

ECE-GY 9383

Special Topics in Network Security

1 - Introduction

Slides credits: Shivendra S. Panwar, Fraida Fund

CSE/ECE zjzhao



NYU

**TANDON SCHOOL
OF ENGINEERING**

In this lecture



- Basic concepts of security
- Security attacks
- Security services
- Security mechanisms
- Model for network security

(Reference: Chapter 1 of Stallings, “Network Security Essentials”)

This course concerns measures to deter, prevent, detect, and correct **security violations** involving the use of a computer network.

For example...

Security violation – example 1

User A transmits a file to user B. The file contains sensitive information (e.g., payroll records) that is to be protected from disclosure. User C, who is not authorized to read the file, is able to monitor the transmission and capture a copy of the file during its transmission.

Security objectives and elements

Important security services

- **Confidentiality** protects transmitted data from analysis – no snooping, no wiretapping, a.k.a. to ensure **Data Privacy**
- **Integrity** ensures that a piece of information is not altered
- **Availability** ensures user accessibility to use a system
- **Authenticity** identifies and ensures the origin of information
- **Non-repudiation** ensures that the sender (or receiver) cannot deny sending (or receiving) a piece of information, a.k.a. **Accountability**

AAA for identity access security

- **Authentication** to ensure users' identity – you are who you say you are
- **Authorization** to assign legitimate privilege to users – access control
- **Accounting** to log user behavior and resource usage for management, planning, billing, security analysis, ...

Pick up what we
discussed in the
IAP class

Security violation – example 2

A network manager, D, transmits a message to a computer, E, under its management. User F intercepts the message, alters its contents to add or delete entries, and then forwards the message to E.

Security violation – example 3

Rather than intercepting a message, user F constructs its own message with the desired entries and transmits that message to computer E as if it had come from manager D. Computer E accepts the message as coming from manager D and updates its authorization file accordingly.

Security violation – example 4

A message is sent from a customer to a stockbroker with instructions for various transactions. Subsequently, the investments lose value and the customer denies sending the message.

Security violation – example 5

An employee is fired without warning. The personnel manager sends a message to a server system to invalidate the employee's account. When the invalidation is accomplished, the server is to post a notice to the employee's file as confirmation of the action. The employee is able to intercept the message and delay it long enough to make a final access to the server to retrieve sensitive information. The message is then forwarded, the action taken, and the confirmation posted. The employee's action may go unnoticed for some considerable time.

Basic concepts of security

Security standards

An organization sets standards as a systematic way to

- Define security requirements/objectives
- Characterize approaches to satisfying these requirements

See e.g.:

- NIST *Standards for Security Categorization of Federal Information Systems* (FIPS 199) <http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf>. FIPS 200 specifies the minimum-security requirements for non-military federal information systems.
- ISO/IEC 27001 developed to help organizations in information protection by a systematic approach through the adoption of an Information Security Management System including security techniques and implementation requirements <https://www.iso.org/isoiec-27001-information-security.html>

NIST “CIA triad” defines 3 key objectives

- **Confidentiality:** information is not disclosed to unauthorized individuals (**data confidentiality**); individuals control what information is collected about them, and to whom it is disclosed (**privacy**).
- **Integrity:** no unauthorized changes to stored or transmitted data (**data integrity**); systems perform as they are supposed to (**system integrity**).
- **Availability:** systems/services should work promptly for authorized users
(Defined in NIST standards)



Other key objectives

Authenticity

- 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


ISO/IEC 27001 ISMS



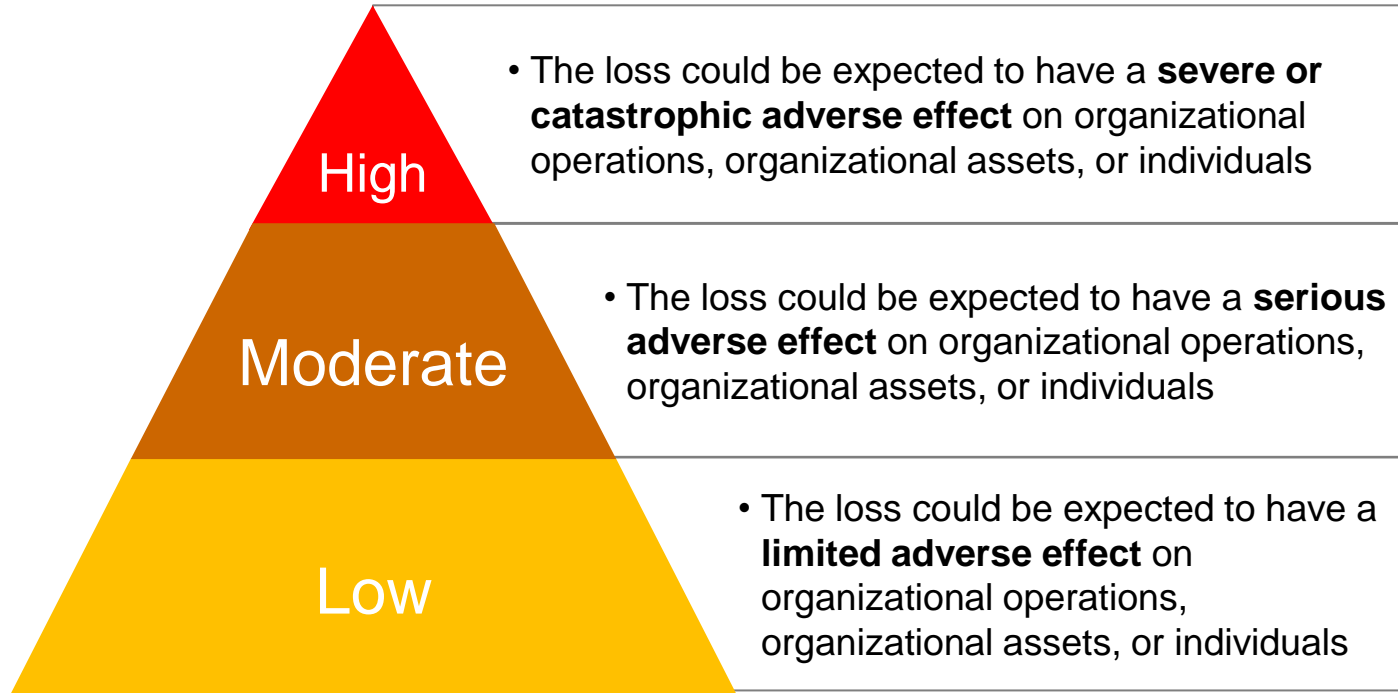
A set of rules that an organization needs to establish and **ensure CIA triad**

