

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

- **This chapter presents the basic concepts of computer security.**
- **Security mechanisms detect and prevent attacks and recover from those that succeed.**
- **Analyzing the security of a system requires an understanding of the mechanisms that enforce the security policy.**
- **Human beings are the weakest link in the security mechanisms of any system.**
- **Hence, policies and procedures must take people into account.**

1.1 The Basic Components

- **Computer security rests on confidentiality, integrity, and availability.**
- **The interpretations of the three aspects vary, as do the context in which they arise.**
- **The interpretation of an aspect in a given environment is dictated by the needs of the individuals, customs, and laws of the particular organization.**

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

- **Confidentiality**
 - Confidentiality is the concealment of information or resources.
 - The need for keeping information secret arises from the use of computers in sensitive fields such as government or industry.
 - Access control mechanisms support confidentiality.
 - One access control mechanism for preserving confidentiality is cryptography, which scrambles data to make it incomprehensible.
 - A cryptographic key controls access to the unscrambled data.
 - However, the cryptographic key itself becomes another datum to be protected.
 - EXAMPLE:
 - Enciphering an income tax return will prevent anyone from reading it.
 - If the owner needs to see the return, it must be deciphered.
 - Only the possessor of the cryptographic key can enter it into a deciphering program.
 - If someone else can read the key when it is entered into the program, the confidentiality of the tax return has been compromised.

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

- **Integrity**

- **Integrity** refers to the trustworthiness of data or resources.
- Integrity includes data integrity (the content of information) and origin integrity (the source of the data).
- **EXAMPLE:**
 - A newspaper may print information obtained from a leak at the White House but attribute it to the wrong source.
 - The information is printed as received (preserving data integrity), but its source is incorrect (corrupting origin integrity).
- Integrity mechanisms fall into two classes: **prevention** mechanisms and **detection** mechanisms.
- Prevention mechanisms seek to maintain the integrity of the data by blocking any unauthorized attempts to change the data or any attempts to change the data in unauthorized ways.
- The distinction between these two types of attempts is important.
 - The former occurs when a user tries to change data which she has no authority to changes.
 - The latter occurs when a user authorized to make certain changes in the data tries to change the data in other ways.

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

- **Availability**
 - **Availability** refers to the ability to use the information or resource desired.
 - **Availability is an important aspect of reliability as well as of system design because an unavailable system is at least as bad as no system at all.**
 - **EXAMPLE:**
 - **Suppose Anne has compromised a bank's secondary system server, which supplies bank account information.**
 - **When anyone else asks that server for information, Anne can supply any information she desires.**
 - **Merchants validate checks by contacting the bank's primary balance server.**
 - **If a merchant gets no response, the secondary server will be asked to supply the data.**
 - **Anne's colleague prevents merchants from contacting the primary balance server, so all merchant queries go to the secondary server.**
 - **Anne will never have a check turned down, regardless of her actual account balance.**
 - **If the bank had only one server (the primary one), this scheme would not work.**

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

1.2 Threats

- A threat is a potential violation of security.
- The violation need not actually occur for there to be a threat.
- The three security services (confidentiality, integrity, and availability) counter threats to the security of a system.
- Shirley (Security Architectures for Internet Protocols: A Guide for Protocol Design and Standards: Internet Draft, November 1994) divides threats into four broad categories:
 - Disclosure, or unauthorized access to information.
 - Deception, or acceptance of false data.
 - Disruption, or interruption or prevention of correct operation.
 - Usurpation, or unauthorized control of some part of a system.
- These four broad classes encompass many common threats.

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

- **Snooping**, the unauthorized interception of information, is a form of disclosure.
- **Wiretapping**, or passive wiretapping, is a form of snooping in which a network is monitored.
- **Confidentiality services** counter this threat.
- **Modification** or alteration, an unauthorized change of information, covers three classes of threats.
 - The goal may be deception, in which some entity relies on the modified data to determine which action to take, or in which incorrect information is accepted as correct and is released.
 - If the modified data controls the operation of the system, the threats of disruption and usurpation arise.
 - Unlike snooping, modification is active; it results from an entity changing information.
 - Active wiretapping is a form of modification in which data moving across a network is altered.
- **Integrity services** counter this threat.

