1 : Computer and Network Security Concepts

IT6406 – Network Security and Audit

Level III - Semester 6

Overview

This section aims at providing the fundamentals of information security in the context of networks. It provide the details on how attacks and threats can affect computer systems and network, and the potential attack surfaces that needs to be protected against such attacks.

Intended Learning Outcomes

At the end of this lesson, you will be able to;

- Describe key concepts of computer security.
- Describe the OSI security architecture with its three focus areas.
- Describe examples of the types of threats and attacks that apply to different categories of computer and network assets.
- Discuss the principle concepts of a network access control systems and access enforcement methods.

List of sub topics

1.1 Computer Security Concepts

1.2 The OSI Security Architecture

1.3 Security Attacks

1.4 Security Services

1.5 Security Mechanisms

1.6 Fundamental Security Design Principles

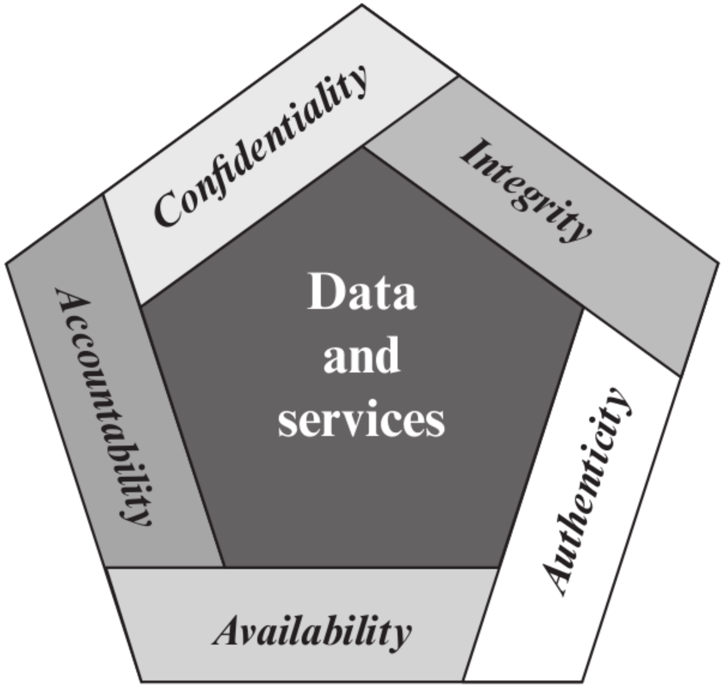
1.7 Attack Surfaces and Attack Trees

1.8 A Model for Network Security

1.9 Standards

1.1 Computer Security Concepts

- **Computer Security:** The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications).



1.1 Computer Security Concepts (cont.)

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

- **Integrity:** Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.

- **Availability:** Ensuring timely and reliable access to and use of information.

- **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.

- **Accountability:** The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity.

1.2 The OSI Security Architecture

- A systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements is needed.

- The International Telecommunication Union (ITU) Telecommunication Standardization Sector (ITU-T) recommends such a systematic approach, called X.800 Security Architecture for OSI.

- Many computer and communications vendors have developed security features for their products and services according to this standard.

1.2 The OSI Security Architecture (cont.)

- The OSI security architecture focuses on security attacks, mechanisms, and services.
- **Security attack:** Any action that compromises the security of information owned by an organization.
- **Security mechanism:** A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
- **Security service:** A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization. The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

