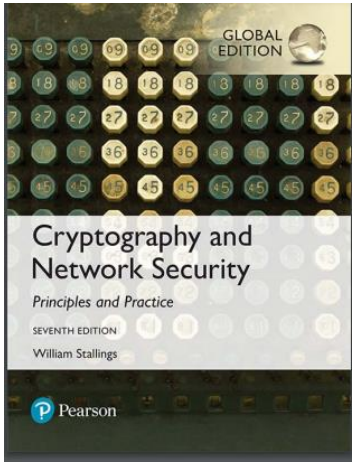
COMPUTER SECURITY
INTRODUCTION

Text Book

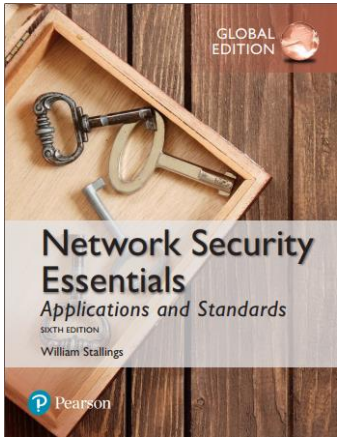
Textbook

Cryptography and Network Security: Principles and Practice, Global Edition

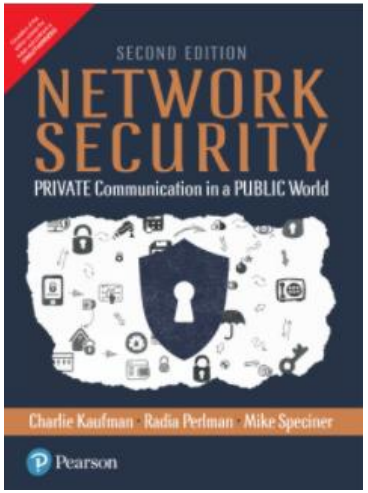


Ref

Network Security: Private Communication in a Public World
Charlie Kaufman, Rad ia Perlman, Mike Speciner, Michael Speciner, Prentice Hall



Network Security Essentials Applications and Standards- William Stalling-Applications and Standards



Learning Objectives

- Describe the key security requirements of confidentiality, integrity, and availability
- Discuss the types of security threats and attacks
- Summarize the functional requirements for computer security
- Describe the X.800 security architecture for OSI
- Cryptography applications

Introduction

- Humans have been in conflict since prehistoric times.
- In The Art of War 1, Sun Tzu says “The entire art of war is based on deception”.

History – Pre-Renaissance

- Paper was first introduced to Europe by Crusaders around 1200 A.D.
- Information was stored using tokens, tablets, knotted strings, notched sticks or handwritten parchment.

History – Pre-Renaissance

- Perhaps the best illustration of the importance of information security to ancient societies is the relatively advanced state of cryptography and steganography, technologies devoted to keeping information secret, when compared to the other technologies available for computing and communication.

- Cryptography is the science of writing in codes that are hard to decipher, and steganography is the art of hiding information to make it hard to detect.

- In Rome, Julius Caesar used a simple substitution cipher to hide information from his enemies

- During Abbasid caliphate [750 A.D], instruction to administrators explained how to use substitution ciphers. Muslim texts of that era explain how frequency counting can easily break substitution ciphers.

History – Pre-Renaissance

- Even more effort was devoted to finding tools for steganography. Recorded ancient approaches for information hiding include

  - Texts written on shaved skulls that were later covered by letting hair grow (Greece),
  - Invisible inks (Rome),
  - Pin pricks placed above letters in a text to indicate letters in a secret message (Greece),
  - Messages hidden in images and hieroglyphics (Egypt), and
  - Messages written on a thin sheet, rolled into a wax ball, and hidden or swallowed (China).

History – Renaissance to World War I

- The Renaissance was a period of renewed intellectual activity in Europe starting in the 14th century.
  - Napier's bones used for multiplication, division, and finding square roots [1617]
  - Blaise Pascal produced around 50 mechanical calculators starting in 1642.
  - In 1800s Herman Hollerith developed a punch card tabulation system
  - Charles Babbage produced the first programmable machines, the difference and analytical engines, in the mid-1800s
  - Poly-alphabetic solution ciphers

History –World War II

- During WWII, German cryptographers secured their communications using the Enigma encryption
- The Japanese had a cipher device that was their equivalent to Enigma. It was code-named Purple.

History –Cold War

- The new availability of computers allowed the science of cryptography to make major advances.
- In the United States, the National Security Agency (NSA) is in charge of cryptographic research for the United States government
- Cryptography also became available for civilian use.
- In the 1970s the U.S. National Bureau of Standards4, with NSA approval, agreed to the release of the Data Encryption Standard (DES) with a 56-bit key-space.
- The development of public key cryptography is a major step towards solving the problem of key distribution

History –Cold War

- The new availability of computers allowed the science of cryptography to make major advances.
- In the United States, the National Security Agency (NSA) is in charge of cryptographic research for the United States government
- Cryptography also became available for civilian use.
- In the 1970s the U.S. National Bureau of Standards4, with NSA approval, agreed to the release of the Data Encryption Standard (DES) with a 56-bit key-space.
- The development of public key cryptography is a major step towards solving the problem of key distribution

History – The Modern Era

- Computers!
- Examples
  - Lucifer
  - Rijndael
  - RSA
  - ElGamal

Organized Crime and Botnets

- Current cybercrime technologies and techniques include

1. botnets – networks of compromised machines,
2. spam – unsolicited e-mail advertisements, usually fraudulent,
3. phishing – attempts to fraudulently collect sensitive personal information,
4. pharming – redirecting web traffic to a fraudulent site,
5. identity theft and identity fraud – fraudulent use of personal information,
6. cross site scripting – inserting script commands into another's website,
7. cross site request forgery – tricking a user's browser to making requests on another party's website, • underground forums, and
8. money laundering.

What is Security?

Security according to two boys of 10 years old-

What is Security?

Security According to Junior High School ICT teacher-

What is Security?

There is no clear cut definition.

What is Security?

Security is a process, not an end state

Computer Security Concepts

- Before the widespread use of data processing equipment, the security of information valuable to an organization was provided primarily by physical and administrative means

- With the introduction of the computer, the need for automated tools for protecting files and other information stored on the computer became evident

- Another major change that affected security is the introduction of distributed systems and the use of networks and communications facilities for carrying data between terminal user and computer and between computers

Computer and Internet Security

- **Computer security**
  - The generic name for the collection of tools designed to protect data and to thwart hackers
- **Internet security**
  - Consists of measures to, deter, prevent, detect and correct security violations that involve the **transmission of information**

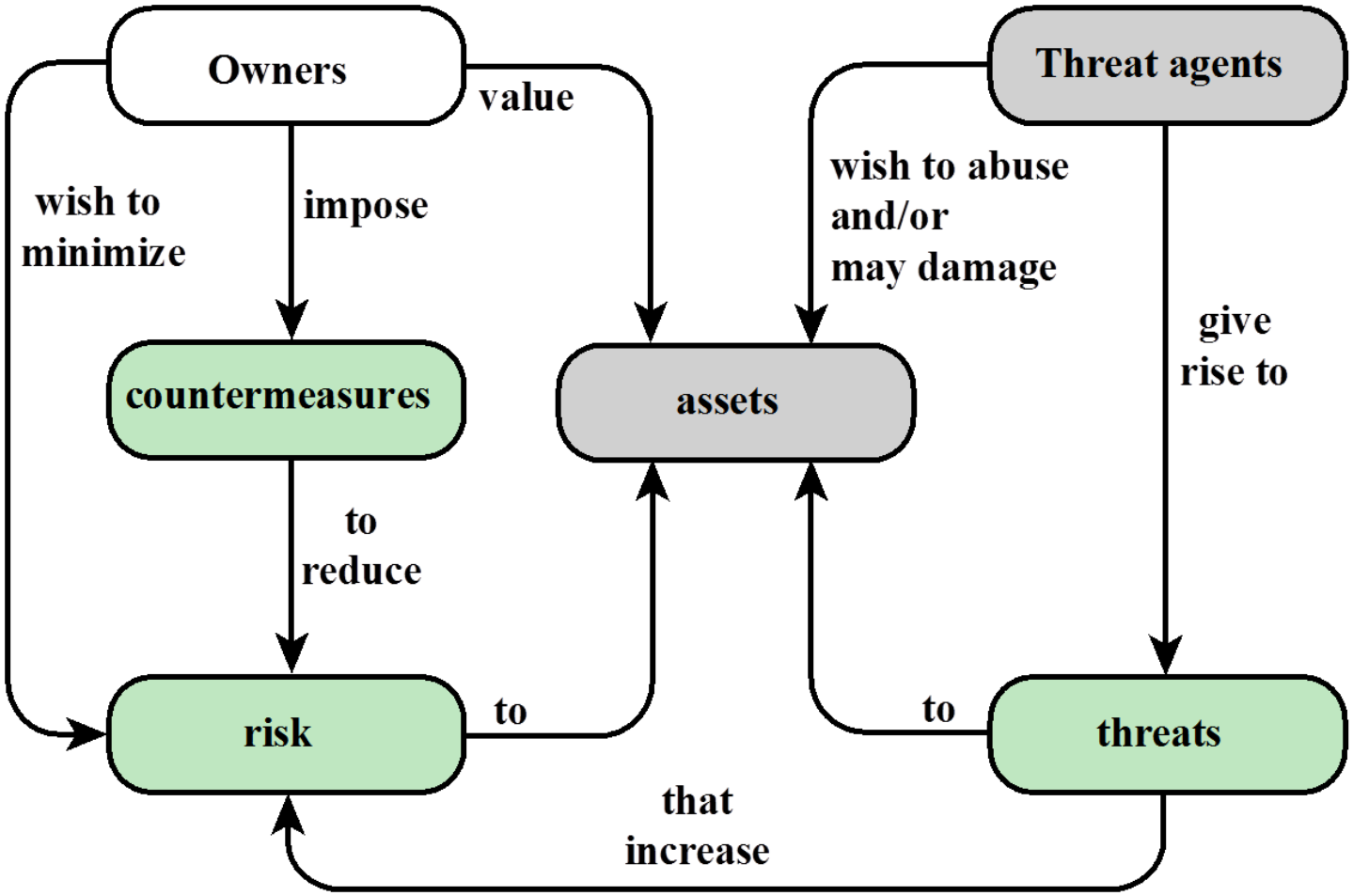
What security is about in general?

- Security is about protection of assets
  - D. Gollmann, Computer Security, Wiley

Need

- Prevention
  - take measures that prevent your assets from being damaged (or stolen)
- Detection
  - take measures so that you can detect when, how, and by whom an asset has been damaged
- Reaction
  - take measures so that you can recover your assets

Relationships among the security Concepts



Real world example

- Prevention
  - locks at doors, window bars, secure the walls around the property, hire a guard
- Detection
  - missing items, burglar alarms, closed circuit TV
- Reaction
  - attack on burglar (not recommended ☺), call the police, replace stolen items, make an insurance claim

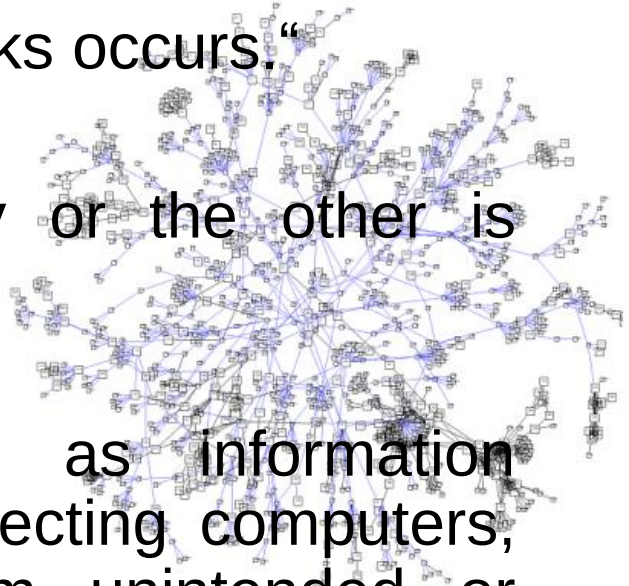
Information security in past & present

- Traditional Information Security
  - keep the cabinets locked
  - put them in a secure room
  - human guards
  - electronic surveillance systems
  - in general: physical and administrative mechanisms
- Modern World
  - Data are in computers
  - Computers are interconnected

Data/ Computer and Network Security-> Cyber Security

Definition

Cyber space: Cyberspace is "the environment in which communication over computer networks occurs.“



And almost everybody in one way or the other is connected to it

Cyber security: also referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction.

https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Introduction%20to%20the%20Concept%20of%20IT%20Security.pdf

