Introduction to Computer & Network Security

Rajesh Palit, Ph.D.

Electrical & Computer Engineering

North South University

Reference Book: Cryptography and Network Security Principles and Practice, 5th Edition William Stallings

Subject Matter

- **Computer Security:** the security of computers against intruders (e.g., hackers) and malicious software (e.g., viruses)
- **Network Security:** use of cryptographic algorithms in network protocols and network applications
- **Mutual Trust:** techniques and algorithms for providing mutual trust in two main areas. First, key management and distribution deals with establishing trust in the encryption keys used between two communicating entities. Second, user authentication deals with establishing trust in the identity of a communicating partner.
- **Cryptographic Algorithms:** techniques for ensuring the secrecy and/or authenticity of information. The three main areas of study in this category are: (1) symmetric encryption, (2) asymmetric encryption, and (3) cryptographic hash functions, with the related topics of message authentication codes and digital signatures

Threat & Attack

A **threat**, in the context of computer **security**, refers to anything that has the potential to cause serious harm to a computer system.

A **threat** is something that may or may not happen, but has the potential to cause serious damage. There is a circumstance, capability, action or event that could breach security and cause harm. A possible danger that might exploit a vulnerability.

Attack is 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.

Who/what sits in the playfield:

- Computers
- Networks
- Humans (naive and smart ones)

The players:

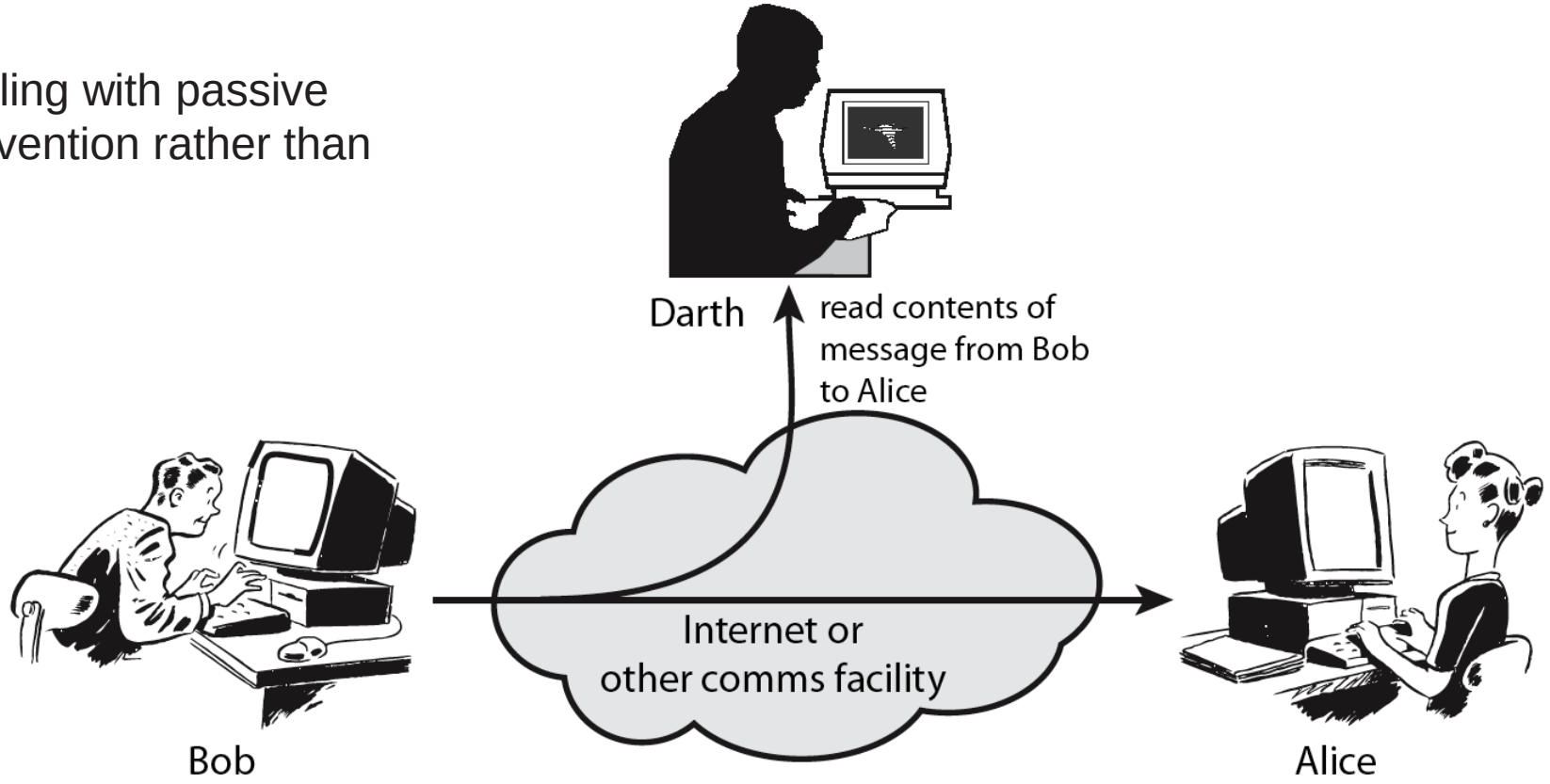
- Attackers: black and white hackers
- Defenders: sysadmins, programmers, users