1.3 Security Attacks

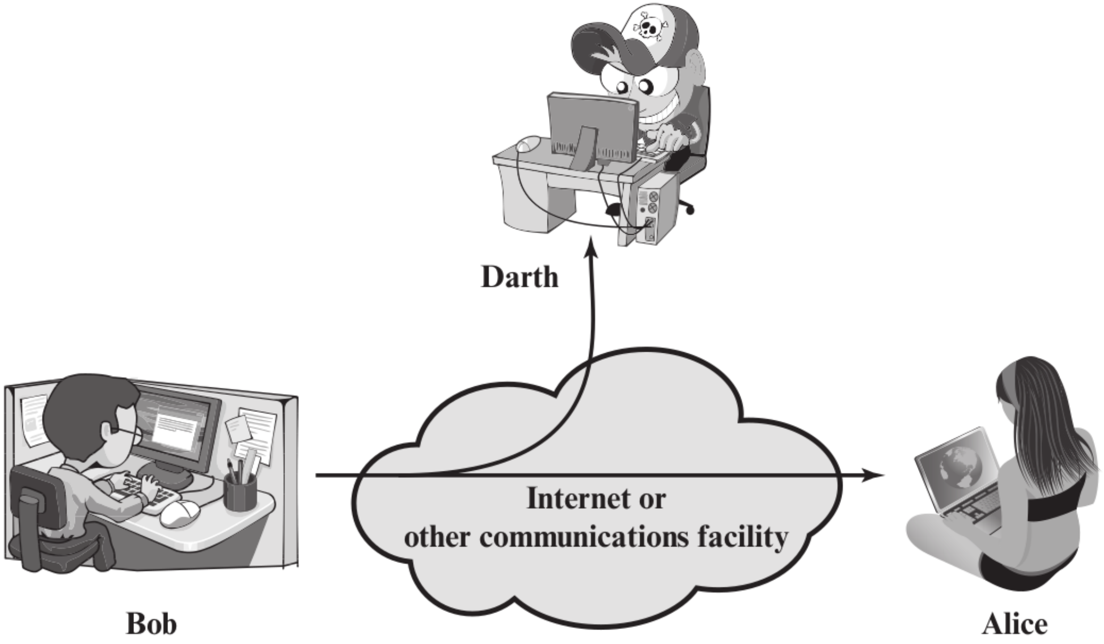
- Security attacks can be classified into two groups as ***passive attacks*** and ***active attacks***.

- 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.

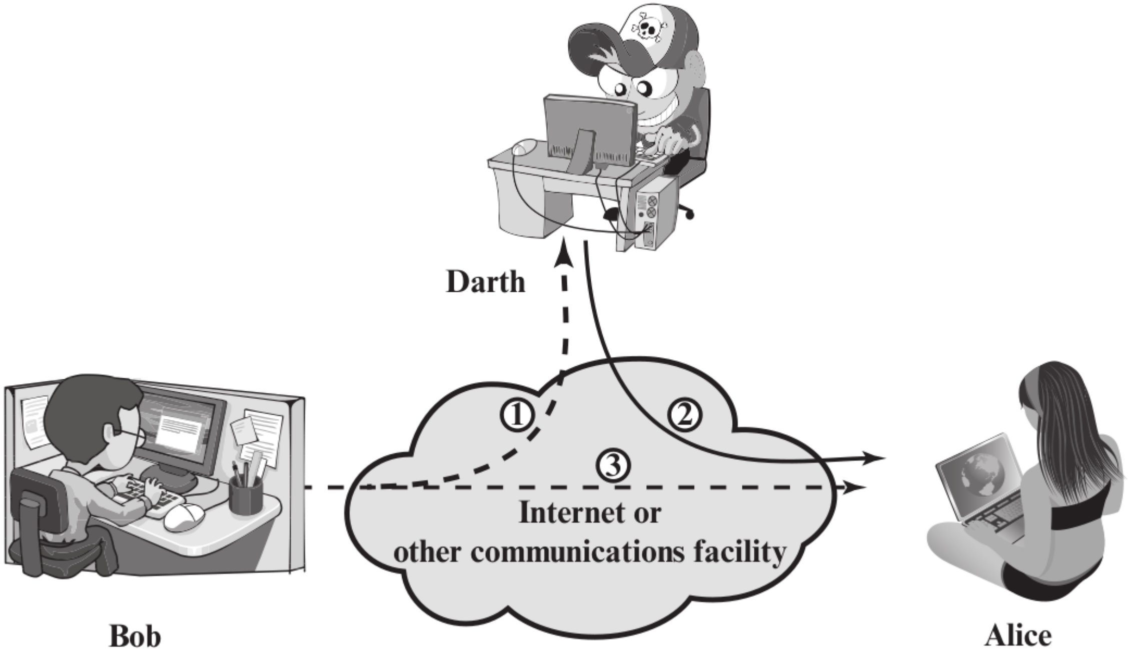
1.3 Security Attacks (cont.)

