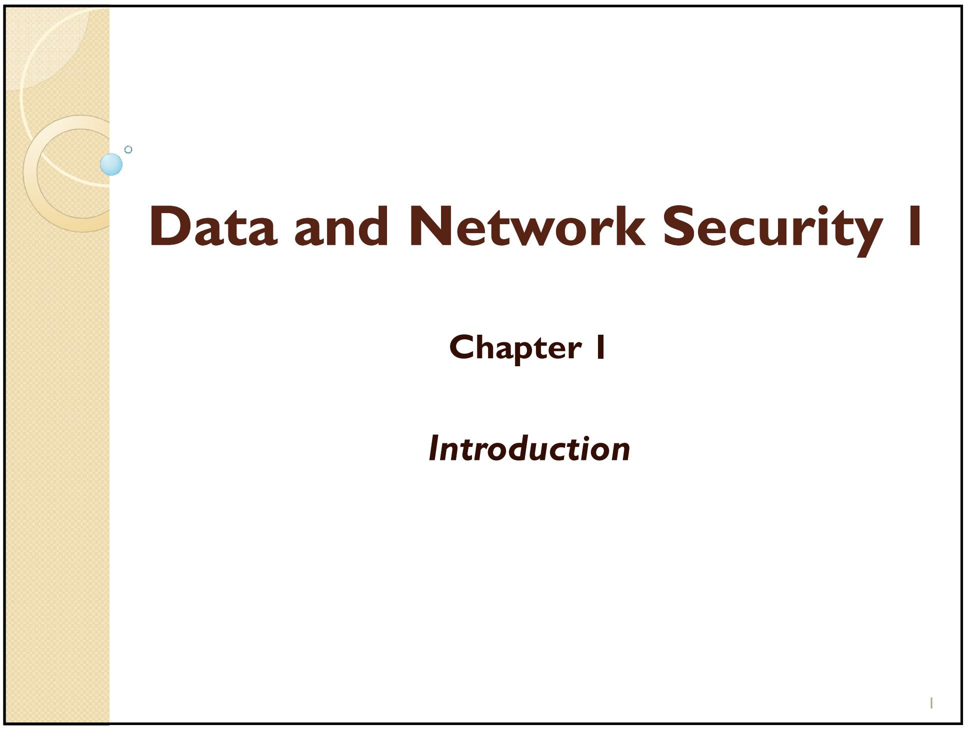
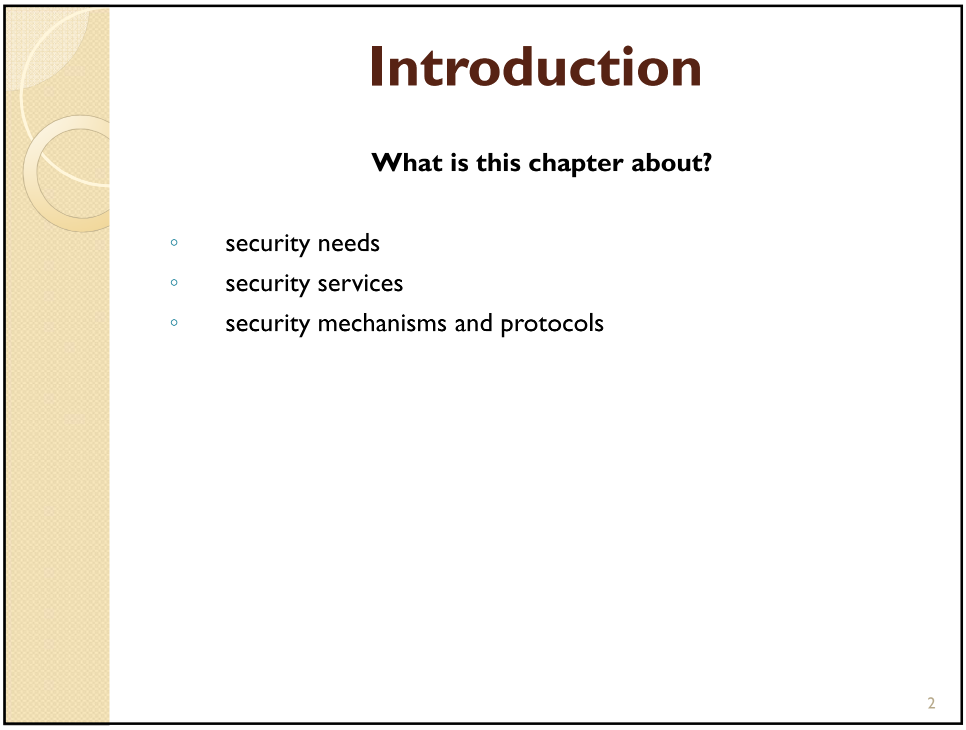


Data and Network Security 1

Chapter 1

Introduction



Introduction

What is this chapter about?

- security needs
- security services
- security mechanisms and protocols

What security is about in general?

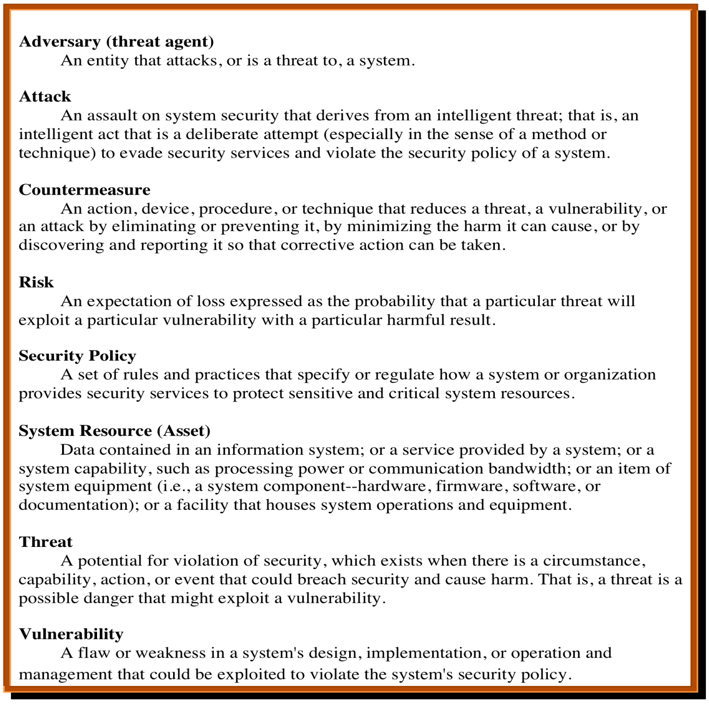
- Security is about protection of assets
  - D. Gollmann, Computer Security, Wiley
- Prevention
  - take measures that prevent your assets from being damaged (or stolen)
- Detection
  - take measures so that you can detect when, how, and by whom an asset has been damaged
- Reaction
  - take measures so that you can recover your assets

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

Internet shopping example

- Prevention
  - encrypt your order and card number, enforce merchants to do some extra checks, using PIN even for Internet transactions, don't send card number via Internet
- Detection
  - an unauthorized transaction appears on your credit card statement
- Reaction
  - complain, dispute, ask for a new card number, sue (if at all possible)
  - Or, pay and forget



Adversary (threat agent)
An entity that attacks, or is a threat to, a system.

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.

Countermeasure
An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.

Risk
An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

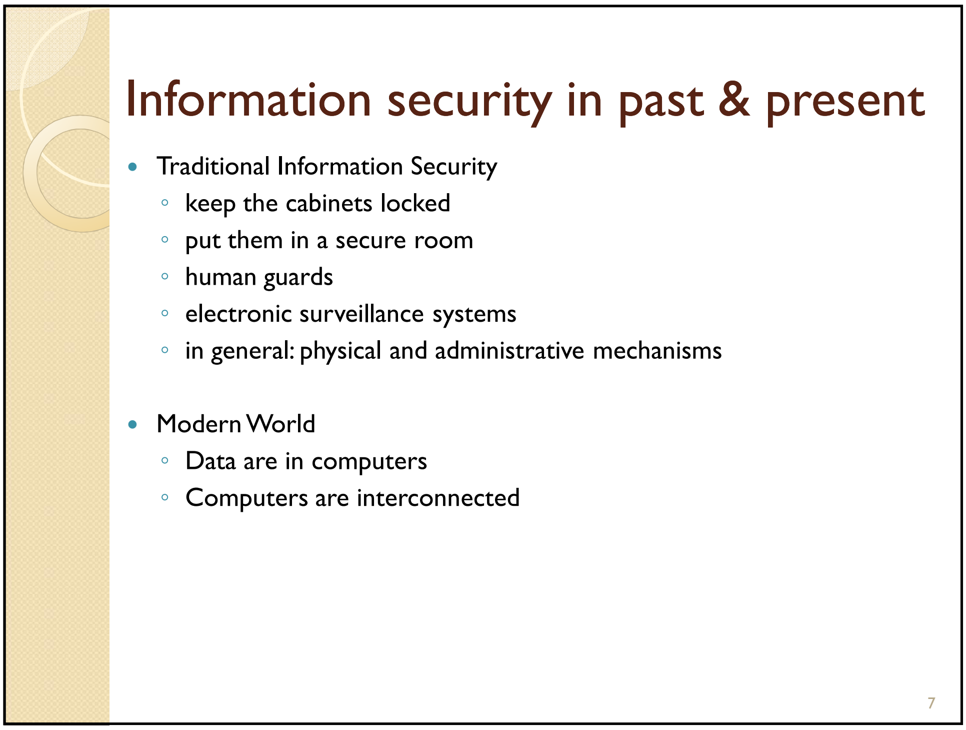
Security Policy
A set of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources.

System Resource (Asset)
Data contained in an information system; or a service provided by a system; or a system capability, such as processing power or communication bandwidth; or an item of system equipment (i.e., a system component--hardware, firmware, software, or documentation); or a facility that houses system operations and equipment.

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.

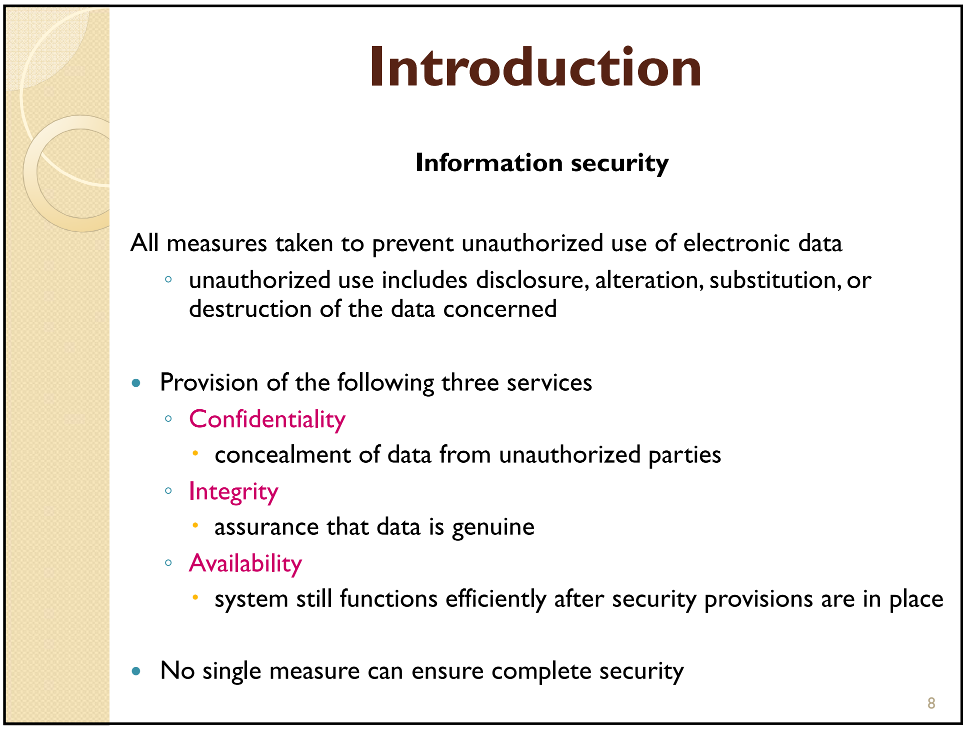
Vulnerability
A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy.

Computer Security Terminology



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



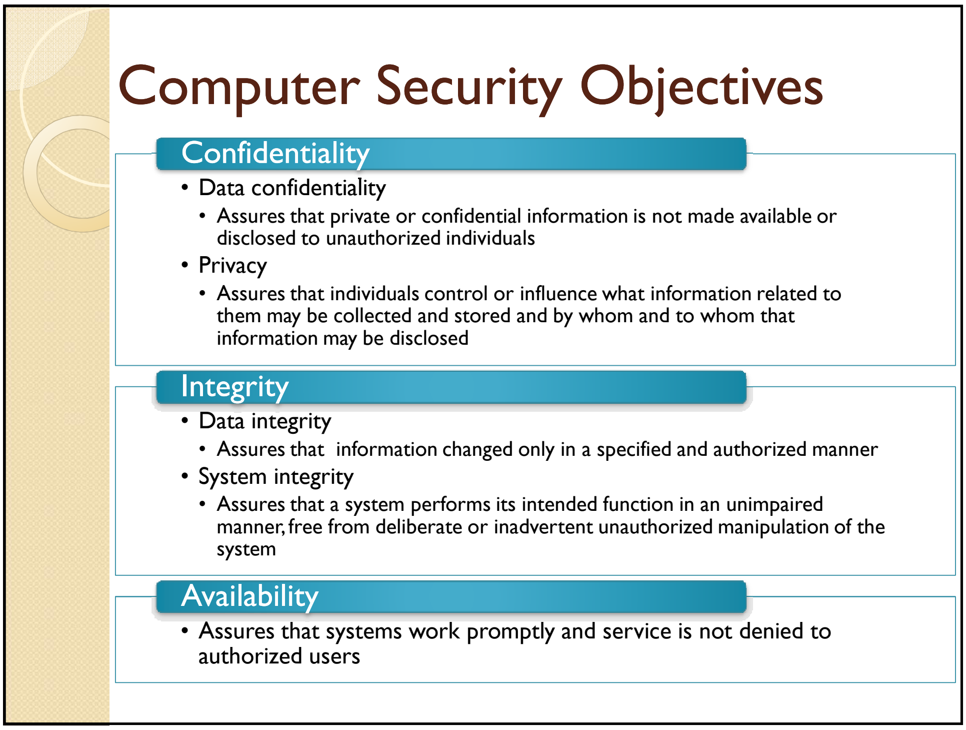
Introduction

Information security

All measures taken to prevent unauthorized use of electronic data

- unauthorized use includes disclosure, alteration, substitution, or destruction of the data concerned

- Provision of the following three services
  - Confidentiality
    - concealment of data from unauthorized parties
  - Integrity
    - assurance that data is genuine
  - Availability
    - system still functions efficiently after security provisions are in place
- No single measure can ensure complete security



Computer Security Objectives

Confidentiality

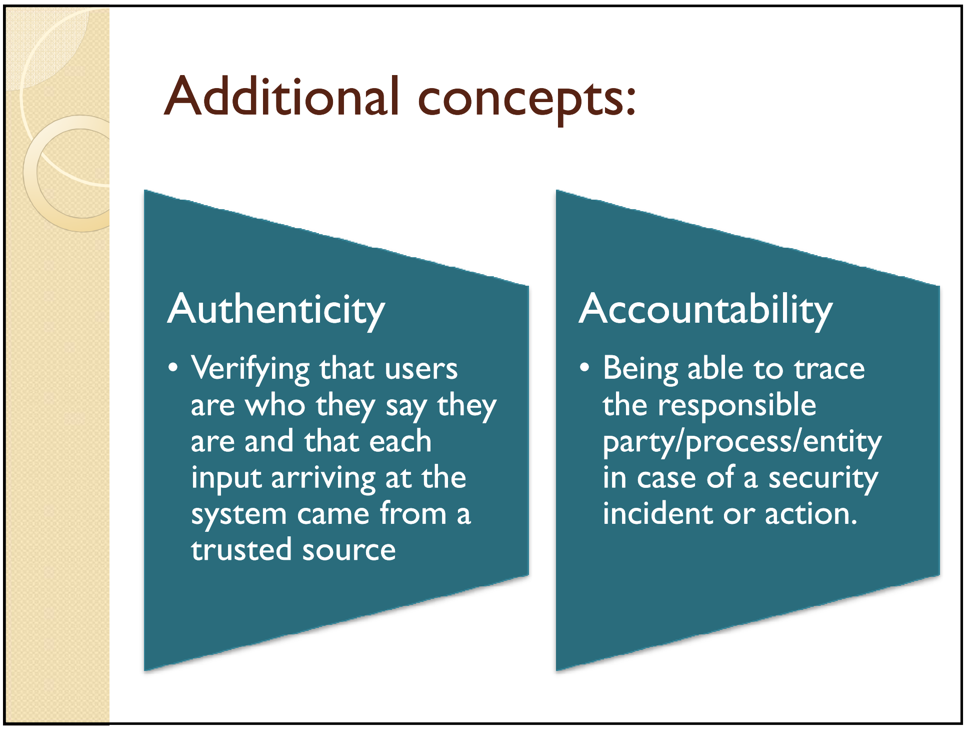
- Data confidentiality
  - Assures that private or confidential information is not made available or disclosed to unauthorized individuals
- Privacy
  - Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Integrity

- Data integrity
  - Assures that information 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