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

- **Masquerading** or spoofing, an impersonation of one entity by another, is a form of both deception and usurpation.
 - It lures a victim into believing that the entity with which it is communicating is a different entity.
 - **EXAMPLE**: If a user tries to log into a computer across the Internet but instead reaches another computer that claims to be the desired one, the user has been spoofed.
- The goal may be deception, in which some entity relies on the modified data to determine which action to take, or in which incorrect information is accepted as correct and is released.
- If the modified data controls the operation of the system, the threats of disruption and usurpation arise.
- Unlike snooping, modification is active; it results from an entity changing information.
- Active wiretapping is a form of modification in which data moving across a network is altered.
- **Delegation** occurs when one entity authorizes a second entity to perform functions on its behalf.

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

- **Repudiation of origin**, a false denial that that an entity sent (or created) something, is a form of deception.
 - **EXAMPLE**: Suppose a customer sends a letter to a vendor agreeing to pay a large number of money for a product. The vendor ships the product and then demands payment. The customer denies having ordered the product and by law is therefore entitled to keep the unsolicited shipment without payment. The customer has repudiated the origin of the letter. If the vendor cannot prove that the letter came from the customer, the attack succeeds.
 - Integrity mechanisms cope with this threat.
- **Denial of receipt**, a false denial that an entity received some information or message, is a form of deception.
 - **EXAMPLE**: Suppose a customer orders an expensive product, but the vendor demands payment before shipment. The customer pays, and the vendor ships the product. The customer then asks the vendor when he will receive the product. If the customer has already received the product, the question constitutes a denial of receipt attack. The vendor can defend against this attacks only by proving that the customer did, despite his denials, receive the product. Integrity and availability mechanisms guard against these attacks.

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

- **Delay**, a temporary inhibition of a service, is a form of usurpation, although it can play a supporting role in deception.
 - **EXAMPLE**: Typically, delivery of a message or service requires some time t ; if an attacker can force the delivery to take more than time t , the attacker has successfully delayed delivery. This requires manipulation of system control structures, and hence is a form of usurpation. If an entity is waiting for an authorization message that is delayed, it may query a secondary server for authorization. Even though the attacker may be unable to masquerade as the primary server, she might be able to masquerade as the secondary sever and supply incorrect information.
 - Availability mechanisms can thwart this threat.
- **Denial of service**, a long-term inhibition of service, is a form of usurpation, although it is often used with other mechanisms to deceive.
 - **EXAMPLE**: The attacker prevents a server from providing a service. The denial may occur at the source (by preventing the server from obtaining the resources needed to perform its function), at the destination (by blocking the communications from the server), or along the intermediate path (by discarding messages from either the client or the server, or both). Denial of service poses the same threat as an infinite delay.
 - Availability mechanisms counter this threat.

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

1.3 Policy and Mechanism

- **Definition:** A **security policy** is a statement of what is, and what is not, allowed.
- **Definition:** A **security mechanism** is a method, tool, or procedure for enforcing a security policy.
- Mechanisms can be nontechnical, such as requiring proof of identity before changes a password.
- Policies often require some procedural mechanisms that technology cannot enforce.
- **EXAMPLE:**
 - A university's computer science laboratory has a policy that prohibits any student from copying another student's homework files.
 - The computer system provides mechanisms for preventing others from reading a user's files.
 - Anna fails to use these mechanisms to protect her homework files, and Bill copies them. A breach of security has occurred because Bill has violated the security policy.
 - Anna's failure to protect her files does not authorize Bill to copy them.
- Policies may be presented mathematically as a list of allowed (secure) and disallowed (nonsecure) states.

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

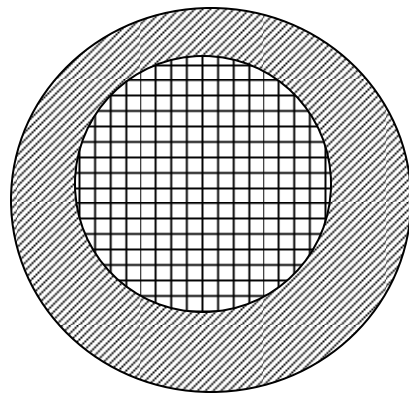
- Given a security policy's specification of secure and nonsecure actions, these security mechanisms can prevent the attack, detect the attack, or recover from the attack.
- Prevention means that an attack will fail.
 - If one attempts to break into a host over the Internet and that host is not connected to the Internet, that attack has been prevented.
- Detection is most useful when an attack cannot be prevented, but it can also indicate the effectiveness of preventative measures.
 - Detection mechanisms accept that an attack will occur. The goal is to determine that an attack is underway, or has occurred, and report it.
 - The attacks may be monitored to provide data about its nature, severity, and results.
- Recovery has two forms: The first is to stop an attack and to assess and repair any damage caused by that attack.
 - EXAMPLE: If the attacker deletes a file, one recovery mechanism would be to restore the file from backup tapes. In practice, recovery is far more complex because of the nature of each attack is unique.
- In a second form of recovery, the system continues to function correctly while an attack is under way.