Passive Attacks

A passive attack attempts to learn or make use of information from the system but does not affect system resources.

Emphasis in dealing with passive attacks is on prevention rather than detection.

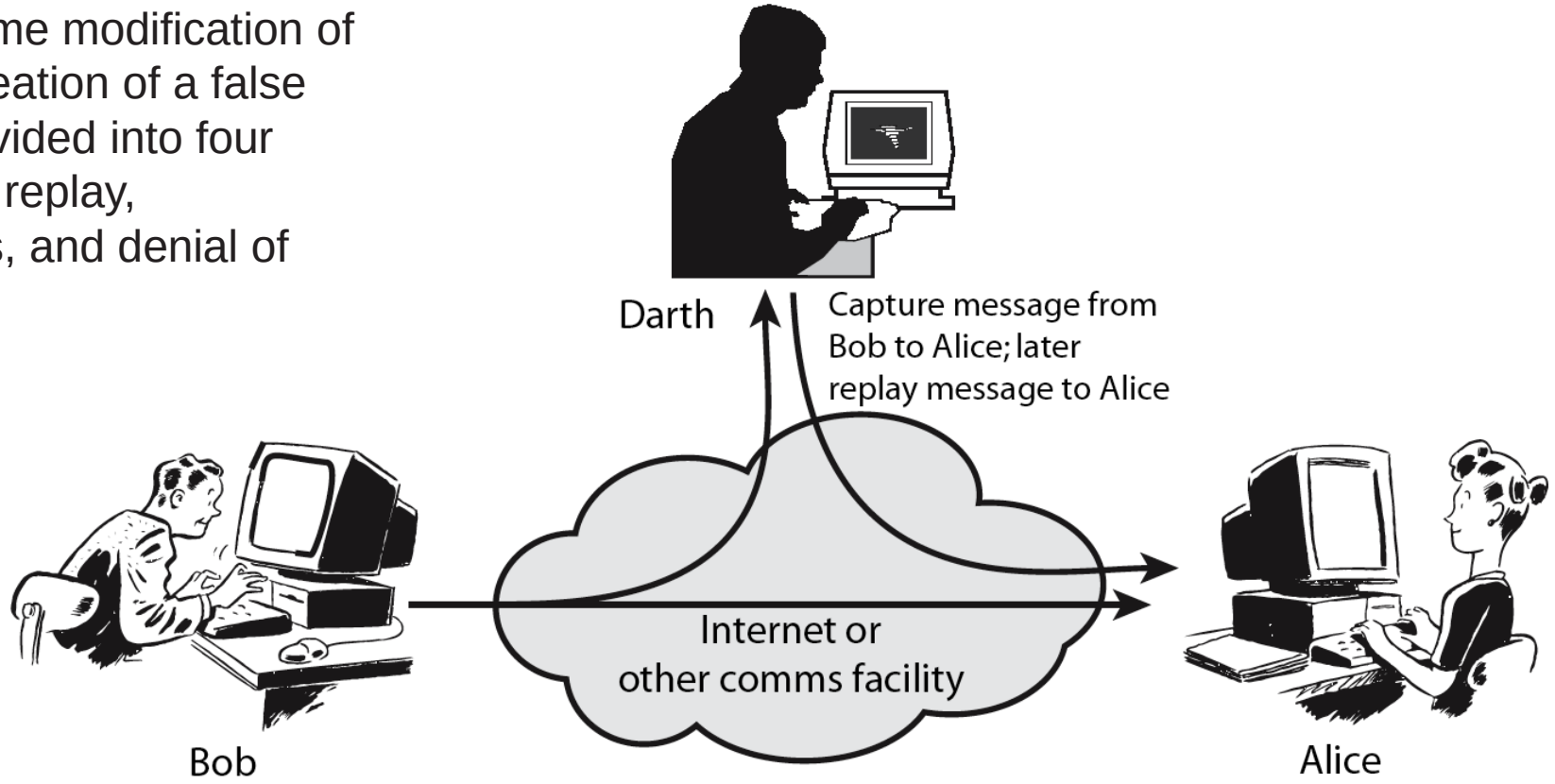
Eavesdropping **Traffic Analysis** **Monitoring**



