Course Title: Information Security (CACS459)

Unit I: Overview of Computer Security

Contents:

1.1 Computer Security Concepts

Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.

This definition introduces three key objectives that are at the heart of computer security:

1. **Confidentiality**: This term covers two related concepts:
    - Data confidentiality: Assures that private or confidential information is not made available or disclosed to unauthorized individuals.
    - Privacy: Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed.
2. **Integrity**: This term covers two related concepts:
    - Data integrity: Assures that information and programs are changed only in a specified and authorized manner.
    - System integrity: Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
3. **Availability**: Assures that systems work promptly and service is not denied to authorized users.

These three concepts form what is often referred to as the CIA triad. The three concepts embody the fundamental security objectives for both data and for information and computing services.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Integrity: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Availability: Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Although the use of the CIA triad to define security objectives is well established, some in the security field feel that additional concepts are needed to present a complete picture (see Figure below). Two of the most commonly mentioned are as follows:

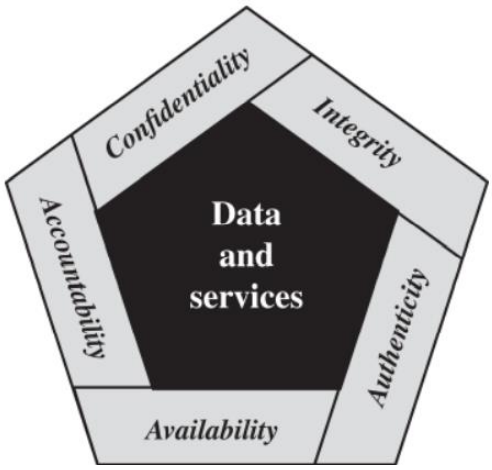

Figure: Essential Network and Computer Security Requirements

Authenticity: The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means verifying that users are who they say they are and that each input arriving at the system came from a trusted source.

Accountability: The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

The Challenges of Computer Security

Computer security is both fascinating and complex. Some of the reasons are as follows:

1. Computer security is not as simple as it might first appear to the novice. The requirements seem to be straightforward; indeed, most of the major requirements for security services can be given self-explanatory one-word labels: confidentiality, authentication, nonrepudiation, and integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning.
2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.
3. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such as TCP/IP (Transmission Control Protocol/Internet Protocol) should mechanisms be placed].
4. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information.
5. Computer security is essentially a battle of wits between a perpetrator who tries to find holes, and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.

6. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.
7. Security requires regular, even constant monitoring, and this is difficult in today's short term, overloaded environment.
8. Security is still too often an afterthought to be incorporated into a system after the design is complete, rather than being an integral part of the design process.
9. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information.

Computer Security Terminologies

Adversary (threat agent): Individual, group, organization, or government that conducts or has the intent to conduct detrimental (harmful) activities.

Attack: Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Countermeasure: A device or techniques that has as its objective the impairment of the operational effectiveness of undesirable or adversarial activity, or the prevention of espionage, sabotage, theft, or unauthorized access to or use of sensitive information or information systems.

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence

Security Policy: A set of criteria for the provision of security services. It defines and constrains the activities of a data processing facility in order to maintain a condition of security for systems and data.

System Resource (Assets): A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Vulnerability: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Threat: A threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

1.2 Computer Security, Information Security, Network Security

Computer Security — is a process and the collection of measures and controls that ensures the Confidentiality, Integrity and Availability (CIA) of the assets in computer systems.

C stands for Confidentiality which ensures authorized access and disclose.

I stands for Integrity that ensures proper modification or destruction

A stands for Availability that ensures timely and reliable access and use.

Computer Security protects from both software and hardware part of a computer systems from getting compromised and be exploited. If a computer can be infected without ever connected to the internet, e.g by USB, then may spread to your LAN and infect other computers or workstations, damage files , if your

workstation is connected to the internet, this could be easily spread over other devices connected to the internet unprotected!

Computer Security concerns with the following asset to protect:

- Computer hardware devices such as PC, servers, tablet, notebook, laptop etc.
- Network devices such as router, switches etc.
- Software, firmware and operating system.

Network Security — is any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. An effective network security manages access to the network. It targets a variety of threats and stop them from entering or spreading on your network.