- **Passive Attacks:**
  - Passive attacks are in the nature of eavesdropping on, or monitoring of, transmissions.
  - The goal of the opponent is to obtain information that is being transmitted.
  - Two types of passive attacks: the release of message contents and traffic analysis.



1.3 Security Attacks (cont.)

- **Active Attacks:**
  - modification of the data stream or the creation of a false stream.
  - *Masquerade* - one entity pretends to be a different entity.
  - *Replay* - passive capture subsequent retransmission of data.
  - *Modification of messages* - some portion of a legitimate message is altered
  - *Denial of service* - prevents the normal use of communications.



© 2022 e-Learning Centre, UCSC

1.4 Security Services

- A processing or communication service that is provided by a system to give a specific kind of protection to system resources.
- X.800 divides these services into five categories.
- Authentication: The authentication service is concerned with assuring that a communication is authentic.
- Access Control: In the context of network security, access control is the ability to limit and control the access to host systems and applications via communications links.
- Data Confidentiality: The protection of transmitted data from passive attacks.
- Data Integrity: Assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays.
- Nonrepudiation: Prevents either sender or receiver from denying a transmitted message.

1.5 Security Mechanisms

- Security mechanisms can be categorised into two groups:
  - Specific security mechanisms
  - Pervasive security mechanisms

- **Specific security mechanisms:** May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

- **Pervasive security mechanisms:** Mechanisms that are not specific to any particular OSI security service or protocol layer.

1.5 Security Mechanisms (cont.)

Specific security mechanisms:

- Encipherment: The use of mathematical algorithms to transform data into a form that is not readily intelligible.
- Digital Signature: A cryptographic transformation of data for a recipient to prove the source and integrity of it.
- Access Control: A variety of mechanisms that enforce access rights to resources.
- Data Integrity: A variety of mechanisms used to assure the integrity of a data unit or stream of data units.
- Authentication Exchange: A mechanism intended to ensure the identity of an entity by means of information exchange.

1.5 Security Mechanisms (cont.)

Specific security mechanisms:

- Traffic Padding: The insertion of bits into gaps in a data stream to frustrate traffic analysis attempts.
- Routing Control: Enables selection of particular physically secure routes for certain data.
- Notarization: The use of a trusted third party to assure certain properties of a data exchange.