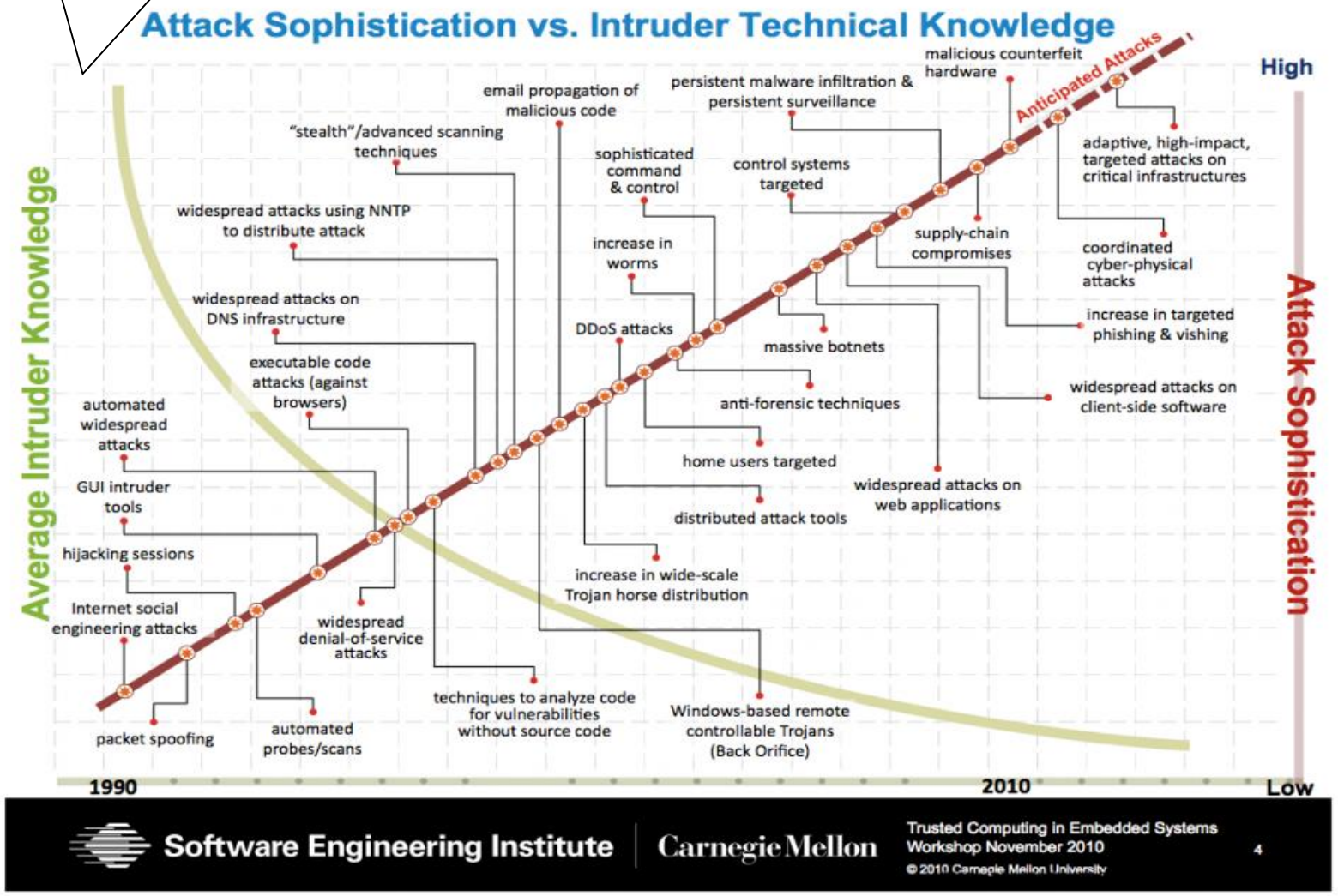
Definition

Four domains of cybersecurity: a risk-based systems approach to cyber decisions

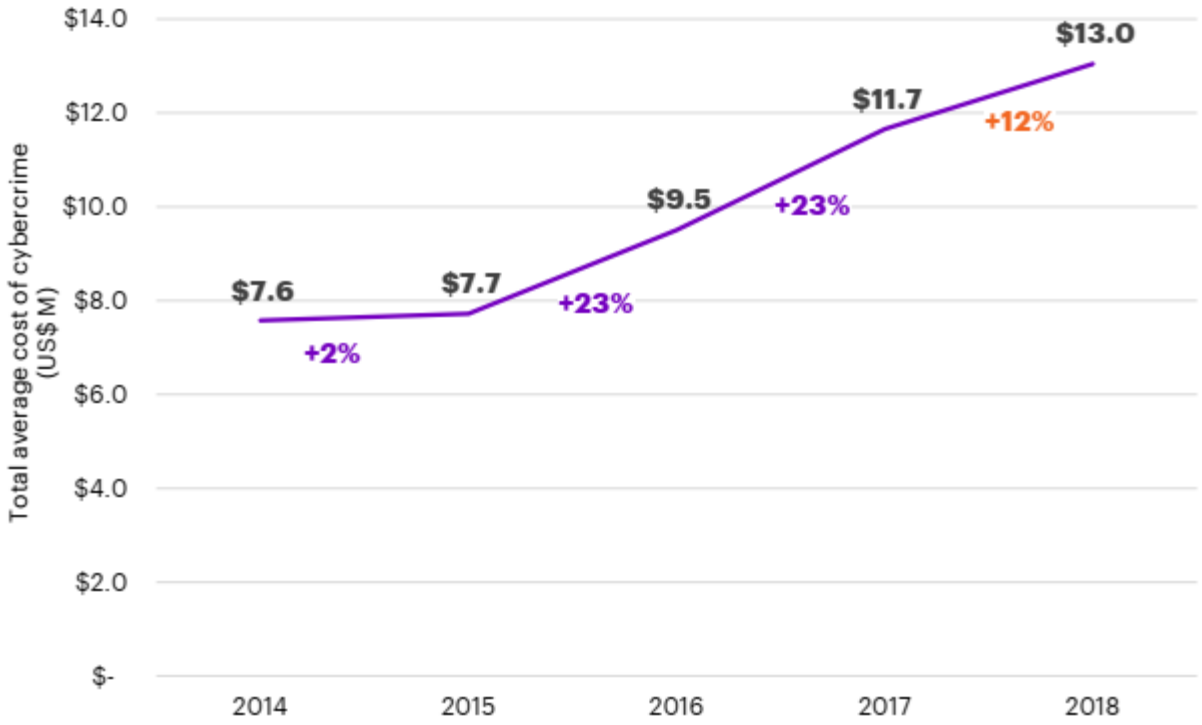
- https://link.springer.com/article/10.1007/s10669-013-9484-z

Security Trends

Skill and knowledge required to mount an attack



The global average cost of cyber crime/attacks

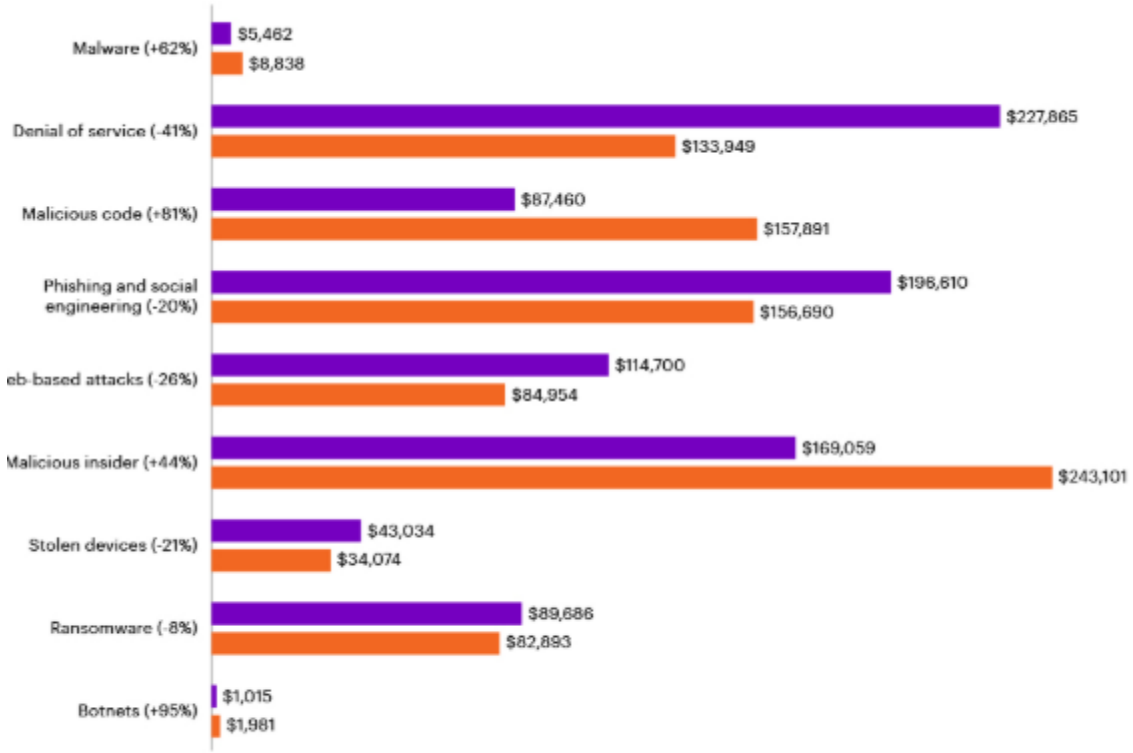


2018 Cost of Cyber Crime Study by Accenture*

Steeper increasing trend in the recent years

https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Types of cyber attacks experienced



Average annual cost of cybercrime by type of attack for financial services firms

2018 Cost of Cyber Crime Study by Accenture*

2017 2018

https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Computer Security

- The NIST *Computer Security Handbook* defines the term computer security as:

NIST: National Institute of Standards and Technology

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

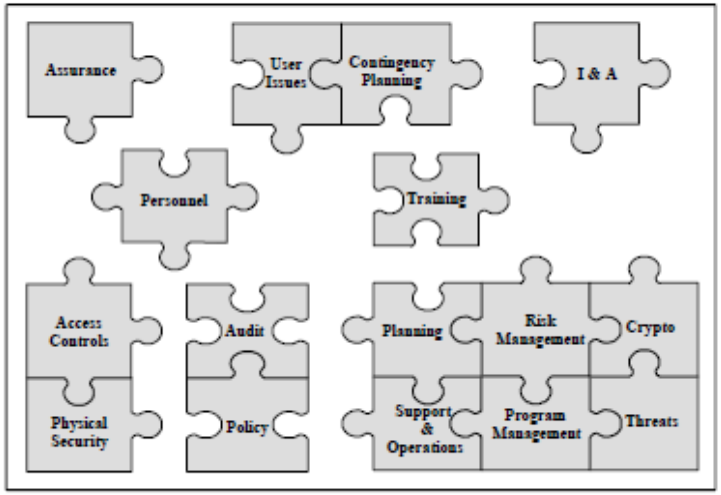
"The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications)"

NIST

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

An Introduction to Computer Security:
The NIST Handbook

Special Publication 800-12



Computer Security Objectives

Confidentiality

- **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

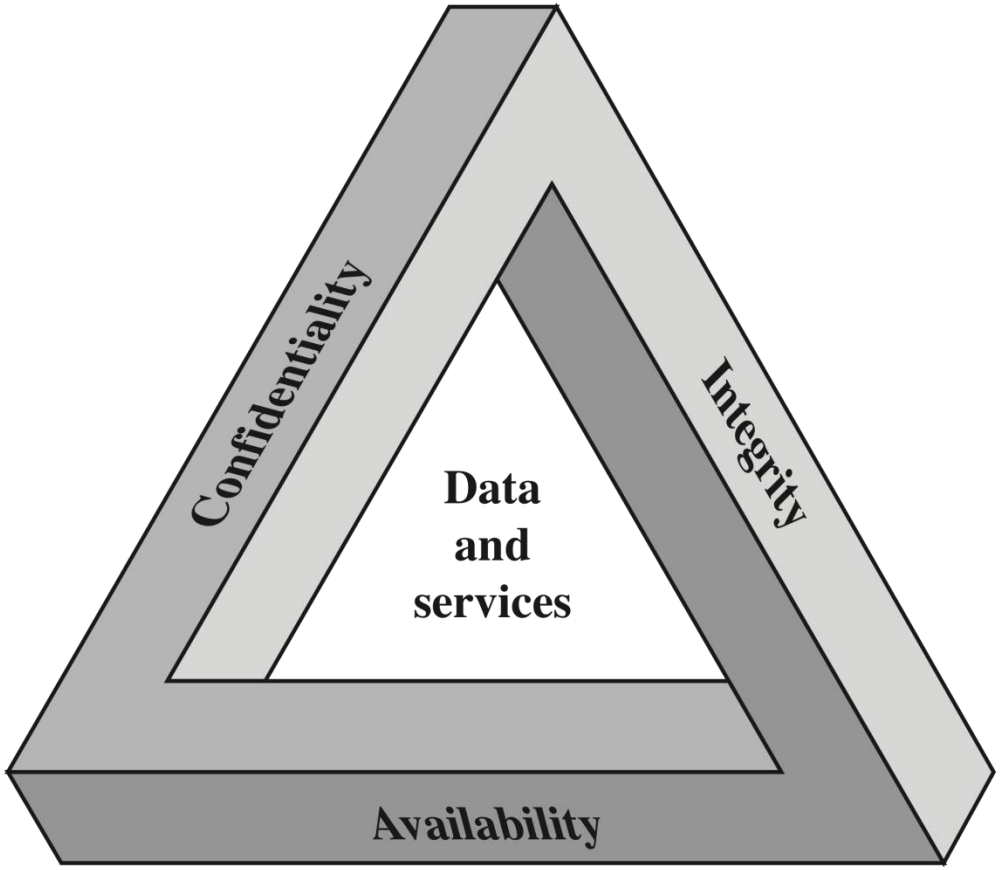
Availability

- Assures that systems work promptly and service is not denied to authorized users