1. **identify stakeholders and their expectations** of the organization in terms of information security
2. identify **which risks exist** for the information
3. **define controls** (safeguards) and other **mitigation methods** to meet the identified expectations and handle risks
4. **set clear objectives on what needs to be achieved** with information security
5. **implement** all the controls and other risk treatment methods
6. **continuously measure** if the implemented controls perform as expected
7. make **continuous improvement** to make the whole ISMS work better

Examples: these support/violate which objective?

- Twitter puts a blue checkmark  next to some accounts of public interest, confirming that these accounts are controlled by the individuals they claim to represent.
- A customer database is breached, and the attackers widely distribute names and email addresses of customers.
- The IP address and username associated with every login to a computer system is stored in a system log.
- A computer virus affects the NYU Classes system, and deletes all grade records.
- A DDoS (distributed denial-of-service) attack prevents access to the NYU WiFi network.

Breach of security levels of impact



The **security category (SC)** of a type of information is expressed as a combination of security objectives + level of impact.

	POTENTIAL IMPACT		
Security Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

TABLE 1: POTENTIAL IMPACT DEFINITIONS FOR SECURITY OBJECTIVES

EXAMPLE: A law enforcement organization managing extremely sensitive investigative information determines that

- the potential impact from a loss of confidentiality is severe,
- the potential loss of data integrity seriously effect the operations, and
- the potential impact from a loss of data availability is moderate.

The resulting **security category**, SC, of this information type is expressed as:

SC_{investigative information} =
{(confidentiality, HIGH),
(integrity, MODERATE),
(availability, MODERATE)}.

Source: NIST FIPS 199

OSI security architecture

- **Security attack:** action that compromises security of information.
- **Security mechanism:** process or device designed to detect, prevent, or recover from security attack.
- **Security service:** processing or communication service that enhances security of information processing or transmission.
- *Security services use security mechanisms to counter security attacks.*

(Defined in ITU-T Recommendation X.800, *Security Architecture for OSI*)

Security attacks

What is Security

- There is safety or reliability
 - Accidental failures
- Usability
 - Problems that occur from builder/user errors
- **Security**
 - Deals with **intentional actions** by intelligent attackers to cause **failures** or gain **unauthorized access**
 - involves safety, reliability, and usability

Attacker Motivations



- Financial
 - Bank fraud, credit cards, identity theft, spam, fake anti-virus, confidence scams
- Fame
 - Website defacements, leaking information
- Political
 - Industrial espionage, steal sensitive information
- Curiosity
 - Learn how a system works
-

Threat vs. attack (IETF RFC 4949)



- **Threat:** there is a **circumstance or action** that could breach security and cause harm (potential for violation of security). That is, a threat is a **possible danger** that might exploit a vulnerability.

- **Attack:** an **intentional violation** of system security (realized violation of network security). That is, an intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.



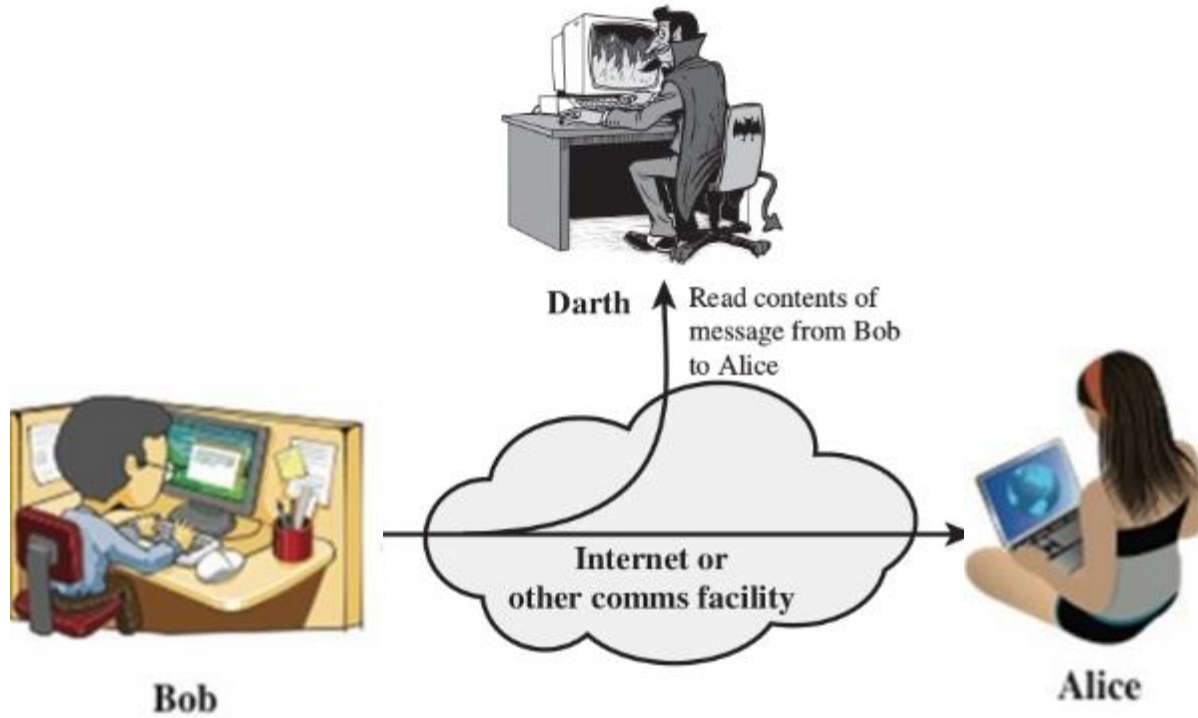
Attack classification: passive vs. active