Network security concerns with the: Firewall, Antivirus, Penetration testing, Intrusion detection, Computer forensics, Access controls, System monitoring, Patch management, Data encryption.

Information Security —is a significant assets that can be stored in different ways such as digitally stored, printed, and written on papers or in human memory. It can be communicated through different channels such as spoken languages, gestures or using digital channel such as email, SMS, social media, video, audio etc.

Information security is primarily concerned with making sure that data in any form is kept secure in terms of preserving its confidentiality, integrity and availability.

Information Security concerns with the: Intellectual property, Regulatory compliance, Business integrity, Industrial espionage or spy, Governance, Crisis management, Business continuity, Risk analysis and more.

Information Security is more business oriented while Network Security and Computer Security are more technology oriented.

1.3 Threats, Attacks and Assets

Threat

A threat is any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Types of Security threats:

1. Unauthorized disclosure
2. Deception
3. Disruption
4. Usurpation

Unauthorized disclosure

A circumstance or event whereby an entity gains access to data for which the entity is not authorized. It is a threat to confidentiality. Some of the unauthorized disclosure attacks are:

- Exposure: Sensitive data are directly released to an unauthorized entity.
  This can be deliberate, as when an insider intentionally releases sensitive information, such as credit card numbers, to an outsider.

- Interception: An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations.
  On a shared local area network (LAN), such as a wireless LAN or a broadcast Ethernet, any device attached to the LAN can receive a copy of packets intended for another device. On the Internet, a determined hacker can gain access to e-mail traffic and other data transfers.
- 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 by-products of communications.
  An example of inference is known as traffic analysis, in which an adversary is able to gain information from observing the pattern of traffic on a network, such as the amount of traffic between particular pairs of hosts on the network.
- Intrusion: An unauthorized entity gains access to sensitive data by circumventing (bypassing) a system's security protections.
  An example of intrusion is an adversary gaining unauthorized access to sensitive data by overcoming the system's access control protections.

Deception

A circumstance or event that may result in an authorized entity receiving false data and believing it to be true. It is a threat to either system integrity or data integrity. Some of the deception attacks are:

- Masquerade: An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity.
  For example, unauthorized user learned and used user ID and password of authorized user.
- Falsification: False data deceive an authorized entity.
  For example, a student may alter his or her grades on a school database.
- Repudiation: An entity deceives another by falsely denying responsibility for an act.
  In this case, a user either denies sending data, or a user denies receiving or possessing the data.

Disruption

A circumstance or event that interrupts or prevents the correct operation of system services and functions. This is the threat to the availability or system integrity. Some of the disruption attacks are:

- Incapacitation: Prevents or interrupts system operation by disabling a system component.
  This could occur as a result of physical destruction of or damage to system hardware. More typically, malicious software, such as Trojan horses, viruses, or worms, could operate in such a way as to disable a system or some of its services.
- Corruption: Undesirably alters system operation by adversely modifying system functions or data.
  For example, user placing backdoor logic in the system to provide subsequent access to a system and its resources by other than the usual procedure.
- Obstruction: A threat action that interrupts delivery of system services by hindering system operation.
  One way to obstruct system operation is to interfere with communications by disabling communication links or altering communication control information. Another way is to overload the system by placing excess burden on communication traffic or processing resources.

Usurpation

A circumstance or event that results in control of system services or functions by an unauthorized entity. This is the threat to the system integrity. Some of the usurpation attacks are:

- Misappropriation: An entity assumes unauthorized logical or physical control of a system resource.
  An example is a distributed denial of service attack, when malicious software is installed on a number of hosts to be used as platforms to launch traffic at a target host. In this case, the malicious software makes unauthorized use of processor and operating system resources.
- Misuse: Causes a system component to perform a function or service that is detrimental (harmful) to system security.
  It can occur by means of either malicious logic or a hacker that has gained unauthorized access to a system. In either case, security functions can be disabled or thwarted.

Attack

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself. An attack is a threat that is carried out (threat action) and, if successful, leads to an undesirable violation of security, or threat consequence. The agent carrying out the attack is referred to as an attacker or threat agent.

We can distinguish two types of attacks:

Active attack: An attempt to alter system resources or affect their operation.

Passive attack: An attempt to learn or make use of information from the system that does not affect system resources.