Integrity

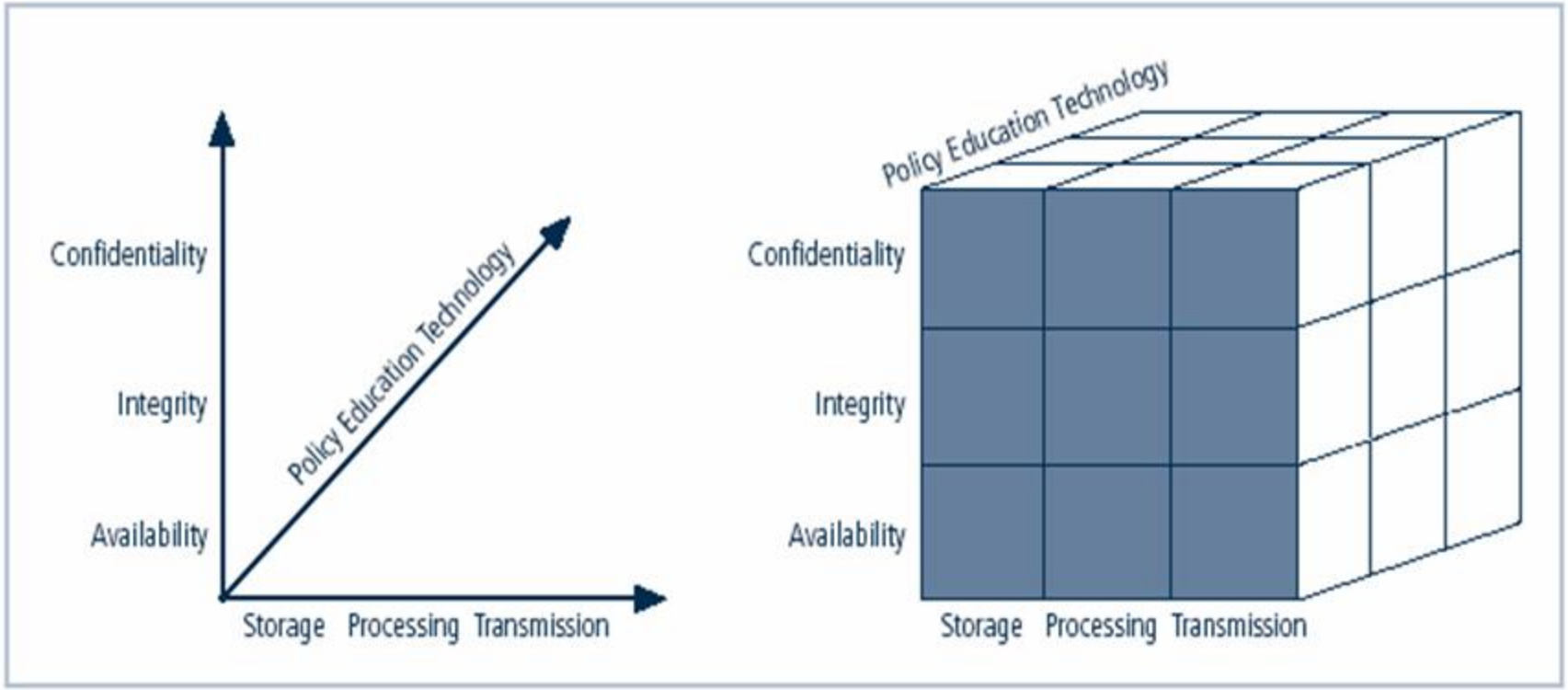
- **Data integrity**
  - Assures that information and programs are changed only in a specified and authorized manner
- **System integrity**
  - Assures that a system performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system

CIA Triad



The Security Requirements Triad

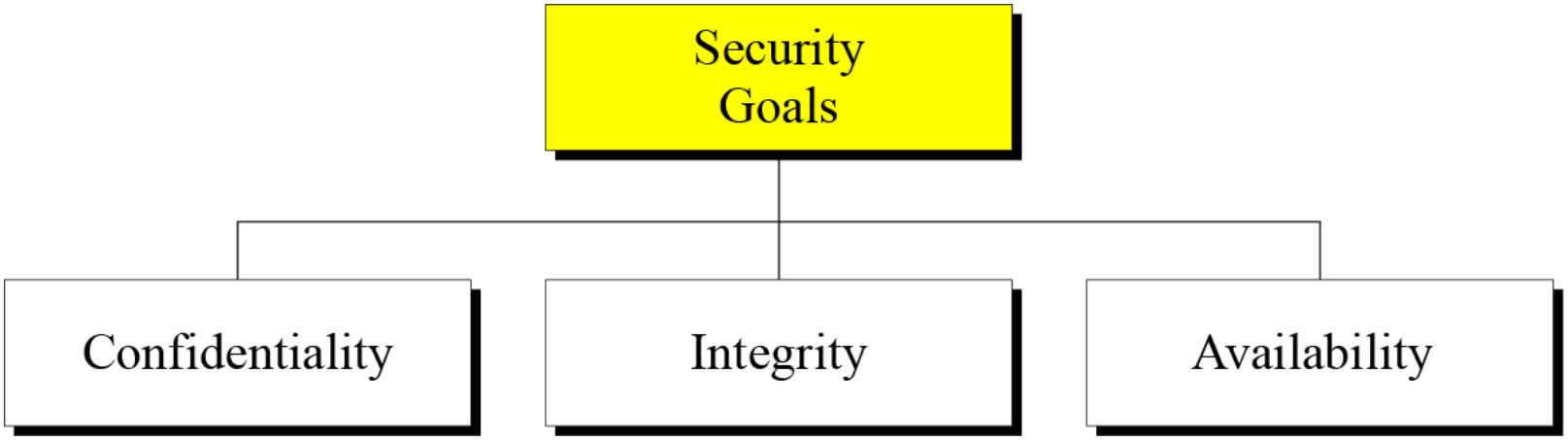
NSTISSC Security Model



NSTISSC Security Model

'National Security Telecommunications & Information systems security committee' document.

It is now called the National Training Standard for Information security professionals.


Security
Goals
Confidentiality
Integrity
Availability

Confidentiality is probably the most common aspect of information security. We need to protect our confidential information. An organization needs to guard against those malicious actions that endanger the confidentiality of its information.

Integrity : Information needs to be changed constantly. Integrity means that changes need to be done only by authorized entities and through authorized mechanisms.

Availability : The information created and stored by an organization needs to be available to authorized entities. Information needs to be constantly changed, which means it must be accessible to authorized entities.

Possible additional concepts:

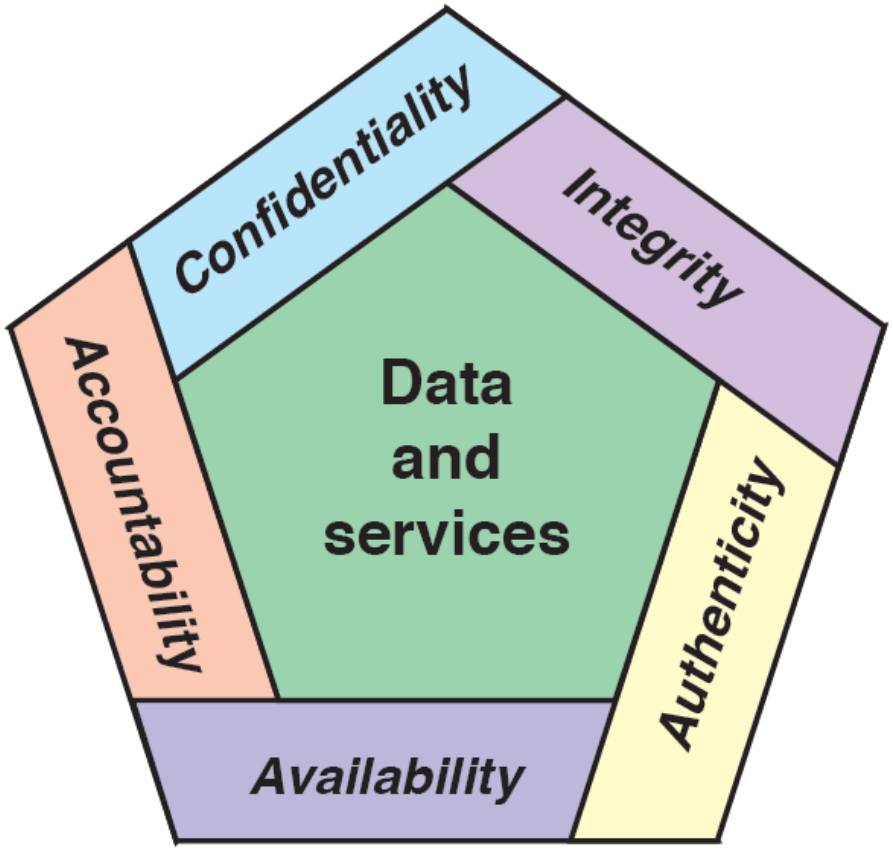
Authenticity

- Verifying that users are who they say they are and that each input arriving at the system came from a trusted source

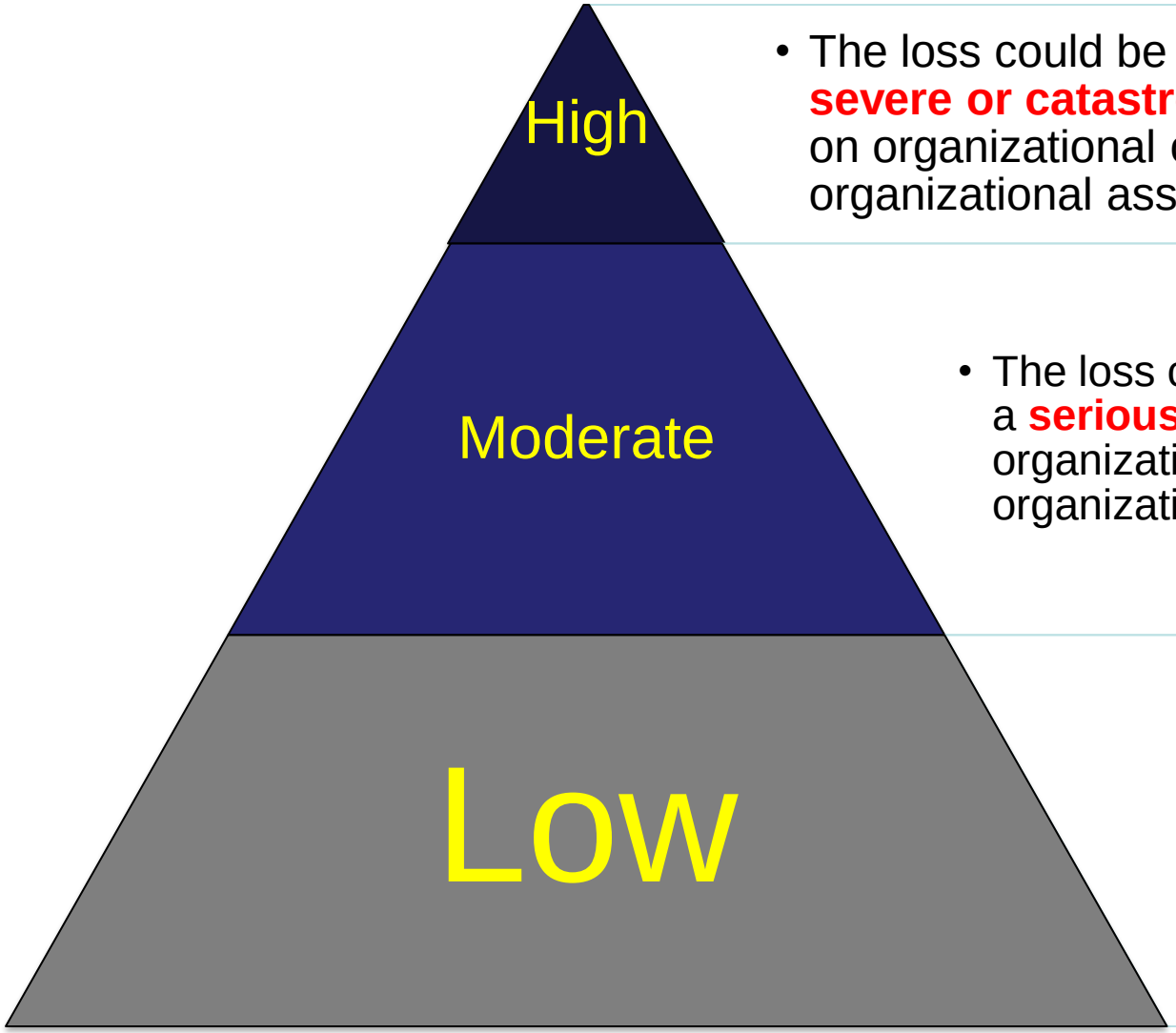
Accountability

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

Possible additional concepts:



Breach of Security
3 Levels of Impact (These levels are defined in FIPS 199)



- The loss could be expected to have a **severe or catastrophic adverse** effect on organizational operations, organizational assets, or individuals

- The loss could be expected to have a **serious adverse effect on** organizational operations, organizational assets, or individuals

- The loss could be expected to have **a limited adverse effect on organizational operations,** organizational assets, or individuals

Examples of Security Requirements

Confidentiality

Student grade information is an asset whose confidentiality is considered to be highly important by students

Regulated by the Family Educational Rights and Privacy Act (FERPA)

Integrity (consistency)

Patient information stored in a database – inaccurate information could result in serious harm or death to a patient and expose the hospital to massive liability

A **Web site that offers a forum to registered users** to discuss some specific topic would be assigned a moderate level of integrity

An example of a low-integrity requirement is an anonymous **online poll**

Availability

The **more critical a component or service**, the higher the level of availability required

A moderate availability requirement is **a public Web site for a university**

An **online telephone directory lookup** application would be classified as a low-availability requirement

Computer Security Challenges

- Security is **not simple**
- **Potential attacks** on the security features need **to be considered**
- Procedures used to provide particular services are often **counter-intuitive**
- It is necessary to decide **where to use** the various security mechanisms
- Requires **constant monitoring**
- Is too often an **afterthought**
- Security mechanisms typically involve **more than a particular algorithm or protocol**
- Security is essentially a **battle of wits** between a perpetrator and the designer
- **Little benefit** from security investment **is perceived** until a security failure occurs
- Strong security is often viewed as **an impediment** to efficient and user-friendly operation

The OSI Security Architecture

- To assess effectively the security needs of an organization and to evaluate and choose various security products and policies, the manager responsible for computer and network security needs some systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements.

- ITU-T Recommendation X.800, Security Architecture for OSI, defines such a systematic approach.

- The OSI security architecture is useful to managers as a way of organizing the task of providing security

ITU-T

The **ITU Telecommunication Standardization Sector** (**ITU-T**) is one of the three sectors (divisions or units) of the International Telecommunication Union (ITU); it coordinates standards for telecommunications.

The ITU-T mission is to ensure the efficient and timely production of standards covering all fields of telecommunications on a worldwide basis, as well as defining tariff and accounting principles for international telecommunication services.

OSI

ISO- The International Organization for Standardization (French: *Organisation internationale de normalisation*;) produced OSI (Open Systems Interconnection Reference Model, the OSI Reference Model, or even just the OSI Model**)**

History of OSI

In the late 1970s, two projects began independently, with the same goal: to define a unifying standard for the architecture of networking systems.

One was administered by the International Organization for Standardization (ISO), while the other was undertaken by the International Telegraph and Telephone Consultative Committee, or CCITT (the abbreviation is from the French version of the name).