- **Passive attack:** attempts to learn or make use of information from the system, but does not affect system resources.
(Two types: Release of message contents, Traffic analysis)



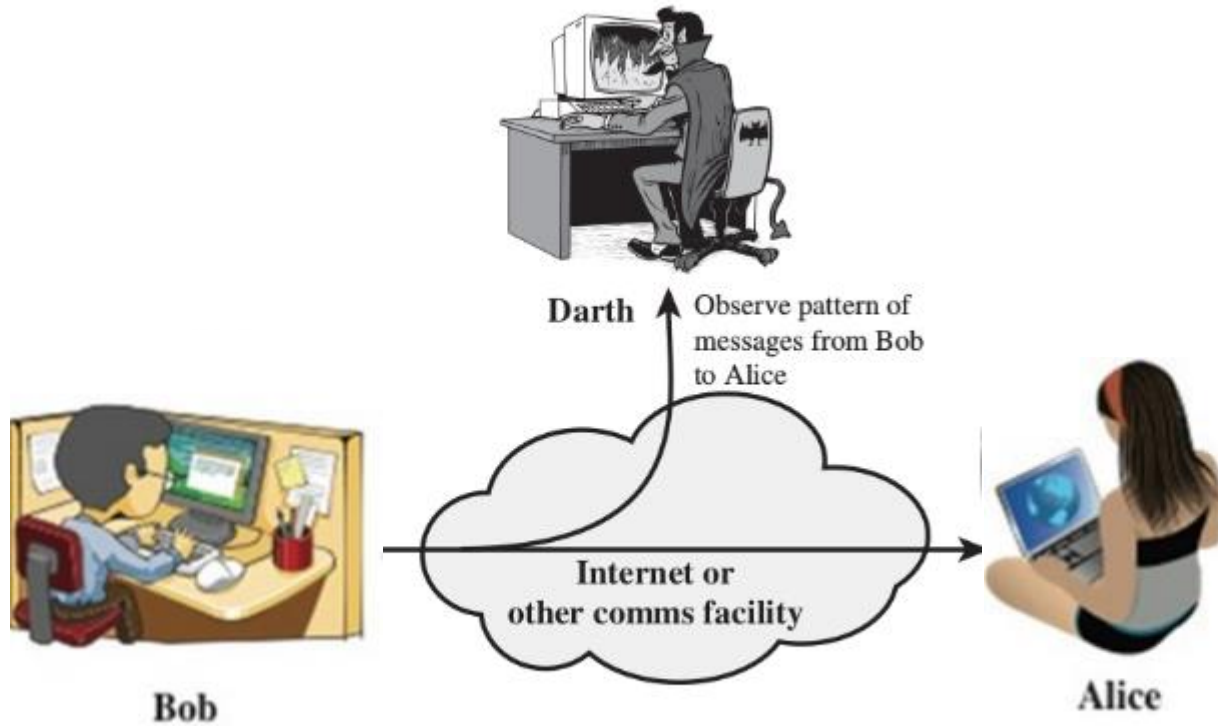
- **Active attack:** attempts to alter system resources or affect their operation.
(Masquerade, replay, modification of message contents, denial of service)