Active Attacks

An active attack attempts to alter system resources or affect their operation.

Active attacks involve some modification of the data stream or the creation of a false stream and can be subdivided into four categories: masquerade, replay, modification of messages, and denial of service.



Levels of Impact

On the occasion of a breach of security (i.e., a loss of confidentiality, integrity, or availability) on organizations or individuals, three levels of impact are used.

Items	Low	Moderate	High
Degradation in mission capability to an extent and duration that the organization is	Able to perform its primary functions, but the effectiveness of the functions is noticeably reduced	Able to perform its primary functions, but the effectiveness of the functions is significantly reduced	Not able to perform one or more of its primary functions
Damage to organizational assets	Minor	Significant	Major
Financial loss	Minor	Significant	Major
Harm to individual(s)	Minor	Significant – but does not involve loss of life or serious, life-threatening injuries	Severe or catastrophic - involving loss of life or serious, life-threatening injuries

Security Mechanism

- Feature designed to detect, prevent, or recover from a security attack
- No single mechanism that will support all services required
- However one particular element underlies many of the security mechanisms in use:

  - **Cryptographic Tools**

- Specific security mechanisms:
  - Encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization
- Pervasive security mechanisms:
  - trusted functionality, security labels, event detection, security audit trails, security recovery

Challenges of Making a System Secure

1. Security is not as simple as it might first appear to the novice. Most of the major requirements for security services can be given self-explanatory, one-word labels: confidentiality, authentication, nonrepudiation, or integrity. But the mechanisms used to meet those requirements can be quite complex, and understanding them may involve rather subtle reasoning
2. In developing a particular security mechanism or algorithm, one must always consider potential attacks on those security features. In many cases, successful attacks are designed by looking at the problem in a completely different way, therefore exploiting an unexpected weakness in the mechanism.
3. Having designed various security mechanisms, it is necessary to decide where to use them. This is true both in terms of physical placement (e.g., at what points in a network are certain security mechanisms needed) and in a logical sense [e.g., at what layer or layers of an architecture such as TCP/IP (Transmission Control Protocol/Internet Protocol) should mechanisms be placed].
4. Security mechanisms typically involve more than a particular algorithm or protocol. They also require that participants be in possession of some secret information (e.g., an encryption key), which raises questions about the creation, distribution, and protection of that secret information. There also may be a reliance on communications protocols whose behavior may complicate the task of developing the security mechanism.

5. Computer and network security is essentially a battle of wits between a perpetrator who tries to find holes and the designer or administrator who tries to close them. The great advantage that the attacker has is that he or she need only find a single weakness, while the designer must find and eliminate all weaknesses to achieve perfect security.
6. There is a natural tendency on the part of users and system managers to perceive little benefit from security investment until a security failure occurs.
7. Security requires regular, even constant, monitoring, and this is difficult in today’s short-term, overloaded environment.
8. Security is still too often an afterthought to be incorporated into a system after the design is complete rather than being an integral part of the design process.
9. Many users and even security administrators view strong security as an impediment to efficient and user-friendly operation of an information system or use of information

Open Systems Interconnection (OSI) Security Architecture

- Provides a systematic framework for defining security attacks, mechanisms, and services.
- **Security attacks** are classified as either **passive attacks**, which include unauthorized reading of a message of file and traffic analysis or active attacks, such as modification of messages or files, and denial of service.
- A **security mechanism** is any process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack. Examples of mechanisms are encryption algorithms, digital signatures, and authentication protocols.
- **Security services** include authentication, access control, data confidentiality, data integrity, nonrepudiation, and availability