These two international standards bodies each developed a document that defined similar networking models. ISO 7498, ITU-T (formerly CCITT) standard X.200 (1984)

Security Services: X.800

X.800 defines a security service as a service that is provided by a protocol layer of communicating open systems and that ensures adequate security of the systems or of data transfers.

X.800 Recommendation:

1. provides a general description of security services and related mechanisms, which may be provided by the Reference Model; and

2. defines the positions within the Reference Model where the services and mechanisms may be provided.

This Recommendation extends the field of application of recommendation X.200, to cover secure communications between open systems.

OSI Security Architecture

ITU-T Recommendation X.800, *Security Architecture for OSI* describes *a* systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements.

Focus

- **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

  Intended to **counter security attacks**, and they make use of one or more security mechanisms to provide the service

IETF and RFC

The **Internet Engineering Task Force** (**IETF**) (1986) develops and promotes voluntary Internet standards, in particular the standards that comprise the Internet protocol suite (TCP/IP).

A **Request for Comments** (**RFC**) is a publication of the Internet Engineering Task Force (IETF) and the Internet Society, the principal technical development and standards-setting bodies for the Internet.

The **Internet Society** (**ISoc**) is an international, non-profit organization founded in 1992 to provide leadership in Internet related standards, education, and policy.

ATTACKS

The three goals of security, confidentiality, integrity, and availability can be threatened by security attacks.

Threats and Attacks (RFC 4949)

Internet Security Glossary, Version 2

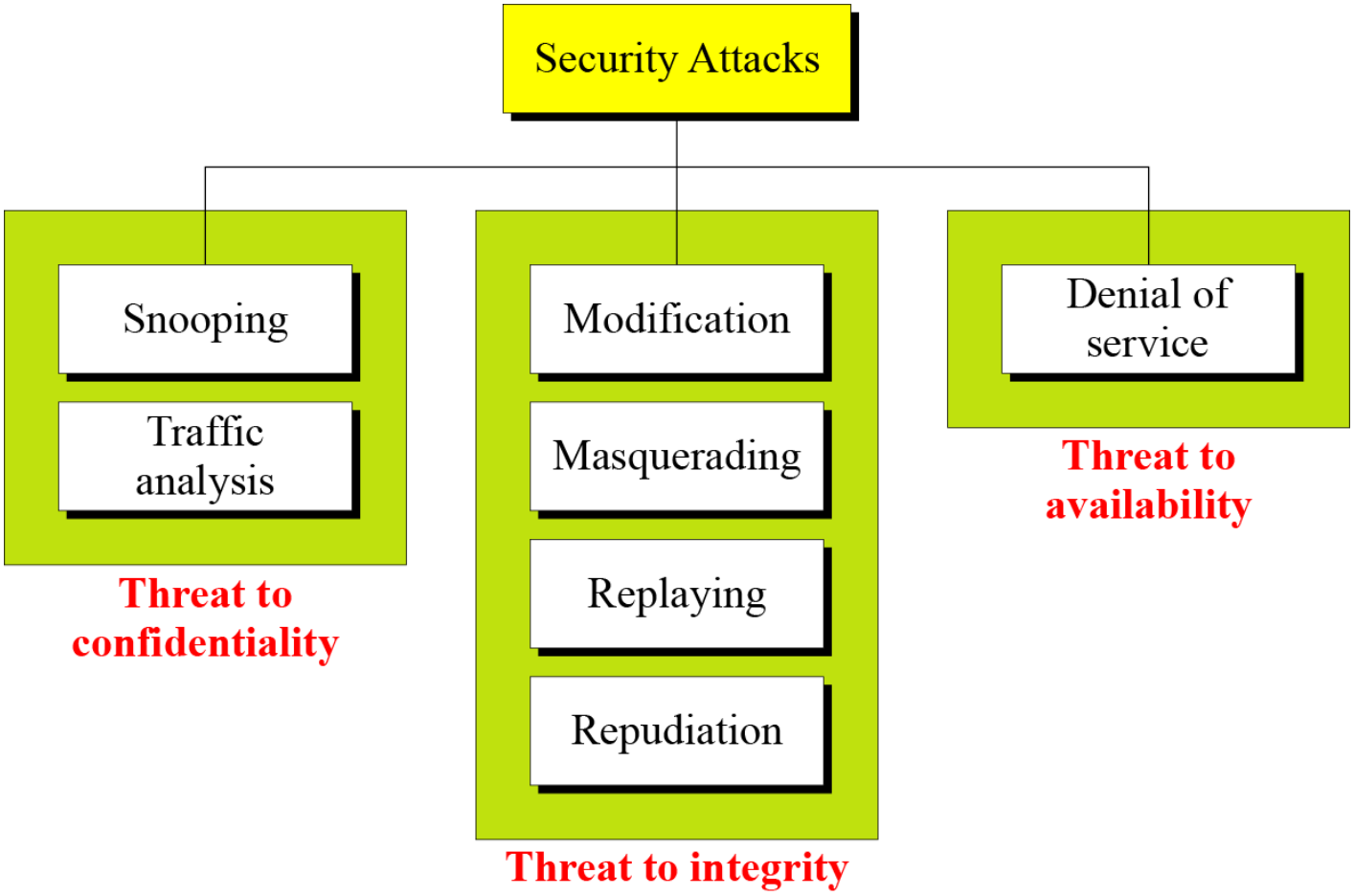
This Glossary provides definitions, abbreviations, and explanations of terminology for information system security.

Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.


Security Attacks
Snooping
Traffic analysis
Threat to confidentiality
Modification
Masquerading
Replaying
Repudiation
Threat to integrity
Denial of service
Threat to availability

Security Attacks

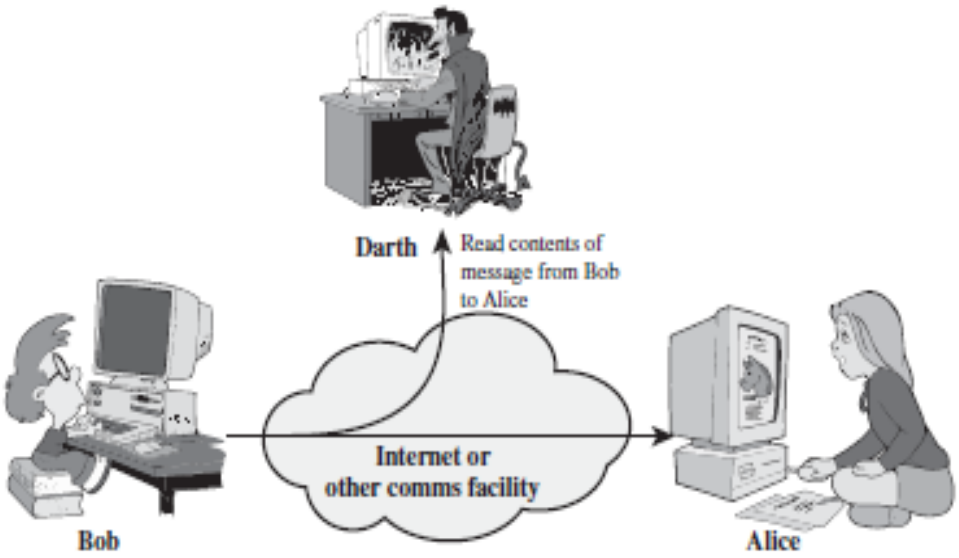
- **A means of classifying** security attacks, used both in X.800 and RFC 4949, is in terms of **passive attacks** and **active attacks**
- **A passive attack** attempts to learn or **make use of information** from the system but **does not affect system resources**
- **An active attack** attempts to **alter** system resources or **affect their operation**

Passive Attacks
(Two types)

- Are in the nature of **eavesdropping on**, or **monitoring of**, transmissions
- Goal of the opponent is to **obtain information** that is being transmitted

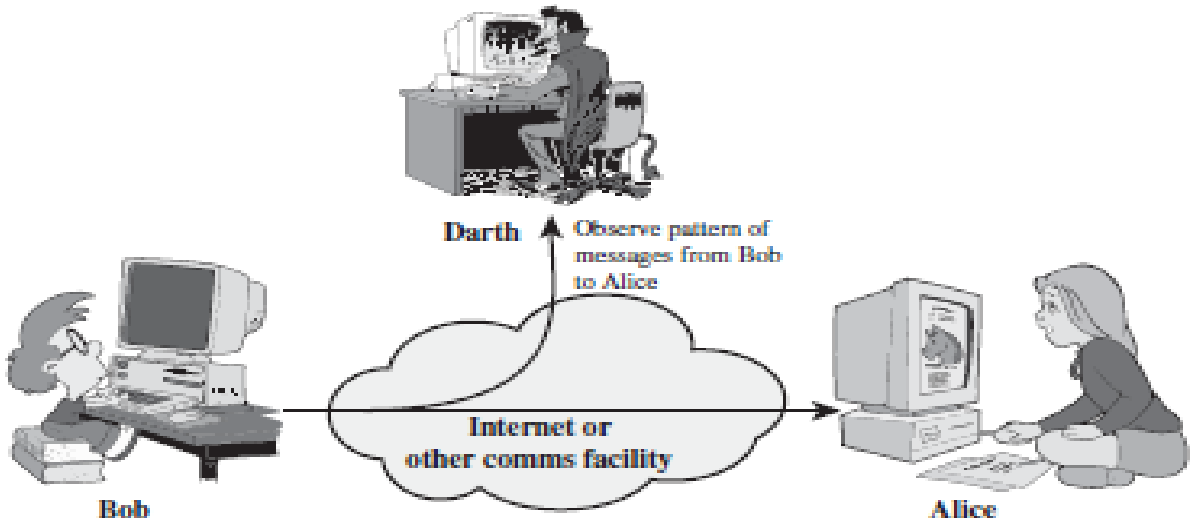
- **Two types** of passive attacks are:
  - ❑ The release of message contents
  - ❑ Traffic analysis

Snooping refers to unauthorized access to or interception of data.



(a) Release of message contents

Traffic analysis refers to obtaining some other type of information by monitoring online traffic.



(b) Traffic analysis

Active Attacks (4 types)

- **Involve some modification** of the data stream or the creation of a false stream
- **Difficult to prevent** because of the wide variety of potential physical, software, and network vulnerabilities
- **Goal** is to **detect attacks** and **to recover** from any disruption or delays caused by them

Modification means that the attacker intercepts the message and changes it.

Masquerading or spoofing happens when the attacker impersonates somebody else.

Replaying means the attacker obtains a copy of a message sent by a user and later tries to replay it.

Repudiation means that sender of the message might later deny that she has sent the message; the receiver of the message might later deny that he has received the message.

Denial of service (DoS) is a very common attack. It may slow down or totally interrupt the service of a system.

Attacks	*Passive/Active*	*Threatening*
Snooping Traffic analysis	Passive	Confidentiality
Modification Masquerading Replaying Repudiation	Active	Integrity
Denial of service	Active	Availability

Active Attacks (4 types)

Masquerade

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

Modification of messages

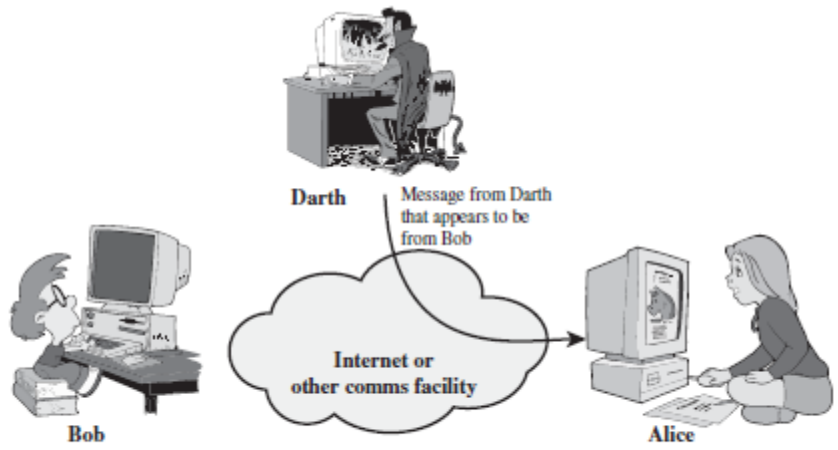
- Some portion of a legitimate message is altered, or messages are delayed or reordered to produce an unauthorized effect

Replay

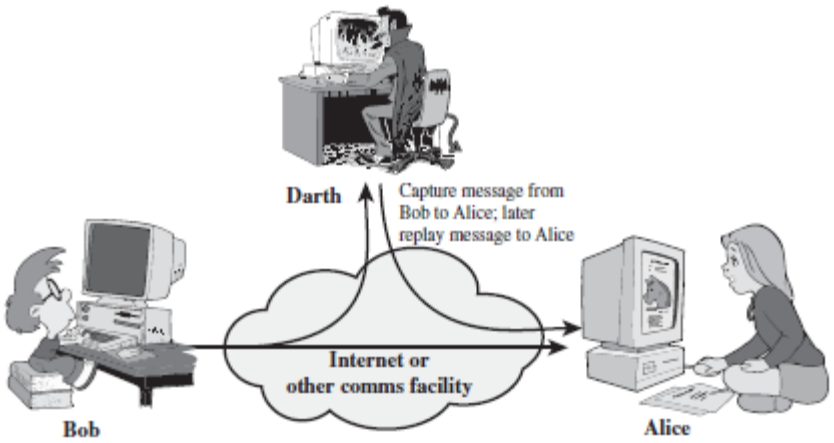
- Involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect

Denial of service

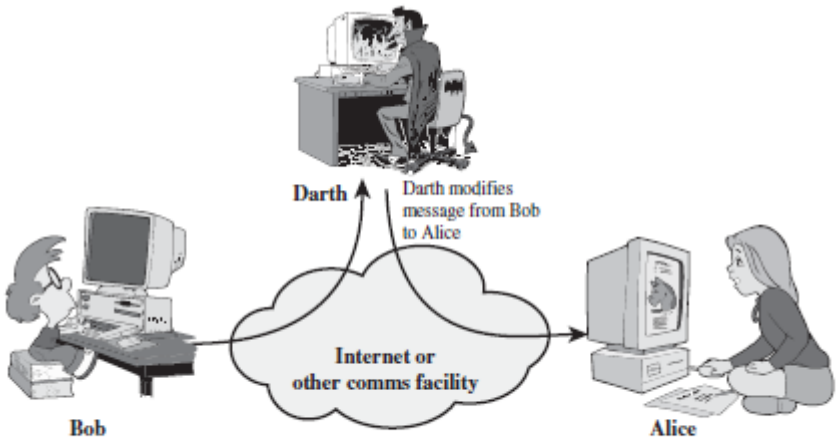
- Prevents or inhibits the normal use or management of communications facilities