Availability

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



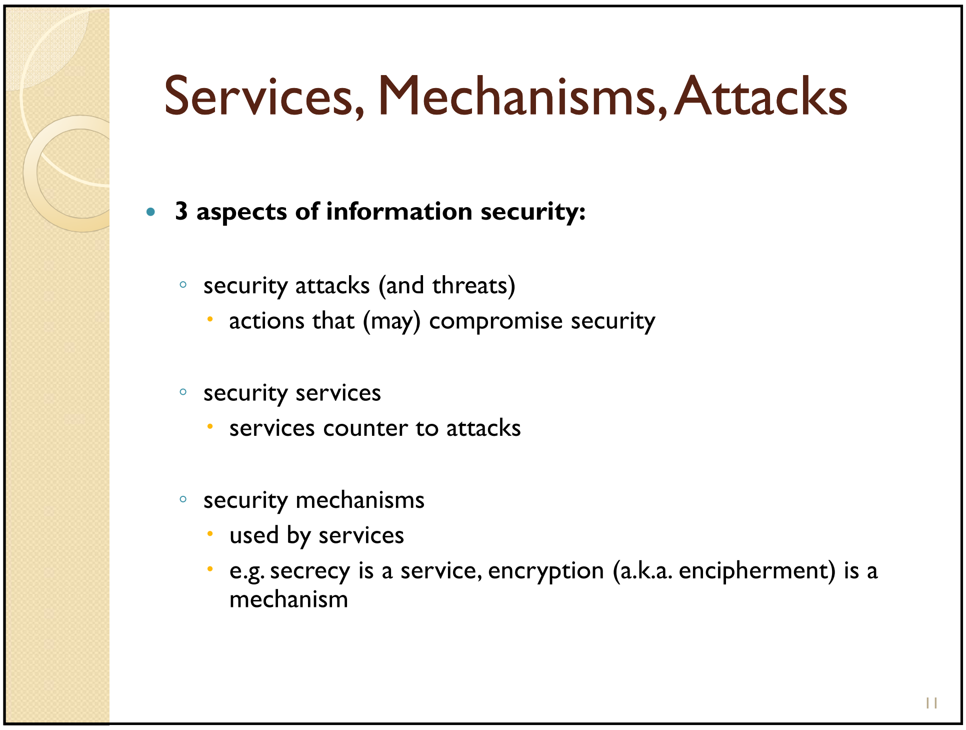
Additional concepts:

Authenticity

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

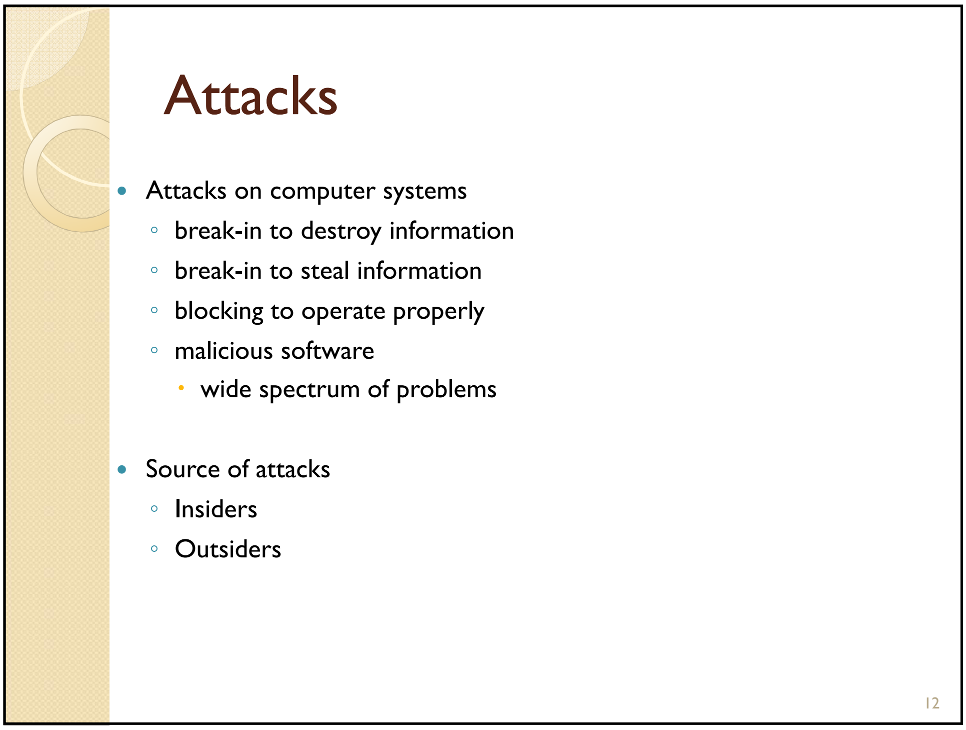
Accountability

- Being able to trace the responsible party/process/entity in case of a security incident or action.



Services, Mechanisms, Attacks

- **3 aspects of information security:**
  - security attacks (and threats)
    - actions that (may) compromise security
  - security services
    - services counter to attacks
  - security mechanisms
    - used by services
    - e.g. secrecy is a service, encryption (a.k.a. encipherment) is a mechanism



Attacks

- Attacks on computer systems
  - break-in to destroy information
  - break-in to steal information
  - blocking to operate properly
  - malicious software
    - wide spectrum of problems
- Source of attacks
  - Insiders
  - Outsiders

Attacks

- Network Security
  - Active attacks
  - Passive attacks
- Passive attacks
  - interception of the messages
  - What can the attacker do?
    - use information internally
      - hard to understand
    - release the content
      - can be understood
    - traffic analysis
      - hard to avoid
  - Hard to detect, try to prevent

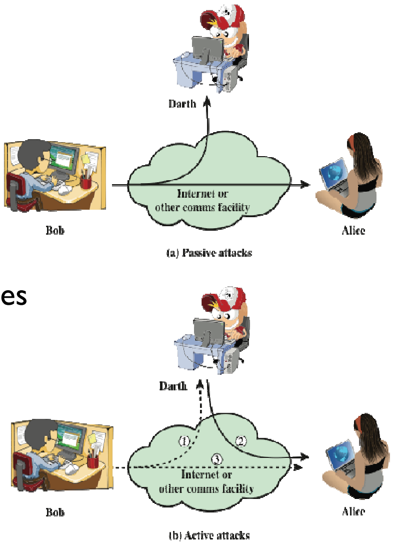
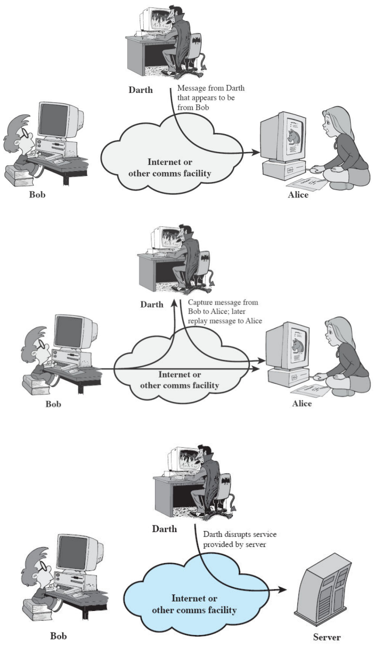
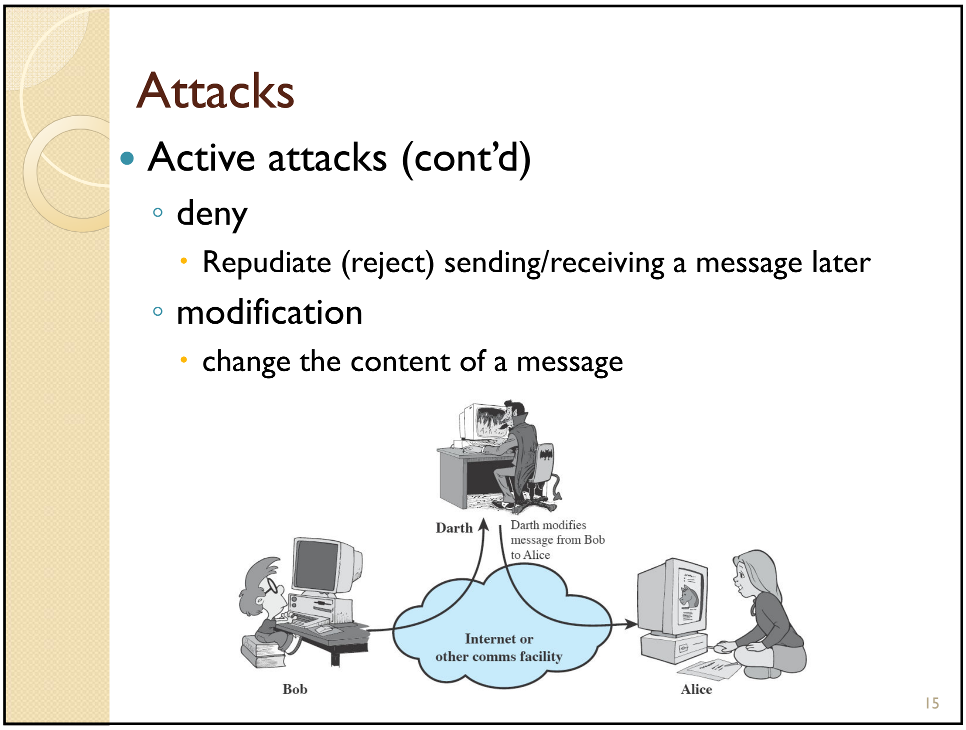


Figure 1.2 Security Attacks

Attacks

- Active attacks
  - Attacker actively manipulates the communication
  - Masquerade
    - pretend as someone else
    - possibly to get more privileges
  - Replay
    - passively capture data and send later
  - Denial-of-service
    - prevention the normal use of servers, end users, or network itself


Darth
Message from Darth that appears to be from Bob
Bob
Internet or other comms facility
Alice
Darth
Capture message from Bob to Alice; later replay message to Alice
Bob
Internet or other comms facility
Alice
Darth
Darth disrupts service provided by server
Bob
Internet or other comms facility
Server

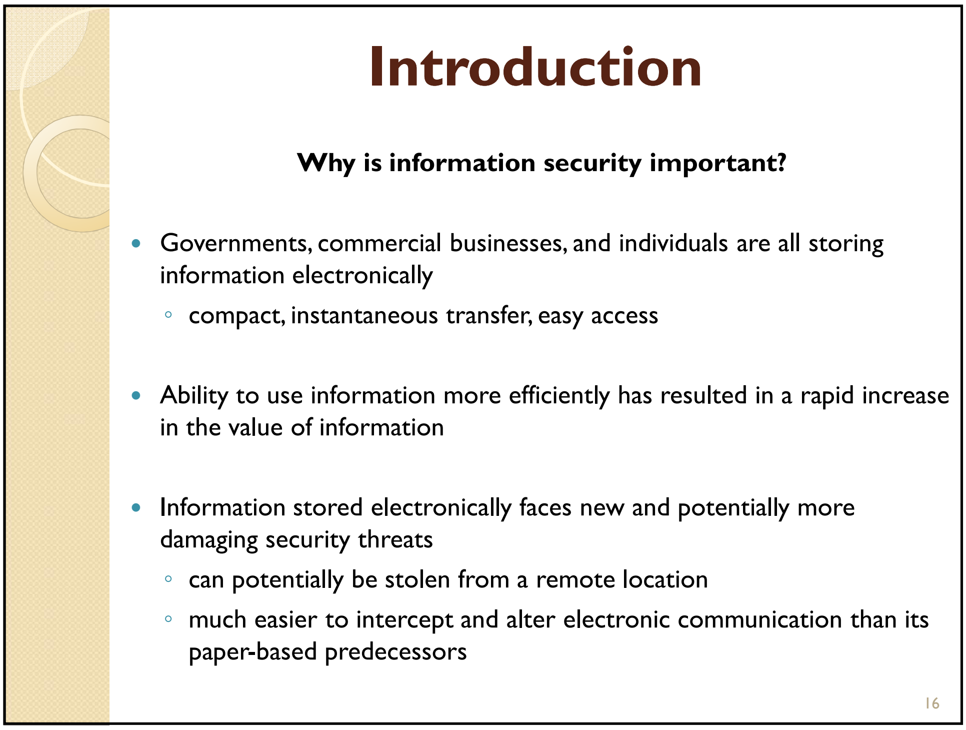


Attacks

- Active attacks (cont'd)
  - deny
    - Repudiate (reject) sending/receiving a message later
  - modification
    - change the content of a message

Darth
Darth modifies message from Bob to Alice
Internet or other comms facility
Bob
Alice

15

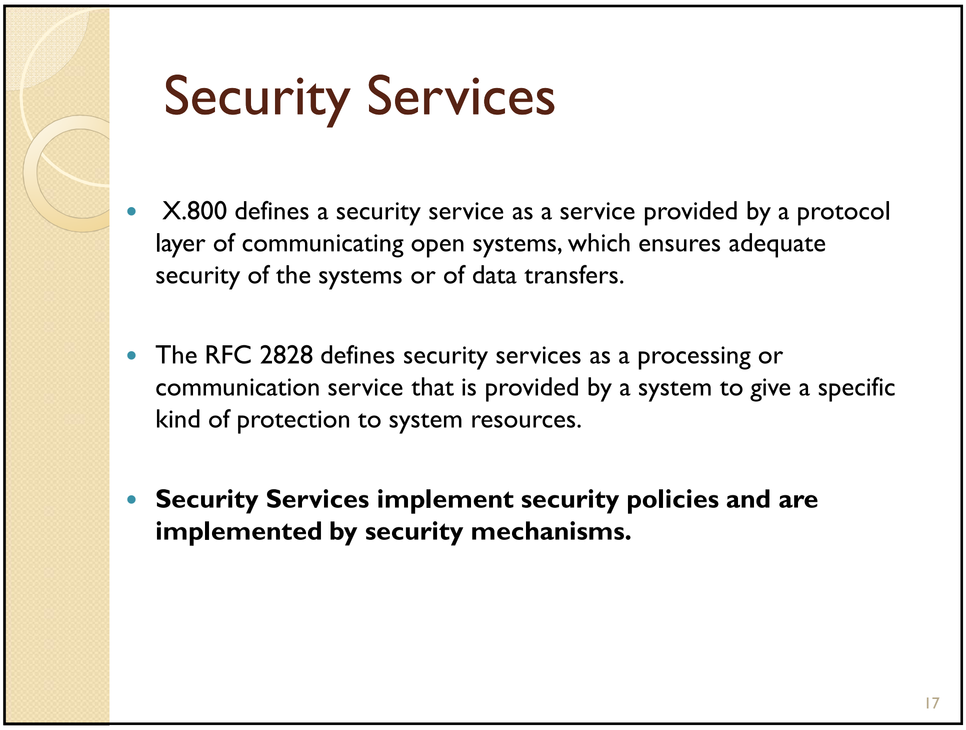


Introduction

Why is information security important?

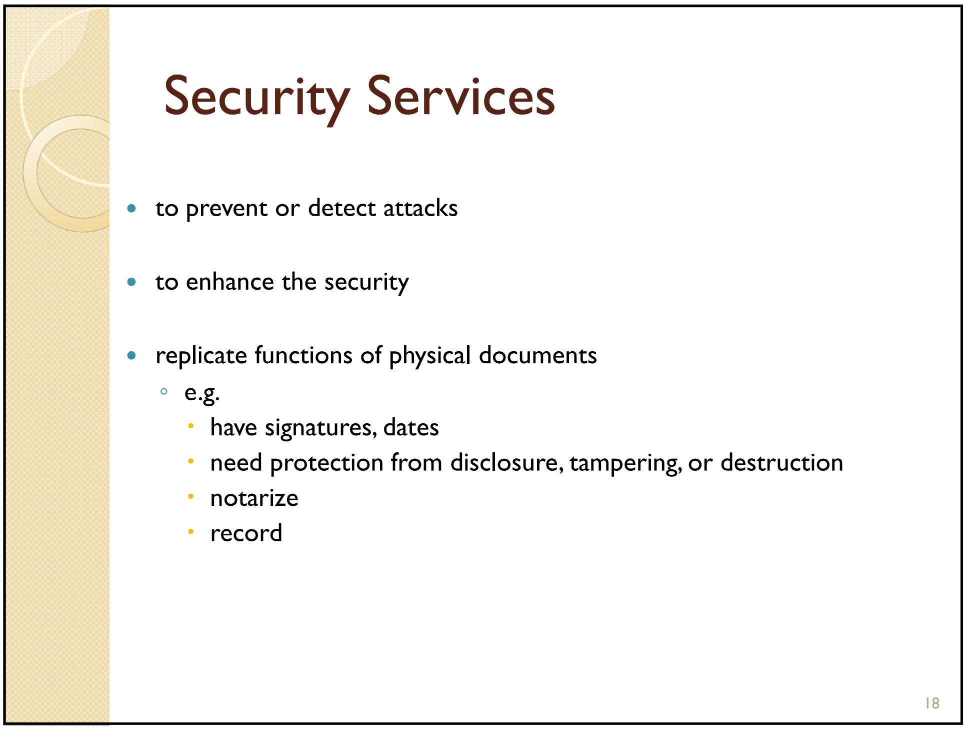
- Governments, commercial businesses, and individuals are all storing information electronically
  - compact, instantaneous transfer, easy access
- Ability to use information more efficiently has resulted in a rapid increase in the value of information
- Information stored electronically faces new and potentially more damaging security threats
  - can potentially be stolen from a remote location
  - much easier to intercept and alter electronic communication than its paper-based predecessors