Passive attack: release of message contents



(a) Release of message contents

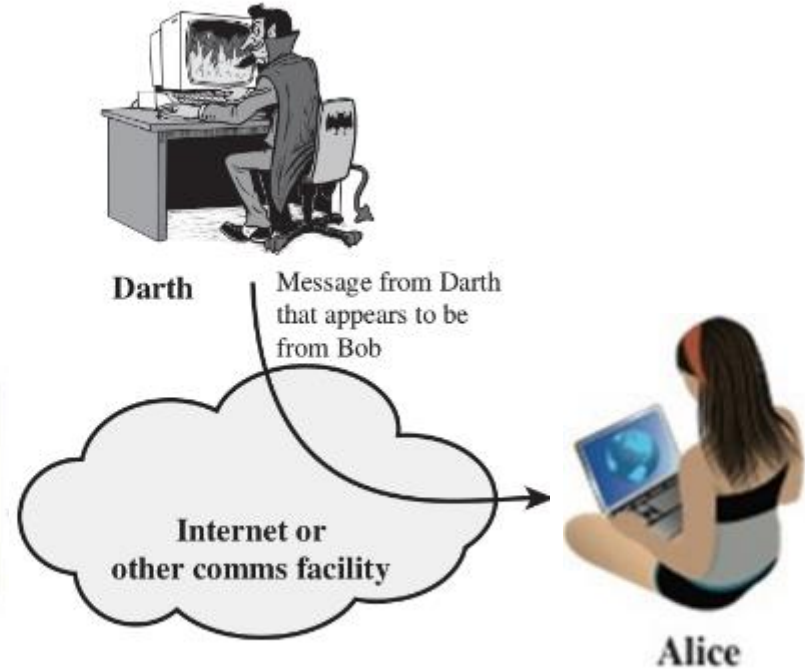
Passive attack: traffic analysis



(b) Traffic analysis

Active attack: masquerade

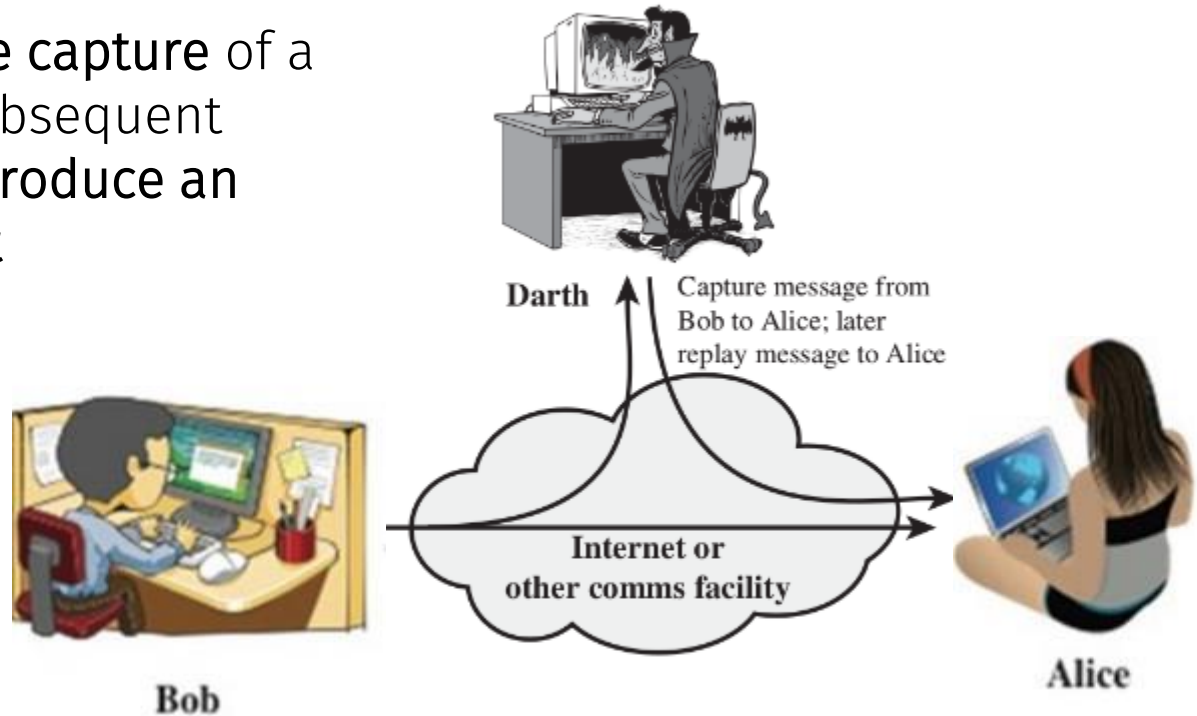
- Takes place when one entity pretends to be a different entity
- Usually includes one of the other forms of active attack



(a) Masquerade

Active attack: replay

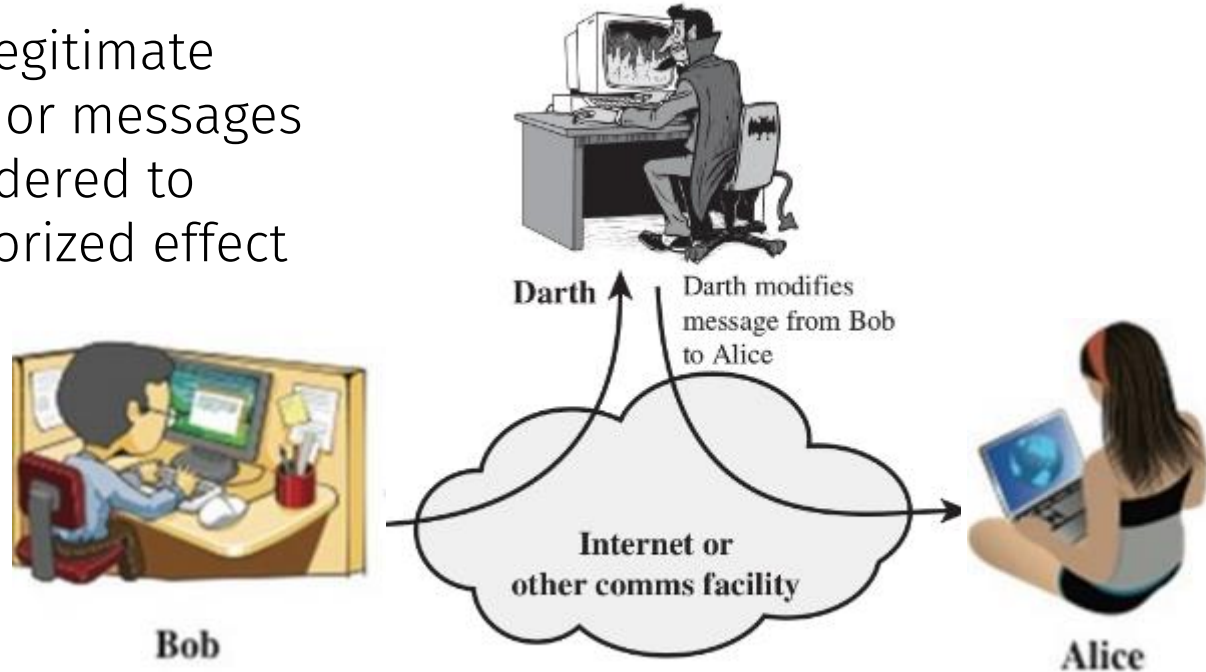
- Involves the **passive capture** of a data unit and its subsequent retransmission to **produce an unauthorized effect**