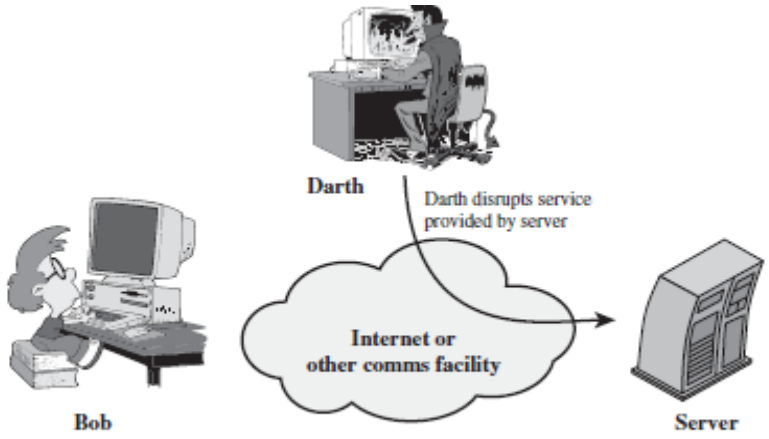
(a) Masquerade



(b) Replay



(c) Modification of messages



(d) Denial of service

Security Services

- to prevent or detect attacks
- to enhance the security
- replicate functions of physical documents
  - e.g.
    - have signatures, dates
    - need protection from disclosure, tampering, or destruction
    - notarize
    - record

Basic Security Services

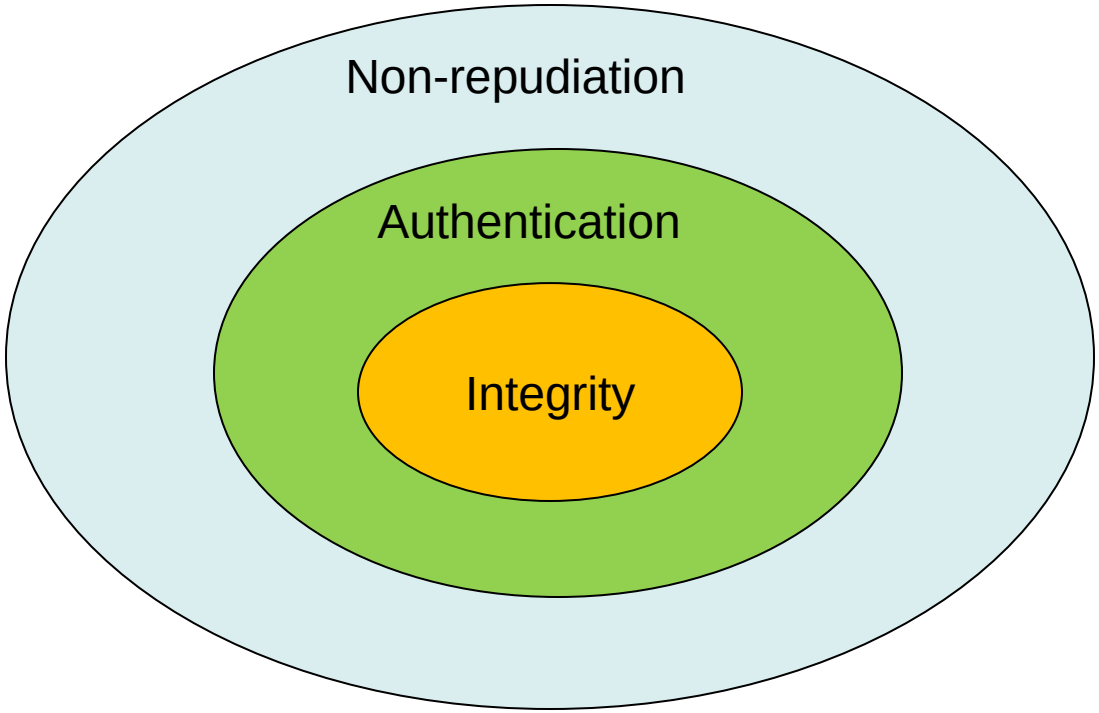
- Authentication
  - assurance that the communicating entity is the one it claims to be
  - peer entity authentication
    - mutual confidence in the identities of the parties involved in a connection
  - Data-origin authentication
    - assurance about the source of the received data
- Access Control
  - prevention of the unauthorized use of a resource
  - to achieve this, each entity trying to gain access must first be identified and authenticated, so that access rights can be tailored to the individual

Basic Security Services

- Non-Repudiation
  - protection against denial by one of the parties in a communication
  - Origin non-repudiation
    - proof that the message was sent by the specified party
  - Destination non-repudiation
    - proof that the message was received by the specified party

Relationships

- among integrity, data-origin authentication and non-repudiation



Services and Mechanisms

ITU-T provides some security services and some mechanisms to implement those services. Security services and mechanisms are closely related because a mechanism or combination of mechanisms are used to provide a service.

Security Services

- Security service 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

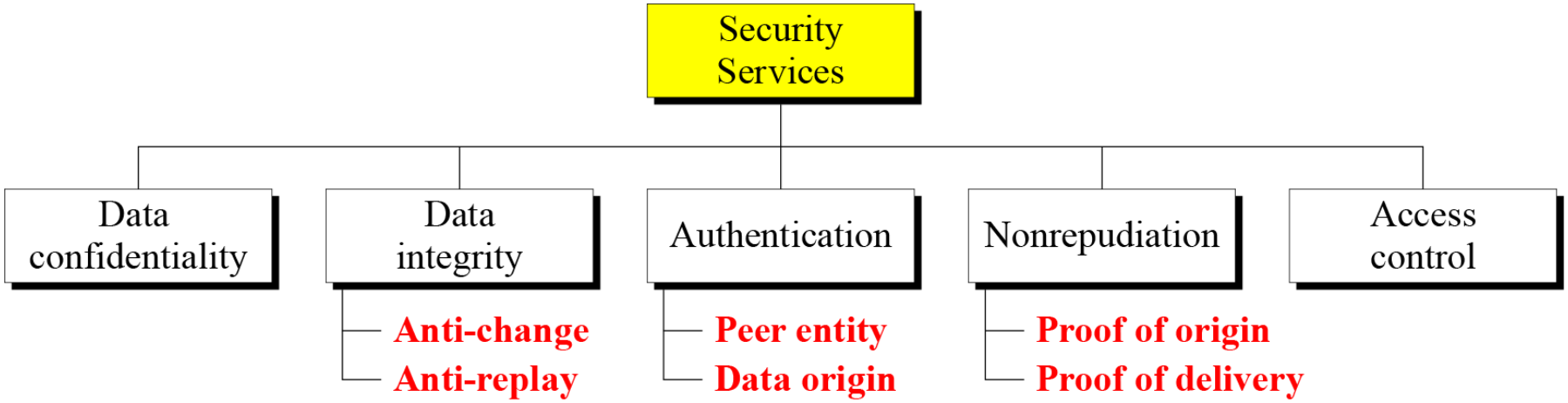
- Defined by RFC 4949 as:

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

X.800 Service Categories

X.800 divides these **services** into five categories and fourteen specific services

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


Security Services
Data confidentiality
Data integrity
Anti-change
Anti-replay
Authentication
Peer entity
Data origin
Nonrepudiation
Proof of origin
Proof of delivery
Access control

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

Security Services (X.800)

Authentication

- Concerned with assuring that a

  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 **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**

Two entities are considered peers if they implement the same protocol in different systems (e.g., two TCP modules in two communicating systems).

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 **identified**, or **authenticated,** so that access rights can be tailored to the individual

Data Confidentiality

- The protection of transmitted data **from passive attacks**

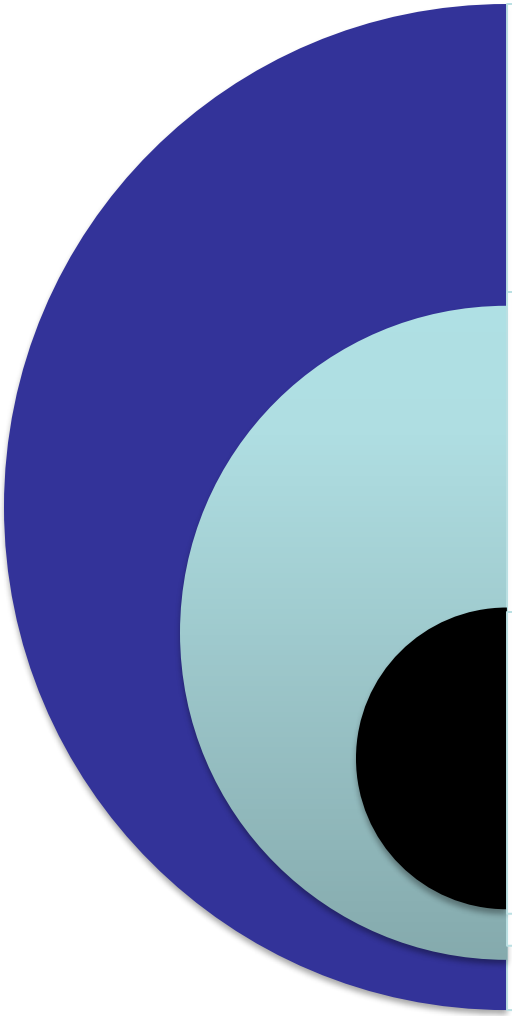
  Broadest service protects **all user data** transmitted between two users over a period of time

  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



Can apply to a **stream of messages**, **a single message,** or **selected fields** **within a message**

Connection-oriented integrity service deals with a **stream of messages** and assures that messages are received as sent with **no duplication**, **insertion, modification, reordering,** or **replays**

A connectionless integrity service deals with **individual messages** without regard to any larger context and generally provides protection against **message modification only**

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

Security mechanisms defined in X.800:

- The mechanisms are di vided into those that are implemented in a specific protocol layer, such as TCP or an application-layer protocol, and those that are not specific to any particular protocol layer or security service.

Table 1.3 Security Mechanisms (X.800)

SPECIFIC SECURITY MECHANISMS	PERVASIVE SECURITY MECHANISMS
May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.	Mechanisms that are not specific to any particular OSI security service or protocol layer.
Encipherment The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	**Trusted Functionality** That which is perceived to be correct with respect to some criteria (e.g., as established by a security policy).
Digital Signature Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).	**Security Label** The marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource.
Access Control A variety of mechanisms that enforce access rights to resources.	**Event Detection** Detection of security-relevant events.
Data Integrity A variety of mechanisms used to assure the integrity of a data unit or stream of data units.	**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.
Authentication Exchange A mechanism intended to ensure the identity of an entity by means of information exchange.	**Security Recovery** Deals with requests from mechanisms, such as event handling and management functions, and takes recovery actions.
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 and allows routing changes, especially when a breach of security is suspected.	
Notarization The use of a trusted third party to assure certain properties of a data exchange.	

Cryptographic Security Mechanisms

- Encryption (a.k.a. Encipherment)
  - use of mathematical algorithms to transform data into a form that is not readily intelligible
    - keys are involved

Cryptographic Security Mechanisms

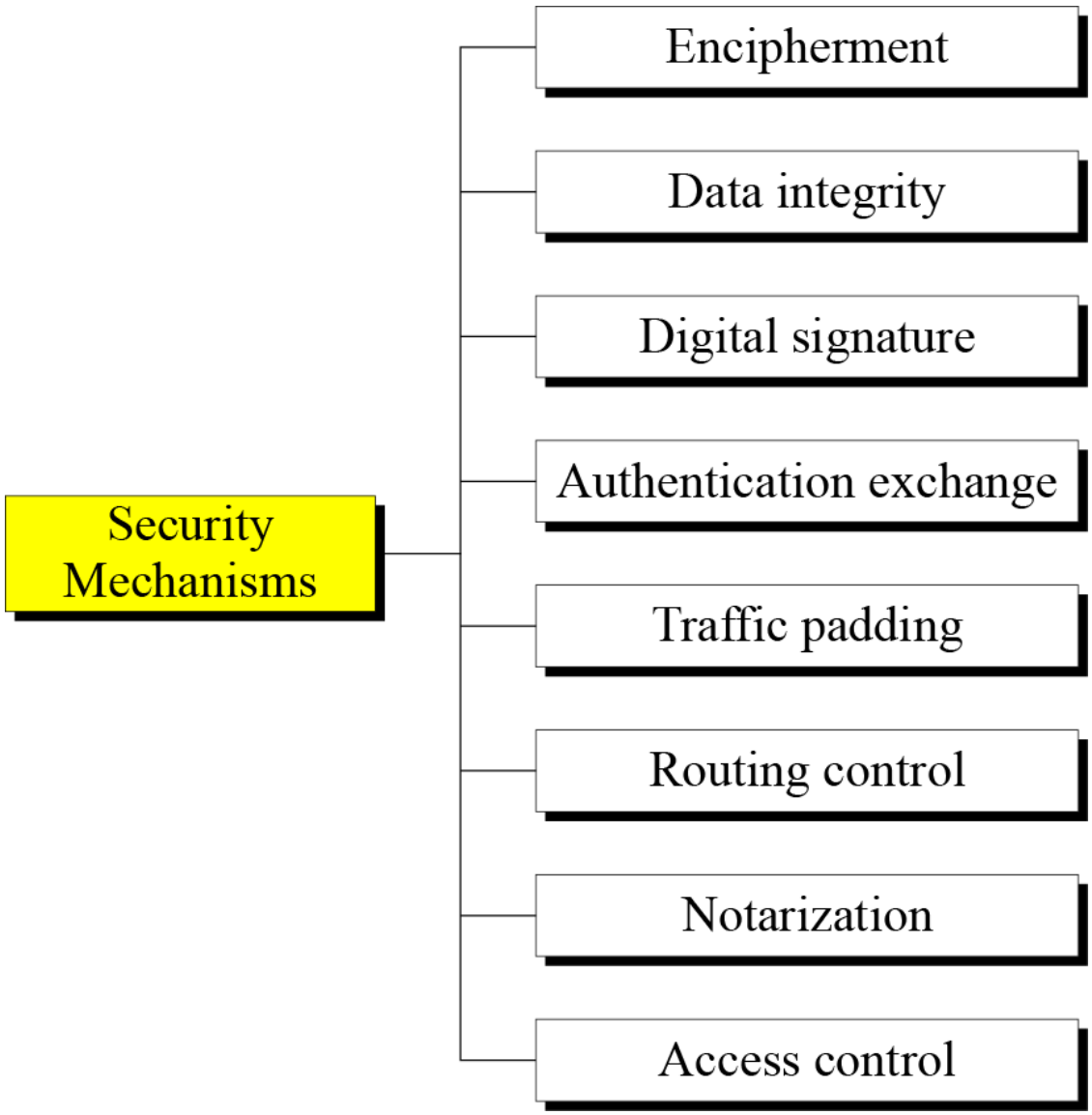
- Message Digest
  - similar to encryption, but one-way (recovery not possible)
  - generally no keys are used
- Digital Signatures and Message Authentication Codes
  - Data appended to, or a cryptographic transformation of, a data unit to prove the source and the integrity of the data
- Authentication Exchange
  - ensure the identity of an entity by exchanging some information