16



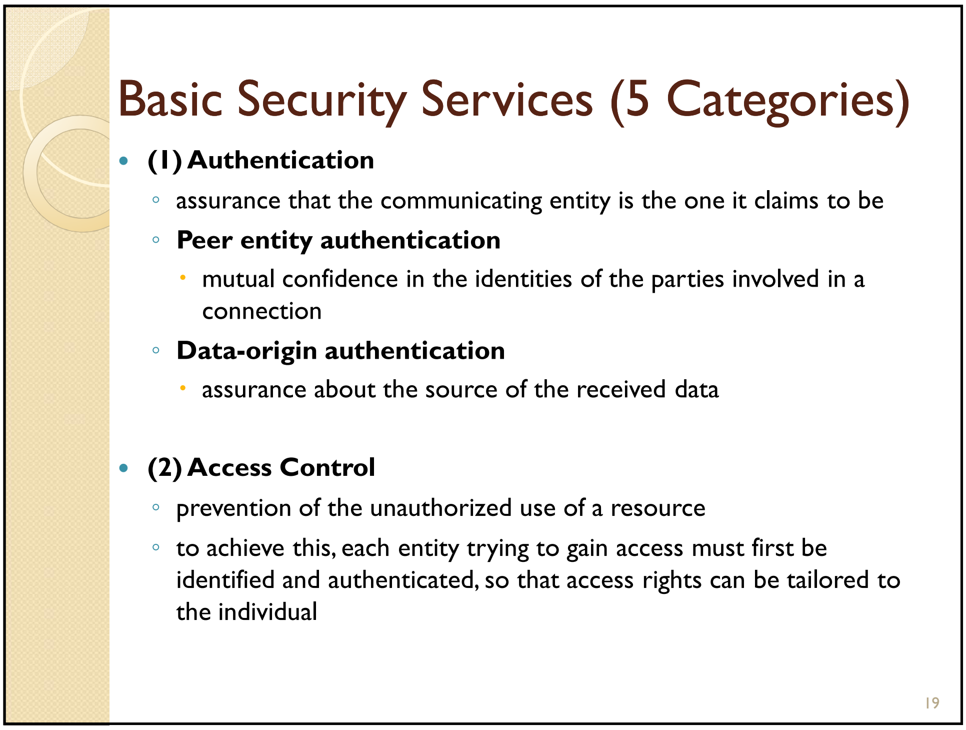
Security Services

- X.800 defines a security service as a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers.
- The RFC 2828 defines security services as a processing or communication service that is provided by a system to give a specific kind of protection to system resources.
- **Security Services implement security policies and are implemented by security mechanisms.**



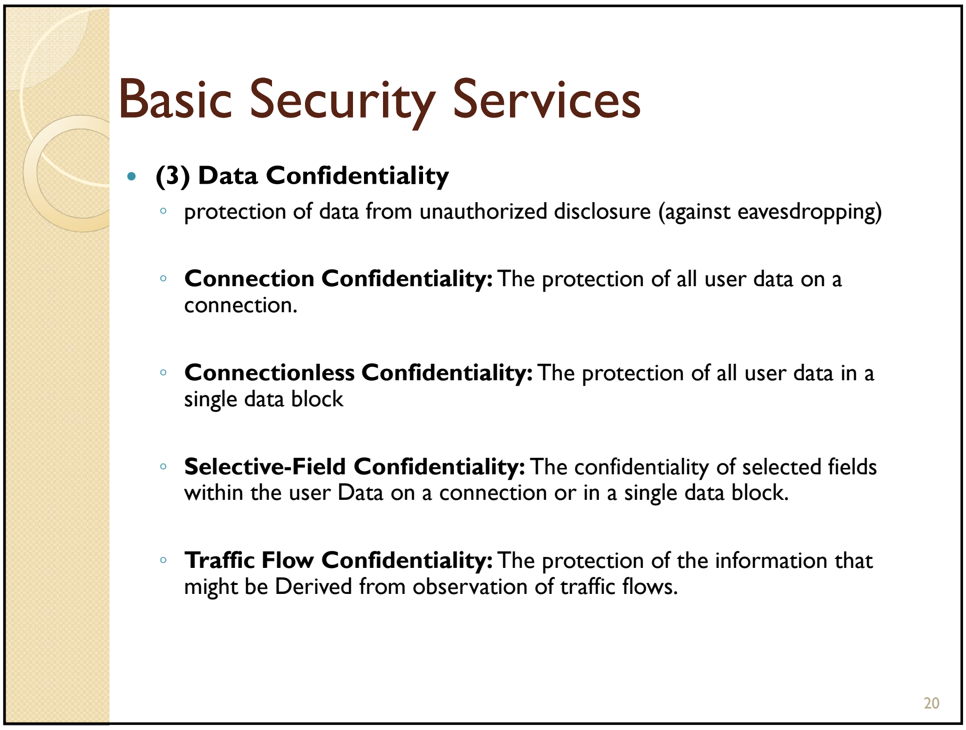
Security Services

- 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



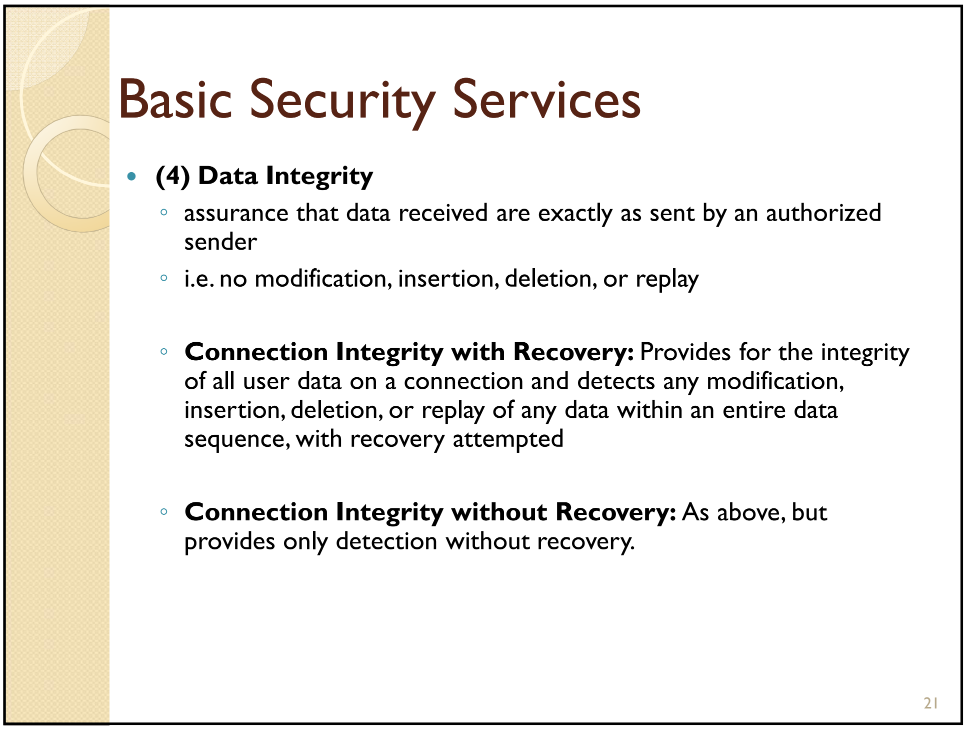
Basic Security Services (5 Categories)

- **(1) 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
- **(2) 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

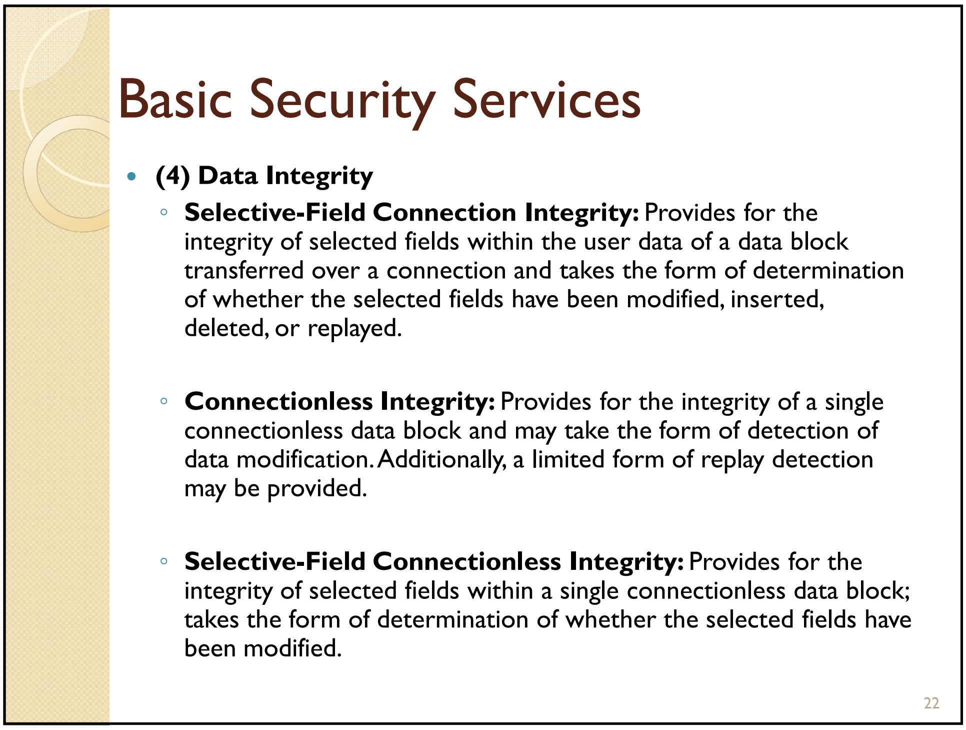
- **(3) Data Confidentiality**
  - protection of data from unauthorized disclosure (against eavesdropping)
  - **Connection Confidentiality:** The protection of all user data on a connection.
  - **Connectionless Confidentiality:** The protection of all user data in a single data block
  - **Selective-Field 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.



Basic Security Services

- **(4) Data Integrity**
  - assurance that data received are exactly as sent by an authorized sender
  - i.e. 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.

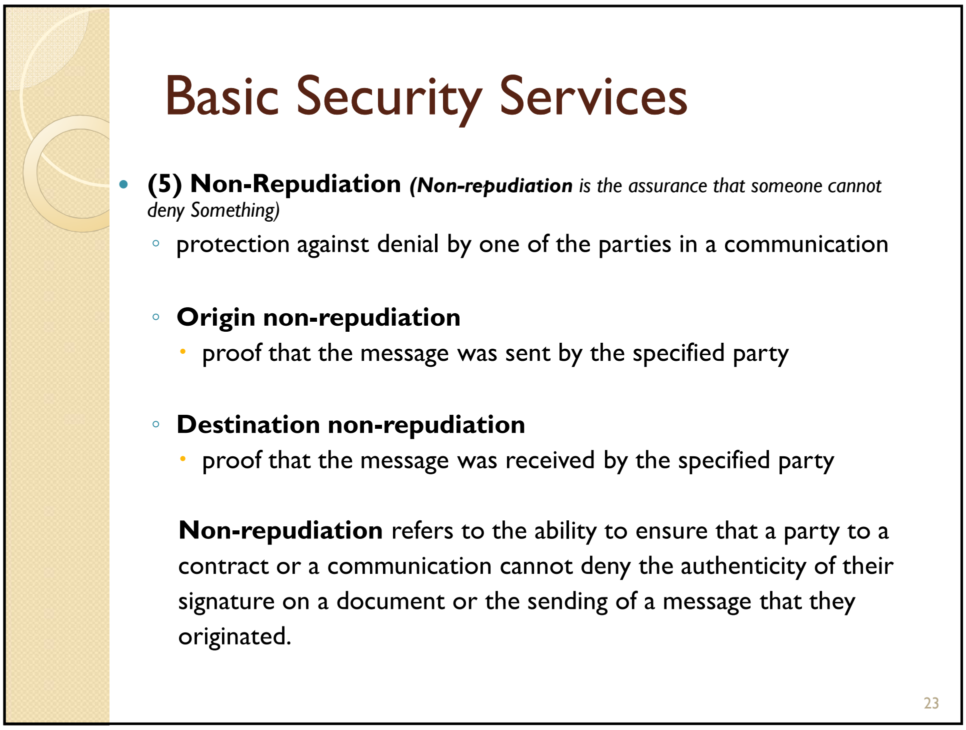
21



Basic Security Services

- **(4) Data Integrity**
  - **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.

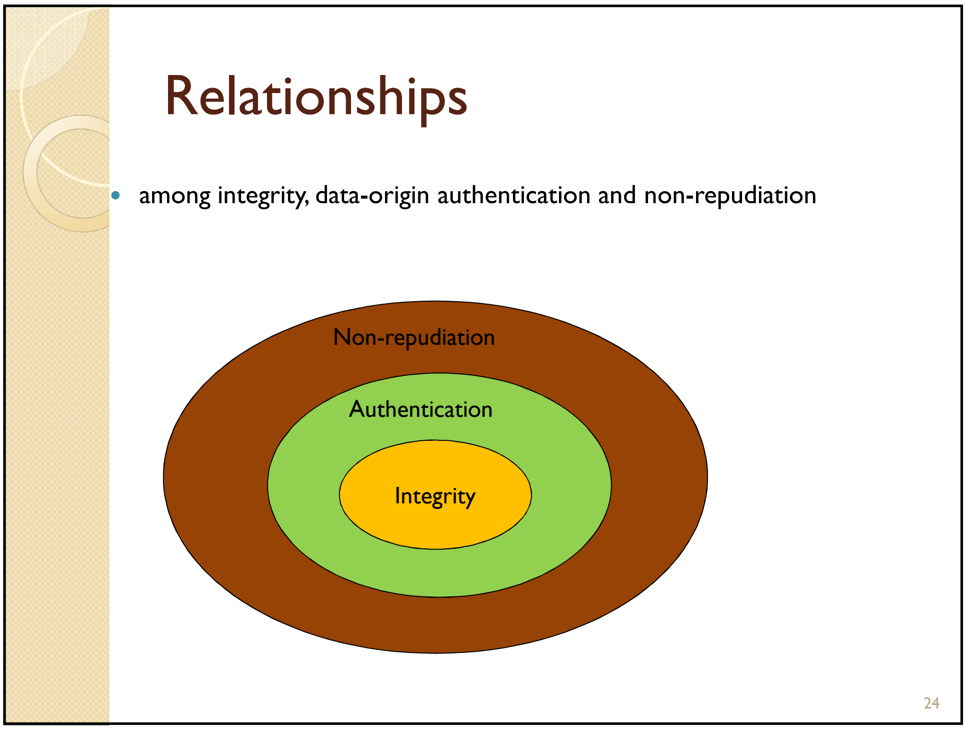
22



Basic Security Services

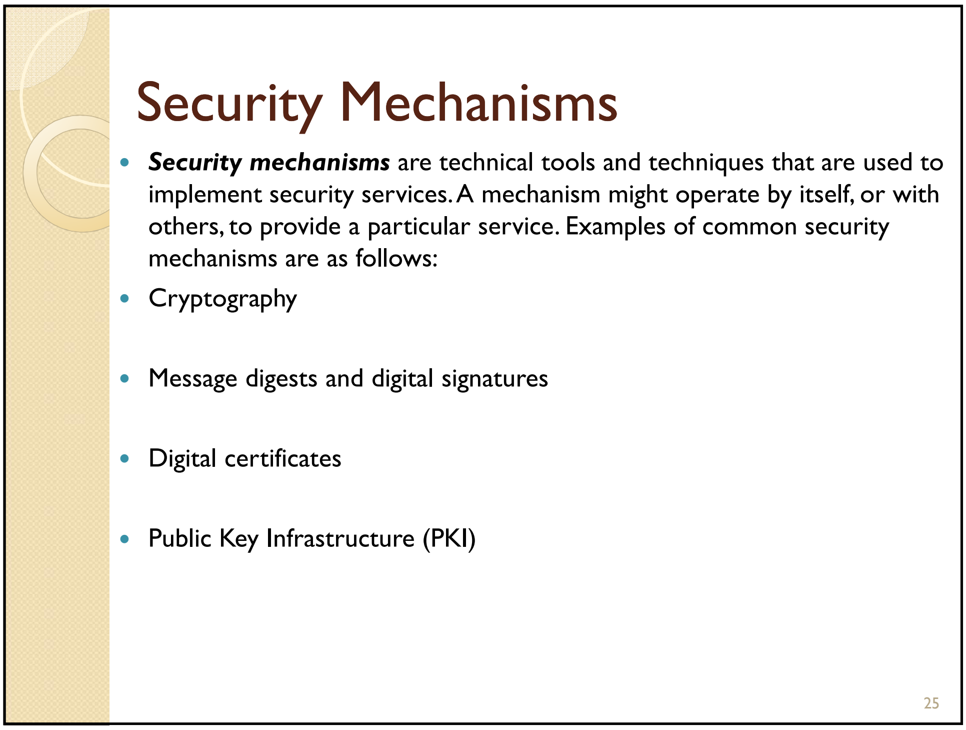
- **(5) Non-Repudiation** *(**Non-repudiation** is the assurance that someone cannot deny Something)*
  - protection against denial by one of the parties in a communication
  - **Origin non-repudiation**
    - proof that the message was sent by the specified party
  - **Destination non-repudiation**
    - proof that the message was received by the specified party

Non-repudiation refers to the ability to ensure that a party to a contract or a communication cannot deny the authenticity of their signature on a document or the sending of a message that they originated.