(b) Replay

Active attack: modification of messages

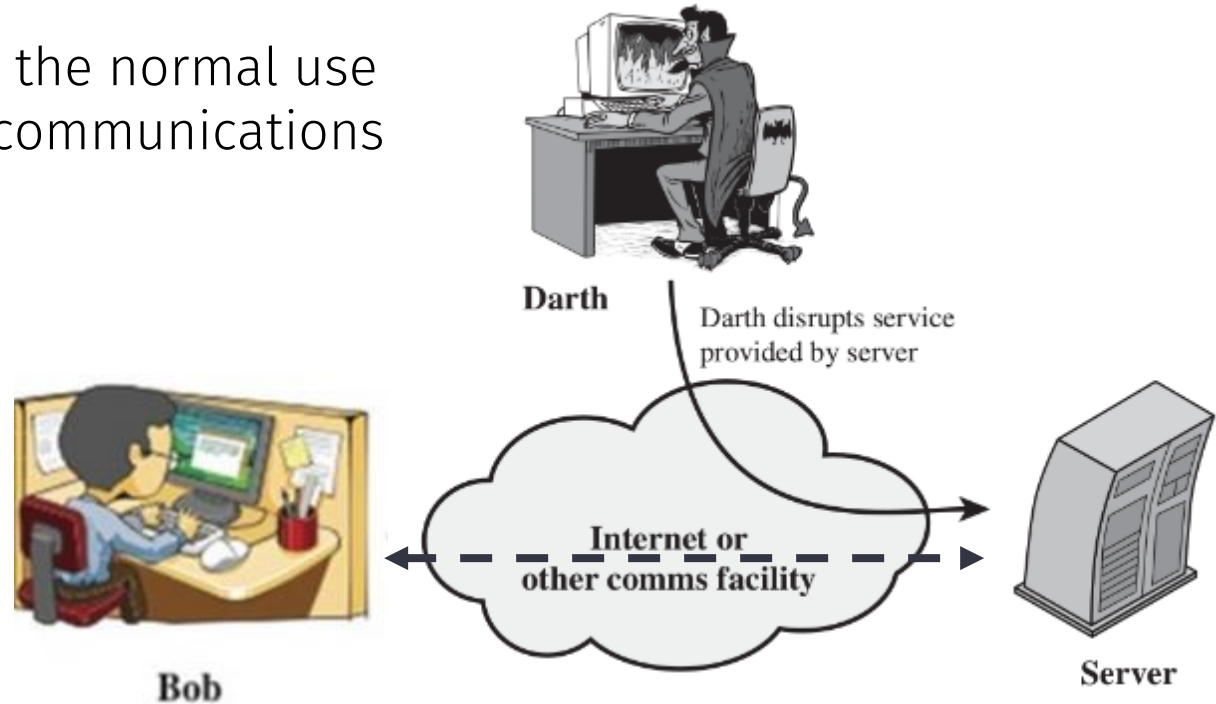
- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect



(c) Modification of messages

Active attack: denial of service

- Prevents or inhibits the normal use or management of communications facilities



(d) Denial of service

Attack surfaces

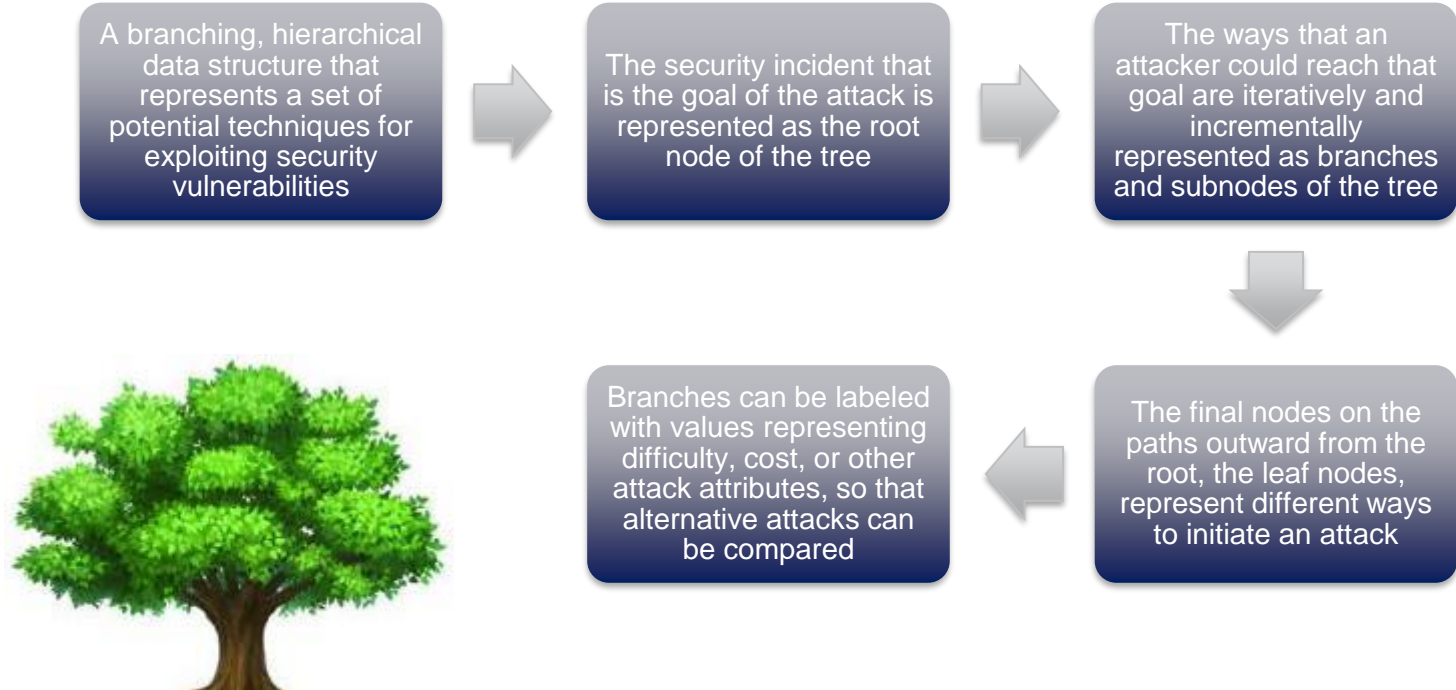


An **attack surface** is a part of a system that may have exploitable vulnerabilities.