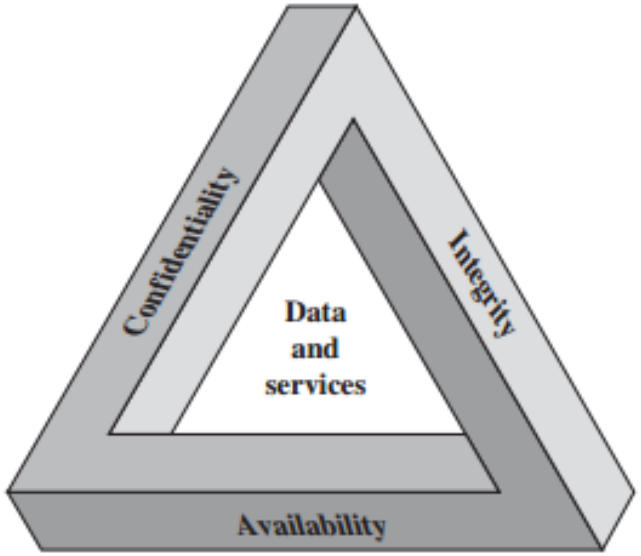
X.800 and RFC 2828

ITU-T Recommendation X.800 (Security Architecture for OSI) and IETF RFC 2828 (Internet Security Glossary) are used as references to systematically evaluate and define security requirements, both have many points in common.

X.800 is used to define general security-related architectural elements needed when protection of communication between open systems is required. X.800 establishes guidelines and constraints to improve existing recommendations and/or to develop new recommendations in the context of OSI. Similarly, RFC 2828 provides abbreviations, explanations and recommendations for information system security terminology.

RFC 2828 is bunch of internet glossary, while X.800 is security architecture for open systems interconnection for CCITT applications.

The Security Requirement



The Security Requirements Triad (CIA Triad)

- **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.

- **Integrity:** This term covers two related concepts:

  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.

- **Availability:** Assures that systems work promptly and service is not denied to authorized users.

The NIST *Computer Security Handbook* (1995)

- **Confidentiality:** Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.
- **Integrity:** Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.
- **Availability:** Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Additional Requirements

- **Authenticity:** The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. This means 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. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Because truly secure systems are not yet an achievable goal, we must be able to trace a security breach to a responsible party. Systems must keep records of their activities to permit later forensic analysis to trace security breaches or to aid in transaction disputes.

Security Services

- **Authentication** - assurance that communicating entity is the one claimed
  - have both peer-entity & data origin authentication
- **Access Control** - prevention of the unauthorized use of a resource
- **Data Confidentiality** –protection of data from unauthorized disclosure
- **Data Integrity** - assurance that data received is as sent by an authorized entity
- **Non-Repudiation** - protection against denial by one of the parties in a communication
- **Availability** – resource accessible/usable

Confidentiality

- Ability to keep information communicated between (among) authorized parties private
- Observer should not be able to recover information
- In a stronger sense, an observer cannot determine the parties involved or whether a communication session occurred

User Authentication

- Ability of the authorized parties in a communication session to ascertain the identity of other authorized parties
  - Mutually Trusting
  - One-Way Authenticated
  - Mutually Suspicious