Relationships

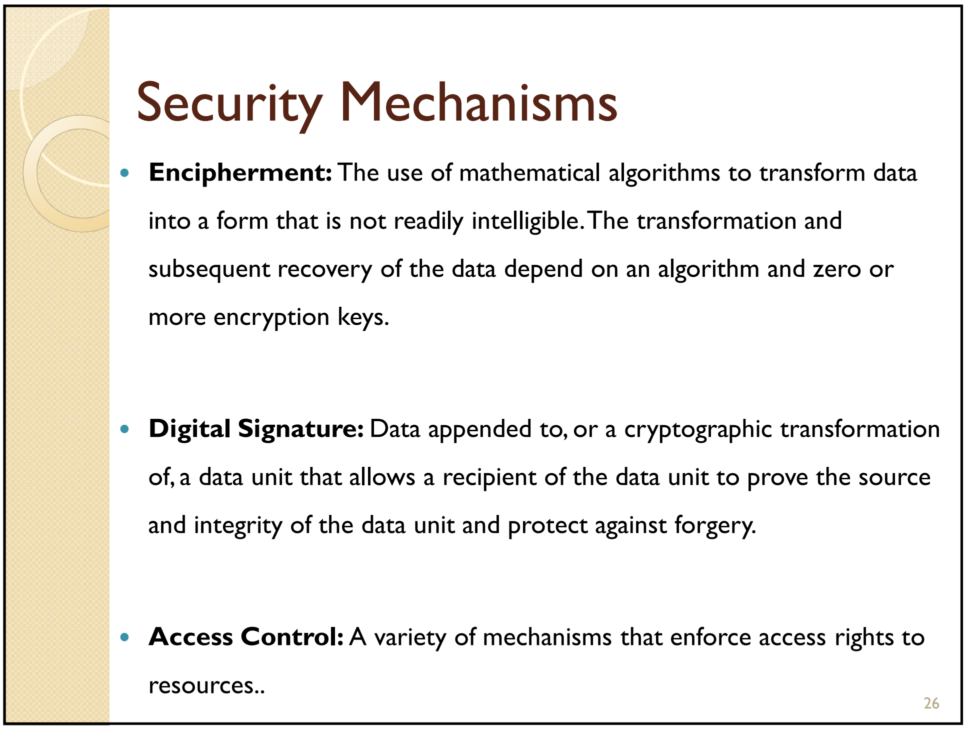
- among integrity, data-origin authentication and non-repudiation



Security Mechanisms

- ***Security mechanisms*** are technical tools and techniques that are used to implement security services. A mechanism might operate by itself, or with others, to provide a particular service. Examples of common security mechanisms are as follows:
- Cryptography
- Message digests and digital signatures
- Digital certificates
- Public Key Infrastructure (PKI)

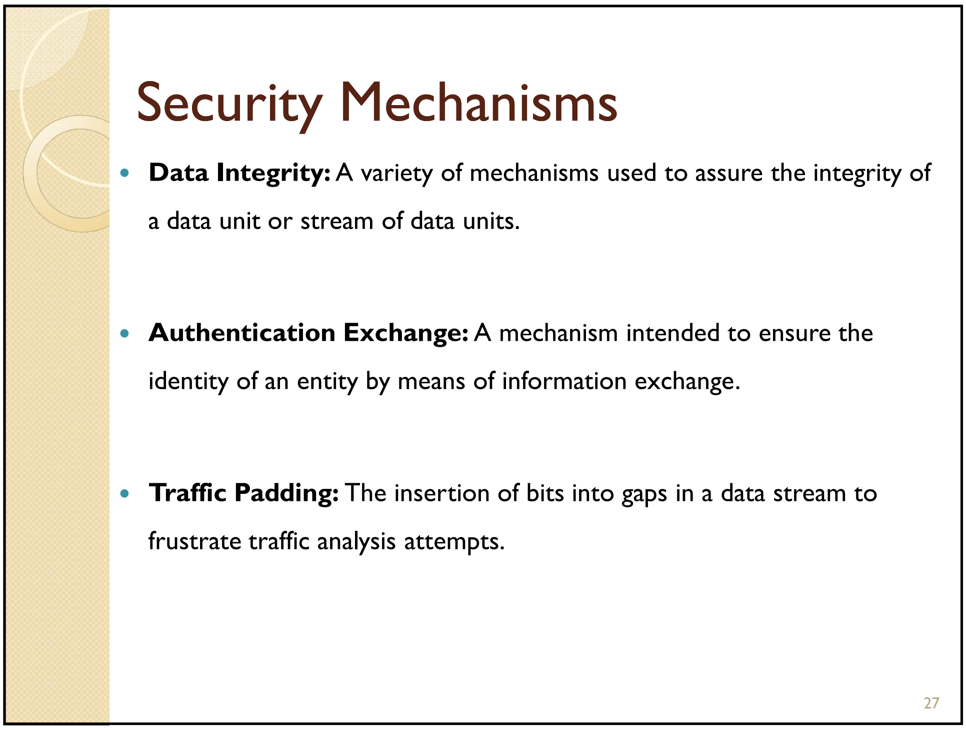
25



Security Mechanisms

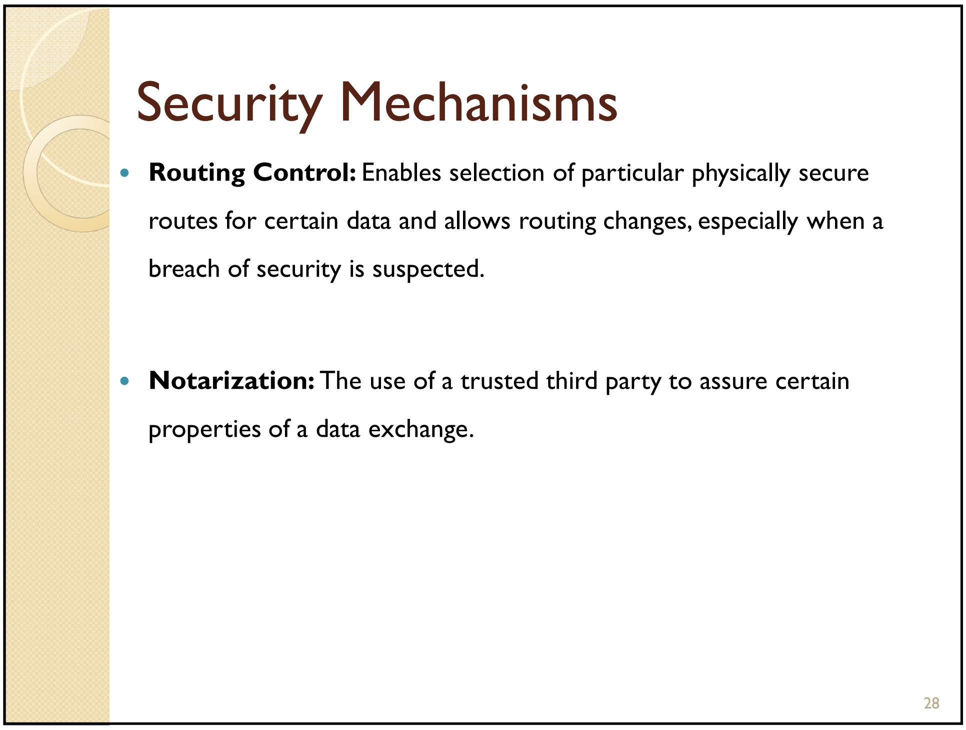
- **Encipherment:** The use of mathematical algorithms to transform data into a form that is not readily intelligible. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.
- **Digital Signature:** Data appended to, or a cryptographic transformation 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.
- **Access Control:** A variety of mechanisms that enforce access rights to resources..

26



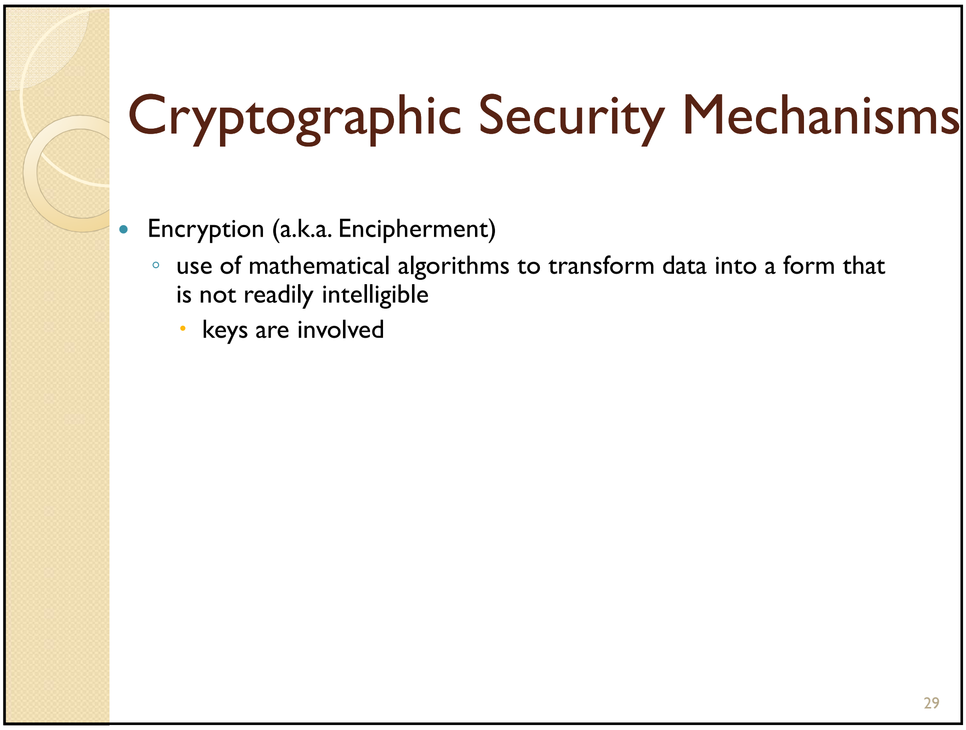
Security Mechanisms

- **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.



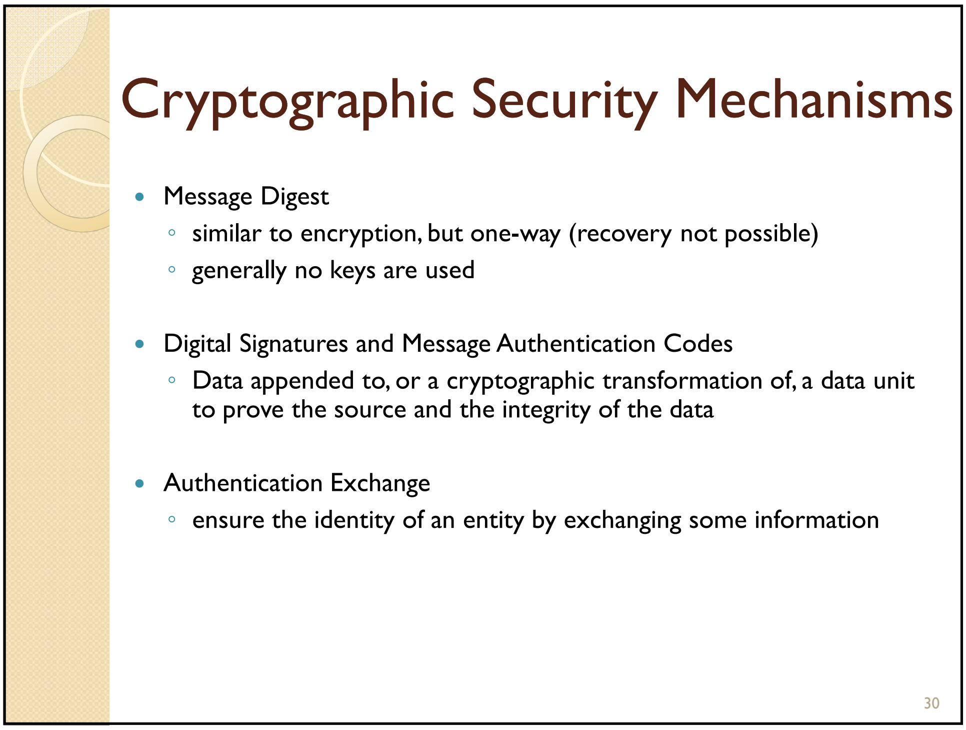
Security Mechanisms

- **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



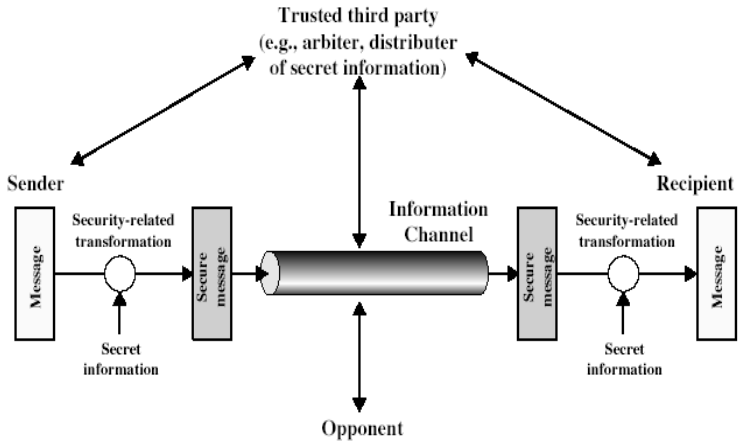
Cryptographic Security Mechanisms

- 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

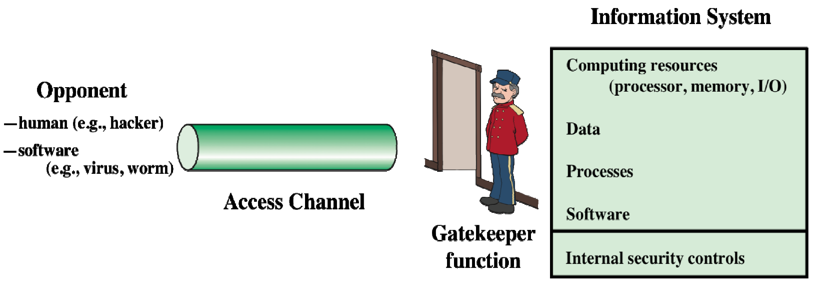
A General Model for Network Security



Model for Network Security

- using this model requires us to:
  - design a suitable algorithm for the security transformation
  - generate the secret information (keys) used by the algorithm
  - develop methods to distribute and share the secret information
  - specify a protocol enabling the principals to use the transformation and secret information for a security service

Model for Network Access Security



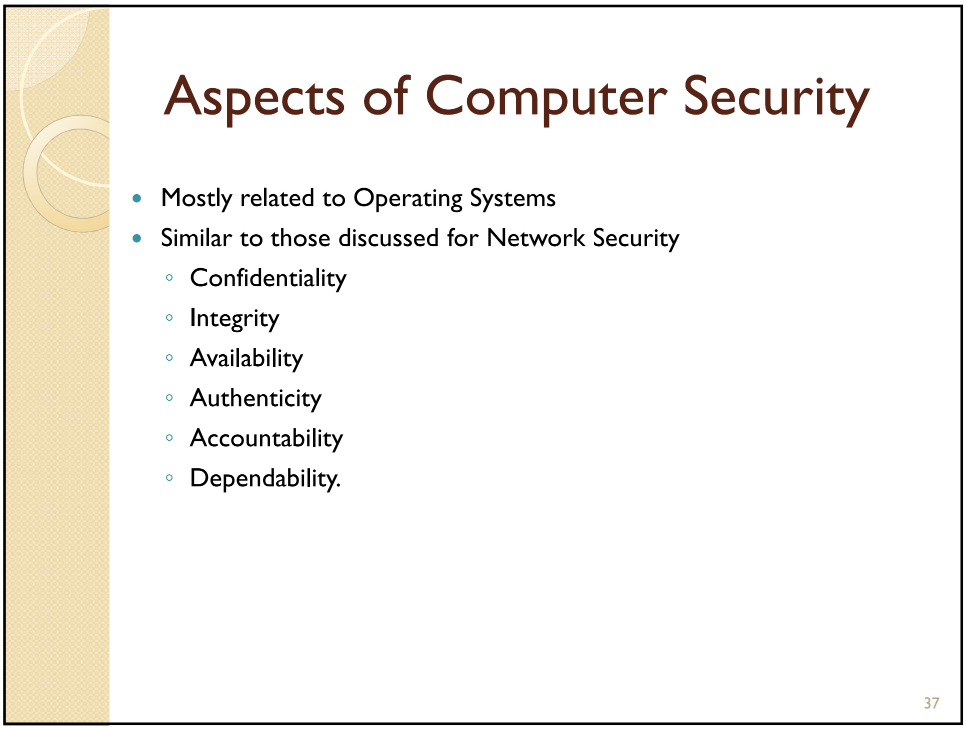
Network Access Security Model

Model for Network Access Security

- using this model requires us to:
    - select appropriate gatekeeper functions to identify users and processes and ensure only authorized users and processes access designated information or resources
    - Internal control to monitor the activity and analyze information to detect unwanted intruders

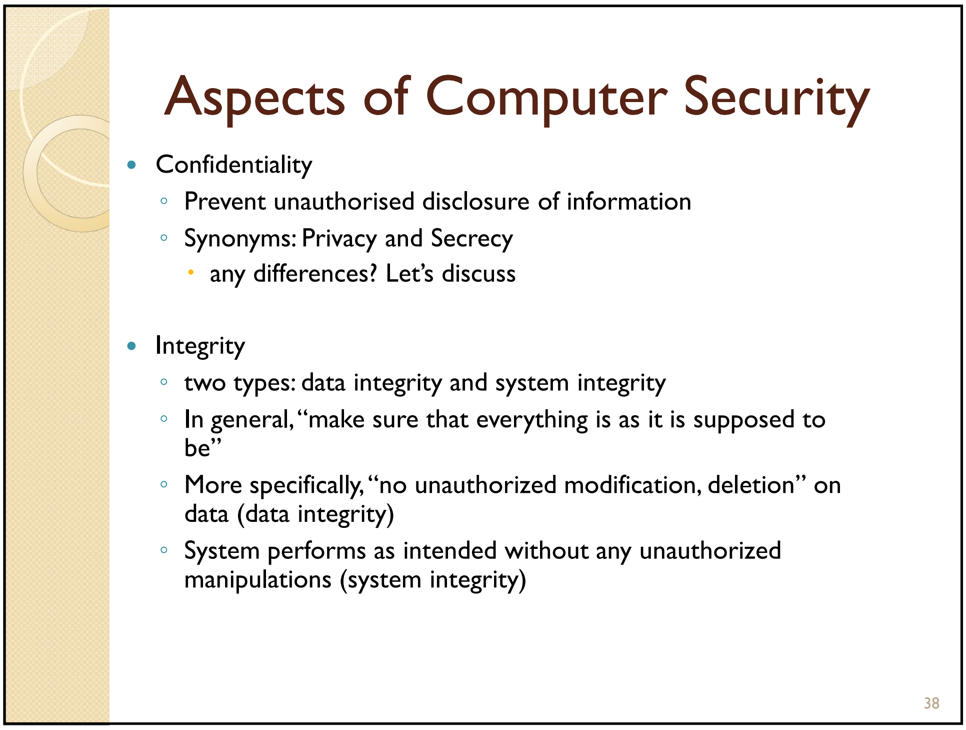
More on Computer System Security

- 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



Aspects of Computer Security

- Mostly related to Operating Systems
- Similar to those discussed for Network Security
  - Confidentiality
  - Integrity
  - Availability
  - Authenticity
  - Accountability
  - Dependability.



