



Internet Security

Chapter 1

Information and Network
Security Concepts

Cybersecurity

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyberspace environment and organization and users' assets.

Organization and users' assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyberspace environment.

Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and users' assets against relevant security risks in the cyberspace environment. The general security objectives comprise the following: **availability**; **integrity**, which may include data authenticity and nonrepudiation; and **confidentiality**

Cybersecurity

Information Security

- This term refers to preservation of confidentiality, integrity, and availability of information. In addition, other properties, such as authenticity, accountability, nonrepudiation, and reliability can also be involved

Network Security

- This term refers to protection of networks and their service from unauthorized modification, destruction, or disclosure, and provision of assurance that the network performs its critical functions correctly and there are no harmful side effects

Security Objectives

- The cybersecurity definition introduces three key objectives that are at the heart of information and network security:
 - **Confidentiality:** This term covers two related concepts:
 - **Data confidentiality:** Assures that private or confidential information is not made available or disclosed to unauthorized individuals
 - **Privacy:** Assures that individuals control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

Security Objectives

- **Integrity:** This term covers two related concepts:
 - **Data integrity:** Assures that data and programs are changed only in a specified and authorized manner. This concept also encompasses data authenticity, which means that a digital object is indeed what it claims to be or what it is claimed to be, and nonrepudiation, which is assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information
 - **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