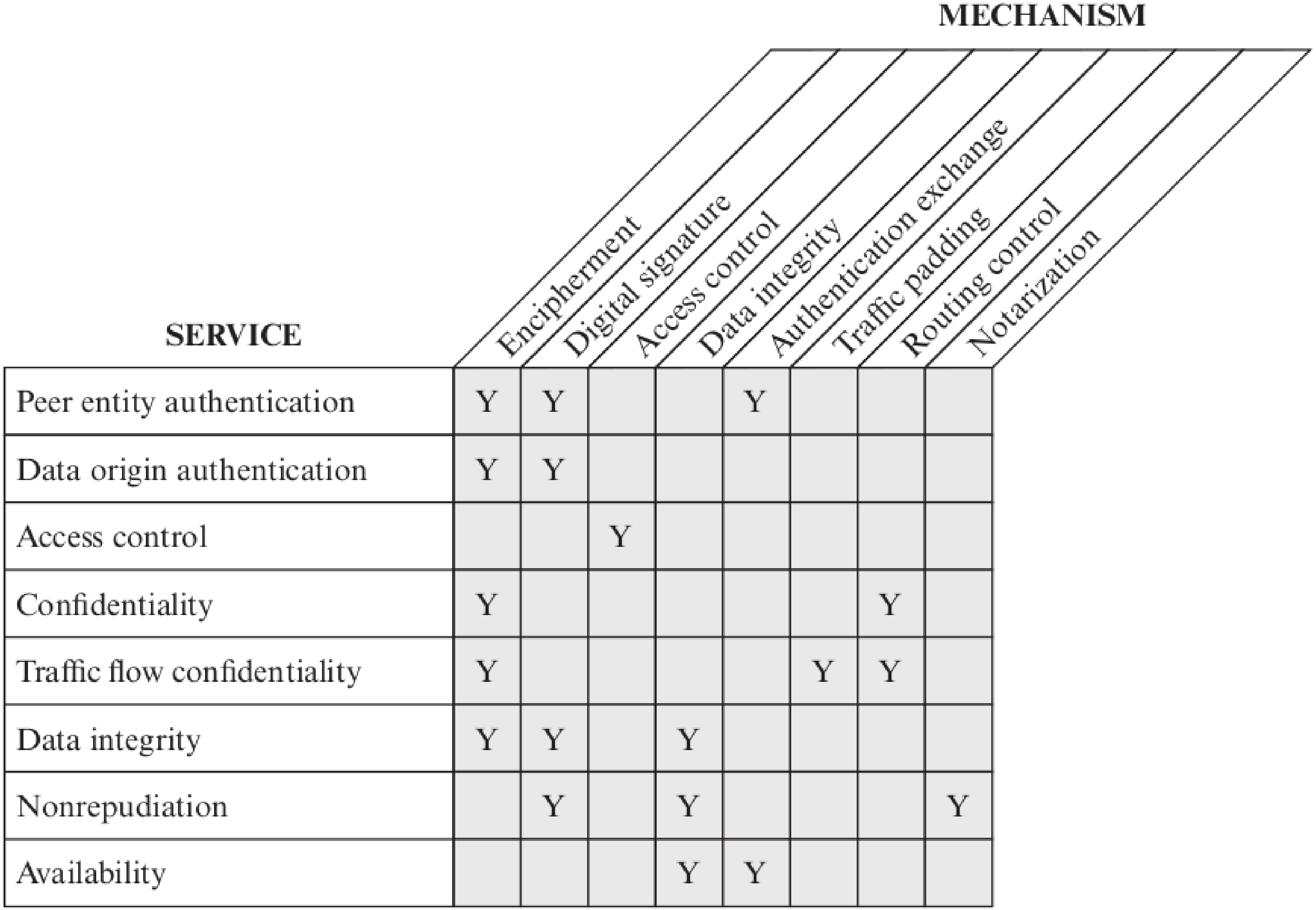
1.5 Security Mechanisms (cont.)

Pervasive security mechanisms:

- Trusted Functionality: That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
- Security Label: The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
- Event Detection: Detection of security-relevant events.
- Security Audit Trail: Data collected and potentially used to facilitate a security audit, which is an independent review and examination of system records and activities.
- Security Recovery: Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.

1.5 Security Mechanisms (cont.)

Relationship Between Security Services and Mechanisms:



MECHANISM

SERVICE	Encipherment	Digital signature	Access control	Data integrity	Authentication exchange	Traffic padding	Routing control	Notarization
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Nonrepudiation		Y		Y				Y
Availability				Y	Y			

1.6 Fundamental Security Design Principles

- There are no foolproof techniques to systematically exclude security flaws and prevent all unauthorized actions.

- So, 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 list the following as fundamental security design principles:
    - 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

1.6 Fundamental Security Design Principles (cont.)

- Economy of mechanism: The design of security measures embodied in both hardware and software should be as simple and small as possible.
- Fail-safe defaults: Access decisions should be based on permission rather than exclusion.
- Complete mediation: Every access must be checked against the access control mechanism. Systems should not rely on access decisions retrieved from a cache.
- Open design: The design of a security mechanism should be open rather than secret.
- Separation of privilege: A practice in which multiple privilege attributes are required to achieve access to a restricted resource.
- Least privilege: Every process and every user of the system should operate using the least set of privileges necessary to perform the task.