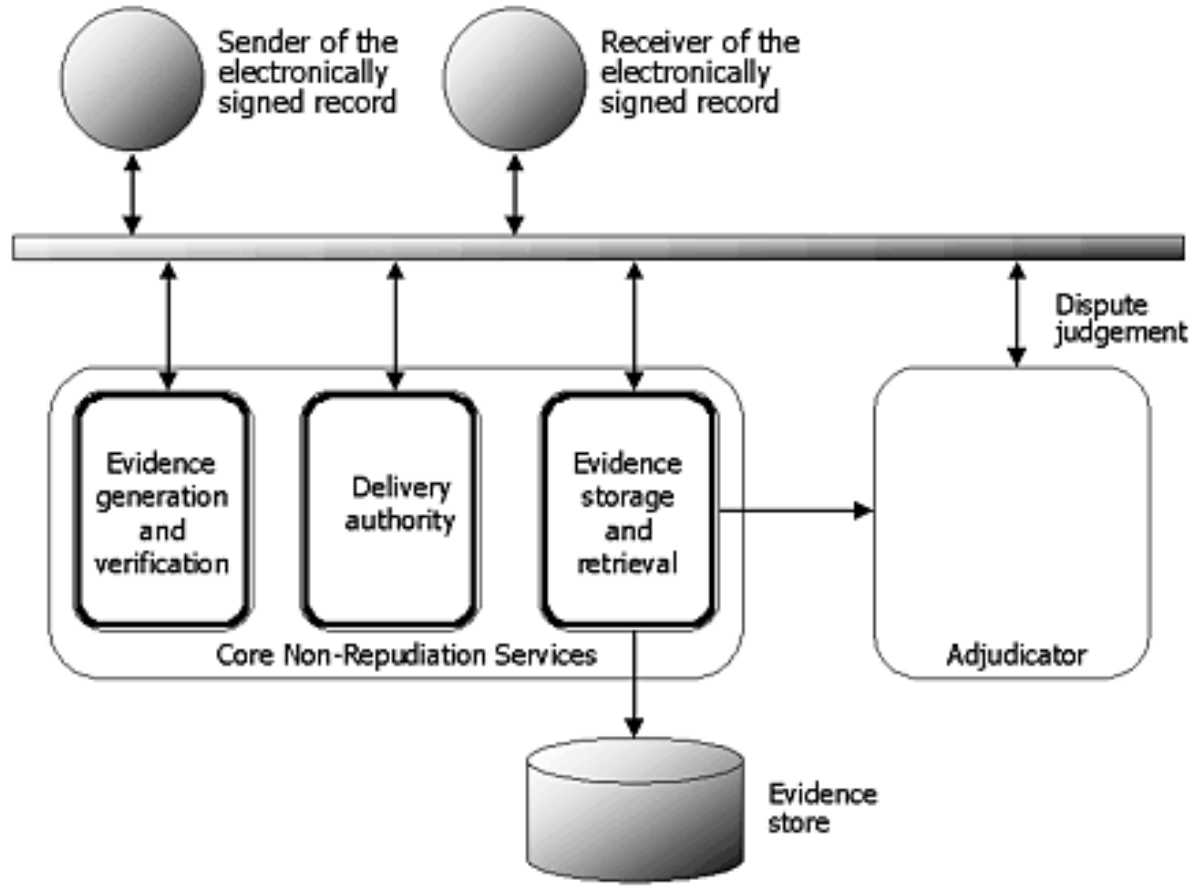
Data Integrity

- Ability to ascertain that information exchanged has not been subject to additions, deletions, modifications or undue delay

If it's not accurate, it might as well not exist.

Non-Repudiation

- Ability to prevent an authorized party from denying the existence or contents of a communication session



Cryptographic Tools

- Encryption/Decryption
- Message Authentication Codes (Hashing)
- Digital Signatures

Encryption/Decryption

- Encryption is the process of transforming a plaintext message M into ciphertext C using an a unique key K

$$C = E_K(M)$$

- Decryption is just the reverse operation; transforming ciphertext C into plaintext M under control of key K