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

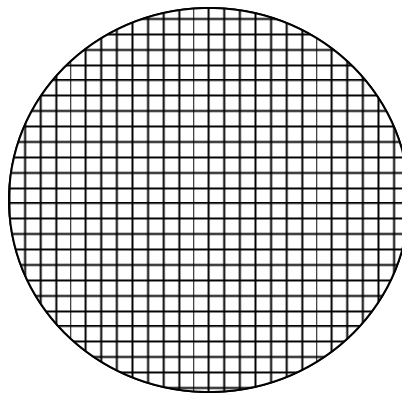
1.4 Assumptions and Trust

- How do we determine if the policy correctly describes the required level and type of security for the site?
- This question lies at the heart of all security, computers and otherwise. Security rests on the assumptions specific to the type of security required and the environment in which it is to be employed.
- **EXAMPLE:**
 - Opening a door lock requires a key. The assumption is that the lock is secure against lock picking.
 - However, a good lock picker can open a lock without a key.
 - If the lock picker is trustworthy, the assumption is valid.
 - The term trustworthy implies that the lock picker will not pick a lock unless the owner of the lock authorizes the lock picking.
- **Definition:** A security mechanism is secure if $R \subseteq Q$; it is precise if $R = Q$; and it is broad if there are states r such that $r \in R$ and $r \notin Q$.

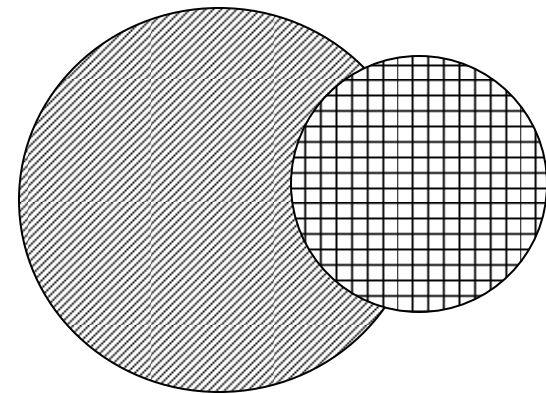
Chapter 1 AN OVERVIEW OF COMPUTER SECURITY



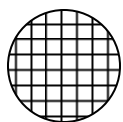
secure



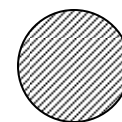
precise



broad



set of reachable states



set of secure states

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

1.5 Assurance

- Trust cannot be quantified precisely.
- System specification, design, and implementation can provide a basis for determining how much to trust a system.
- This aspect of trust is called assurance.
- EXAMPLE:
 - In the United States, aspirin from a nationally known and reputable manufacturer, delivered to the drugstore in a safety-sealed, and sold with the seal still in place, is considered trustworthy by most people.
 - The bases for that trust are as follows:
 - The testing and certification of the drug (aspirin) by the Food and Drug Administration. The FDA has jurisdiction over many types of medicines and allows medicines to be marketed only if they meet certain clinical conditions.
 - The manufacturer standards of the company and the precautions it takes to ensure that the drug is not contaminated. National and state regulatory commissions and groups ensure that the manufacturer of the drug meets specific acceptable standards.
 - The safety seal on the bottle. To insert dangerous chemicals into a safety-sealed bottle without damaging the seal is very difficult.

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

- **Specification** is a (formal or informal) statement of the desired functioning of the system.
- It can be highly mathematically using any of several languages defined for that purpose.
- This aspect of trust is called **assurance**.
- **EXAMPLE:**
 - In the United States, aspirin from a nationally known and reputable manufacturer, delivered to the drugstore in a safety-sealed, and sold with the seal still in place, is considered trustworthy by most people.
 - The **bases** for that trust are as follows:
 - The testing and certification of the drug (aspirin) by the Food and Drug Administration. The FDA has jurisdiction over many types of medicines and allows medicines to be marketed only if they meet certain clinical conditions.
 - The manufacturer standards of the company and the precautions it takes to ensure that the drug is not contaminated. National and state regulatory commissions and groups ensure that the manufacturer of the drug meets specific acceptable standards.
 - The safety seal on the bottle. To insert dangerous chemicals into a safety-sealed bottle without damaging the seal is very difficult.