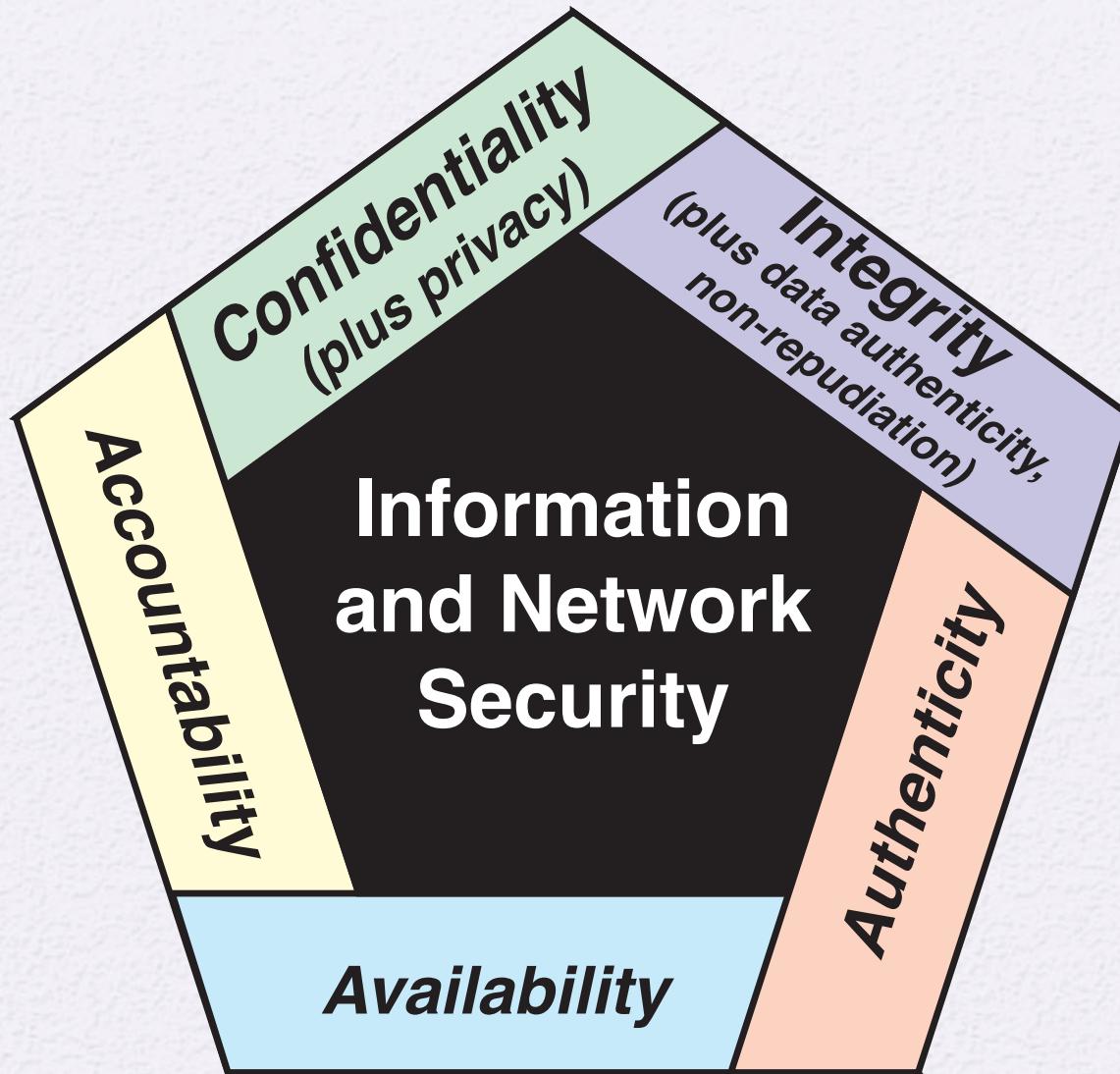


Figure 1.1 Essential Information and Network Security Objectives

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

X.800 OSI Security Architecture

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

Threats and Attacks

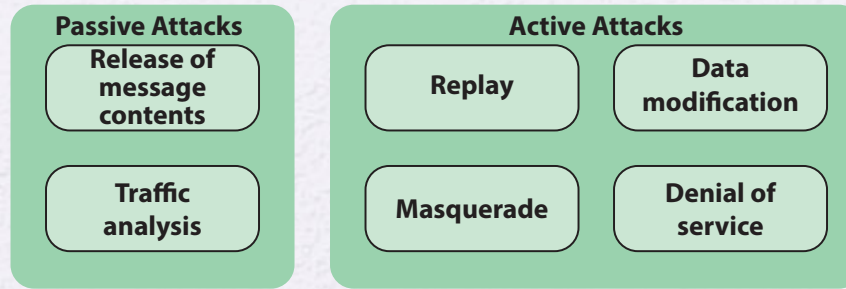


Threat

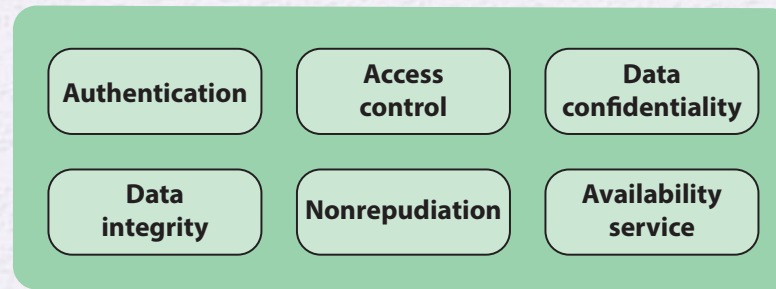
A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

Attack

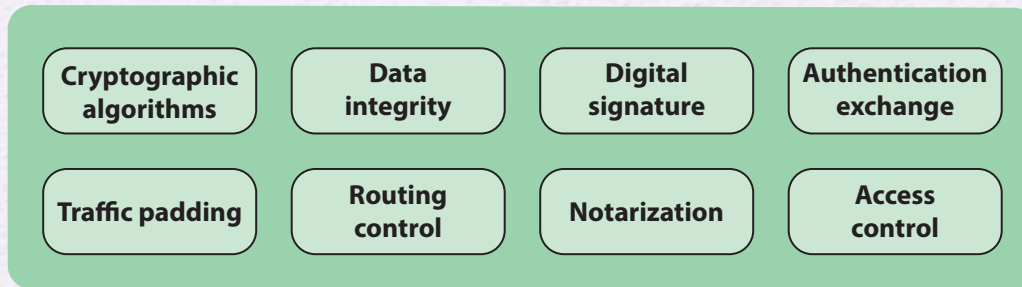
An assault on system security that derives from an intelligent threat; that is, an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security services and violate the security policy of a system.



(a) Attacks



(b) Services



(c) Mechanisms