1.6 Fundamental Security Design Principles (cont.)

- Least common mechanism: The design should minimize the functions shared by different users, providing mutual security.

- Psychological acceptability: The security mechanisms should not interfere unduly with the work of users, while at the same time meeting the needs of those who authorize access.

- Isolation: Public access systems should be isolated from critical resources (data, processes, etc.) to prevent disclosure or tampering.

- Encapsulation: A specific form of isolation based on object-oriented functionality.

- Modularity: 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.

1.6 Fundamental Security Design Principles (cont.)

- Layering: The use of multiple, overlapping protection approaches addressing the people, technology, and operational aspects of information systems.

- Least astonishment: A program or user interface should always respond in the way that is least likely to astonish the user.

1.7 Attack Surfaces and Attack Trees

- An ***attack surface*** consists of the reachable and exploitable vulnerabilities in a system.

- Examples:

  - 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, email, 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

1.7 Attack Surfaces and Attack Trees (cont.)

- Attack surfaces can be categorized as follows:
- **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.

1.7 Attack Surfaces and Attack Trees (cont.)

- 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 that an attacker could reach that goal are iteratively and incrementally represented as branches and subnodes of the tree.

- Each subnode defines a subgoal, and each subgoal may have its own set of further subgoals, and so on.

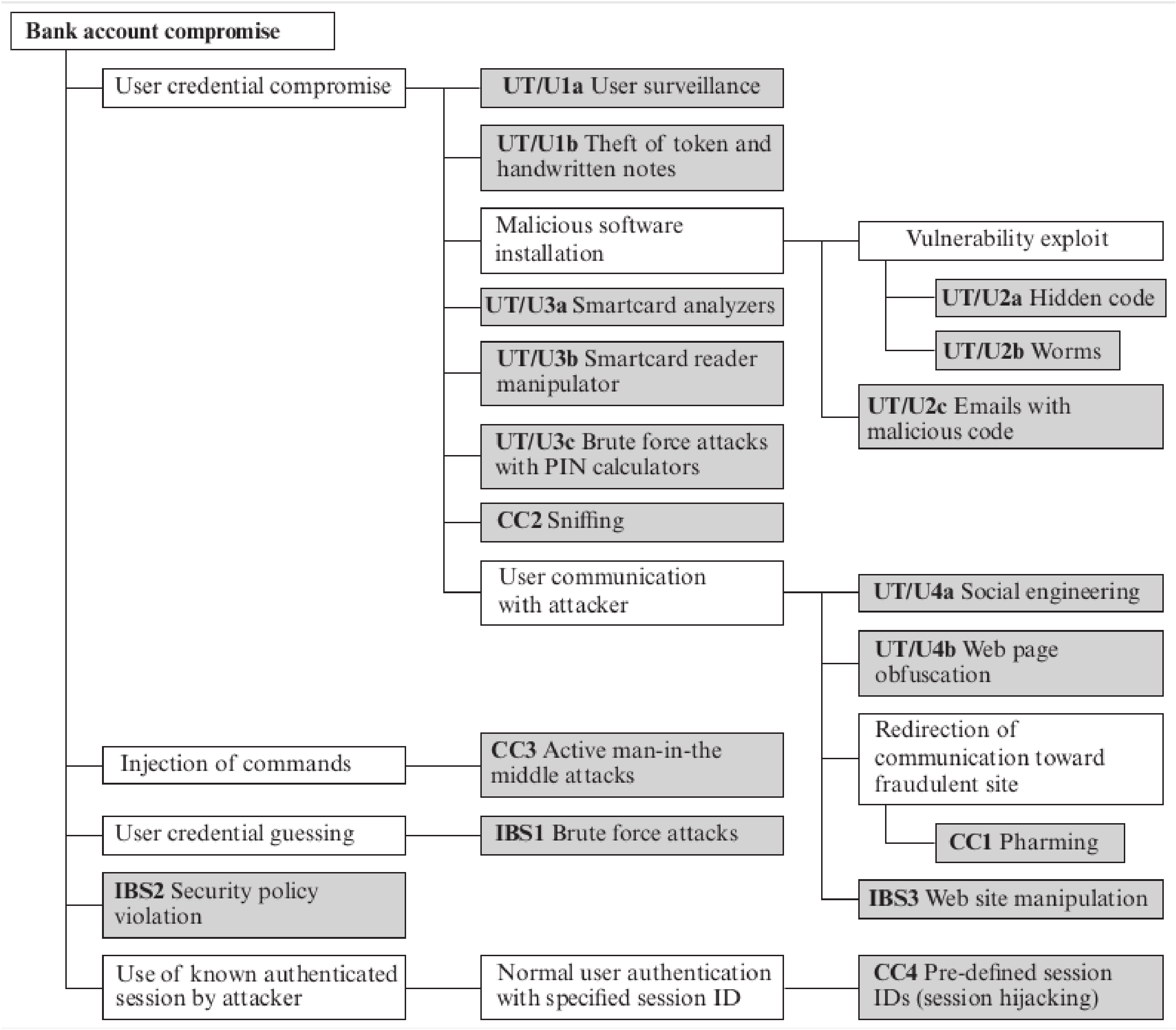
- The leaf nodes, represent different ways to initiate an attack.