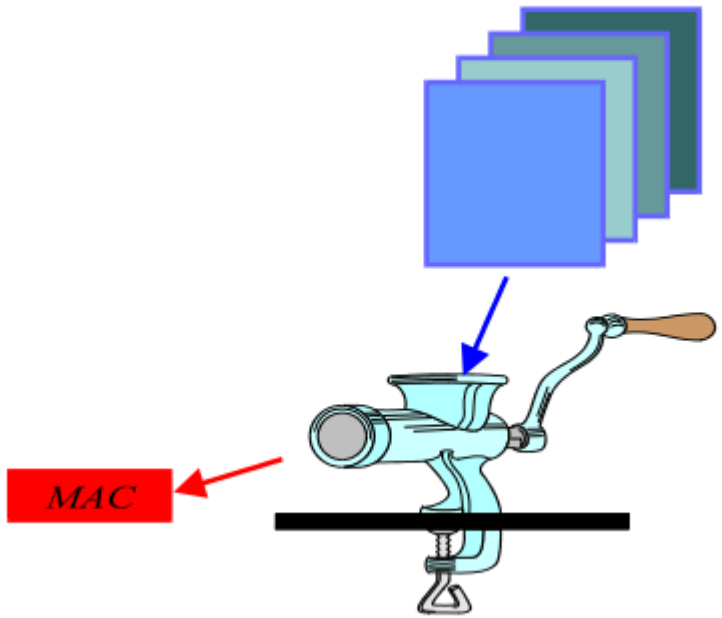
$$M = D_K(C)$$

Security Requirement

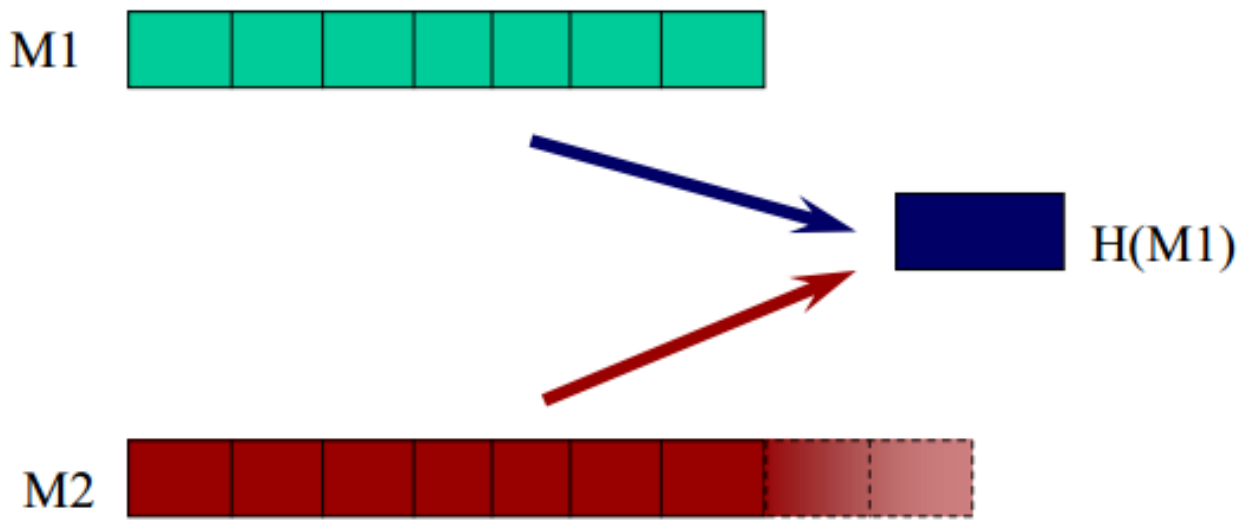
- It should be (computationally) infeasible for an observer of C to recover either M or K (in a *reasonable* time)

Message Authentication/Hashing

- This function allows the detection of any modification of the plaintext message
- It is usually a *digest* of the message created in such a way that as little as one bit change in the message will produce an unpredictable change in approximately 50% of the bits or characters of the digest



Hashing



It should not be possible to deterministically find M2 (of any length) that creates the same Hash value - Collision

Digital Signatures

- Ability to prove to an independent third party at a later date the author and contents of a message

Objectives and Tools

- Confidentiality/Privacy
  - Encryption
- Data Integrity
  - Cipher Chaining
  - Hashing
- User Integrity/Non-Repudiation
  - Digital Signatures