Figure 1.2 Key Concepts in Security

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

- 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

Active Attacks

- 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



Masquerade

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

Replay

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

Data Modification

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

Denial of service

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

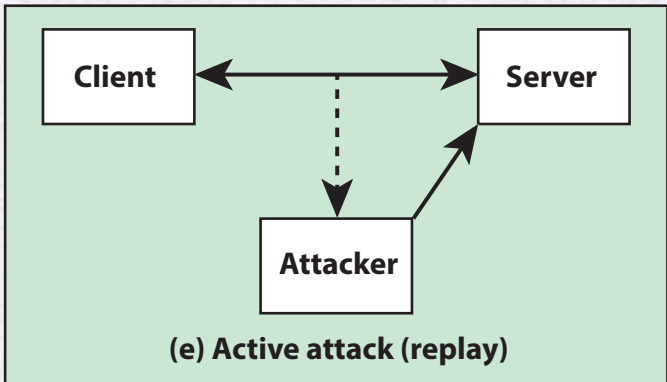
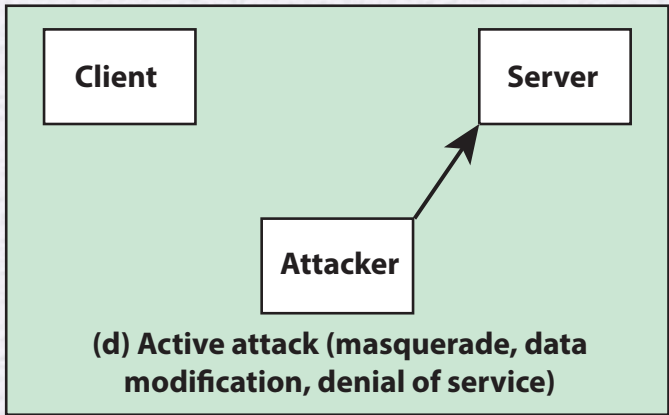
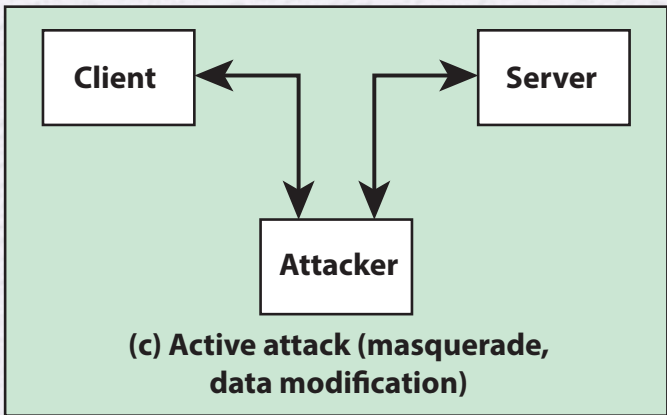
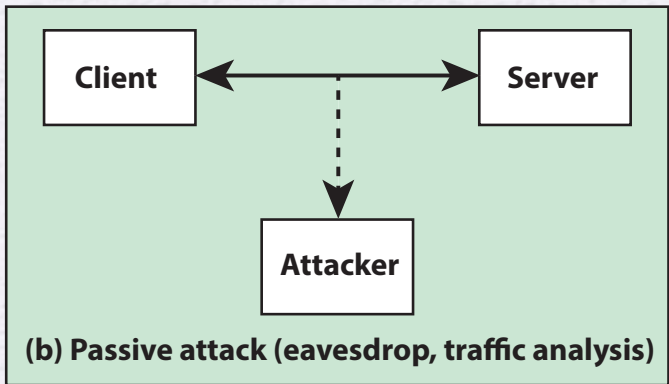
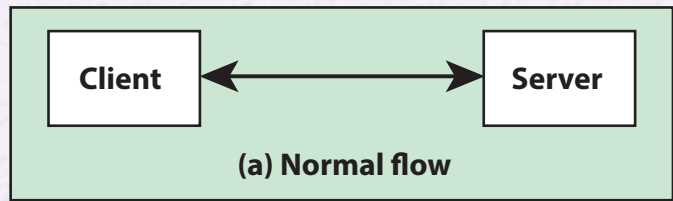