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

- **EXAMPLE:**
 - A company is purchasing a new computer for internal use. They need to trust the system to be invulnerable to attack over the Internet. One of their English specifications would read “The system cannot be attacked over the Internet.”
- The **design** of a system translates the specifications into components that will implement them.
- **EXAMPLE:**
 - A design of the computer system for the company mentioned above had no network interface cards, no modem cards, and no network drivers in the kernel.
 - This design satisfied the specification because the system would not connect to the Internet. So, it would not be attacked over the Internet.
- Given a design, the implementation creates a system that satisfies the specifications, then by transitivity the implementation will also satisfy the specifications.
 - **Definition:** A program is correct if its implementation performs as specified.
 - Because formal proofs of correctness are so-time consuming, a posteriori verification techniques known as testing have become widespread.

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

1.6 Operational Issues

- Any useful policy and mechanism must balance the benefits of the protection against the cost of designing, implementing, and using the mechanism.
- **Cost-Benefit Analysis:** Like any factor in a complex system, the benefits of computer security are weighed against their total cost
- **EXAMPLE:**
 - A database provides salary information to a second system that prints checks.
 - If the database is altered, the company could suffer grievous financial loss.
 - Suppose the company has several branch offices, and every day the database downloads a copy of the data to each branch office.
 - The branch offices use the data to recommend salaries for new employees. However, the main office makes the final decision using the original database (not one of the copies). In this case, guarding the integrity of the copies is not particularly important, because the branch offices cannot make any financial decisions based on the data in their copies.
 - Both of these situations are extreme situations in which the analysis is clear-cut.
 - As an example of a situation in which the analysis is less clear, consider the need for confidentiality of the salaries in the database. The officers of the company must decide the financial cost to the company should the salaries be disclosed; changes in policies, procedures, and personnel; and the effect on future business.

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

- **Risk Analysis**: To determine whether an asset should be protected, and to what level, requires analysis of the potential threats against that asset and the likelihood that they will materialize.
- **EXAMPLE**:
 - Let us revisit our company with the salary database that transmits salary information over a network to a second computer system that prints employees' checks.
 - The data is stored on the database system and then moved over the network to the second system.
 - The risk of unauthorized changes in the data occurs in three places: on the database system, on the network, and on the printing system.
 - If the network is a local (company-wide) one and no wide area networks are accessible, the threat of the attackers entering the system is confined to untrustworthy internal personnel.
 - If the network is connected to the Internet, the risk of geographically distant attackers attempting to intrude is substantial enough to warrant consideration.

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

- **Laws and Customs:** Laws restrict the availability and use of technology and affect procedural controls.
- Hence, any policy and any selection of mechanisms must take into account legal considerations.
- **EXAMPLE:**
 - Until the year 2000, the United States controlled the export of cryptographic hardware and software.
 - If a U.S. software company worked with a computer manufacturer in London, the U.S. company could not send cryptographic software to the manufacturer.
 - The U.S. company would have to obtain a license to export the software from the United States.
 - Any security policy that depended on the London manufacturer using that cryptographic software would need to take this into account.

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

1.7 Human Issues

- Implementing computer security controls is complex, and in a large organization procedural controls often become vague or cumbersome.
- Regardless of the strength of the technical controls, if nontechnical considerations affect their implementation and use, the effect on security can be severe.
- Moreover, if configured or used incorrectly, even the best security controls is useless at best and dangerous at worst.
- **Organizational Problems:** Security provides no direct financial rewards to the user. It limits losses, but it also requires the expenditure of resources that could be used elsewhere. Unless losses occur, organizations often believe they are wasting effort related to security. After a loss, the value of these controls suddenly becomes appreciated. Furthermore, security controls often add complexity to otherwise simple operations.
 - **EXAMPLE:** If concluding a stock trade takes two minutes without security controls and three minutes with security controls, adding those controls results in a 50% loss of productivity.

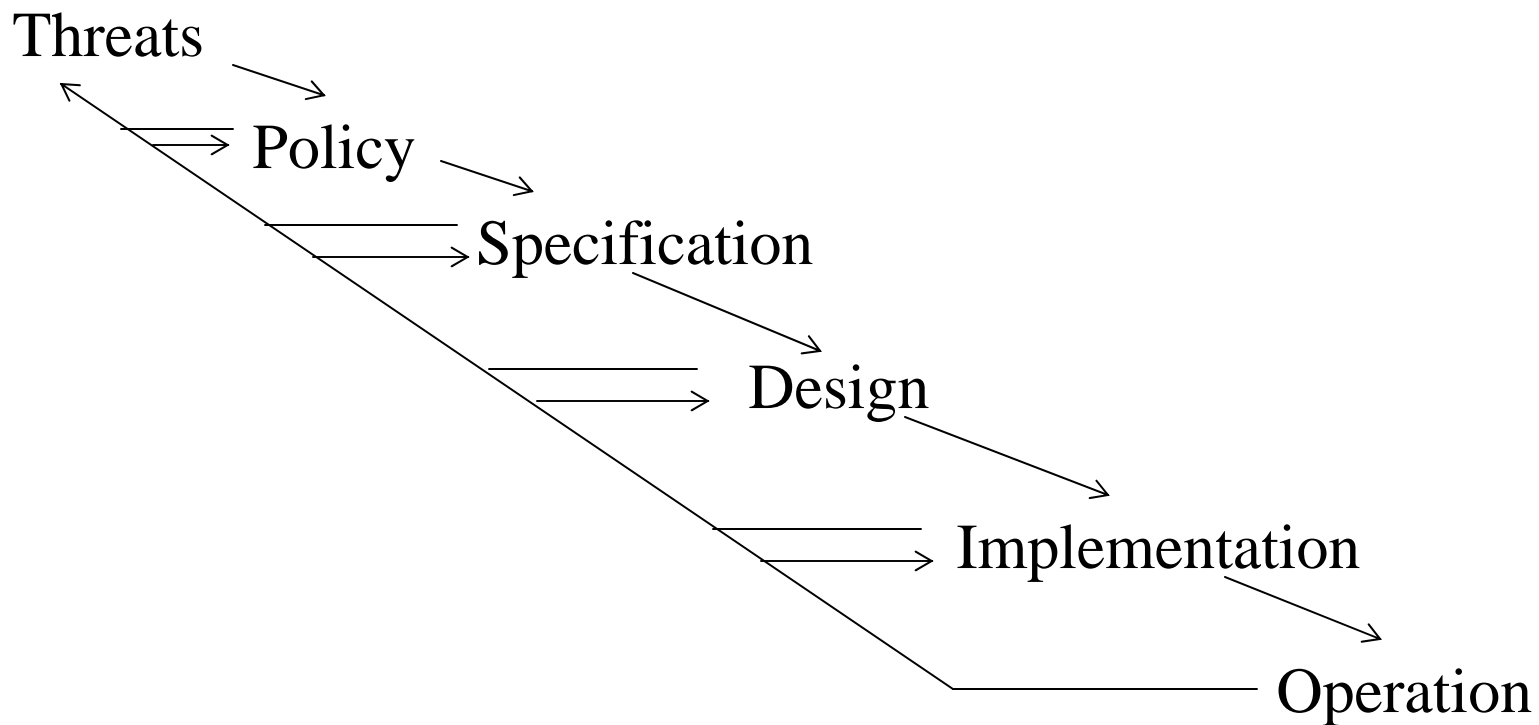
Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

- Losses occur when security protections are in place, but such losses are expected to be less than they would have been without security mechanisms.
- Compounding this problem is the question of who is responsible for the security of the company's computers.
- Lack of resources is another common problem. Securing a system requires resources as well as people.
- People Problems: The heart of any security system is people.
 - EXAMPLE: A computer system authenticates a user by asking that user for a secret code. If the correct secret code is supplied, the computer assumes that the user is authorized to use the system. If an authorized user tells another person his secret code, the unauthorized user can masquerade as the authorized user with significantly less likelihood of detection.
 - People who have some motive to attack an organization and are not authorized to use that organization's systems are called outsiders and can pose a serious threat.
 - A far more dangerous threat comes from the disgruntled employees and other insiders who are authorized to use the computers.

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY

- **Lack of training need not be in the technical arena.**
- **Many successful break-ins have arisen from the art of social engineering.**
- **Social engineering is the practice of obtaining confidential information by manipulation of legitimate users.**
- **A social engineer will commonly use the telephone or the Internet to trick people into revealing sensitive information or getting them to do something that is against typical policies.**
- **If operators will change passwords based on telephone requests, all an attacker needs to do is to determine the name of someone who uses the computer.**
- **A common tactic is to pick someone fairly far above the operator (such as a vice president of the company) and to feign an emergency (such as calling at night and saying that a report to the president of the company is due the next morning) so that the operator will be reluctant to refuse the request. Once the password has been changed to one that the attacker knows, he can simply log in as a normal user.**

Chapter 1 AN OVERVIEW OF COMPUTER SECURITY



The Security Life Cycle