We can also classify attacks based on the origin of the attack:

Inside attack: Initiated by an entity inside the security perimeter (an “insider”). The insider is authorized to access system resources but uses them in a way not approved by those who granted the authorization.

Outside attack: Initiated from outside the perimeter, by an unauthorized or illegitimate user of the system (an “outsider”). On the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments.

Finally, a countermeasure is any means taken to deal with a security attack. Ideally, a countermeasure can be devised to prevent a particular type of attack from succeeding. When prevention is not possible, or fails in some instance, the goal is to detect the attack then recover from the effects of the attack. A countermeasure may itself introduce new vulnerabilities. In any case, residual vulnerabilities may remain after the imposition of countermeasures. Such vulnerabilities may be exploited by threat agents representing a residual level of risk to the assets. Owners will seek to minimize that risk given other constraints.

Assets

The assets of a computer system can be categorized as hardware, software, data, and communication lines and networks. The physical security of the assets is one of the concerned area, including access to computers system, safeguarding of data transmitted over communication systems, and safeguarding of stored data.

Table: Computer and Network Assets, with Examples of Threats

	Availability	Confidentiality	Integrity
Hardware	Equipment is stolen or disabled, thus denying service	An unencrypted USB drive is stolen.	
Software	Programs are deleted, denying access to users.	An authorized copy of software is made.	A working program is modified, either to cause it to 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.	Message are read. The traffic pattern of messages is observed.	Messages are modified, delayed, reordered, or duplicated. False messages are fabricated.

Hardware: A major threat to computer system hardware is the threat to availability. Hardware is the most vulnerable to attack and the least susceptible to automated controls. Threats include accidental and deliberate damage to equipment as well as theft. The proliferation of personal computers and workstations and the widespread use of LANs increase the potential for losses in this area. Theft of USB drives can lead to loss of confidentiality. Physical and administrative security measures are needed to deal with these threats.

Software: It includes the operating system, utilities, and application programs. A key threat to software is an attack on availability. Software, especially application software, is often easy to delete. Software can also be altered or damaged to render it useless. Careful software configuration management, which includes making backups of the most recent version of software, can maintain high availability. A more difficult problem to deal with is software modification that results in a program that still functions but that behaves differently than before, which is a threat to integrity/authenticity. Computer viruses and related attacks fall into this category. A final problem is protection against software piracy. Although certain countermeasures are available, by and large the problem of unauthorized copying of software has not been solved.

Data: Hardware and software security are typically concerns of computing center professionals or individual concerns of personal computer users. A much more widespread problem is data security, which involves files and other forms of data controlled by individuals, groups, and business organizations.

Security concerns with respect to data are broad, encompassing availability, secrecy, and integrity. In the case of availability, the concern is with the destruction of data files, which can occur either accidentally or maliciously.

The obvious concern with secrecy is the unauthorized reading of data files or databases, and this area has been the subject of perhaps more research and effort than any other area of computer security.

Communication Lines and Networks: Network security attacks can be classified as passive attacks and active attacks. A passive attack attempts to learn or 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 in the nature of eavesdropping on, or monitoring of, transmissions. The goal of the attacker is to obtain information that is being transmitted. Two types of passive attacks are the release of message contents and traffic analysis.

Active attacks involve some modification of the data stream or the creation of a false stream, and can be subdivided into four categories: replay, masquerade, modification of messages, and denial of service.

1.3 Security Requirements

There are a number of ways of classifying and characterizing the countermeasures that may be used to reduce vulnerabilities and deal with threats to system assets. FIPS 200 (Minimum Security Requirements for Federal Information and Information Systems) has defined 17 security-related areas with regard to protecting the confidentiality, integrity, and availability of information systems and the information processed, stored, and transmitted by those systems.

1. Access Control: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

2. Awareness and Training:

(i) Ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, regulations, and policies related to the security of organizational information systems; and

(ii) Ensure that personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

3. Audit and Accountability:

(i) Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and

(ii) Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

4. Certification, Accreditation, and Security Assessments:

(i) Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application;

(ii) Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems;

(iii) Authorize the operation of organizational information systems and any associated information system connections; and

(iv) Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

5. Configuration Management:

(i) Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and

(ii) Establish and enforce security configuration settings for information technology products employed in organizational information systems.