Figure 1.3 Security Attacks

Authentication

- Concerned with assuring that a communication is authentic
 - In the case of a single message, assures the recipient that the message is from the source that it claims to be from
 - In the case of ongoing interaction, assures the two entities are authentic and that the connection is not interfered with in such a way that a third party can masquerade as one of the two legitimate parties

Two specific authentication services are defined in X.800:

- Peer entity authentication
- Data origin authentication

Authentication

- **Peer entity authentication**

- Provides for the corroboration of the identity of a peer entity in an association. Two entities are considered peers if they implement the same protocol in different systems. Peer entity authentication is provided for use at the establishment of, or at times during the data transfer phase of, a connection. It attempts to provide confidence that an entity is not performing either a masquerade or an unauthorized replay of a previous connection

- **Data origin authentication**

- Provides for the corroboration of the source of a data unit. It does not provide protection against the duplication or modification of data units. This type of service supports applications like electronic mail, where there are no ongoing interactions between the communicating entities

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 includes 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, one that deals with a stream of messages, assures that messages are received as sent with no duplication, insertion, modification, reordering, or replays

A connectionless integrity service, one that deals with individual messages without regard to any larger context, 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

- Protects a system to ensure its availability
- This service addresses the security concerns raised by denial-of-service attacks
- It depends on proper management and control of system resources and thus depends on access control service and other security services

Security Mechanisms

- **Cryptographic algorithms:** Reversible cryptographic mechanisms and irreversible cryptographic mechanisms
- **Data integrity:** This category covers a variety of mechanisms used to assure the integrity of a data unit or stream of data units.
- **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.
- **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 or logically 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
- **Access control:** A variety of mechanisms that enforce access rights to resources.