- Each node other than a leaf is either an AND-node or an OR-node.

- The motivation for the use of attack trees is to effectively exploit the information available on attack patterns.

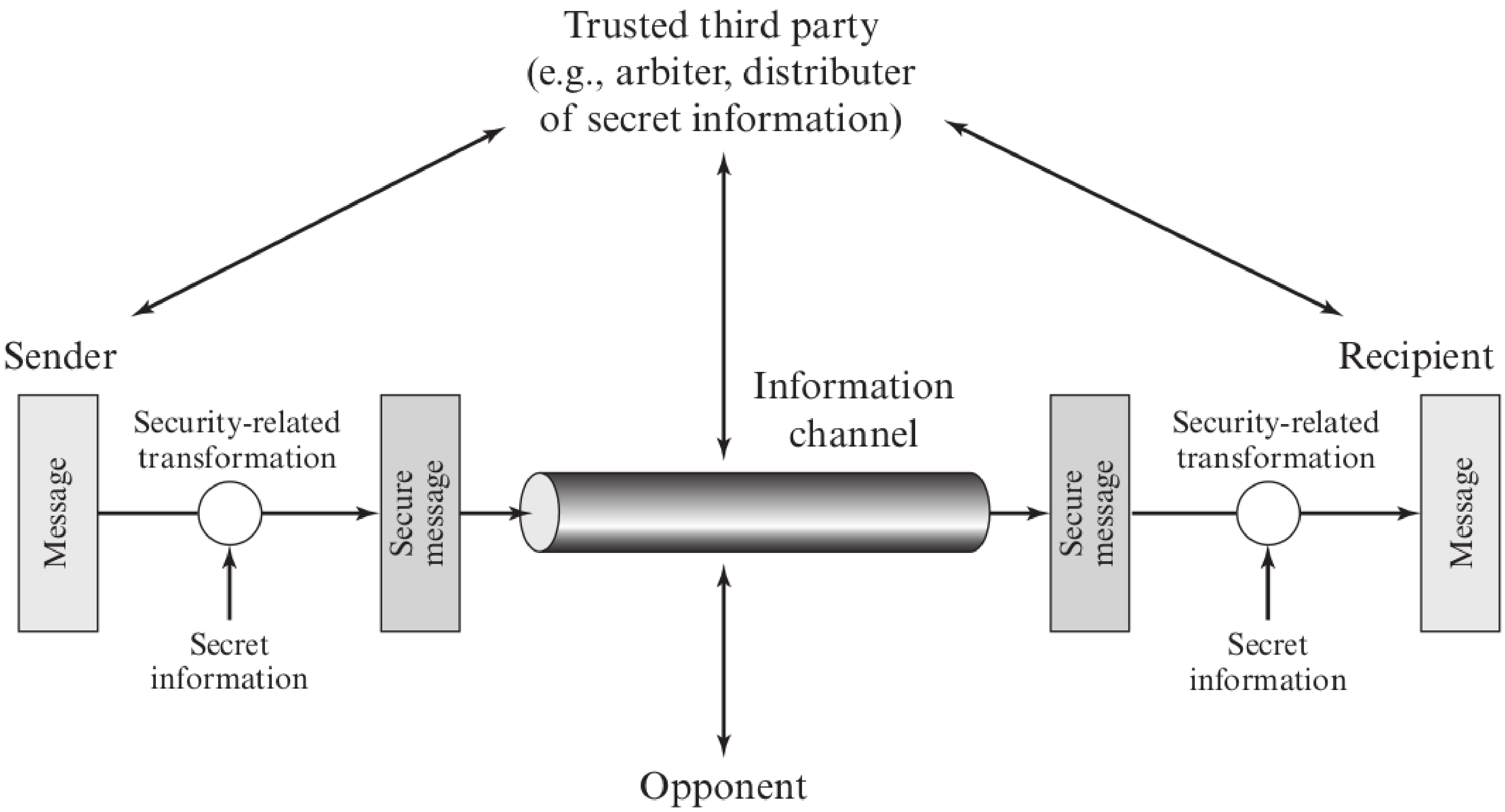
1.7 Attack Surfaces and Attack Trees (cont.)