Aspects of Computer Security

- Confidentiality
  - Prevent unauthorised disclosure of information
  - Synonyms: Privacy and Secrecy
    - any differences? Let’s discuss

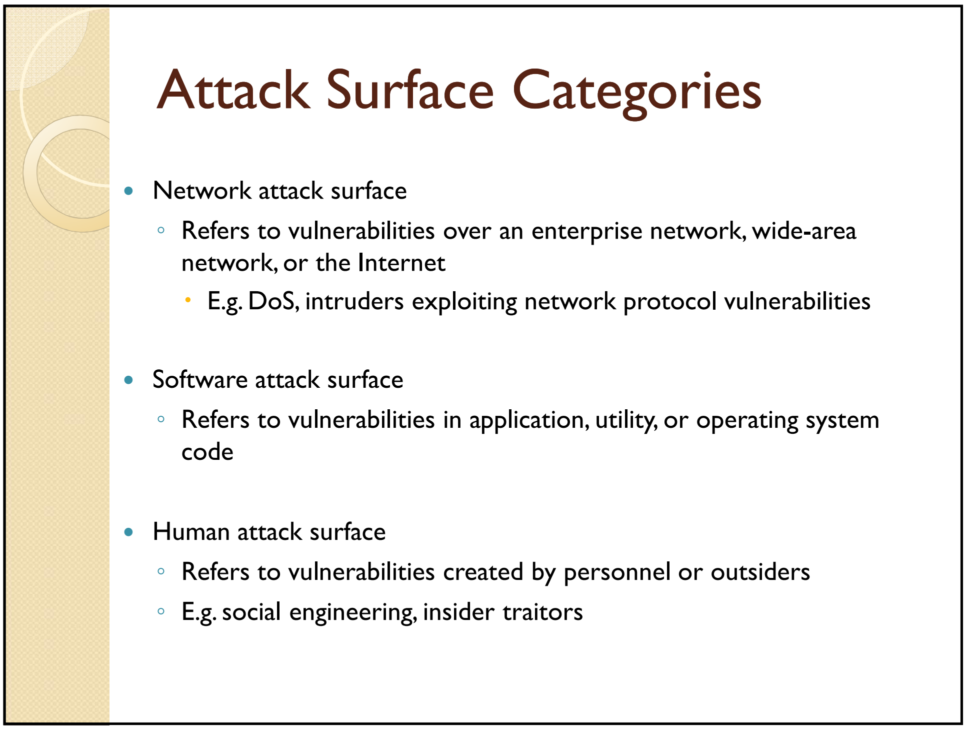
- Integrity
  - two types: data integrity and system integrity
  - In general, “make sure that everything is as it is supposed to be”
  - More specifically, “no unauthorized modification, deletion” on data (data integrity)
  - System performs as intended without any unauthorized manipulations (system integrity)

Aspects of Computer Security

- Availability
  - services should be accessible when needed and without extra delay
- Accountability
  - audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party
  - How can we do that?
    - Users have to be **identified** and **authenticated** to have a basis for access control decisions and to find out responsible party in case of a violation.
    - The security system keeps an **audit log (audit trail)** of security relevant events to detect and investigate intrusions.
- Dependability
  - Can we trust the system as a whole?

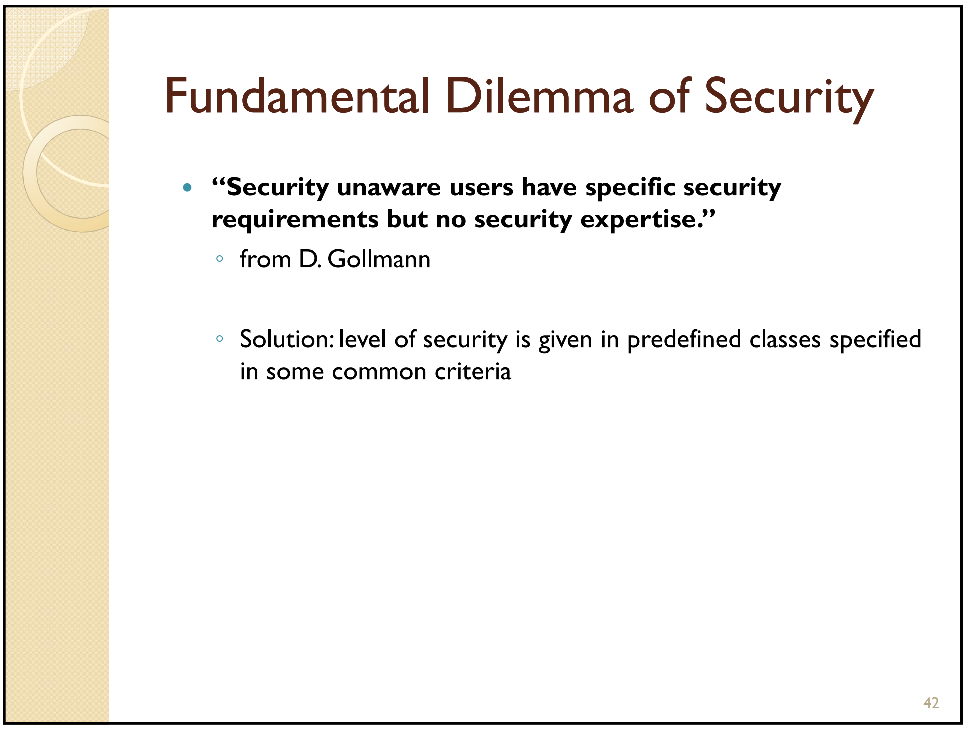
Attack Surfaces

- 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



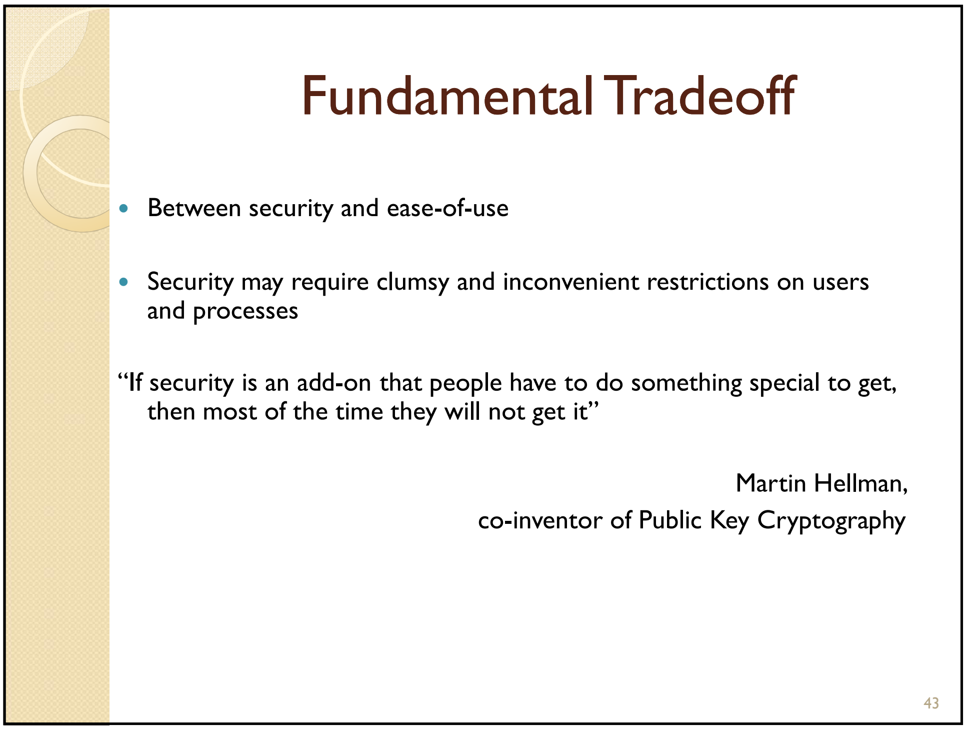
Attack Surface Categories

- 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



Fundamental Dilemma of Security

- **"Security unaware users have specific security requirements but no security expertise."**
  - from D. Gollmann
  - Solution: level of security is given in predefined classes specified in some common criteria

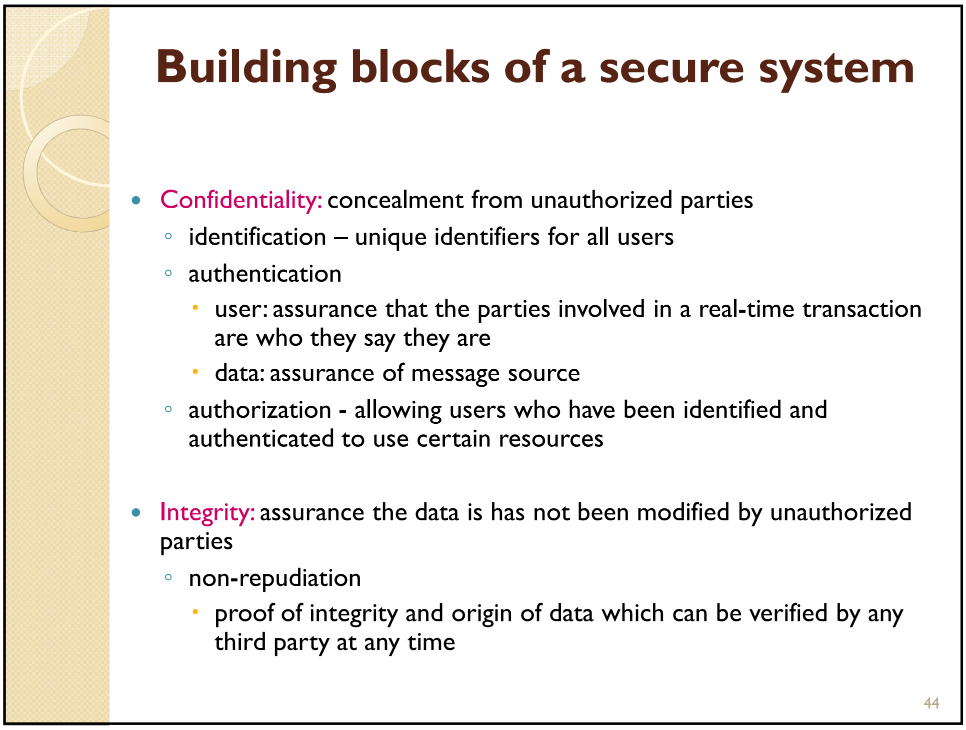


Fundamental Tradeoff

- Between security and ease-of-use
- Security may require clumsy and inconvenient restrictions on users and processes

"If security is an add-on that people have to do something special to get, then most of the time they will not get it"

Martin Hellman,
co-inventor of Public Key Cryptography



Building blocks of a secure system

- Confidentiality: concealment from unauthorized parties
  - identification – unique identifiers for all users
  - authentication
    - user: assurance that the parties involved in a real-time transaction are who they say they are
    - data: assurance of message source
  - authorization - allowing users who have been identified and authenticated to use certain resources
- Integrity: assurance the data is has not been modified by unauthorized parties
  - non-repudiation
    - proof of integrity and origin of data which can be verified by any third party at any time

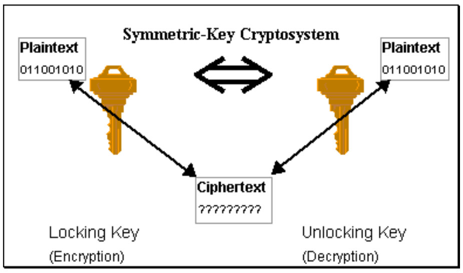
Completing the security process

- Confidentiality + integrity → system security
- However, it is not enough for system to be secure
- System must also be available
  - must allow guaranteed, efficient and continuous use of information
  - security measures should not prohibitively slow down or crash system or make it difficult to use
    - what good is a secure system if you can't use it?
- Cryptographic systems
  - high level of security and flexibility
  - can potentially provide all objectives of information security: confidentiality, integrity, and availability

Symmetric and public key cryptosystems

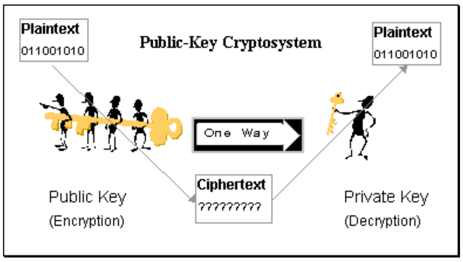
Symmetric-key cryptosystem

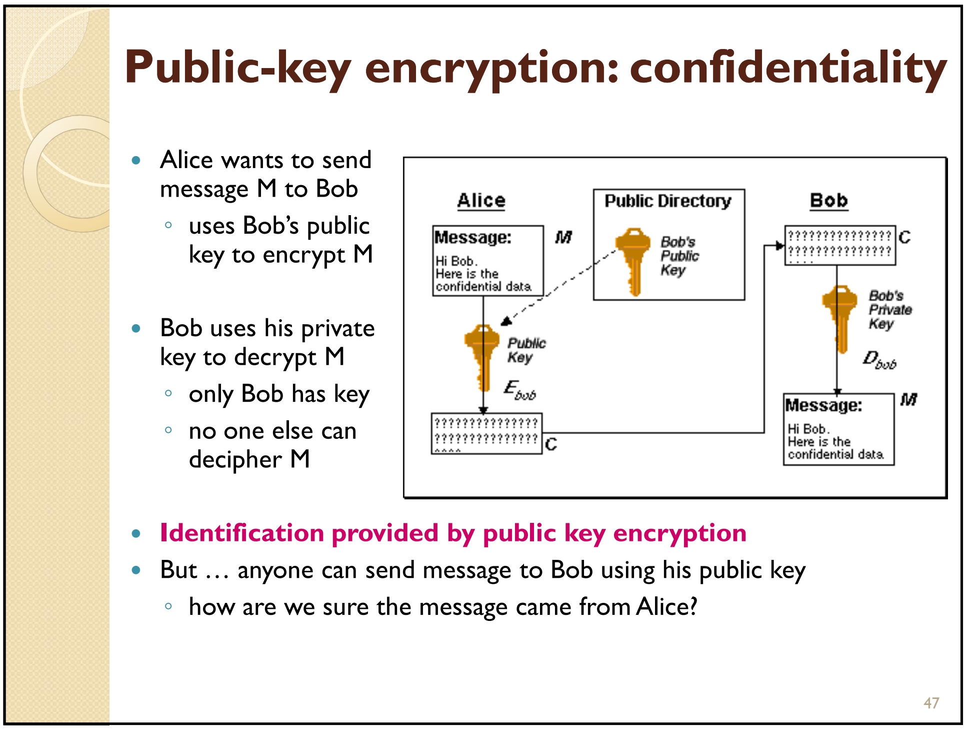
- same key is used for encryption and decryption
- system with 1000 users requires 499,500 keys
  - each pair of users requires a different key



Public-key cryptosystem

- separate keys for encryption and decryption
- system with 1000 users requires 2000 keys
  - each individual user has
  - exactly two keys



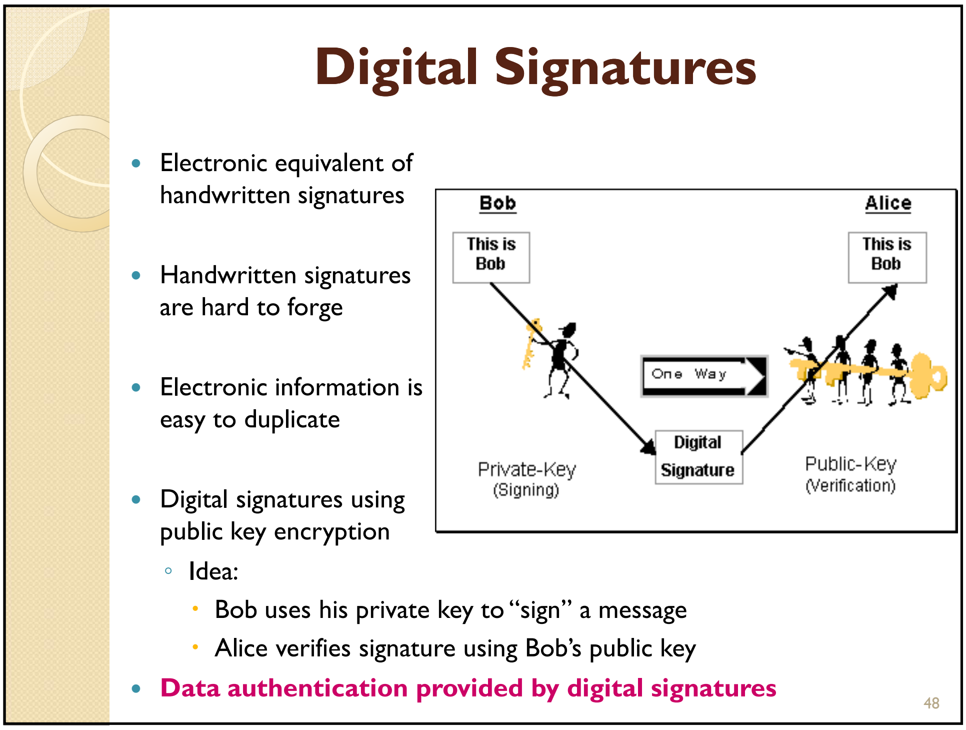


Public-key encryption: confidentiality

- Alice wants to send message M to Bob
  - uses Bob's public key to encrypt M
- Bob uses his private key to decrypt M
  - only Bob has key
  - no one else can decipher M