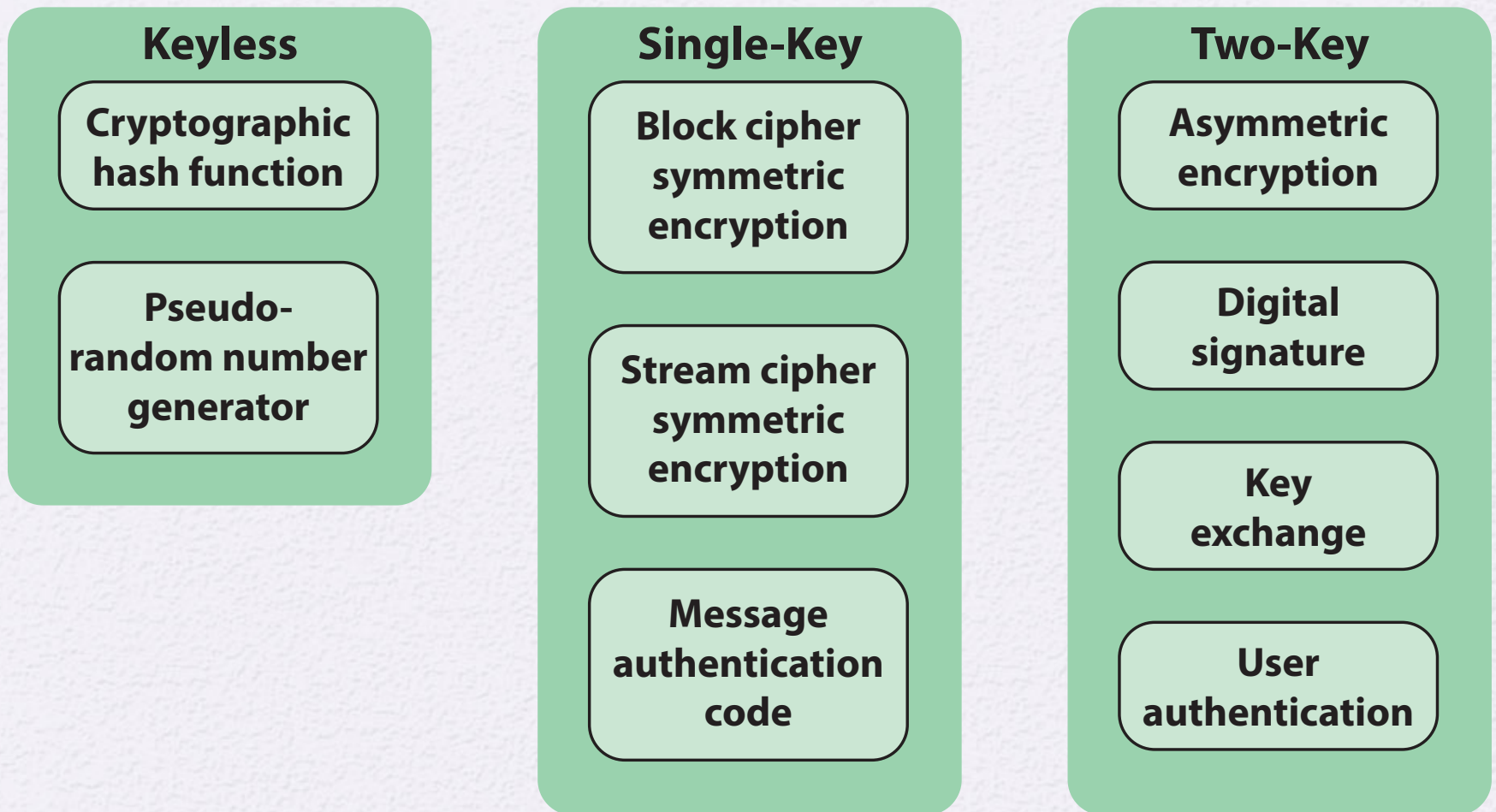


Figure 1.4 Cryptographic Algorithms

Keyless Algorithms

- Deterministic functions that have certain properties useful for cryptography
- One type of keyless algorithm is the cryptographic hash function
 - A hash function turns a variable amount of text into a small, fixed-length value called a *hash value*, *hash code*, or *digest*
 - A *cryptographic hash function* is one that has additional properties that make it useful as part of another cryptographic algorithm, such as a message authentication code or a digital signature
- A *pseudorandom number generator* produces a deterministic sequence of numbers or bits that has the appearance of being a truly random sequence

Single-Key Algorithms

Single-key cryptographic algorithms depend on the use of a secret key

Encryption algorithms that use a single key are referred to as *symmetric encryption algorithms*

With symmetric encryption, an encryption algorithm takes as input some data to be protected and a secret key and produces an unintelligible transformation on that data

A corresponding decryption algorithm takes the transformed data and the same secret key and recovers the original data

Symmetric encryption takes the following forms:

Block cipher

- A block cipher operates on data as a sequence of blocks
- In most versions of the block cipher, known as modes of operation, the transformation depends not only on the current data block and the secret key but also on the content of preceding blocks

Stream cipher

- A stream cipher operates on data as a sequence of bits
- As with the block cipher, the transformation depends on a secret key

Single-Key Algorithms

Another form of single-key cryptographic algorithm is the *message authentication code (MAC)*

A MAC is a data element associated with a data block or message

The MAC is generated by a cryptographic transformation involving a secret key and, typically, a cryptographic hash function of the message

The MAC is designed so that someone in possession of the secret key can verify the integrity of the message

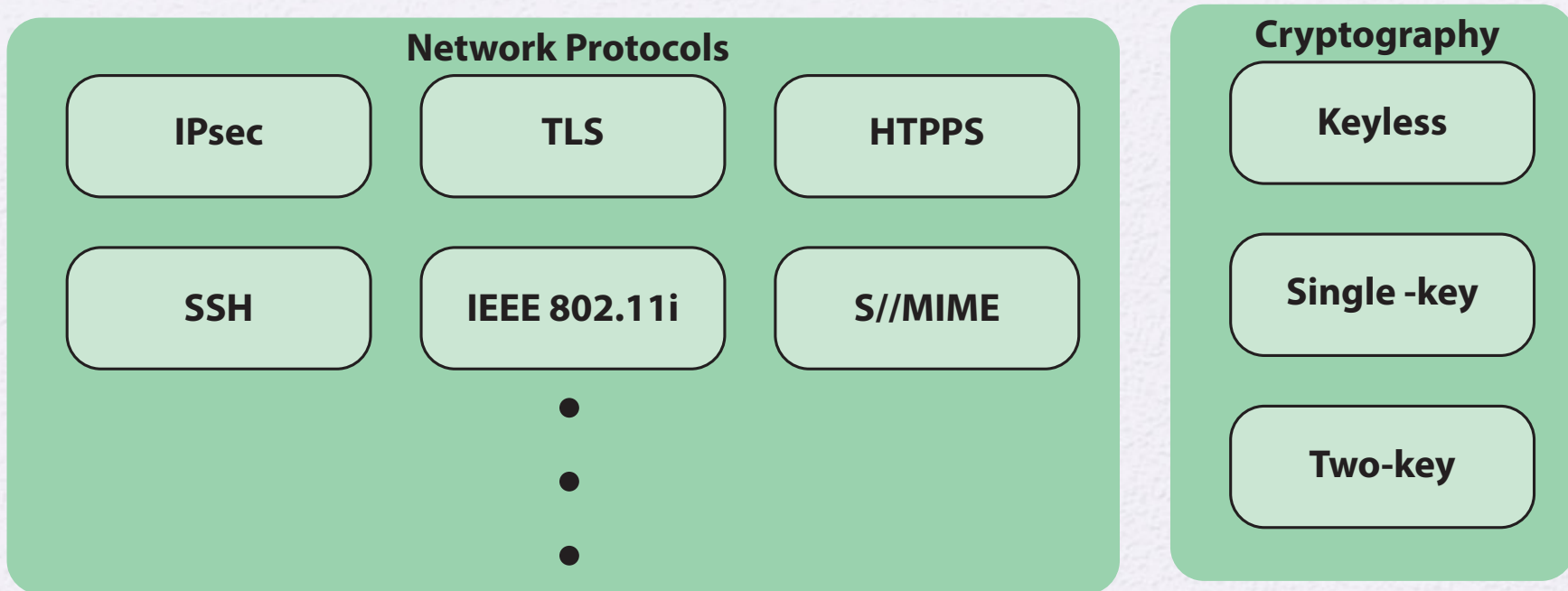
The recipient of the message plus the MAC can perform the same calculation on the message; if the calculated MAC matches the MAC accompanying the message, this provides assurance that the message has not been altered