Security Mechanisms

- Notarization
  - use of a trusted third party to assure certain properties of a data exchange
- Timestamping
  - inclusion of correct date and time within messages

Security Mechanisms (X.800)

- Specific security mechanisms: incorporated into the appropriate protocol layer in order to provide some of the OSI security services
  - Encipherment
  - digital signatures
  - access controls
  - data integrity
  - authentication exchange
  - traffic padding
  - routing control
  - notarization


Security Mechanisms
Encipherment
Data integrity
Digital signature
Authentication exchange
Traffic padding
Routing control
Notarization
Access control

SPECIFIC SECURITY MECHANISMS

May be incorporated into the appropriate protocol layer in order to provide some of the OSI security services.

Encipherment
The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.

Digital Signature
Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery (e.g., by the recipient).

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.

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 and allows routing changes, especially when a breach of security is suspected.

Notarization
The use of a trusted third party to assure certain properties of a data exchange.

PERVASIVE SECURITY MECHANISMS

Mechanisms that are not specific to any particular OSI security service or protocol layer.

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.

Security Mechanisms (X.800)

Relationship Between Security Services and Mechanisms

	Mechanism				
Service	**Encipherment**	**Digital Signature**	**Access Control**	**Data Integrity**	**Authentication Exchange**
Peer Entity Authentication	Y	Y			Y
Data Origin Authentication	Y	Y			
Access Control			Y		
Confidentiality	Y				
Traffic Flow Confidentiality	Y				
Data Integrity	Y	Y		Y	
Nonrepudiation		Y		Y	
Availability				Y	Y

Relationship Between Security Services and Mechanisms

Security Service	*Security Mechanism*
Data confidentiality	Encipherment and routing control
Data integrity	Encipherment, digital signature, data integrity
Authentication	Encipherment, digital signature, authentication exchanges
Nonrepudiation	Digital signature, data integrity, and notarization
Access control	Access control mechanism

Model for Network Security

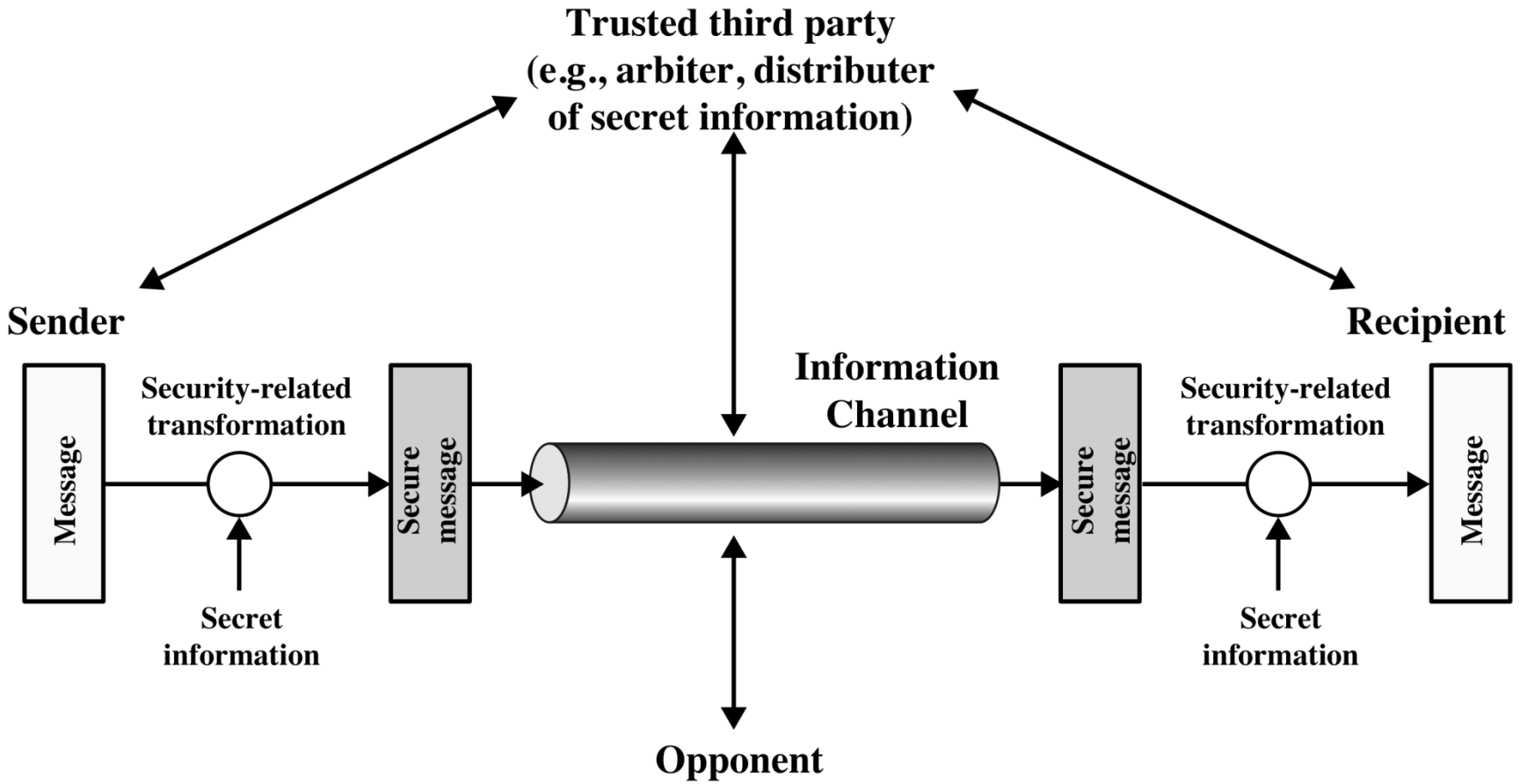


Figure 1.2 Model for Network Security

A Model for Network Security

- Using this model requires us to:
  1. Design a suitable algorithm for the security transformation
  2. Generate the secret information (keys) used by the algorithm
  3. Develop methods to distribute and share the secret information
  4. Specify a protocol enabling the principals to use the transformation and secret information for a security service

Network Access Security Model

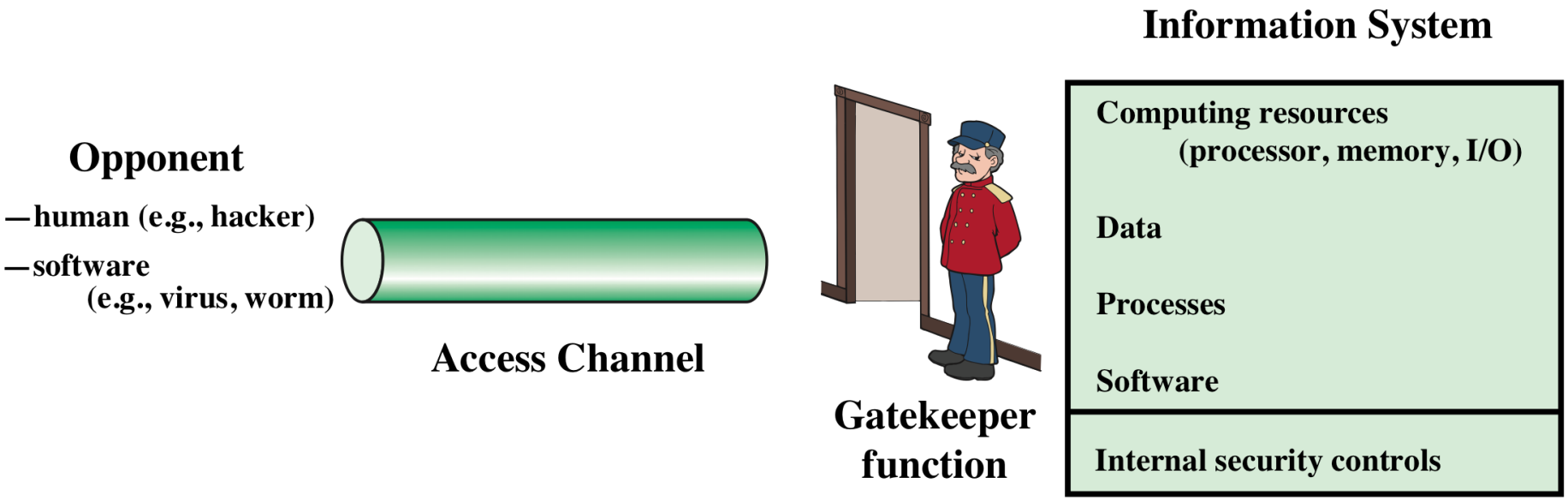


Figure 1.3 Network Access Security Model

Fundamental Security design Principals

- Economy of mechanism
- Fail-safe defaults (default is lack of access)
- Complete mediation (every access must be checked against the access control mechanism.)
- Open design
- Separation of privilege (practice in which multiple privilege attributes are required to achieve access to a restricted resource.)
- Least privilege
- Least common mechanism
- Psychological acceptability
- Isolation
- Encapsulation
- Modularity
- Layering
- Least astonishment

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]:

A Model for Network Access Security

- Using this model requires us to:
  1. Select appropriate gatekeeper functions to identify users
  2. Implement security controls to ensure only authorized users access designated information or resources

More on Computer System Security

- Based on “Security Policies”
  - Set of rules that specify
    - How resources are managed to satisfy the security requirements
    - Which actions are permitted, which are not
  - Ultimate aim
    - Prevent security violations such as unauthorized access, data loss, service interruptions, etc.
  - Scope
    - Organizational or Individual
  - Implementation
    - Partially automated, but mostly humans are involved
  - Assurance and Evaluation
    - Assurance: degree of confidence to a system
    - Security products and systems must be evaluated using certain criteria in order to decide whether they assure security or not

Attack Surfaces

- 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 in a firewall
  - Code that processes incoming data, email, XML, office documents, etc.
  - Interfaces and Web forms
  - An employee with access to sensitive information vulnerable to a social engineering attack

Attack Surface Categories

- Network attack surface
  - Refers to vulnerabilities over an enterprise network, wide-area network, or the Internet
    - E.g. DoS, intruders exploiting network protocol vulnerabilities
- Software attack surface
  - Refers to vulnerabilities in application, utility, or operating system code
- Human attack surface
  - Refers to vulnerabilities created by personnel or outsiders
  - E.g. social engineering, insider traitors

An attack surface analysis is useful for assessing the scale and severity of threats to a system.

Attack Surface Categories

- As illustrated in Figure 1.3, the use of layering, or defense in depth, and attack surface reduction complement each other in mitigating security risk.

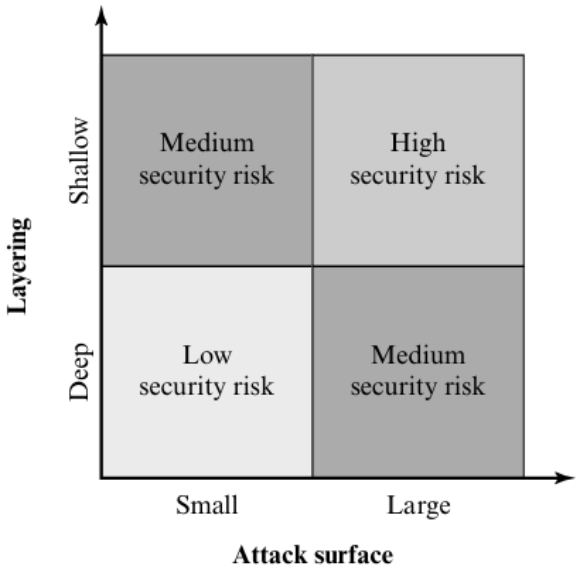


Figure 1.3 Defense in Depth and Attack Surface

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 that an attacker could reach that goal are itera tively and incrementally represented as branches and sub nodes of the tree.