Alice
Public Directory
Bob
Message:
M
Hi Bob.
Here is the confidential data
Bob's Public Key
Public Key
E_{bob}
???????????????
???????????????
C
Bob's Private Key
D_{bob}
Message:
M
Hi Bob.
Here is the confidential data

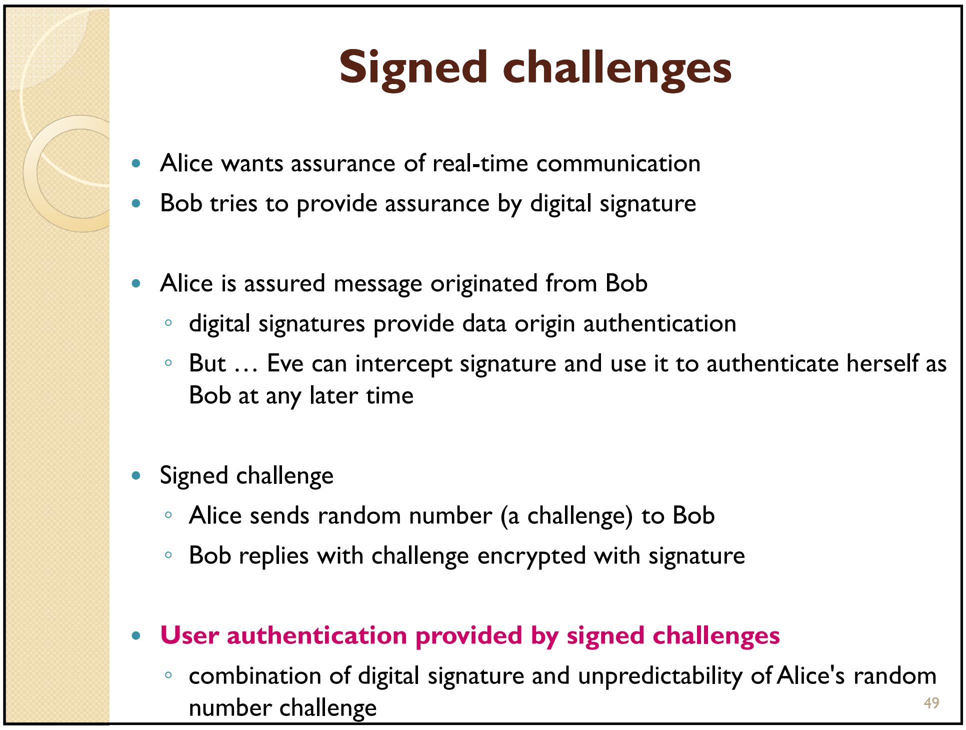
- **Identification provided by public key encryption**
- But … anyone can send message to Bob using his public key
  - how are we sure the message came from Alice?



Digital Signatures

- Electronic equivalent of handwritten signatures
- Handwritten signatures are hard to forge
- Electronic information is easy to duplicate
- Digital signatures using public key encryption
  - Idea:
    - Bob uses his private key to "sign" a message
    - Alice verifies signature using Bob's public key
- **Data authentication provided by digital signatures**

Bob
Alice
This is Bob
This is Bob
One Way
Digital Signature
Private-Key (Signing)
Public-Key (Verification)



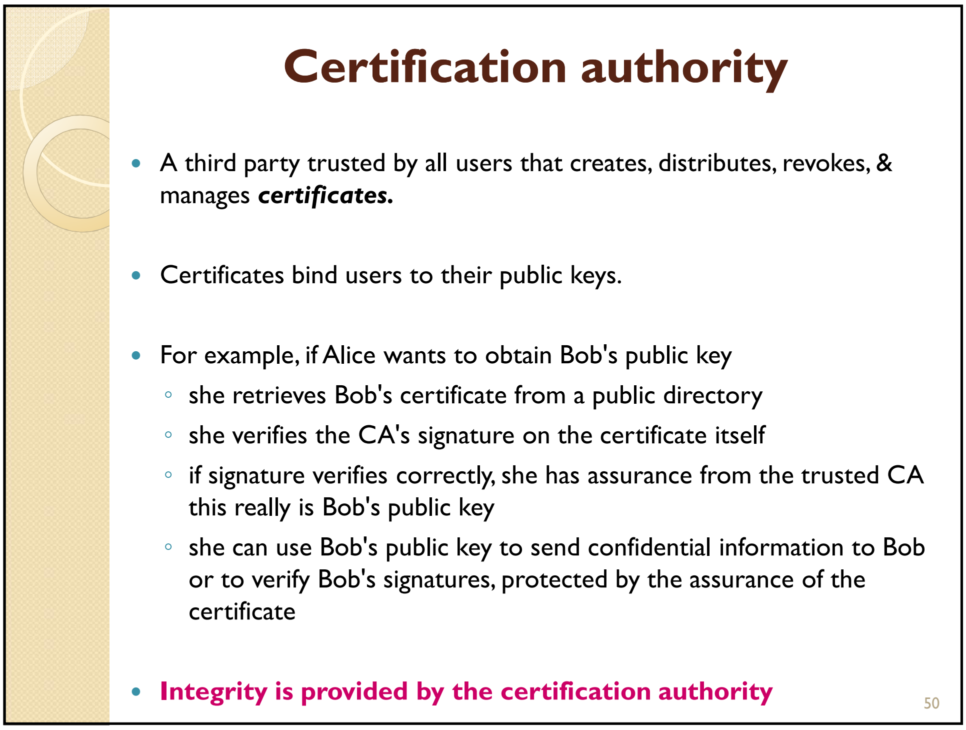
Signed challenges

- Alice wants assurance of real-time communication
- Bob tries to provide assurance by digital signature

- Alice is assured message originated from Bob
  - digital signatures provide data origin authentication
  - But … Eve can intercept signature and use it to authenticate herself as Bob at any later time

- Signed challenge
  - Alice sends random number (a challenge) to Bob
  - Bob replies with challenge encrypted with signature

- **User authentication provided by signed challenges**
  - combination of digital signature and unpredictability of Alice's random number challenge



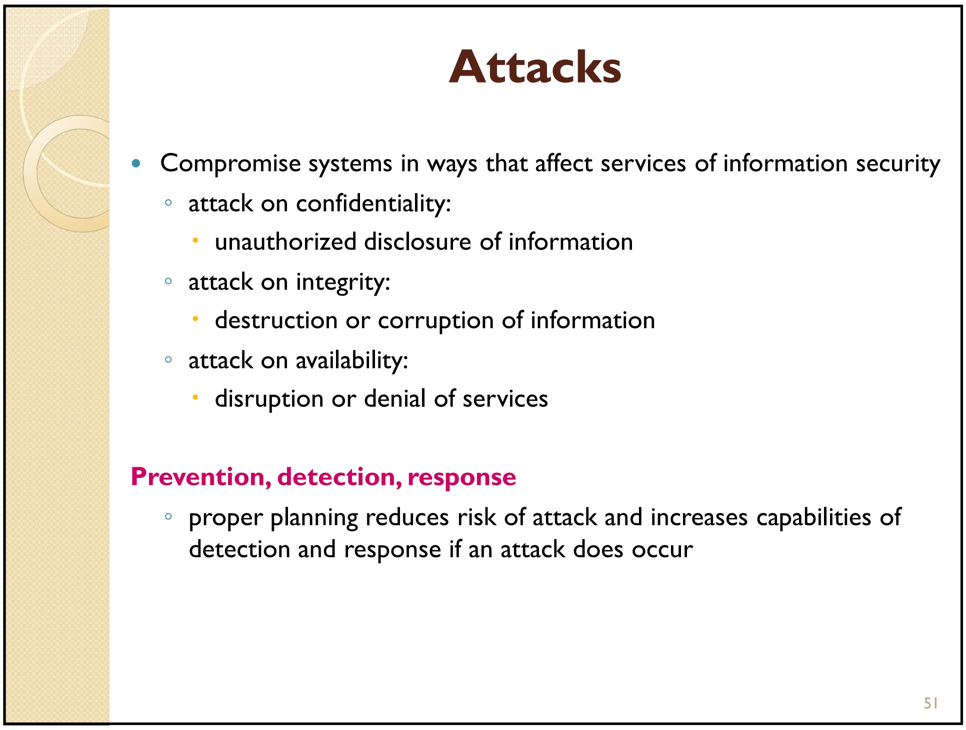
Certification authority

- A third party trusted by all users that creates, distributes, revokes, & manages ***certificates.***

- Certificates bind users to their public keys.

- For example, if Alice wants to obtain Bob's public key
  - she retrieves Bob's certificate from a public directory
  - she verifies the CA's signature on the certificate itself
  - if signature verifies correctly, she has assurance from the trusted CA this really is Bob's public key
  - she can use Bob's public key to send confidential information to Bob or to verify Bob's signatures, protected by the assurance of the certificate

- **Integrity is provided by the certification authority**

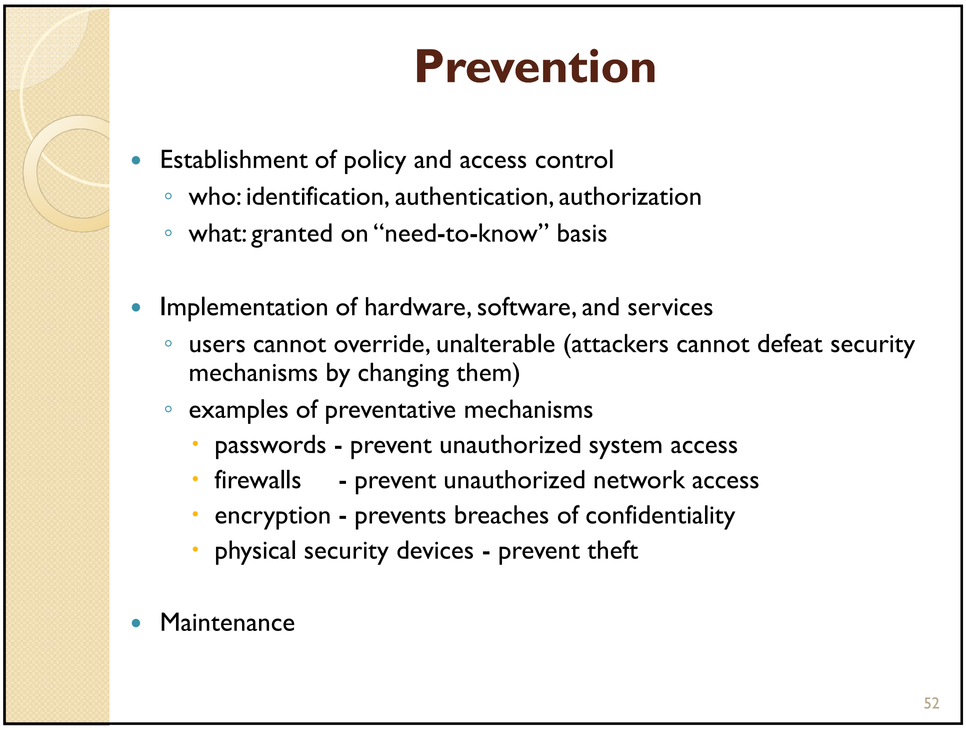


Attacks

- Compromise systems in ways that affect services of information security
  - attack on confidentiality:
    - unauthorized disclosure of information
  - attack on integrity:
    - destruction or corruption of information
  - attack on availability:
    - disruption or denial of services

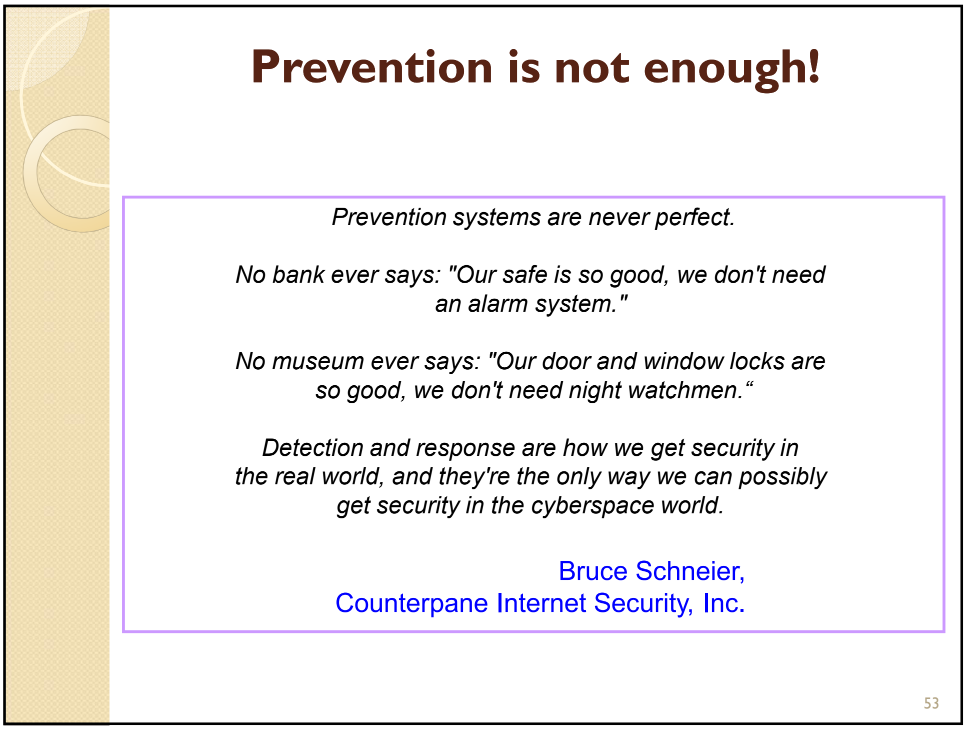
Prevention, detection, response

- proper planning reduces risk of attack and increases capabilities of detection and response if an attack does occur



Prevention

- Establishment of policy and access control
  - who: identification, authentication, authorization
  - what: granted on “need-to-know” basis
- Implementation of hardware, software, and services
  - users cannot override, unalterable (attackers cannot defeat security mechanisms by changing them)
  - examples of preventative mechanisms
    - passwords - prevent unauthorized system access
    - firewalls - prevent unauthorized network access
    - encryption - prevents breaches of confidentiality
    - physical security devices - prevent theft
- Maintenance



Prevention is not enough!

Prevention systems are never perfect.

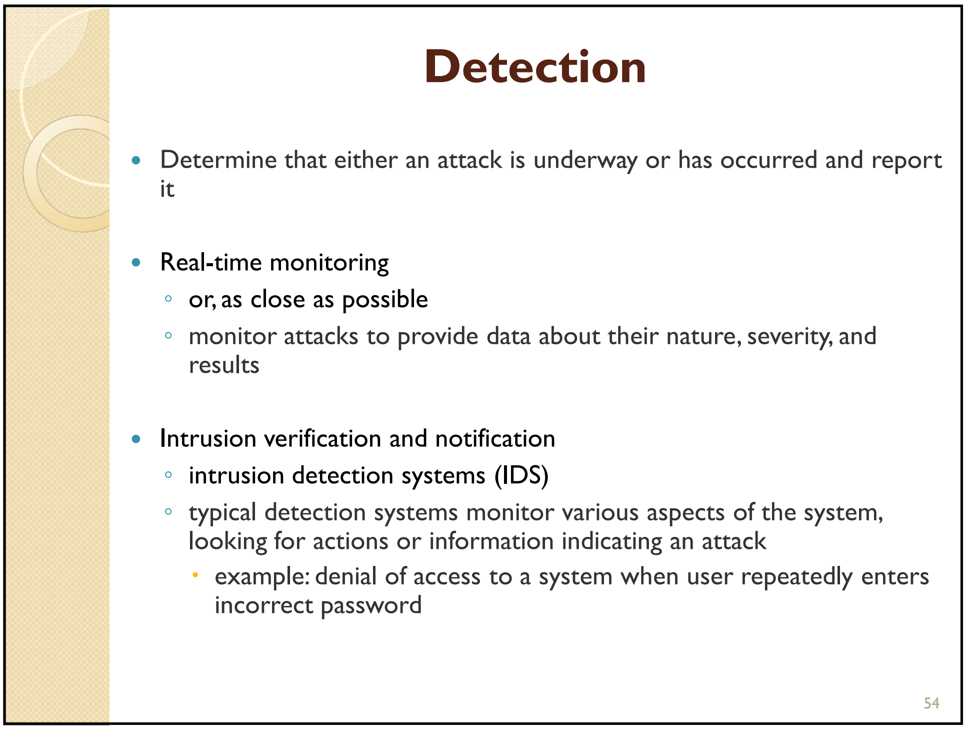
No bank ever says: "Our safe is so good, we don't need an alarm system."

No museum ever says: "Our door and window locks are so good, we don't need night watchmen.“

Detection and response are how we get security in the real world, and they're the only way we can possibly get security in the cyberspace world.

Bruce Schneier,
Counterpane Internet Security, Inc.