Asymmetric Algorithms

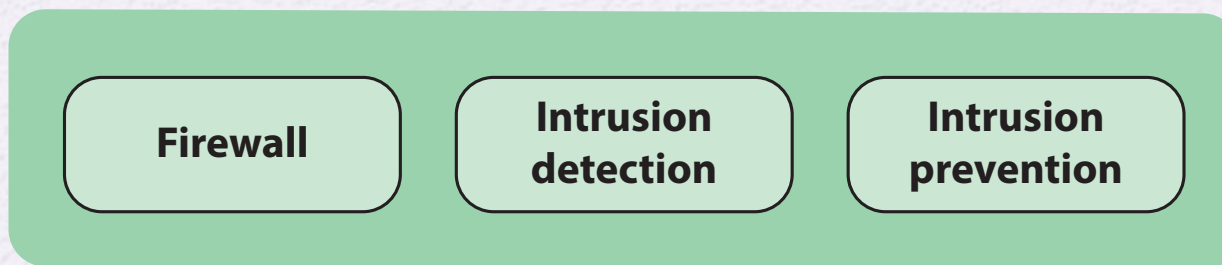
- Encryption algorithms that use a single key are referred to as *asymmetric encryption algorithms*
- Digital signature algorithm
 - A digital signature is a value computed with a cryptographic algorithm and associated with a data object in such a way that any recipient of the data can use the signature to verify the data's origin and integrity
- Key exchange
 - The process of securely distributing a symmetric key to two or more parties
- User authentication
 - The process of authenticating that a user attempting to access an application or service is genuine and, similarly, that the application or service is genuine

Security Services vs Mechanisms

Service	Mechanism							
	Enciph- erment	Digital signature	Access control	Data integrity	Authenti- cation exchange	Traffic padding	Routing control	Notari- zation
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			



(a) Communications Security



(b) Device Security

Figure 1.5 Key Elements of Network Security

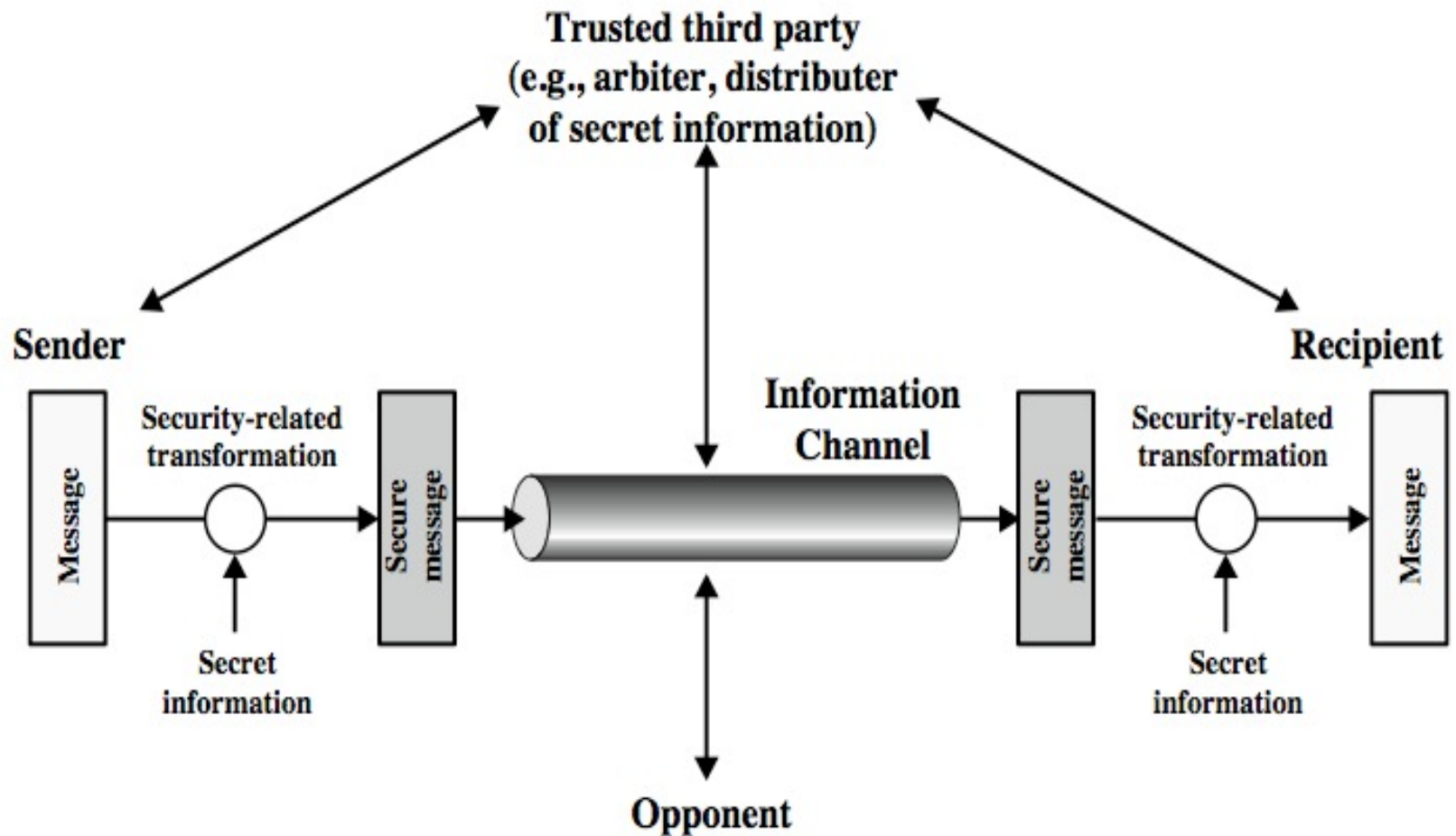
Communications Security

- Deals with the protection of communications through the network, including measures to protect against both passive and active attacks
- Communications security is primarily implemented using network protocols
 - A network protocol consists of the format and procedures that governs the transmitting and receiving of data between points in a network
 - A protocol defines the structure of the individual data units and the control commands that manage the data transfer
- With respect to network security, a security protocol may be an enhancement that is part of an existing protocol or a standalone protocol