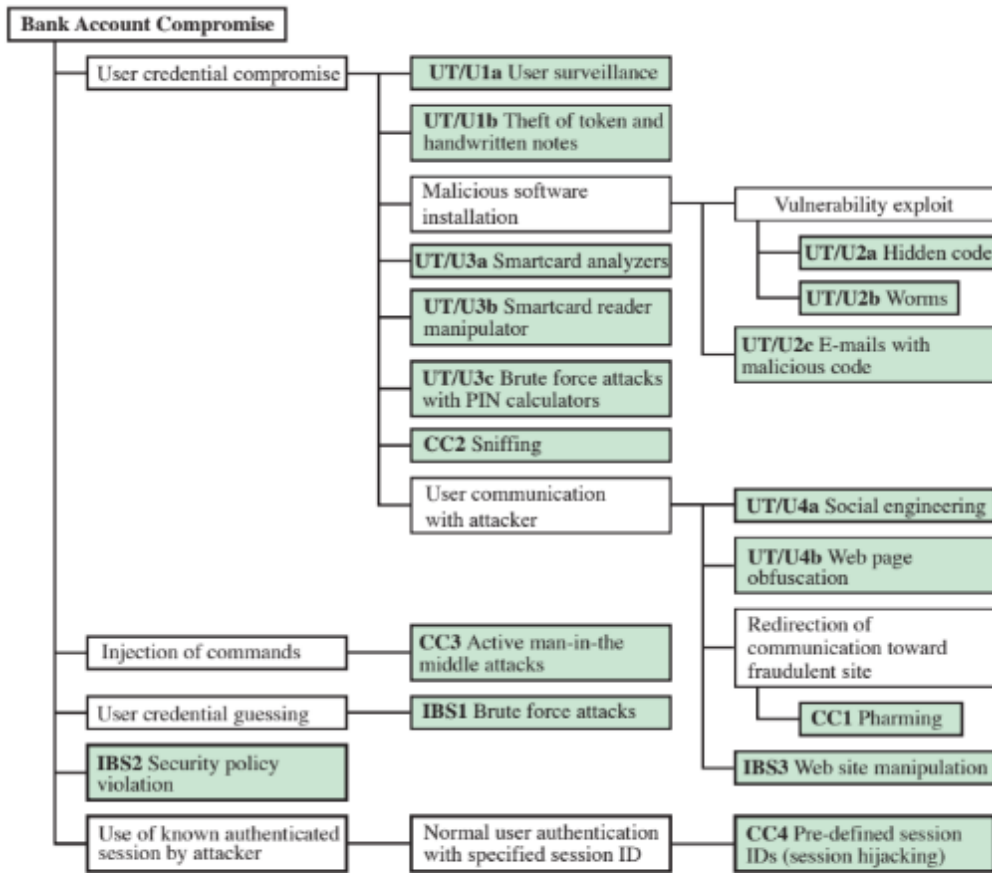
- **Network attack surface** may include network protocol vulnerabilities, intruder attacks.
- **Software attack surface** may include application code, operating system code.
- **Human attack surface** may include social engineering, human error.

Attack surface analysis helps define scale of threats to system.

Attack trees



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



EXAMPLE: Attack tree for Internet banking application

Objective of attacker: compromise user account (root of tree)

Analysis reveals **three components** that may be attacked: user terminal and user (UT/U), communications channel (CC), Internet banking server (IBS).

Attack **strategies:** listed in white boxes.

Figure 1.4 An Attack Tree for Internet Banking Authentication

Security services

Security Services

- Defined by X.800 as:

A service provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers in following categories:

- Authentication
- Access control
- Data confidentiality
- Data integrity
- Nonrepudiation



- Defined by RFC 4949 as:

A processing or communication service provided by a system to give a specific kind of protection to system resources

Categories of security services (1/2)

- **Authentication:** assures that communicating entity is who/what it claims to be (e.g. proof of identity of a peer, proof that message actually came from that source)
- **Access control:** limits and controls access to systems and applications
- **Data confidentiality:** keeps information secret during transmission (potentially including data, packet headers, protection against traffic analysis)

(Defined in ITU-T Recommendation X.800, *Security Architecture for OSI*)

Categories of security services (2/2)

- **Data integrity:** assures that messages are sent with no modification, insertion, etc.
- **Nonrepudiation:** provides protection so that an entity can't deny participation in the communication (e.g.: proof that message was sent by a particular entity, proof that message was received by particular entity)
- **Availability:** assures that system is accessible and usable by authorized users, according to performance specifications (e.g. protection against denial of service)

(Defined in ITU-T Recommendation X.800, *Security Architecture for OSI*)

Authentication

- Concerned with assuring that a communication is authentic

In the case of a single message, assures the recipient that the message is from the source that it claims to be from

In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties

Two specific authentication services are defined in X.800:

- **Peer entity authentication**
- **Data origin authentication**

Access Control

- The ability to limit and control the access to host systems and applications via communications links
- To achieve this, each entity trying to gain access must first be indentified, or authenticated, so that access rights can be tailored to the individual



Data Confidentiality

- The protection of transmitted data from passive attacks

Broadest service protects all user data transmitted between two users over a period of time