Security Services and Mechanisms

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

Cryptography

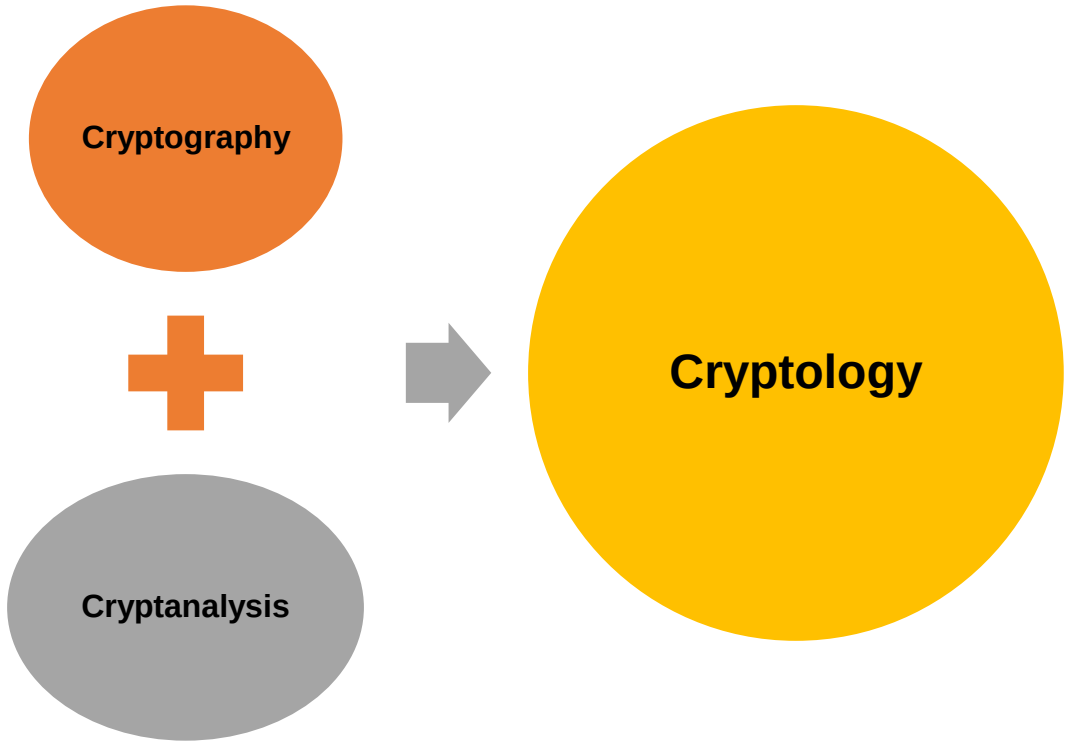
The science of "secret" writing

- a cipher is a function which transforms a plaintext message into a ciphertext (cryptogram) by the process of encipherment
- plaintext is recovered from the ciphertext by the process of deciphering

Cryptanalysis

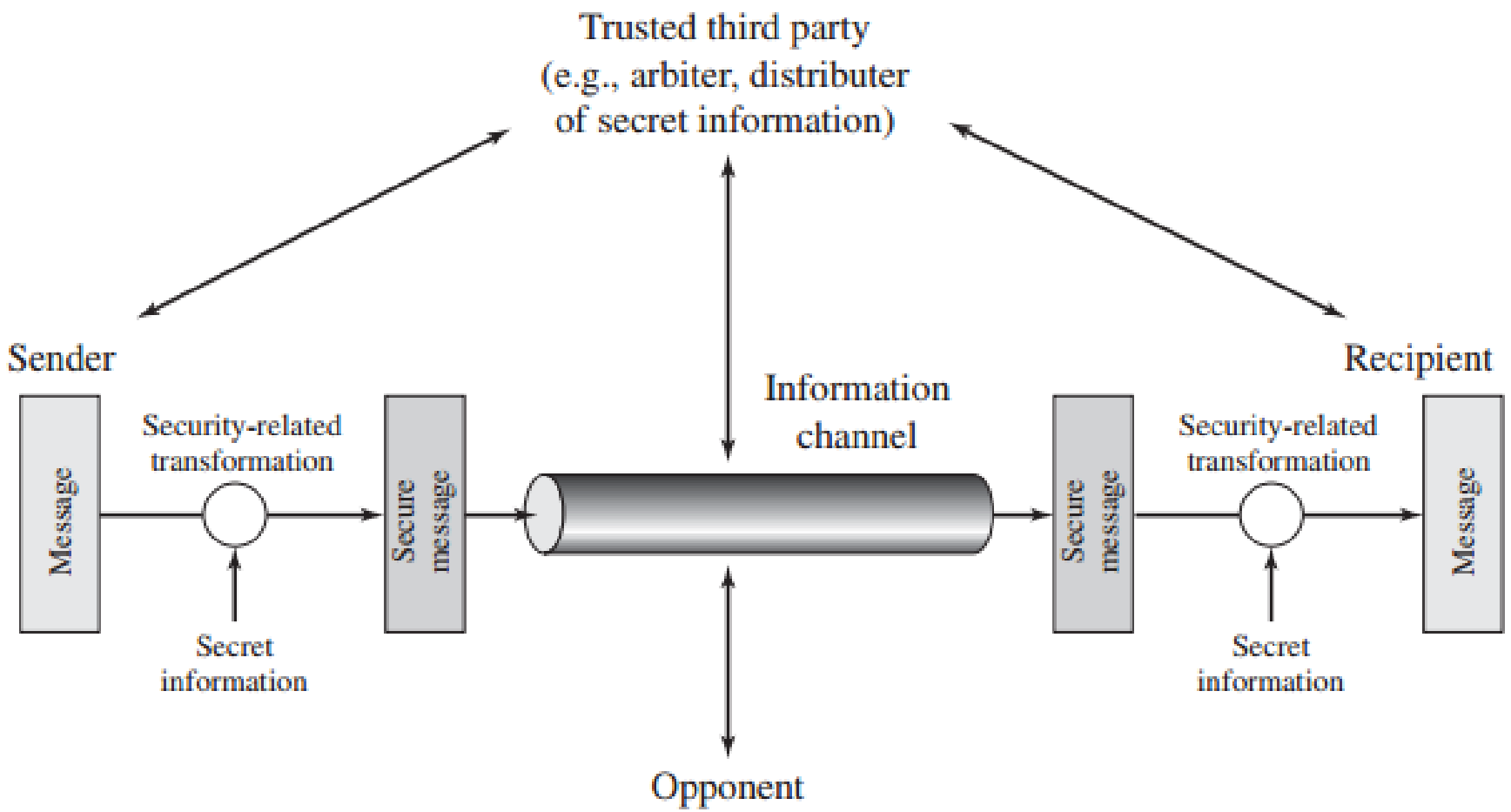
The science and study of breaking ciphers, i.e., the process of determining the plaintext message from the ciphertext