Device Security

- The other aspect of network security is the protection of network devices, such as routers and switches, and end systems connected to the network, such as client systems and servers
- The primary security concerns are intruders that gain access to the system to perform unauthorized actions, insert malicious software (malware), or overwhelm system resources to diminish availability
- Three types of device security are:
 - **Firewall**
 - **Intrusion detection**
 - **Intrusion prevention**

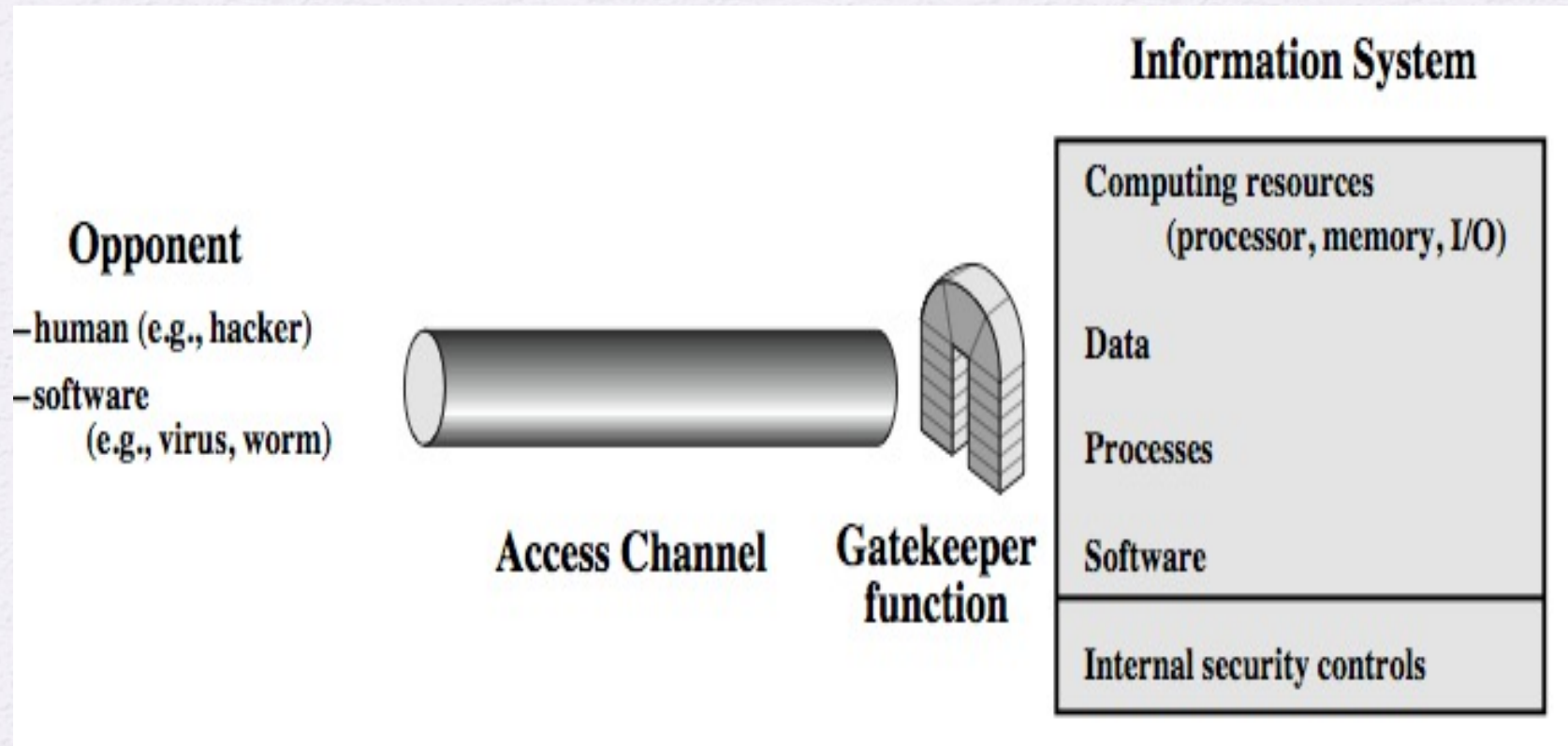
Model for Communication Security



Model for Communication 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

Model for Device Security

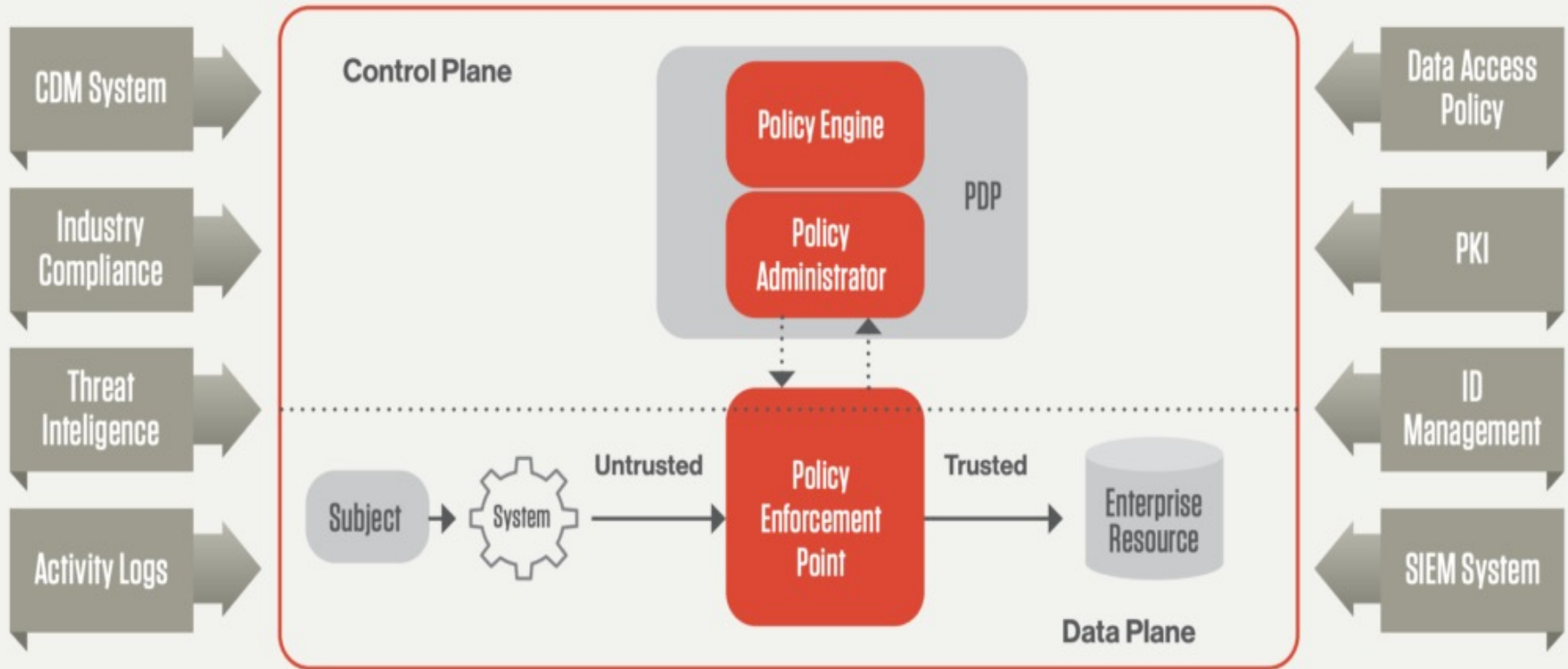


Model for Device Security

- using this model requires us to:
 1. select appropriate gatekeeper functions to identify users
 2. implement security controls to ensure only authorised users access designated information or resources

Model

Zero Trust Security



NIST 800-207 Zero Trust Framework

Model

Zero Trust Security

- New alternative model to the Model for Security
- Zero Trust assumes that there is no traditional network edge; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location
- Zero Trust seeks to address the following key principles
 1. **Continuous verification.** Always verify access, all the time, for all resources.
 2. **Limit the “blast radius.”** Minimize impact if an external or insider breach does occur.
 3. **Automate context collection and response.** Incorporate behavioral data and get context from the entire IT stack (identity, endpoint, workload, etc..) for the most accurate response.

Trust Model

- One of the most widely accepted and most cited definitions of trust is:

“the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party”

- Three related concepts are relevant to a trust model:
 - **Trustworthiness:** A characteristic of an entity that reflects the degree to which that entity is deserving of trust
 - **Propensity to trust:** A tendency to be willing to trust others across a broad spectrum of situations and trust targets. This suggests that every individual has some baseline level of trust that will influence the person’s willingness to rely on the words and actions of others
 - **Risk:** A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of 1) the adverse impacts that would arise if the circumstance or event occurs; and 2) the likelihood of occurrence