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

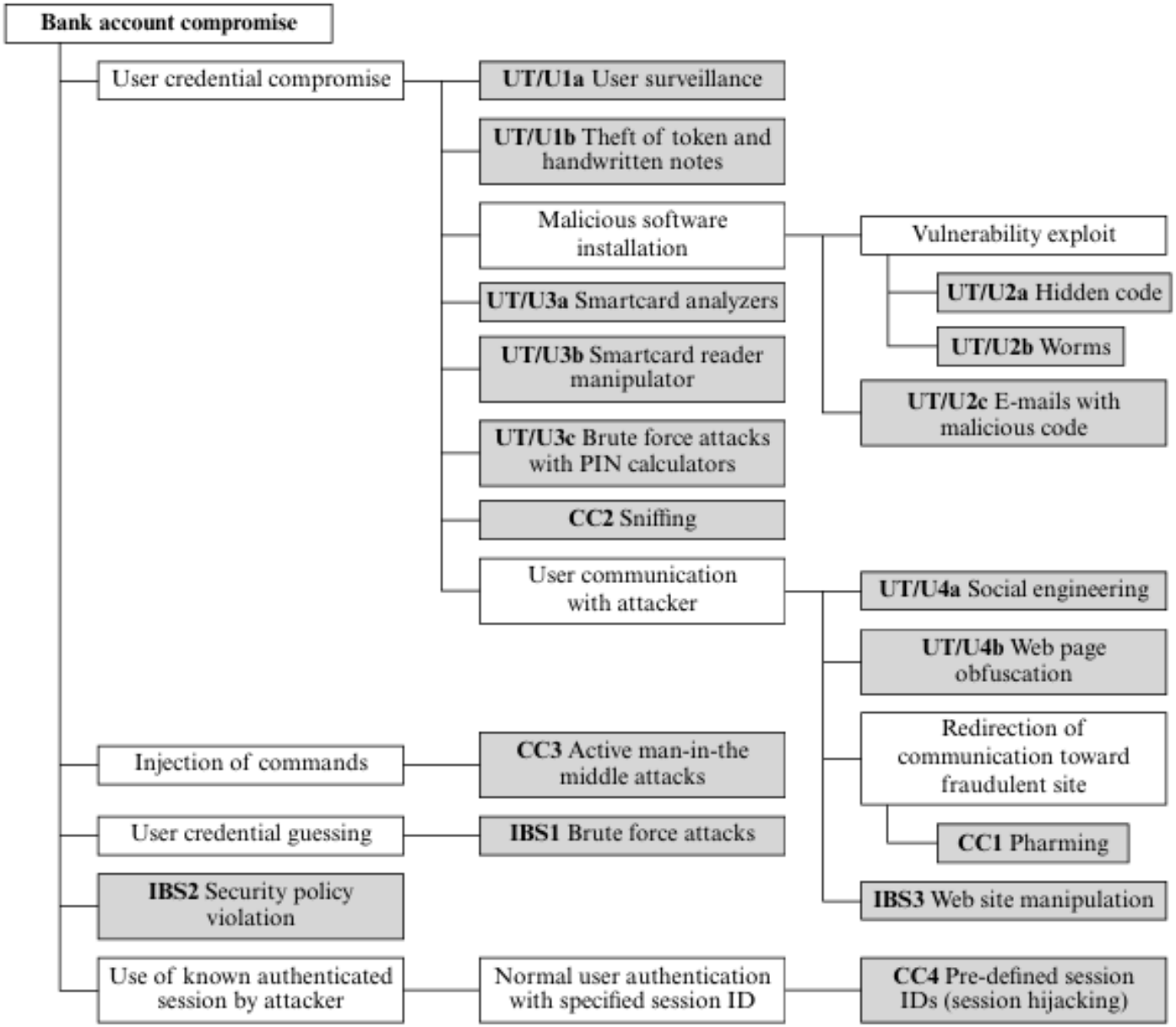
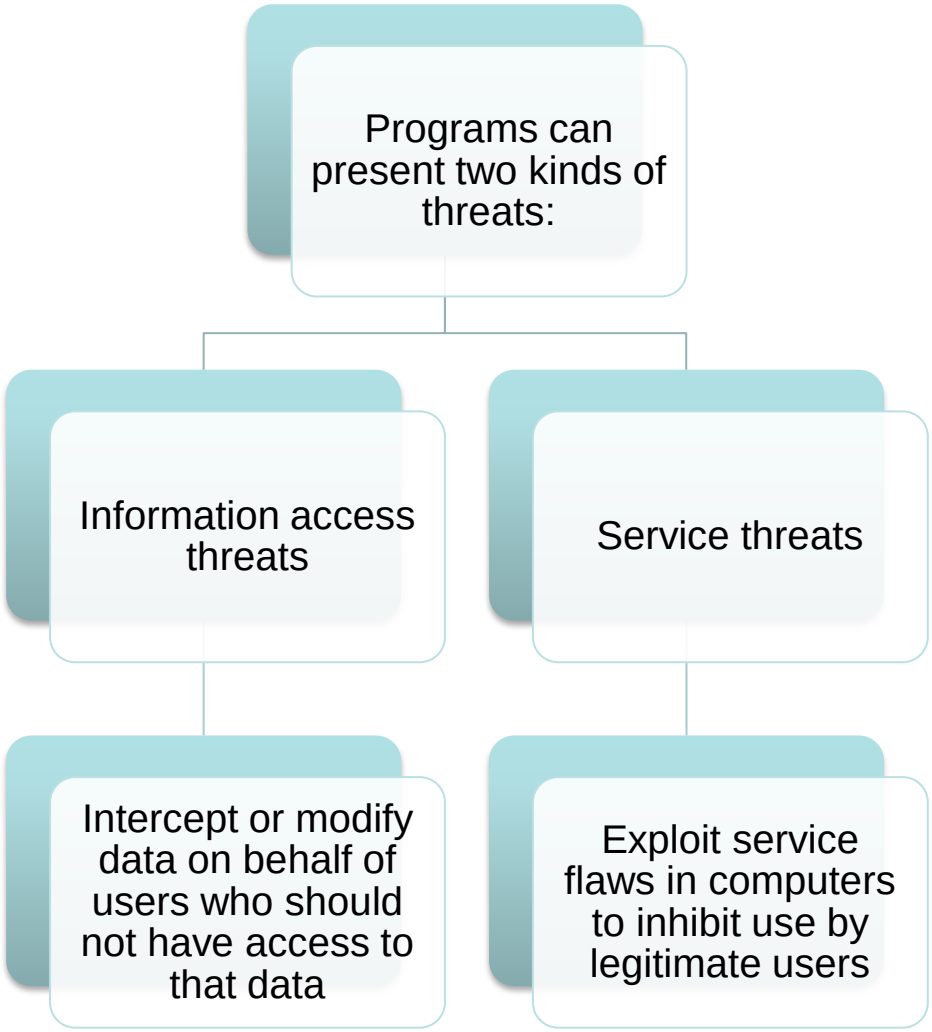


Figure 1.4 An Attack Tree for Internet Banking Authentication

Unwanted Access

- Placement in a computer system of logic that exploits vulnerabilities in the system and that can affect application programs as well as utility programs



Standards

- NIST

- National Institute of Standards and Technology
- 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
- NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact

- ISOC

- Internet Society
- Professional membership society with worldwide organizational and individual membership
- Provides leadership in addressing issues that confront the future of the Internet
- 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)
- Internet standards and related specifications are published as Requests for Comments (RFCs)

Techniques

Mechanisms discussed already are only theoretical recipes to implement security. The actual implementation of security goals needs some techniques. Two techniques are prevalent today: **cryptography and steganography.**

Cryptography

Cryptography, a word with Greek origins, means “secret writing.” However, we use the term to refer to the science and art of transforming messages to make them secure and immune to attacks.

Steganography

The word steganography, with origin in Greek, means “covered writing,” in contrast with cryptography, which means “secret writing.”

Example: covering data with text

This book □ is mostly about cryptography, not □□ steganography.
□ □□ □ □ □ □ □□
0 1 0 0 0 0 1

Example: using dictionary

A	friend	called	a	doctor.
0	10010	0001	0	01001

Example: covering data under color image

01010011	10111100	01010101
01011110	10111100	01100101
01111110	01001010	00010101

Cryptographic Services

Cryptography supports the following services:

1. Confidentiality

2. Integrity

3. Authentication

4. Identity

5. Timeliness

6. Proof of ownership

Each has various different requirements in different circumstances, and each issupported by a wide variety of schemes.

Applications

1. Communications (encryption or authentication)
2. File and data base security
3. Electronic funds transfer
4. Electronic Commerce
5. Digital cash
6. Contract signing
7. Electronic mail
8. Authentication: Passwords, PINs
9. Secure identification, Access control
10. Secure protocols
11. Proof of knowledge

Applications (cont.)

12. Construction by collaborating parties (secret sharing)
13. Copyright protection
14. etc.

Some Other Security Facts

- Not as simple as it might first appear to the novice
- Must consider all potential attacks when designing a system
- Generally yields complex and counterintuitive systems
- Battle of intelligent strategies between attacker and admin
- Requires regular monitoring
- Not considered as a beneficial investment until a security failure occurs
  - Actually security investments must be considered as insurance against attacks
- too often an afterthought
  - Not only from investment point of view, but also from design point of view

Summary

- Computer security concepts
  - Definition
  - Examples
  - Challenges
- The OSI security architecture
- Security attacks
  - Passive attacks
  - Active attacks
- Security services
  - Authentication
  - Access control
  - Data confidentiality
  - Data integrity
  - Nonrepudiation
  - Availability service
- Security mechanisms
- Model for network security
- Standards

Cryptographic Functions

- A communication game
- Protocol
- Magic function
- Cryptographic functions

Cryptographic Functions

- Alice and Bob are two parties
- Want to go for dinner
- Alice for Chinese, Bob for Japanese
- How to resolve?

Use of Unbiased Coin

- Alice tosses an unbiased coin with her hands covering, asks Bob of his choice: HEADS or TAILS
- If Bob's choice matches with the outcome of the toss, they go for Japanese food
- Consider the situation when they are far apart
- They can communicate with a telephone
- What is the problem?

Problem of Trust

- Bob can not trust Alice, as Alice can tell a lie:
  - How do we solve the problem
- Solution to these kind of multi-party(plural number of players) problem are called technically "protocols"
- In order to resolve the problem, they engage "a protocol"
  - They use a magic function, f(x)

The Protocol

- Both of them agree on the function f(x)
- An even number x represents HEAD
- An odd number x represents TAIL

The Protocol

- Both of them agree on the function f(x)
- An even number x represents HEAD
- An odd number x represents TAIL

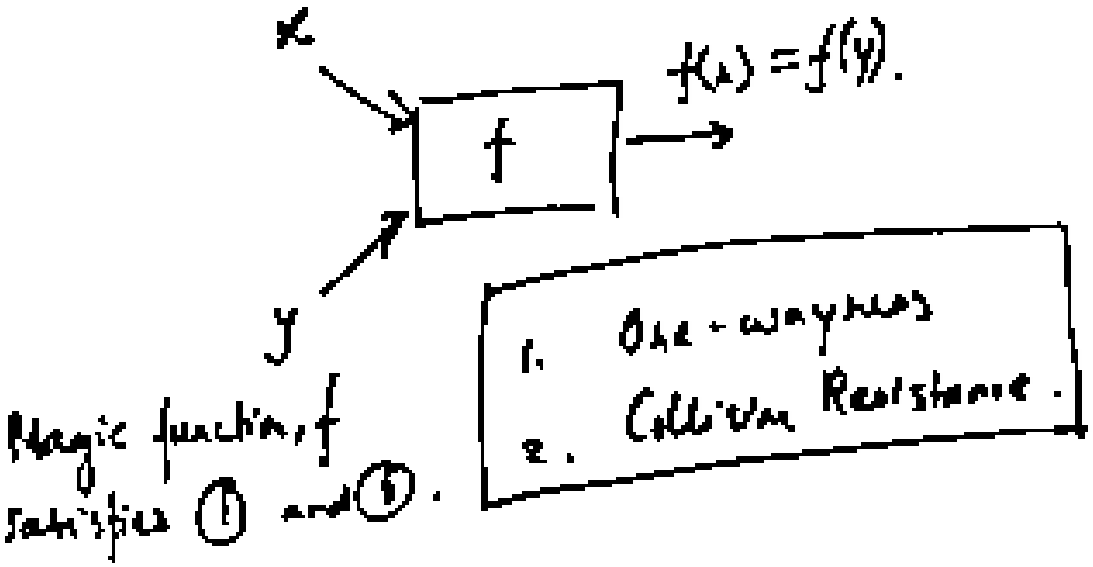
Problem of Trust

Collision-resistance.

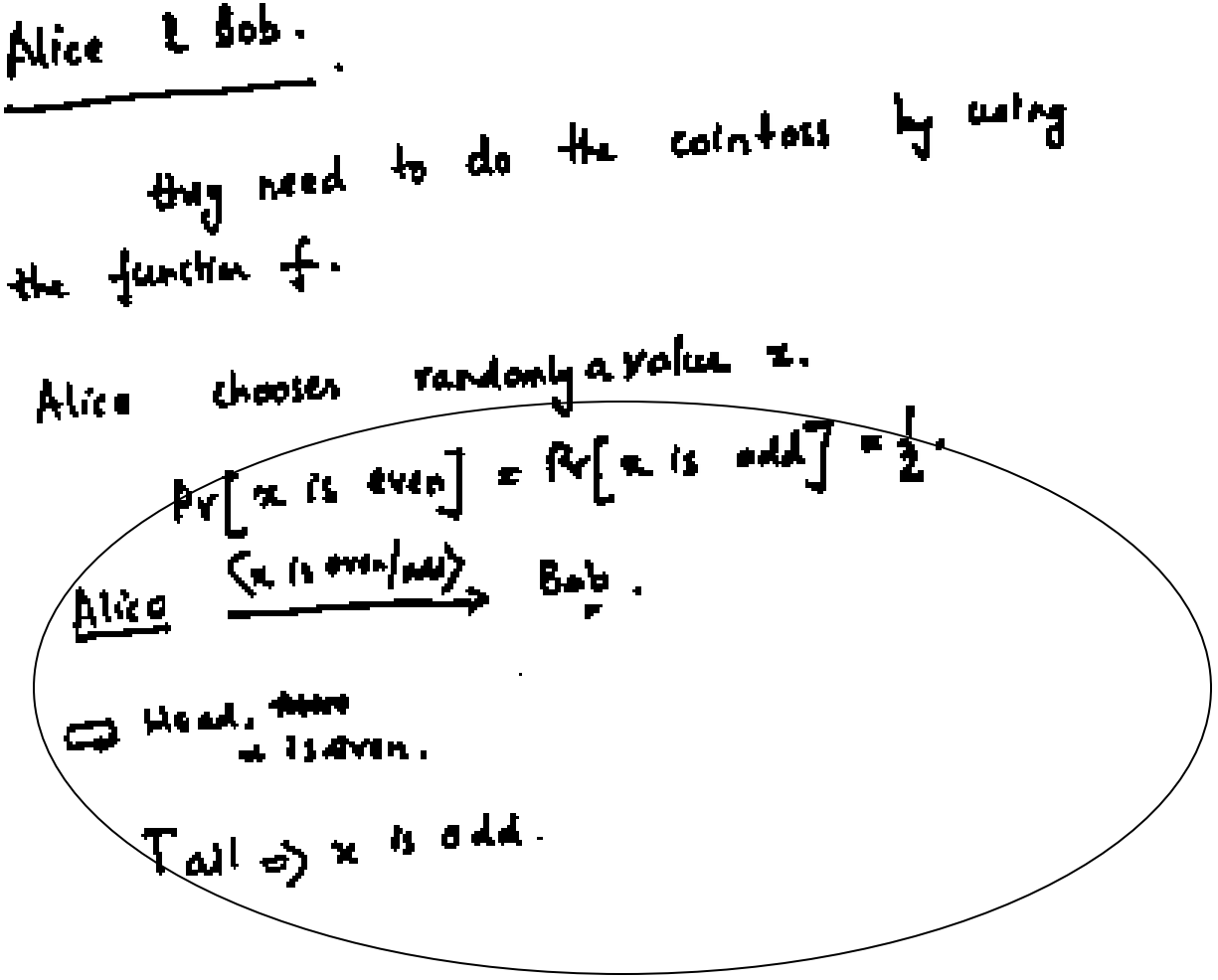
Given $f(\cdot)$, output two values $x \neq y$,

s.t. $f(x) = f(y)$.

