Security Strategy

- A comprehensive security strategy involves three aspects
  - **Specification/Policy**
    - *What is the security scheme supposed to do?*
  - **Implementation/Mechanisms**
    - *How does it do it?*
  - **Correctness/Assurance**
    - *Does it really work?*
- The first step in devising security services and mechanisms is to establish a *security policy*
- In developing such a policy, a security manager needs to consider the following factors

    - The value of the assets being protected
    - The vulnerabilities of the system
    - Potential threats and the likelihood of attacks
- Additionally, the manager must consider the following trade-offs
    - **Ease of Use vs. Security**
    - **Cost of Security vs. Cost of Failure and Recovery**
- In terms of security implementation, four complementary courses of actions exist
    - **Prevention**
        - Measures should be taken to prevent potential attacks
    - **Detection**
        - Mechanisms should be in place in order to detect potential attacks that are not outright prevented
    - **Response**
        - If a mechanism does detect an ongoing attack, the system should be able to respond in such a way as to halt the attack and prevent it from causing any more damage
    - **Recovery**
        - In the case of a successful attack, a recovery strategy such as a data backup should occur
- **Assurance and Evaluation**
    - The consumers of applications which include security features wish to be affirmed that the security measures in place will work as intended
    - **Assurance** is an attribute of an information system that provides grounds for having confidence in a system's correct operation
    - **Evaluation** is the process of thoroughly testing security measures with respect to certain criteria

1.7: Standards

- Over the history of computing a variety of standards of institutions have emerged, the most important of which are as follows
    - **National Institute of Standards and Technology (NIST)** which is a US federal agency
    - **Internet Society** which is a professional membership society with worldwide organizational and individual membership
    - **International Telecommunication Union** which is a UN agency
    - **International Organization for Standardization (ISO)** which is a worldwide federation of national standards bodies from more than 140 countries