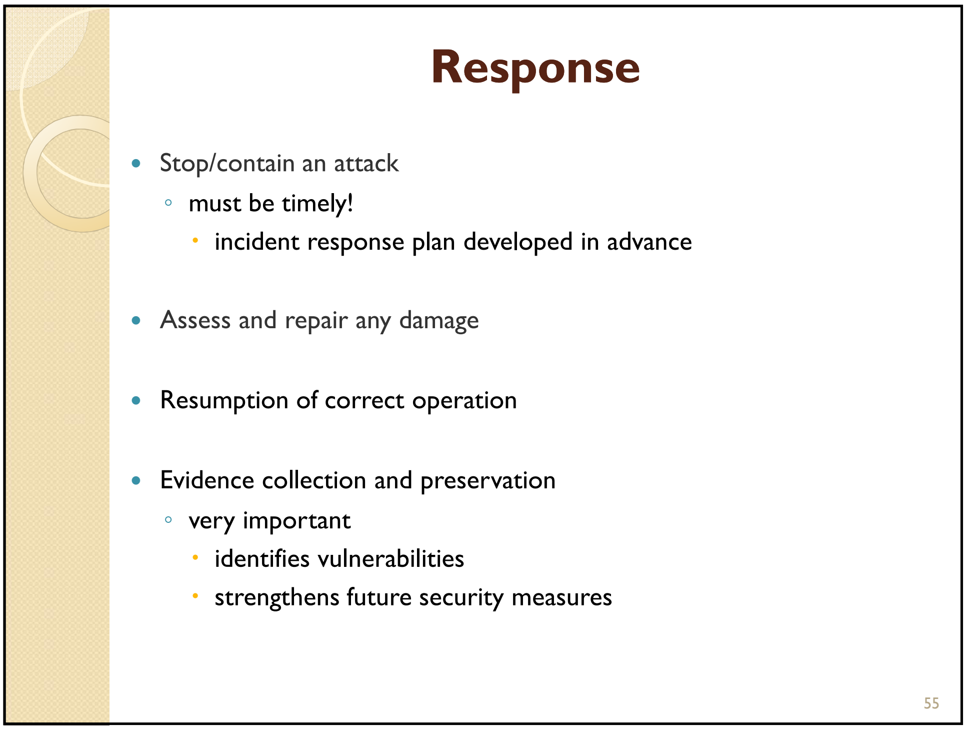
53



Detection

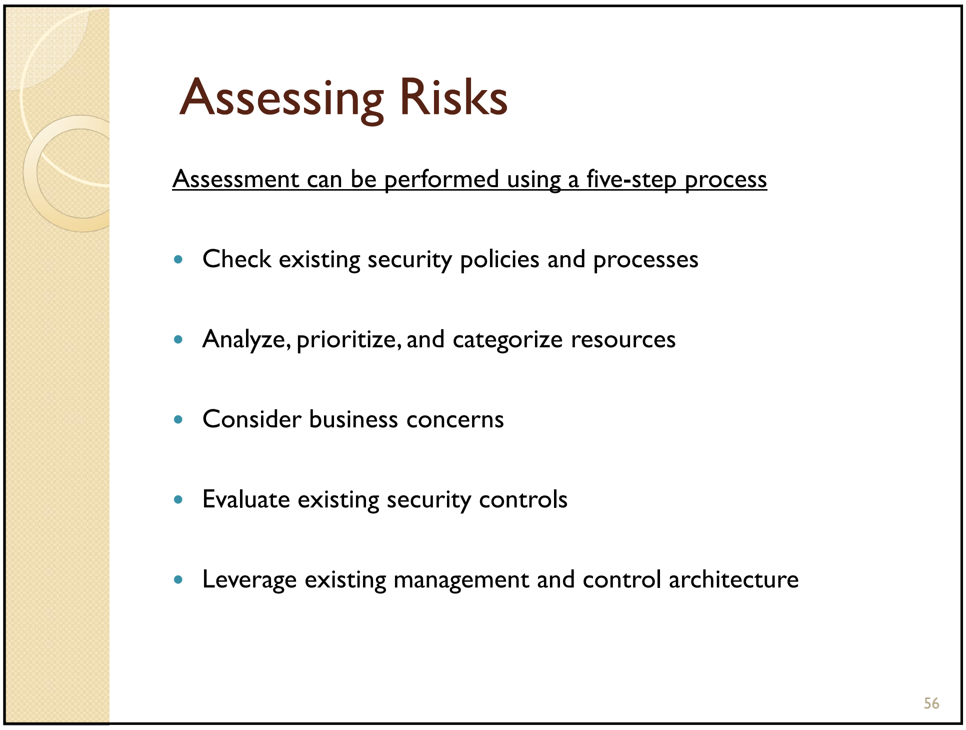
- Determine that either an attack is underway or has occurred and report it
- Real-time monitoring
  - or, as close as possible
  - monitor attacks to provide data about their nature, severity, and results
- Intrusion verification and notification
  - intrusion detection systems (IDS)
  - typical detection systems monitor various aspects of the system, looking for actions or information indicating an attack
    - example: denial of access to a system when user repeatedly enters incorrect password

54



Response

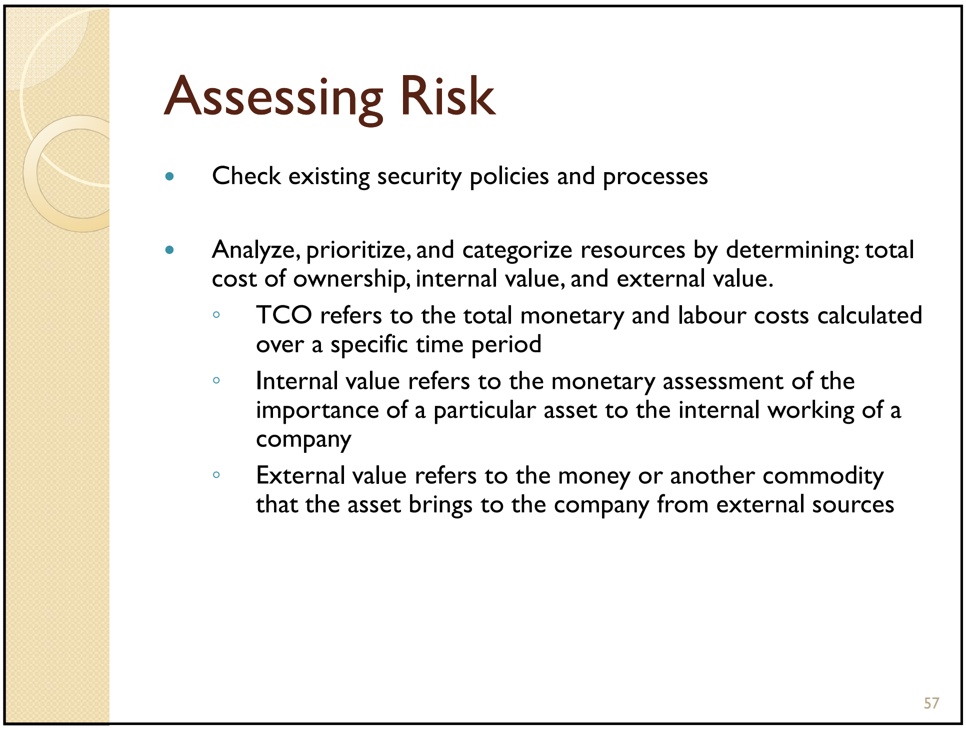
- Stop/contain an attack
  - must be timely!
    - incident response plan developed in advance
- Assess and repair any damage
- Resumption of correct operation
- Evidence collection and preservation
  - very important
    - identifies vulnerabilities
    - strengthens future security measures



Assessing Risks

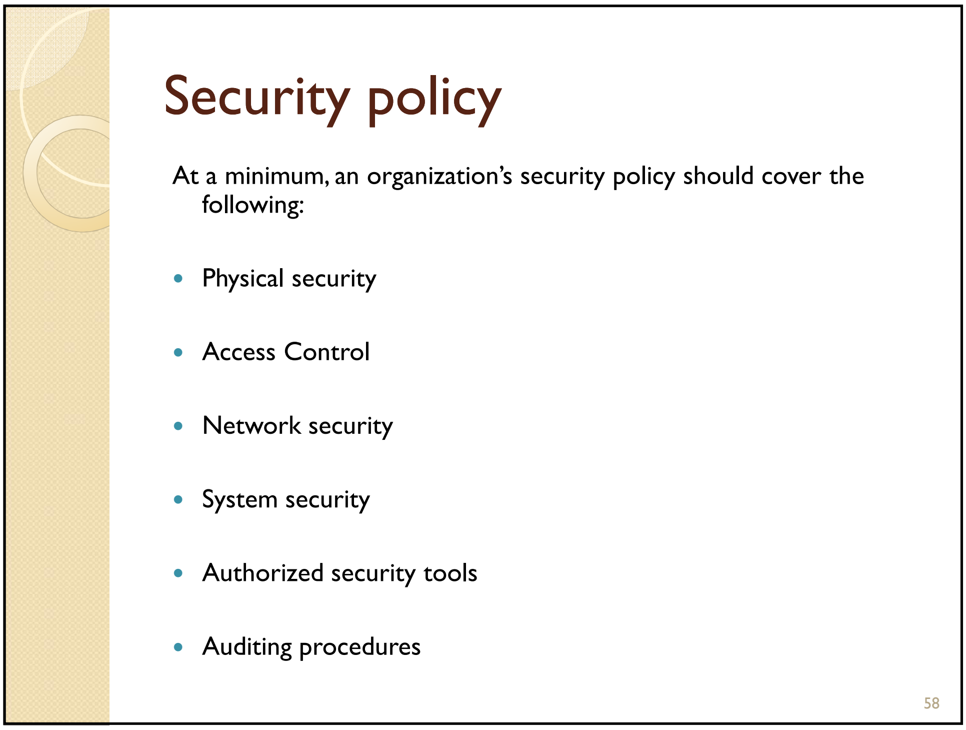
Assessment can be performed using a five-step process

- Check existing security policies and processes
- Analyze, prioritize, and categorize resources
- Consider business concerns
- Evaluate existing security controls
- Leverage existing management and control architecture



Assessing Risk

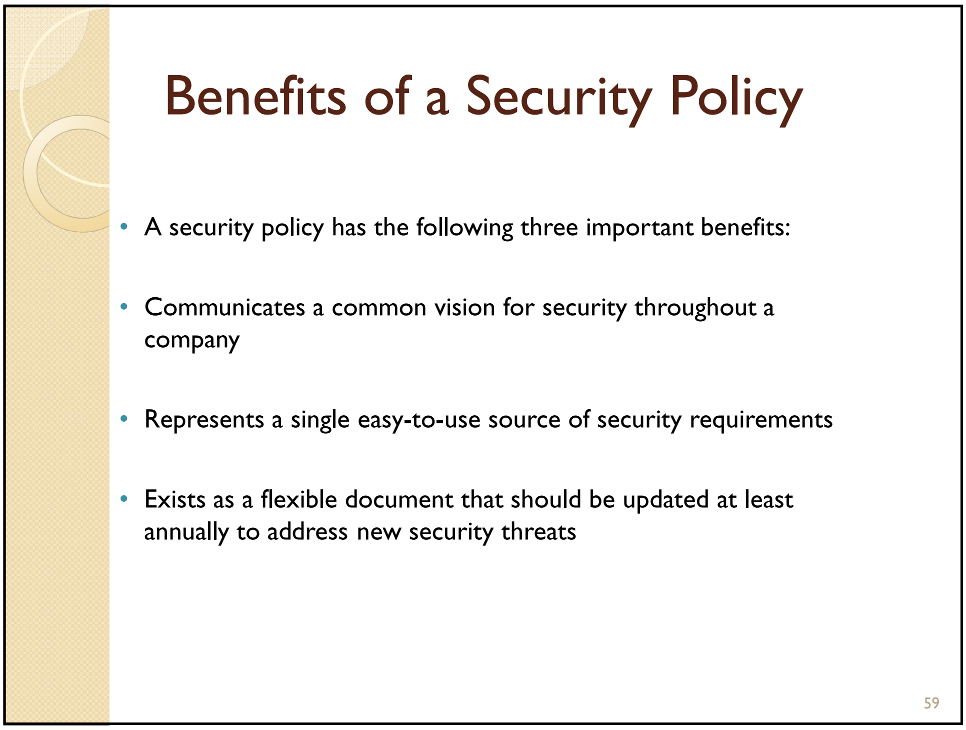
- Check existing security policies and processes
- Analyze, prioritize, and categorize resources by determining: total cost of ownership, internal value, and external value.
  - TCO refers to the total monetary and labour costs calculated over a specific time period
  - Internal value refers to the monetary assessment of the importance of a particular asset to the internal working of a company
  - External value refers to the money or another commodity that the asset brings to the company from external sources



Security policy

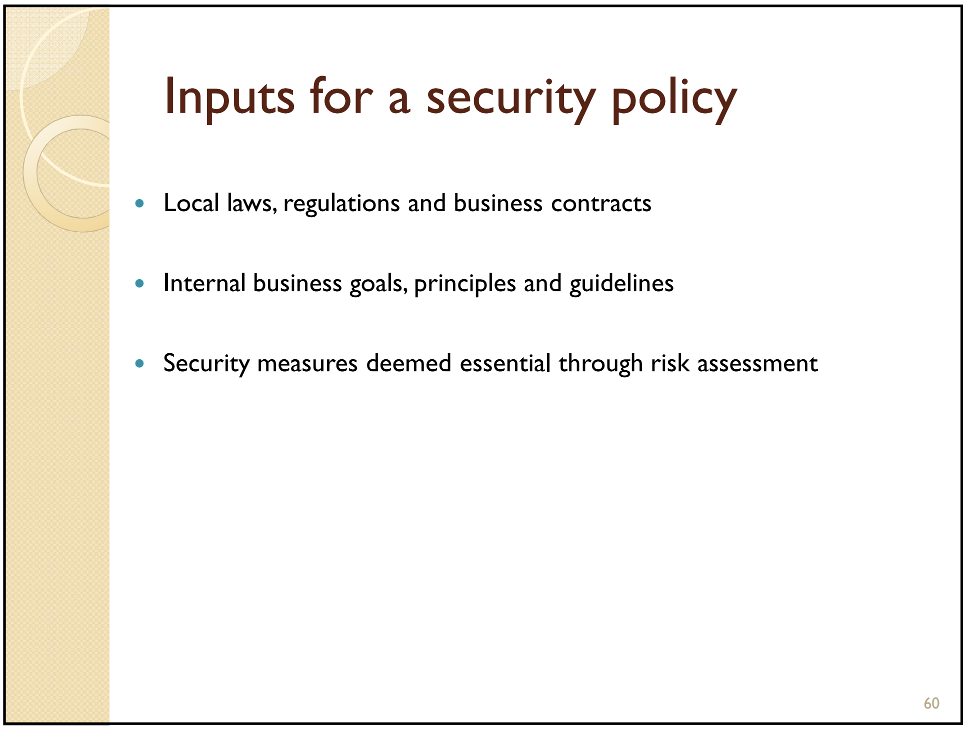
At a minimum, an organization's security policy should cover the following:

- Physical security
- Access Control
- Network security
- System security
- Authorized security tools
- Auditing procedures



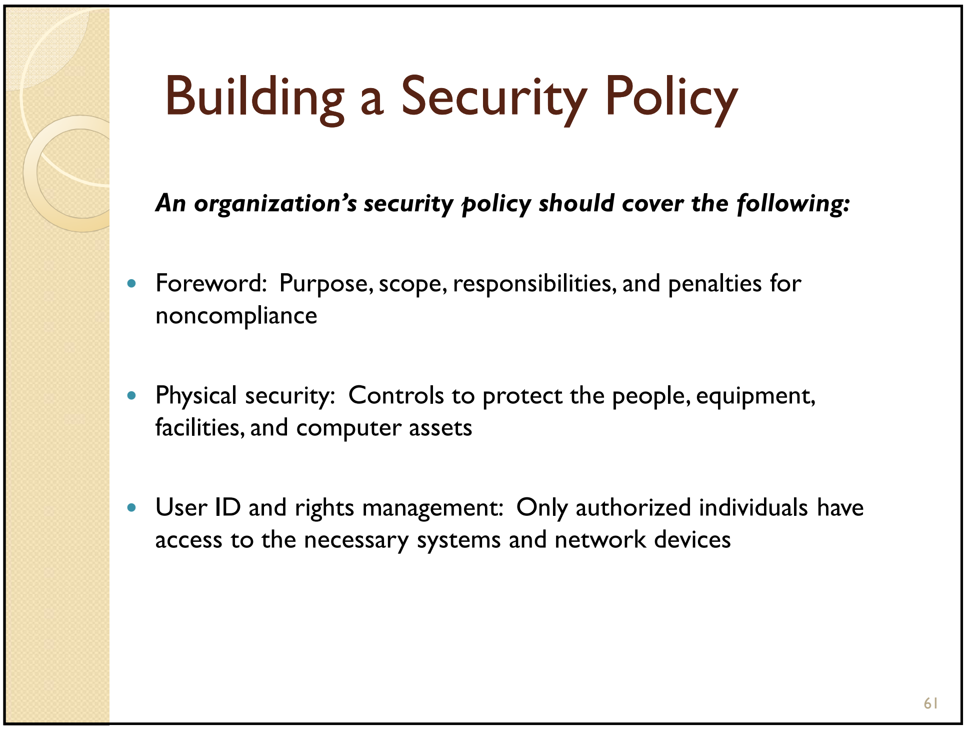
Benefits of a Security Policy

- A security policy has the following three important benefits:
- Communicates a common vision for security throughout a company
- Represents a single easy-to-use source of security requirements
- Exists as a flexible document that should be updated at least annually to address new security threats