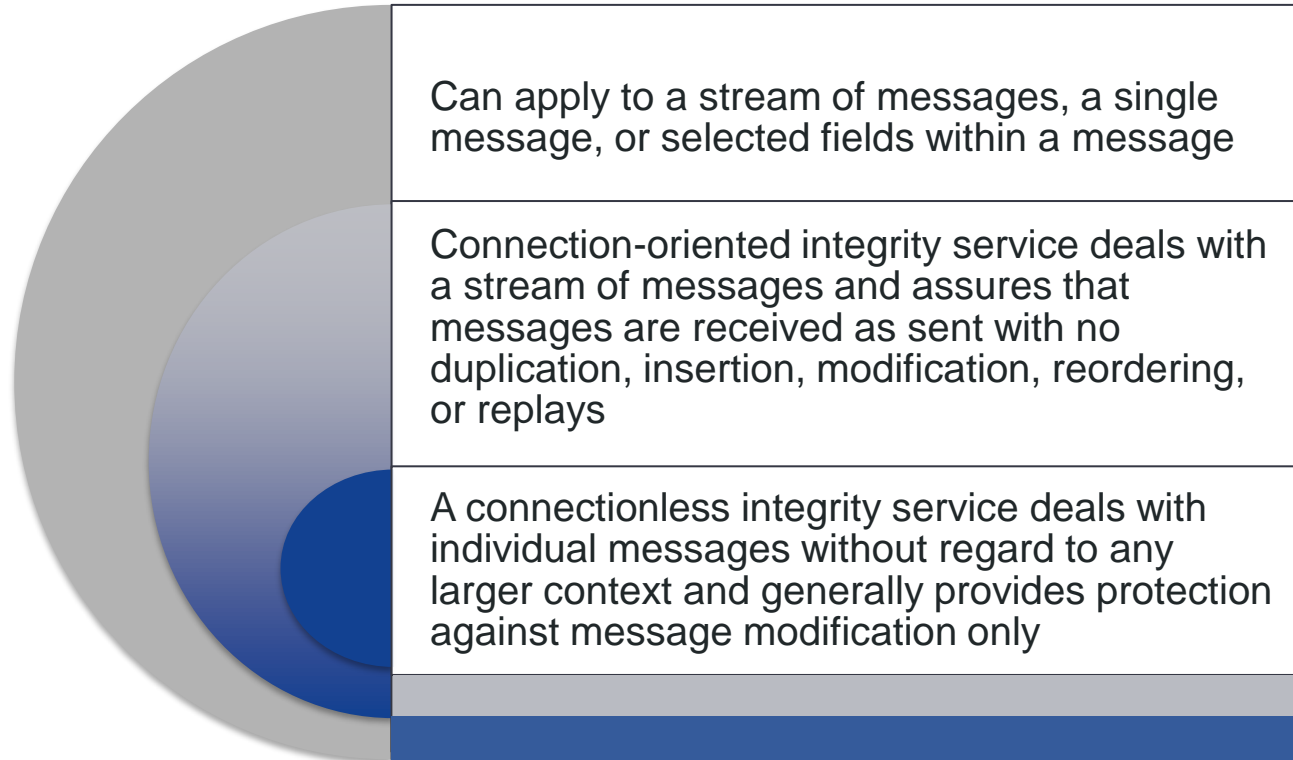
Narrower forms of service include the protection of a single message or even specific fields within a message

- The protection of traffic flow from analysis

This requires that an attacker not be able to observe the source and destination, frequency, length, or other characteristics of the traffic on a communications facility

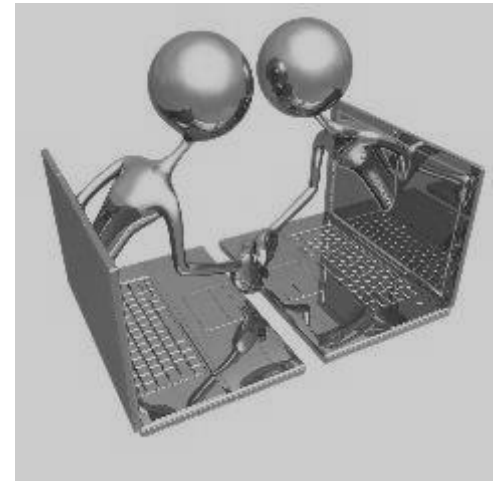


Data Integrity



Nonrepudiation

- Prevents either sender or receiver from denying a transmitted message
- When a message is sent, the receiver can prove that the alleged sender in fact sent the message
- When a message is received, the sender can prove that the alleged receiver in fact received the message



Availability service

- Availability

The property of a system or a system resource being accessible and usable upon demand by an authorized system entity, according to performance specifications for the system

- Availability service

One that protects a system to ensure its availability

Addresses the security concerns raised by denial-of-service attacks

Depends on proper management and control of system resources



Security mechanisms

Mechanisms that may be incorporated into protocol layer (specific)

- **Encipherment** uses mathematical algorithms to transform data and then recover it in its original form later.
- A **digital signature** is appended to data and allows recipient to prove source and integrity of the data.
- **Access control** mechanisms enforce access rights to resources.
- **Data integrity** mechanisms ensure integrity of data or data stream.

(Defined in ITU-T Recommendation X.800, *Security Architecture for OSI*)

Mechanisms that may be incorporated into protocol layer (specific)

- **Authentication exchange** uses some information exchange to ensure identity.
- **Traffic padding** adds bits into data stream to prevent traffic analysis.
- **Routing control** enables selection of secure routes through the network.
- **Notarization** uses third party to assure some security properties.

(Defined in ITU-T Recommendation X.800, *Security Architecture for OSI*)

Mechanisms that are not specific to a protocol layer (pervasive)

- **Trusted functionality** - any functionality providing or accessing security mechanisms should be trustworthy.
- A **security label** marks a resource to designate its security properties.
- **Event detection** mechanisms detect violations or other security-relevant events.
- A **security audit trail** is data that is collected and can be used to review and evaluate system security.
- **Security recovery** mechanisms deal with events and take recovery actions.

(Defined in ITU-T Recommendation X.800, *Security Architecture for OSI*)

Relationship between security services and security mechanisms.