Hard/Difficult problem.



The Protocol



Use function f to resove

Coin Flipping over Telephone

- Alice picks up a randomly large integer, x and computes f(x)
- Bob tells Alice his guess of whether x is odd or even
- Alice hen sends x to Bob
- Bob verifies by computing f(x)

Security Analysis

- Can Alice cheat?
- For that Alice need to create a y<>x, st f(x)=f(y). Hard to do.
- Can Bob guess beter than a random guess?
- Bob listens to f(x) which speaks nothing of x. so his probability of guess is ½ (random guess)

An Example

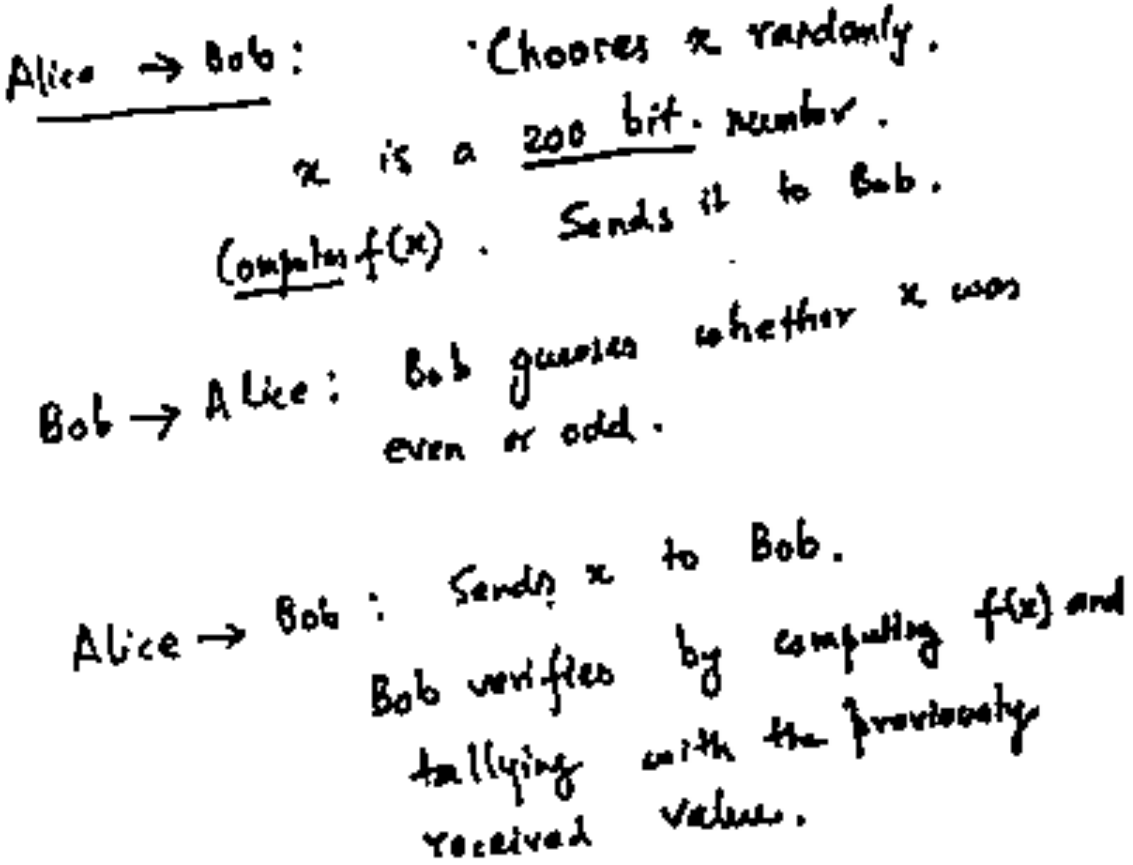
- Alice and Bob wish to resole a dispute over telephone. We can encode the possibilties of the dispute by a binary value. For this they engage a protocol:

- Alice to Bob: Alice picks up randomly an x, which is a 200 bit number and comptes the function f(x). Alice sends f(x) to Bob.

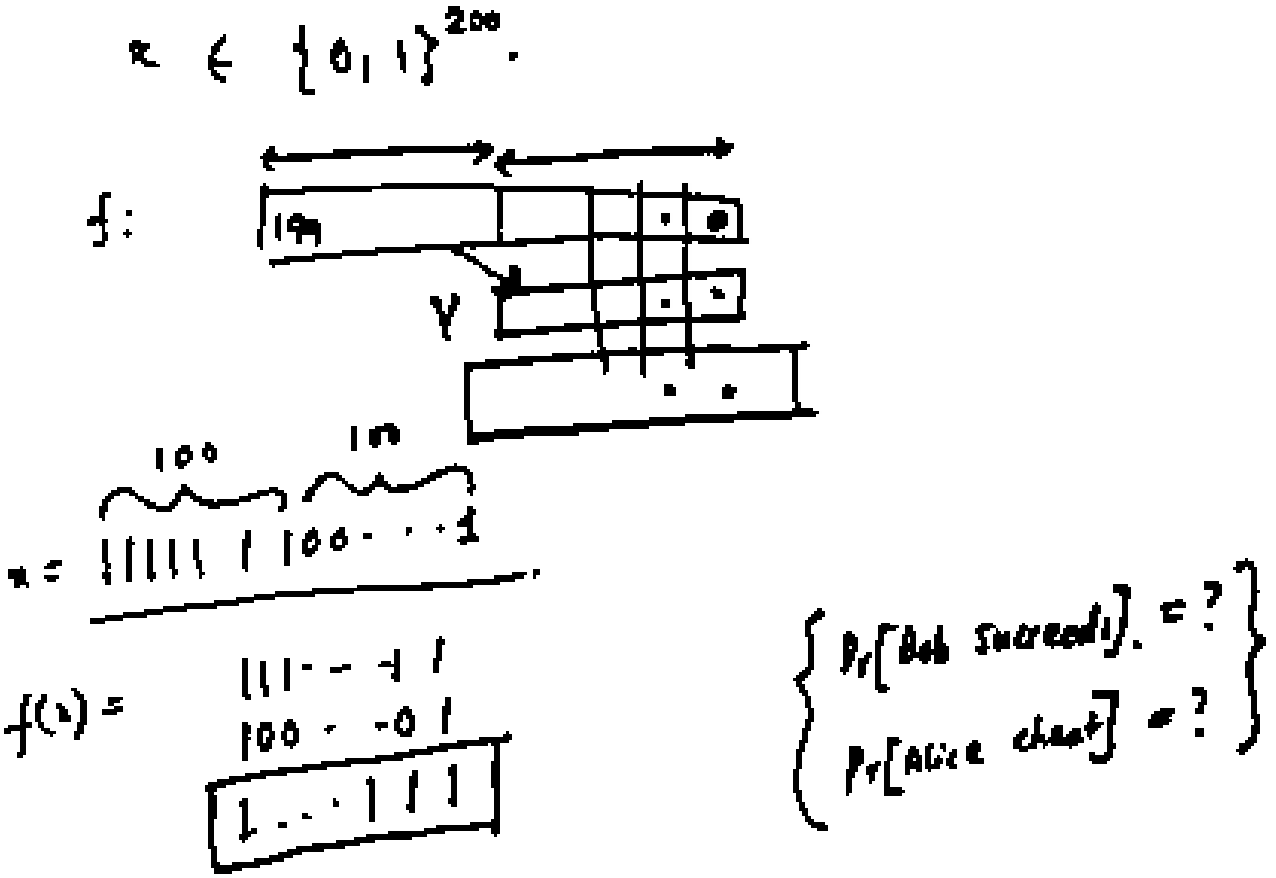
- Bob to Alice: Bob tells Alice whether x was even or odd

- Alice to Bob: lice then sends x to Bob, so Bob can verify whether his guess is correct.

An Example


Alice → Bob : · Chooses x randomly.
x is a 200 bit number.
(compute f(x). Sends it to Bob.
Bob → Alice : Bob guesses whether x was even or odd.
Alice → Bob : Sends x to Bob.
Bob verifies by computing f(x) and tallying with the previously received values.

An Example

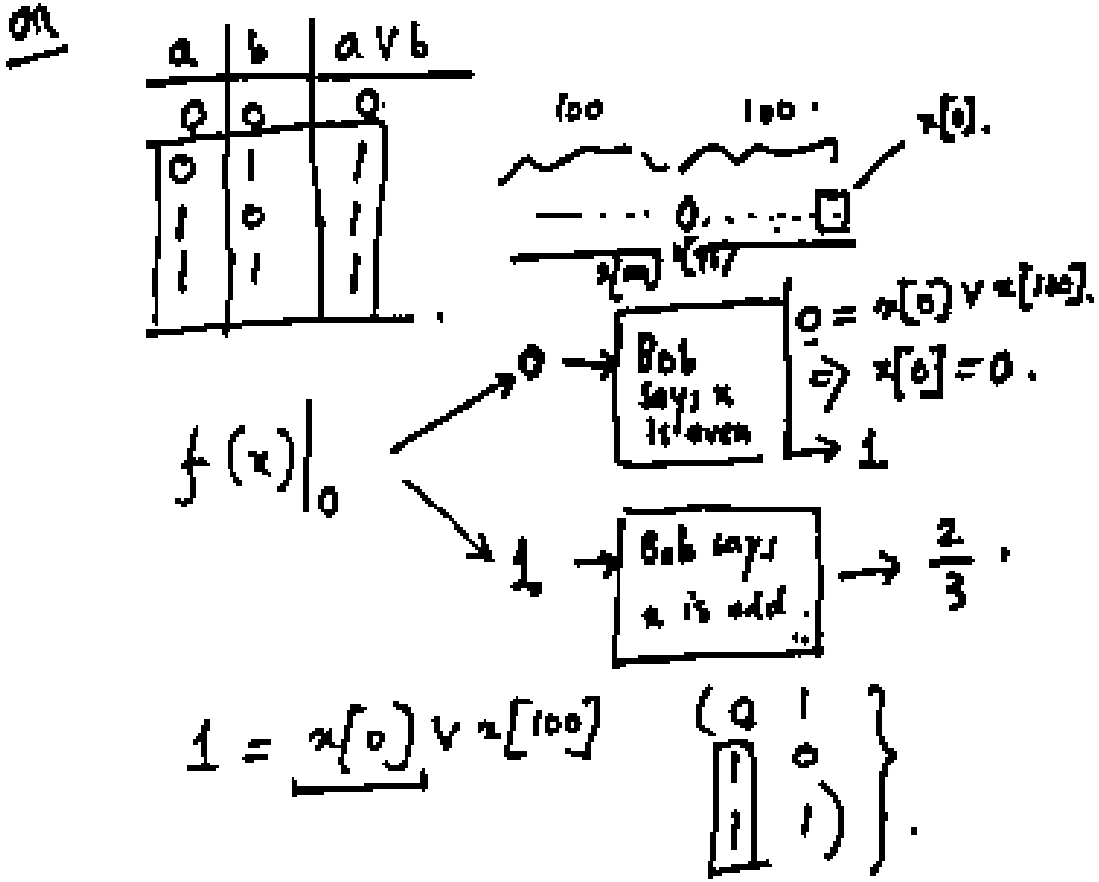

$x \in \{0,1\}^{200}$.
f:
100
100
x =
f(x) =
$\Pr[\text{Bob succeeds}] = ?$
$\Pr[\text{Alice cheats}] = ?$

Bob's Strategy

- Bob's Experiment:
  -Input f(x)
  -Output parity of x

- Algorithm
  If $[f(x)]_0=0$ the x is even
  Else x is odd

Bob's Strategy



Bob's Prob of Success

- If X is chosen at random

  Pr[X is even]=Pr[X is odd]=1/2

  Pr[Bob succeds] = Pr[X is even] Pr[Bob succeeds|X is even] + Pr[X is odd]Pr[Bob succeeds|X is odd]=1/2 ½ +1/2 1=3/4

Bob's Prob of Success

- Remember we compute alice's cheating probability irrespective of Bob's strategy

Bob's Prob of Success

$$\Pr[\text{Bob succeeds}] = \Pr[X \text{ is even}]\Pr[\text{Bob succeeds} \mid X \text{ is even}] + \Pr[X \text{ is odd}]\Pr[\text{Bob succeeds} \mid X \text{ is odd}].$$

$$= \frac{1}{2}\left(\Pr[\text{Bob succeeds} \mid X \text{ is even}] + \Pr[\text{Bob succeeds} \mid X \text{ is odd}]\right).$$

$x[0] = 0$: $f(x)|_0 = x[00] \vee x[0] = x[10]$.

$x[0] = 1$: $f(x)|_0 = x[00] \vee 1 = 1$.