Inputs for a security policy

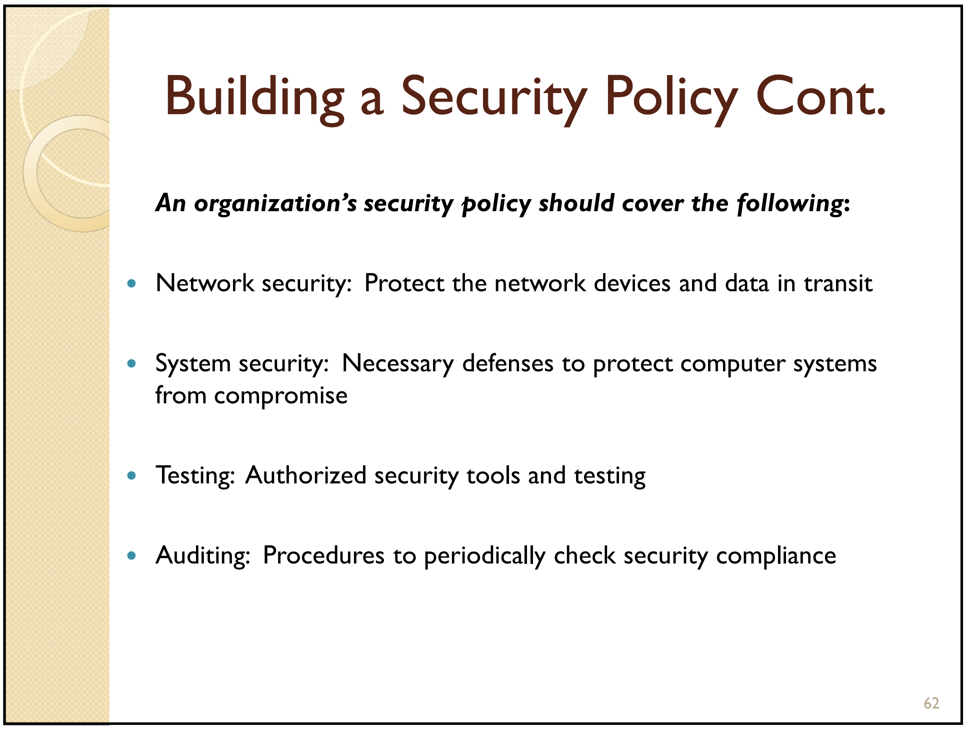
- Local laws, regulations and business contracts
- Internal business goals, principles and guidelines
- Security measures deemed essential through risk assessment



Building a Security Policy

An organization's security policy should cover the following:

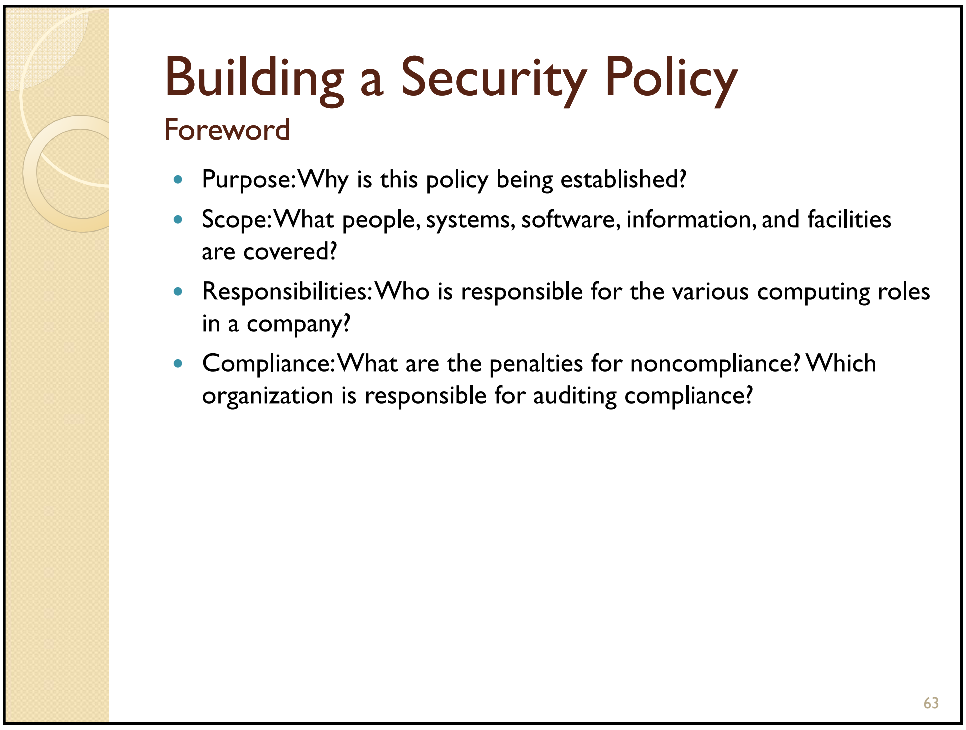
- Foreword: Purpose, scope, responsibilities, and penalties for noncompliance
- Physical security: Controls to protect the people, equipment, facilities, and computer assets
- User ID and rights management: Only authorized individuals have access to the necessary systems and network devices



Building a Security Policy Cont.

An organization's security policy should cover the following:

- Network security: Protect the network devices and data in transit
- System security: Necessary defenses to protect computer systems from compromise
- Testing: Authorized security tools and testing
- Auditing: Procedures to periodically check security compliance

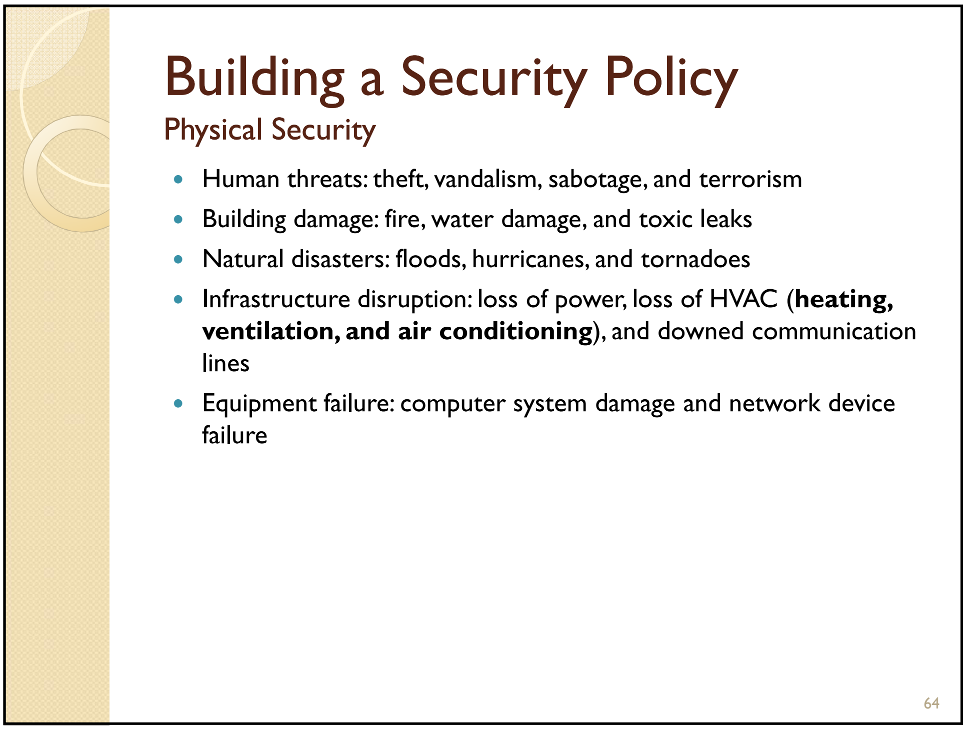


Building a Security Policy

Foreword

- Purpose: Why is this policy being established?
- Scope: What people, systems, software, information, and facilities are covered?
- Responsibilities: Who is responsible for the various computing roles in a company?
- Compliance: What are the penalties for noncompliance? Which organization is responsible for auditing compliance?

63

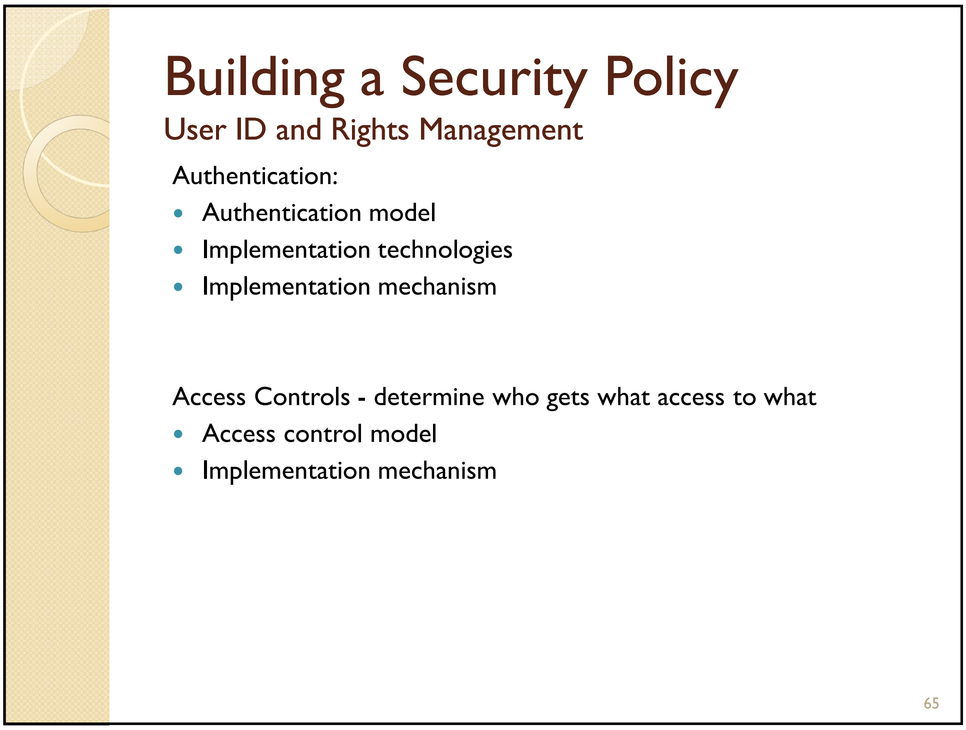


Building a Security Policy

Physical Security

- Human threats: theft, vandalism, sabotage, and terrorism
- Building damage: fire, water damage, and toxic leaks
- Natural disasters: floods, hurricanes, and tornadoes
- Infrastructure disruption: loss of power, loss of HVAC (**heating, ventilation, and air conditioning**), and downed communication lines
- Equipment failure: computer system damage and network device failure

64



Building a Security Policy

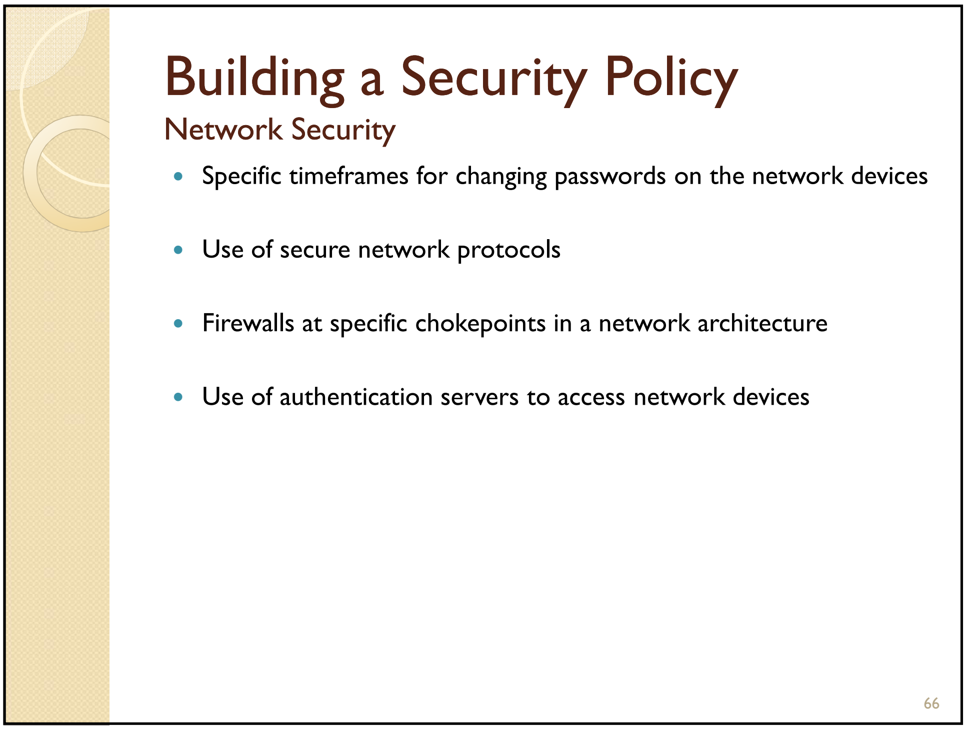
User ID and Rights Management

Authentication:

- Authentication model
- Implementation technologies
- Implementation mechanism

Access Controls - determine who gets what access to what

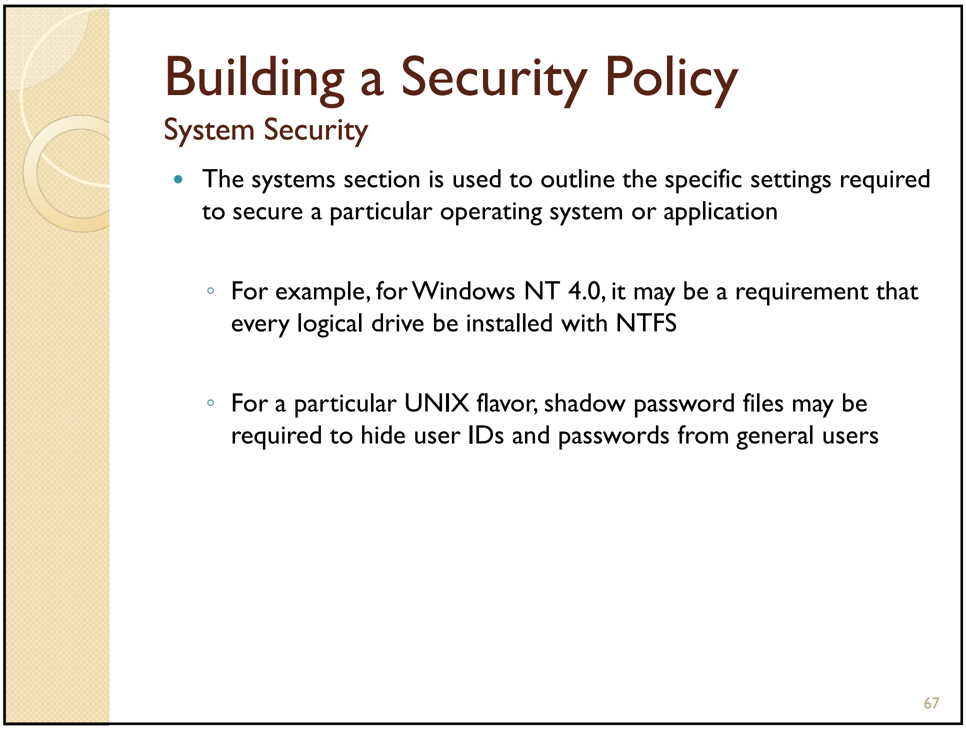
- Access control model
- Implementation mechanism



Building a Security Policy

Network Security

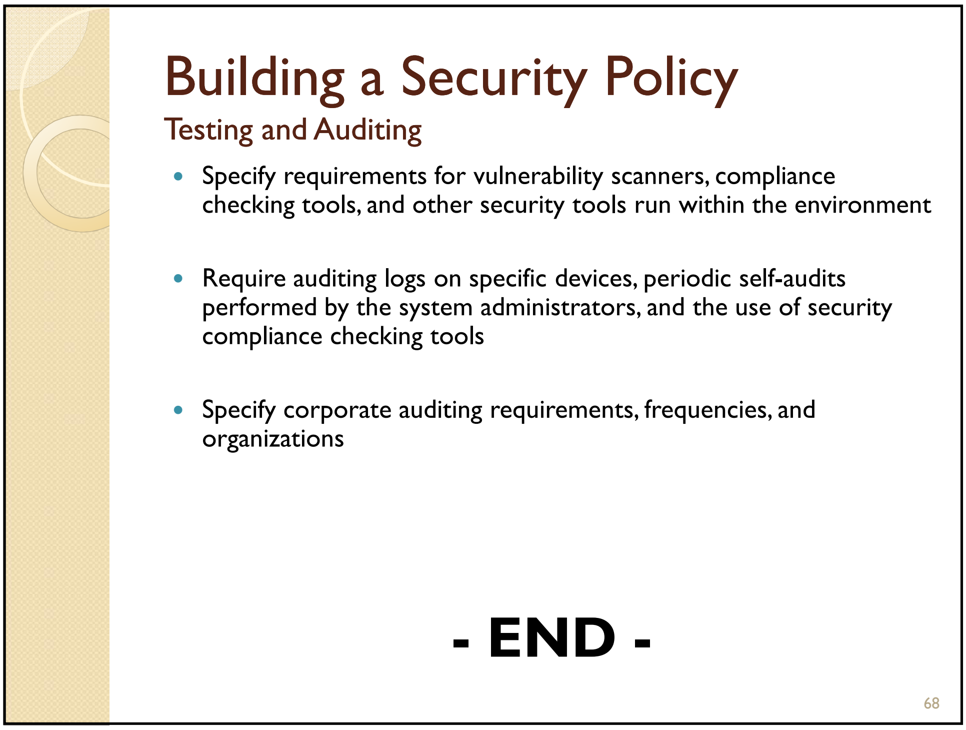
- Specific timeframes for changing passwords on the network devices
- Use of secure network protocols
- Firewalls at specific chokepoints in a network architecture
- Use of authentication servers to access network devices



Building a Security Policy

System Security

- The systems section is used to outline the specific settings required to secure a particular operating system or application
  - For example, for Windows NT 4.0, it may be a requirement that every logical drive be installed with NTFS
  - For a particular UNIX flavor, shadow password files may be required to hide user IDs and passwords from general users



Building a Security Policy

Testing and Auditing

- Specify requirements for vulnerability scanners, compliance checking tools, and other security tools run within the environment
- Require auditing logs on specific devices, periodic self-audits performed by the system administrators, and the use of security compliance checking tools
- Specify corporate auditing requirements, frequencies, and organizations

- END -