SERVICE	MECHANISM							
	Enchipherment	Digital signature	Access control	Data integrity	Authentication	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			

ITU-T Recommendation
X.800, *Security
Architecture for OSI*)

Network security models

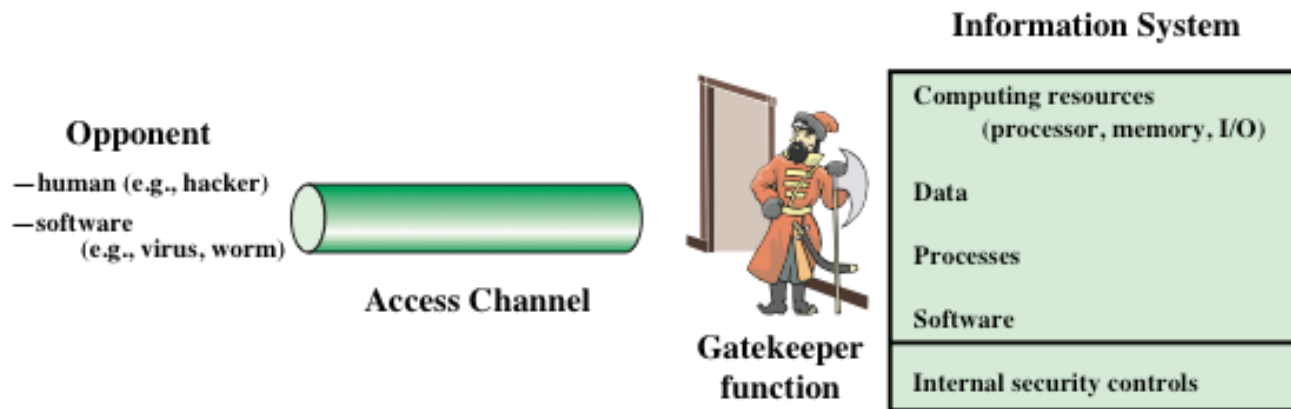


Figure 1.6 Network Access Security Model

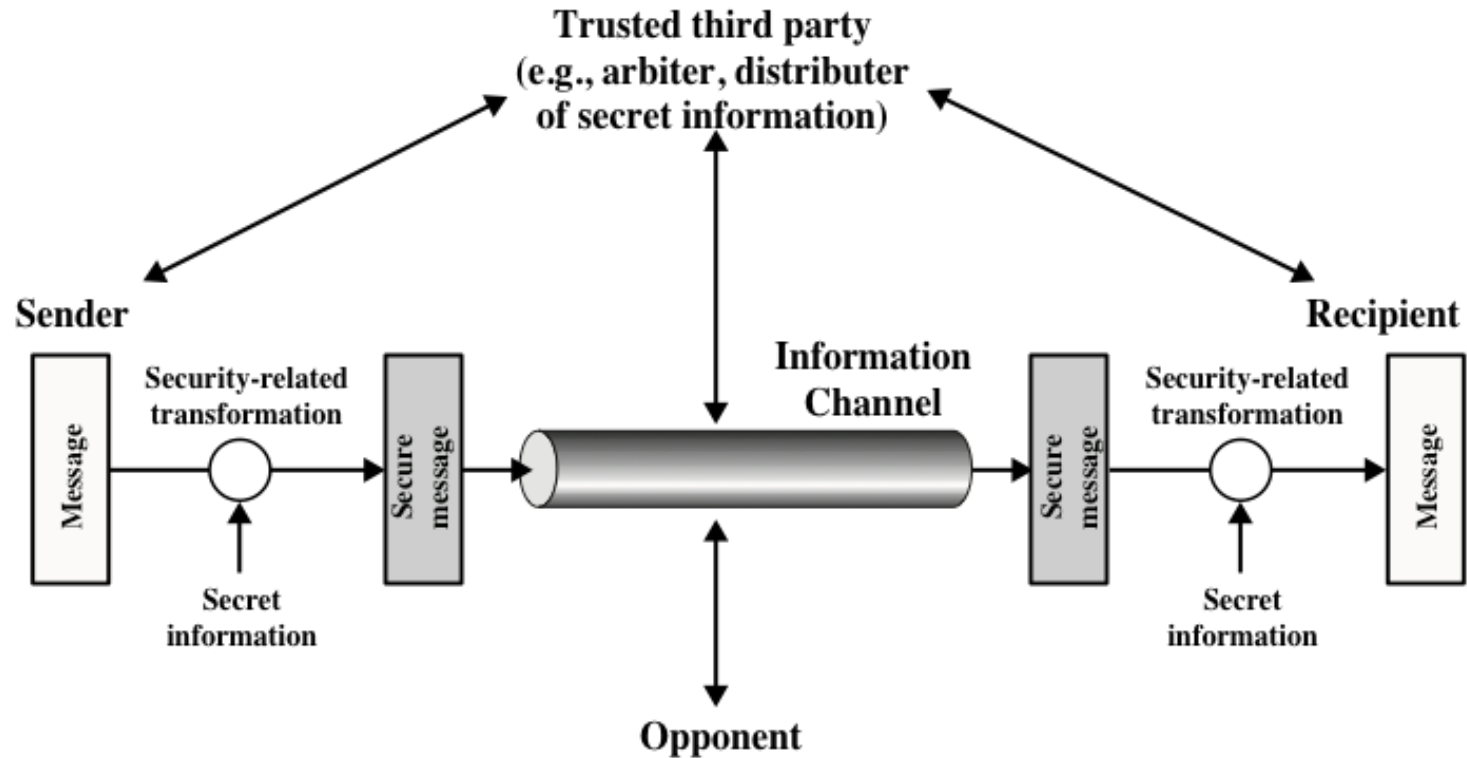


Figure 1.5 Model for Network Security