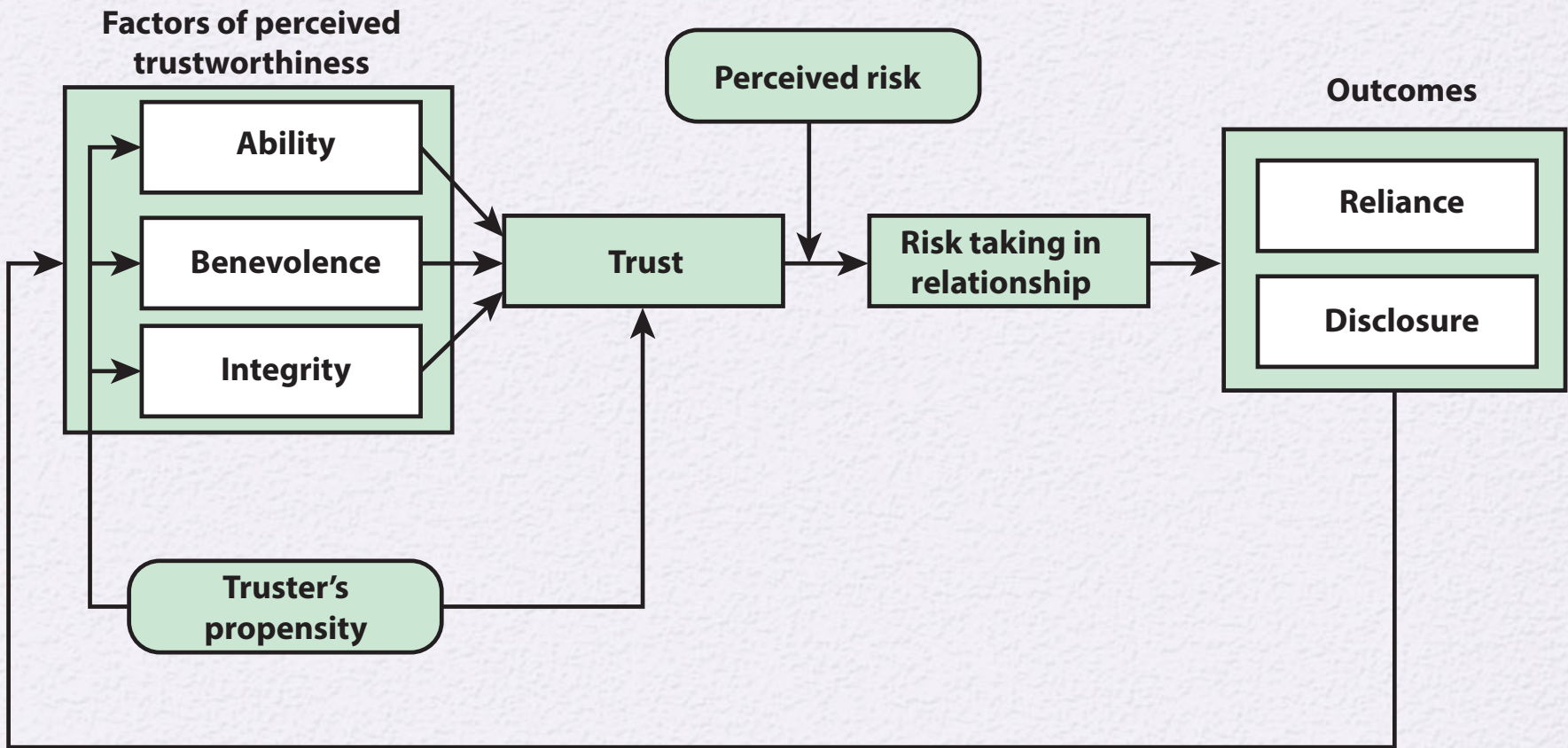


Figure 1.6 Trust Model

The Trust Model and Information Security

Trust is confidence that an entity will perform in a way that will not prejudice the security of the user of the system of which that entity is a part

Trust is always restricted to specific functions or ways of behavior and is meaningful only in the context of a security policy

Generally, an entity is said to trust a second entity when the first entity assumes that the second entity will behave exactly as the first entity expects

In this context, the term entity may refer to a single hardware component or software module, a piece of equipment identified by make and model, a site or location, or an organization

Trustworthiness of an Individual

- Organizations need to be concerned about both internal users (employees, on-site contractors) and external users (customers, suppliers) of their information systems
- With respect to internal users, an organization develops a level of trust in individuals by policies in the following two areas:
 - Human resource security
 - Sound security practice dictates that information security requirements be embedded into each stage of the employment life cycle, specifying security-related actions required during the induction of each individual, their ongoing management, and termination of their employment. Human resource security also includes assigning ownership of information (including responsibility for its protection) to capable individuals and obtaining confirmation of their understanding and acceptance
 - Security awareness and training
 - This area refers to disseminating security information to all employees, including IT staff, IT security staff, and management, as well as IT users and other employees. A workforce that has a high level of security awareness and appropriate security training for each individual's role is as important, if not more important, than any other security countermeasure or control

Trustworthiness of an Organization

- Most organizations rely on information system service and information provided by external organizations, as well as partnerships to accomplish missions and business functions (examples are cloud service providers and companies that form part of the supply chain for the organization)
- To manage risk to the organization, it must establish trust relationships with these external organizations
- NIST SP 800-39 (*Managing Information Security Risk*, March 2011) indicates that such trust relationships can be:
 - Formally established, for example, by documenting the trust-related information in contracts, service-level agreements, statements of work, memoranda of agreement/understanding, or interconnection security agreements
 - Scalable and inter-organizational or intra-organizational in nature
 - Represented by simple (bilateral) relationships between two partners or more complex many-to-many relationships among many diverse partners

Trustworthiness of Information Systems

- SP 800-39 defines trustworthiness for information systems as
 - “the degree to which information systems (including the information technology products from which the systems are built) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the systems across the full range of threats”
- Two factors affecting the trustworthiness of information systems are:
 - **Security functionality:** The security features/functions employed within the system. These include cryptographic and network security technologies
 - **Security assurance:** The grounds for confidence that the security functionality is effective in its application. This area is addressed by security management techniques, such as auditing and incorporating security considerations into the system development life cycle

Establishing Trust Relationships

Validated trust:

- Trust is based on evidence obtained by the trusting organization about the trusted organization or entity. The information may include information security policy, security measures, and level of oversight

Direct historical trust:

- This type of trust is based on the security-related track record exhibited by an organization in the past, particularly in interactions with the organization seeking to establish trust

Mediated trust:

- Mediated trust involves the use of a third party that is mutually trusted by two parties, with the third party providing assurance or guarantee of a given level of trust between the first two parties

Mandated trust:

- An organization establishes a level of trust with another organization based on a specific mandate issued by a third party in a position of authority

Standards

National Institute of Standards and Technology:

- NIST is a U.S. federal agency that deals with measurement science, standards, and technology related to U.S. government use and to the promotion of U.S. private-sector innovation. Despite its national scope, NIST Federal Information Processing Standards (FIPS) and Special Publications (SP) have a worldwide impact

Internet Society:

- ISOC is a professional membership society with worldwide organizational and individual membership. It provides leadership in addressing issues that confront the future of the Internet and 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). These organizations develop Internet standards and related specifications, all of which are published as Requests for Comments (RFCs).

ITU-T:

- The International Telecommunication Union (ITU) is an international organization within the United Nations System in which governments and the private sector coordinate global telecom networks and services. The ITU Telecommunication Standardization Sector (ITU-T) is one of the three sectors of the ITU. ITU-T's mission is the development of technical standards covering all fields of telecommunications. ITU-T standards are referred to as Recommendations

ISO:

- The International Organization for Standardization (ISO) is a worldwide federation of national standards bodies from more than 140 countries, one from each country. ISO is a nongovernmental organization that promotes the development of standardization and related activities with a view to facilitating the international exchange of goods and services and to developing cooperation in the spheres of intellectual, scientific, technological, and economic activity. ISO's work results in international agreements that are published as International Standards

Summary

- Describe the key security requirements of confidentiality, integrity, and availability
- List and briefly describe key organizations involved in cryptography standards
- Provide an overview of keyless, single-key and two-key cryptographic algorithms
- Provide an overview of the main areas of network security
- Describe a trust model for information security
- Discuss the types of security threats and attacks that must be dealt with and give examples of the types of threats and attacks that apply to different categories of computer and network assets