6. Contingency Planning: Establish, maintain, and implement plans for emergency response, backup operations, and post disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

7. Identification and Authentication: Identify information system users, processes acting on behalf of users, or devices, and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

8. Incident Response:

(i) Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user-response activities; and
(ii) Track, document, and report incidents to appropriate organizational officials and/or authorities.

9. Maintenance:

(i) Perform periodic and timely maintenance on organizational information systems; and
(ii) Provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

10. Media Protection:

(i) Protect information system media, both paper and digital;
(ii) Limit access to information on information system media to authorized users; and
(iii) Sanitize or destroy information system media before disposal or release for reuse.

11. Physical and Environmental Protection:

(i) Limit physical access to information systems, equipment, and the respective operating environments to authorized individuals;
(ii) Protect the physical plant and support infrastructure for information systems;
(iii) Provide supporting utilities for information systems;
(iv) Protect information systems against environmental hazards; and
(v) Provide appropriate environmental controls in facilities containing information systems.

12. Planning: Develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.

13. Personnel Security:

(i) Ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions;

(ii) Ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and
(iii) Employ formal sanctions for personnel failing to comply with organizational security policies and procedures.

14. Risk Assessment: Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

15. Systems and Services Acquisition:

(i) Allocate sufficient resources to adequately protect organizational information systems;
(ii) Employ system development life cycle processes that incorporate information security considerations;
(iii) Employ software usage and installation restrictions; and
(iv) Ensure that third party providers employ adequate security measures to protect information, applications, and/or services outsourced from the organization.

16. System and Communications Protection:

(i) Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and
(ii) Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.

17. System and Information Integrity:

(i) Identify, report, and correct information and information system flaws in a timely manner;
(ii) Provide protection from malicious code at appropriate locations within organizational information systems; and
(iii) Monitor information system security alerts and advisories and take appropriate actions in response

1.4 Security Design Principles

Despite years of research and development, it has not been possible to develop security design and implementation techniques that systematically exclude security flaws and prevent all unauthorized actions. In the absence of such foolproof techniques, it is useful to have a set of widely agreed design principles that can guide the development of protection mechanisms.

The National Centers of Academic Excellence in Information Assurance/Cyber Defense, which is jointly sponsored by the U.S. National Security Agency and the U. S. Department of Homeland Security, list the following as fundamental security design principles [NCAE13]:

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege
- Least privilege
- Least common mechanism
- Psychological acceptability
- Isolation
- Encapsulation
- Modularity
- Layering
- Least astonishment

Economy of mechanism means the design of security measures embodied in both hardware and software should be as simple and small as possible. The motivation for this principle is that relatively simple, small design is easier to test and verify thoroughly. With a complex design, there are many more opportunities for an adversary to discover subtle weaknesses to exploit that may be difficult to spot ahead of time.

Fail-safe default means access decisions should be based on permission rather than exclusion. That is, the default situation is lack of access, and the protection scheme identifies conditions under which access is permitted. This approach exhibits a better failure mode than the alternative approach, where the default is to permit access.

Complete mediation means every access must be checked against the access control mechanism. Systems should not rely on access decisions retrieved from a cache. In a system designed to operate continuously, this principle requires that, if access decisions are remembered for future use, careful consideration be given to how changes in authority are propagated into such local memories.

Open design means the design of a security mechanism should be open rather than secret. For example, although encryption keys must be secret, encryption algorithms should be open to public scrutiny. The algorithms can then be reviewed by many experts, and users can therefore have high confidence in them. This is the philosophy behind the National Institute of Standards and Technology (NIST) program of standardizing encryption and hash algorithms, and has led to the widespread adoption of NIST-approved algorithms.

Separation of privilege is defined as a practice in which multiple privilege attributes are required to achieve access to a restricted resource. A good example of this is multifactor user authentication, which requires the use of multiple techniques, such as a password and a smart card, to authorize a user. The term is also now applied to any technique in which a program is divided into parts that are limited to the specific privileges they require in order to perform a specific task. This is used to mitigate the potential damage of a computer security attack.

Least privilege means every process and every user of the system should operate using the least set of privileges necessary to perform the task. A good example of the use of this principle is role-based access control. The system security policy can identify and define the various roles of users or processes. Each role is assigned only those permissions needed to perform its functions. Each permission specifies a permitted access to a particular resource (such as read and write access to a specified file or directory, and connect access to a given host and port). Unless permission is granted explicitly, the user or process should not be able to access the protected resource.