- Ciphertext only
- Known-plaintext
- Chosen plaintext
- Chosen ciphertext

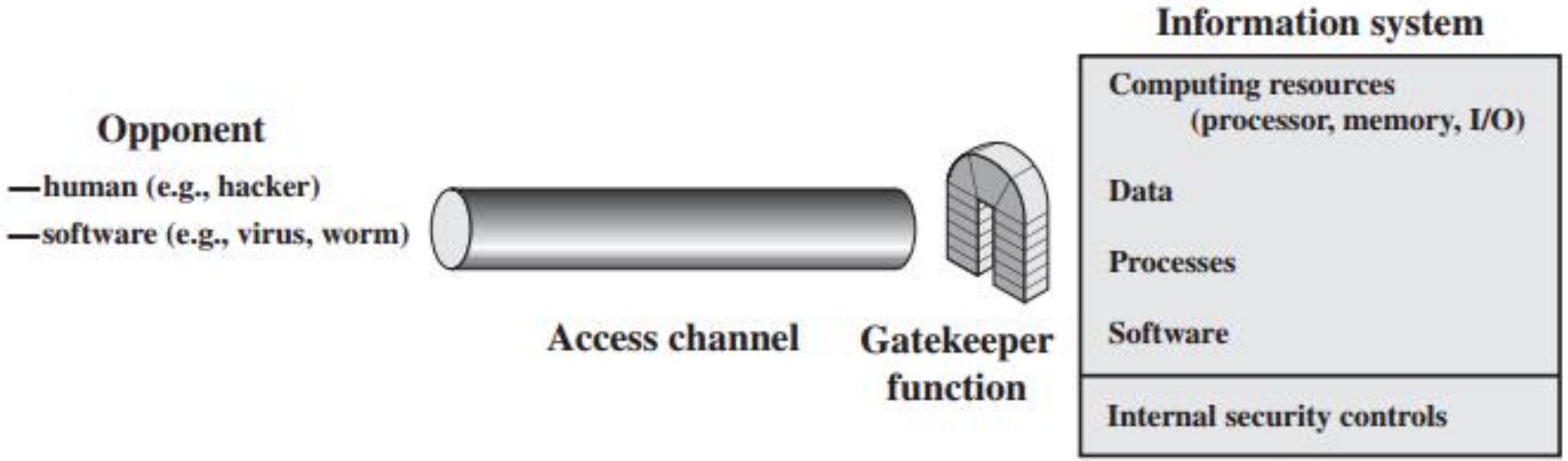


Network & Systems

Model for Network Security



Network Access Security Model



Network Security Considerations

- Security Functions can be applied at various points (layers) in the network
  - ❑ Link-to-Link: Contents and headers are encrypted, information appears in-the-clear within switch. Lots of keys in the system!
  - ❑ Transport: Provides protection of user identity and data from external observers, Requires high-speed (bulk) encryption processing. No protection from other users in the same node
  - ❑ End-to-End: Encryption and Authentication Functions performed by end user, Lower speed requirements. Attackers can monitor header information for sender/receiver pairs (traffic analysis)

Computer System Security

- Cybersecurity, computer security or IT security is the protection of computer systems from theft of or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide.
- Cybersecurity includes controlling physical access to system hardware, as well as protecting against harm that may be done via network access, malicious data and code injection.
- Due to malpractice by operators, whether intentional or accidental, IT security personnel are susceptible to being tricked into deviating from secure procedures through various methods of social engineering.
- The field is of growing importance due to increasing reliance on computer systems, the Internet and wireless networks such as Bluetooth and Wi-Fi, and due to the growth of "smart" devices, including smartphones, televisions and the various tiny devices that constitute the Internet of Things.