- An example attack tree:



- Bank account compromise
  - User credential compromise
    - **UT/U1a** User surveillance
    - **UT/U1b** Theft of token and handwritten notes
    - Malicious software installation
      - Vulnerability exploit
        - **UT/U2a** Hidden code
        - **UT/U2b** Worms
      - **UT/U2c** Emails with malicious code
    - **UT/U3a** Smartcard analyzers
    - **UT/U3b** Smartcard reader manipulator
    - **UT/U3c** Brute force attacks with PIN calculators
    - **CC2** Sniffing
    - User communication with attacker
      - **UT/U4a** Social engineering
      - **UT/U4b** Web page obfuscation
      - Redirection of communication toward fraudulent site
        - **CC1** Pharming
      - **IBS3** Web site manipulation
  - Injection of commands
    - **CC3** Active man-in-the middle attacks
  - User credential guessing
    - **IBS1** Brute force attacks
  - **IBS2** Security policy violation
  - Use of known authenticated session by attacker
    - Normal user authentication with specified session ID
      - **CC4** Pre-defined session IDs (session hijacking)

1.8 A Model for Network Security



1.8 A Model for Network Security

- This general model shows that there are four basic tasks in designing a particular security service:

  1. Design an algorithm for performing the security-related transformation. The algorithm should be such that an opponent cannot defeat its purpose.

  2. Generate the secret information to be used with the algorithm.

  3. Develop methods for the distribution and sharing of the secret information.

  4. Specify a protocol to be used by the two principals that makes use of the security algorithm and the secret information to achieve a particular security service.

1.9 Standards

- Many of the security techniques and applications have been standardised.

- Various organizations have been involved in the development or promotion of these standards.

- National Institute of Standards and Technology (NIST): a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private-sector innovation.

- Internet Society (ISOC): a professional membership society with worldwide organizational and individual membership. It is the organization home for the groups responsible for Internet infrastructure standards, including the Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB).

1.9 Standards (cont.)

- The International Telecommunication Union (ITU): an international organization within the United Nations System in which governments and the private sector coordinate global telecom networks and services.

- The International Organization for Standardization (ISO): a worldwide federation of national standards bodies from more than 140 countries, one from each country.

References

- Cryptography and Network Security, Principles and Practice, 7th Edition, William Stallings.