Least common mechanism means the design should minimize the functions shared by different users, providing mutual security. This principle helps reduce the number of unintended communication paths and reduces the amount of hardware and software on which all users depend, thus making it easier to verify if there are any undesirable security implications.

Psychological acceptability implies the security mechanisms should not interfere unduly with the work of users, and at the same time meet the needs of those who authorize access. If security mechanisms hinder the usability or accessibility of resources, users may opt to turn off those mechanisms. Where possible, security mechanisms should be transparent to the users of the system or at most introduce minimal obstruction.

Isolation is a principle that applies in three contexts. First, public access systems should be isolated from critical resources (data, processes, etc.) to prevent disclosure or tampering. In cases where the

sensitivity or criticality of the information is high, organizations may want to limit the number of systems on which that data are stored and isolate them, either physically or logically.

Second, the processes and files of individual users should be isolated from one another except where it is explicitly desired. All modern operating systems provide facilities for such isolation, so individual users have separate, isolated process space, memory space, and file space, with protections for preventing unauthorized access.

And finally, security mechanisms should be isolated in the sense of preventing access to those mechanisms. For example, logical access control may provide a means of isolating cryptographic software from other parts of the host system and for protecting cryptographic software from tampering and the keys from replacement or disclosure.

Encapsulation can be viewed as a specific form of isolation based on object-oriented functionality. Protection is provided by encapsulating a collection of procedures and data objects in a domain of its own so that the internal structure of a data object is accessible only to the procedures of the protected subsystem and the procedures may be called only at designated domain entry points.

Modularity in the context of security refers both to the development of security functions as separate, protected modules, and to the use of a modular architecture for mechanism design and implementation. With respect to the use of separate security modules, the design goal here is to provide common security functions and services, such as cryptographic functions, as common modules. For example, numerous protocols and applications make use of cryptographic functions. Rather than implementing such functions in each protocol or application, a more secure design is provided by developing a common cryptographic module that can be invoked by numerous protocols and applications.

Layering refers to the use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems. By using multiple, overlapping protection approaches, the failure or circumvention of any individual protection approach will not leave the system unprotected.

Least astonishment means a program or user interface should always respond in the way that is least likely to astonish (surprise) the user. For example, the mechanism for authorization should be transparent enough to a user that the user has a good intuitive understanding of how the security goals map to the provided security mechanism.

1.5 Attack Surfaces and Attack Trees

Attack Surfaces

An attack surface consists of the reachable and exploitable vulnerabilities in a system. 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 processes incoming data, e-mail, XML, office documents, and industry-specific custom data exchange formats
- Interfaces, SQL, and web forms
- An employee with access to sensitive information vulnerable to a social engineering attack

Attack surfaces can be categorized in the following way:

Network attack surface: This category refers to vulnerabilities over an enterprise network, wide-area network, or the Internet. Included in this category are network protocol vulnerabilities, such as those used for a denial-of-service attack, disruption of communications links, and various forms of intruder attacks.

Software attack surface: This refers to vulnerabilities in application, utility, or operating system code. A particular focus in this category is Web server software.

Human attack surface: This category refers to vulnerabilities created by personnel or outsiders, such as social engineering, human error, and trusted insiders.

An attack surface analysis is a useful technique for assessing the scale and severity of threats to a system. A systematic analysis of points of vulnerability makes developers and security analysts aware of where security mechanisms are required. Once an attack surface is defined, designers may be able to find ways to make the surface smaller, thus making the task of the adversary more difficult. The attack surface also provides guidance on setting priorities for testing, strengthening security measures, or modifying the service or application.

Attack Trees

An attack tree is a branching, hierarchical data structure that represents a set of potential techniques for exploiting security vulnerabilities.

The security incident that is the goal of the attack is represented as the root node of the tree, and the ways by which an attacker could reach that goal are iteratively and incrementally represented as branches and sub nodes of the tree.

Each sub node defines a sub goal, and each sub goal may have its own set of further sub goals, and so on. The final nodes on the paths outward from the root, that is, the leaf nodes, represent different ways to initiate an attack.

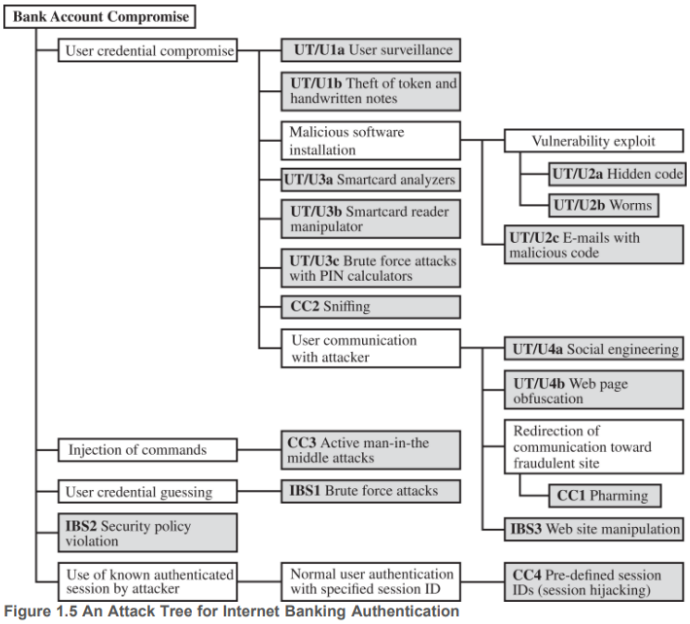

Figure 1.5 An Attack Tree for Internet Banking Authentication

1.6 Computer Security Strategy

Computer 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?

Security Policy

The first step in devising security services and mechanisms is to develop a security policy. Those involved with computer security use the term security policy in various ways. At the least, a security policy is an informal description of desired system behavior. Such informal policies may reference requirements for security, integrity, and availability.

More usefully, a security policy is a formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources. Such a formal security policy lends itself to being enforced by the system's technical controls as well as its management and operational controls.

In developing a security 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

Further, the manager must consider the following trade-offs:

- Ease of use versus security
- Cost of security versus cost of failure and recovery

Security policy is thus a business decision, possibly influenced by legal requirements.

Security Implementation

Security implementation involves four complementary courses of action:

Prevention: An ideal security scheme is one in which no attack is successful. Although this is not practical in all cases, there is a wide range of threats in which prevention is a reasonable goal. For example, consider the transmission of encrypted data. If a secure encryption algorithm is used, and if measures are in place to prevent unauthorized access to encryption keys, then attacks on confidentiality of the transmitted data will be prevented.

Detection: In a number of cases, absolute protection is not feasible, but it is practical to detect security attacks. For example, there are intrusion detection systems designed to detect the presence of unauthorized individuals logged onto a system. Another example is detection of a denial of service attack, in which communications or processing resources are consumed so they are unavailable to legitimate users.

Response: If security mechanisms detect an ongoing attack, such as a denial of service attack, the system may be able to respond in such a way as to halt the attack and prevent further damage.

Recovery: An example of recovery is the use of backup systems, so if data integrity is compromised, a prior, correct copy of the data can be reloaded.

Assurance and Evaluation

Those who are "consumers" of computer security services and mechanisms (e.g., system managers, vendors, customers, and end users) desire a belief that the security measures in place work as intended. That is, security consumers want to feel that the security infrastructure of their systems meet security requirements and enforce security policies. These considerations bring us to the concepts of assurance and evaluation.

Assurance is an attribute of an information system that provides grounds for having confidence that the system operates such that the system's security policy is enforced. This encompasses both system design and system implementation. Thus, assurance deals with the questions, "Does the security system design meet its requirements?" and "Does the security system implementation meet its specifications?" Assurance is expressed as a degree of confidence, not in terms of a formal proof that a design or implementation is correct.

Evaluation is the process of examining a computer product or system with respect to certain criteria. Evaluation involves testing and may also involve formal analytic or mathematical techniques. The central thrust of work in this area is the development of evaluation criteria that can be applied to any security system (encompassing security services and mechanisms) and that are broadly supported for making product comparisons.

Practice Questions

1. Define computer security.
2. What is the difference between passive and active security threats?
3. List and briefly define categories of passive and active network security attacks.
4. List and briefly define the fundamental security design principles.
5. Explain the difference between an attack surface and an attack tree.
6. Consider an automated teller machine (ATM) to which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement.