Cryptography and Network Security

What is Security ?

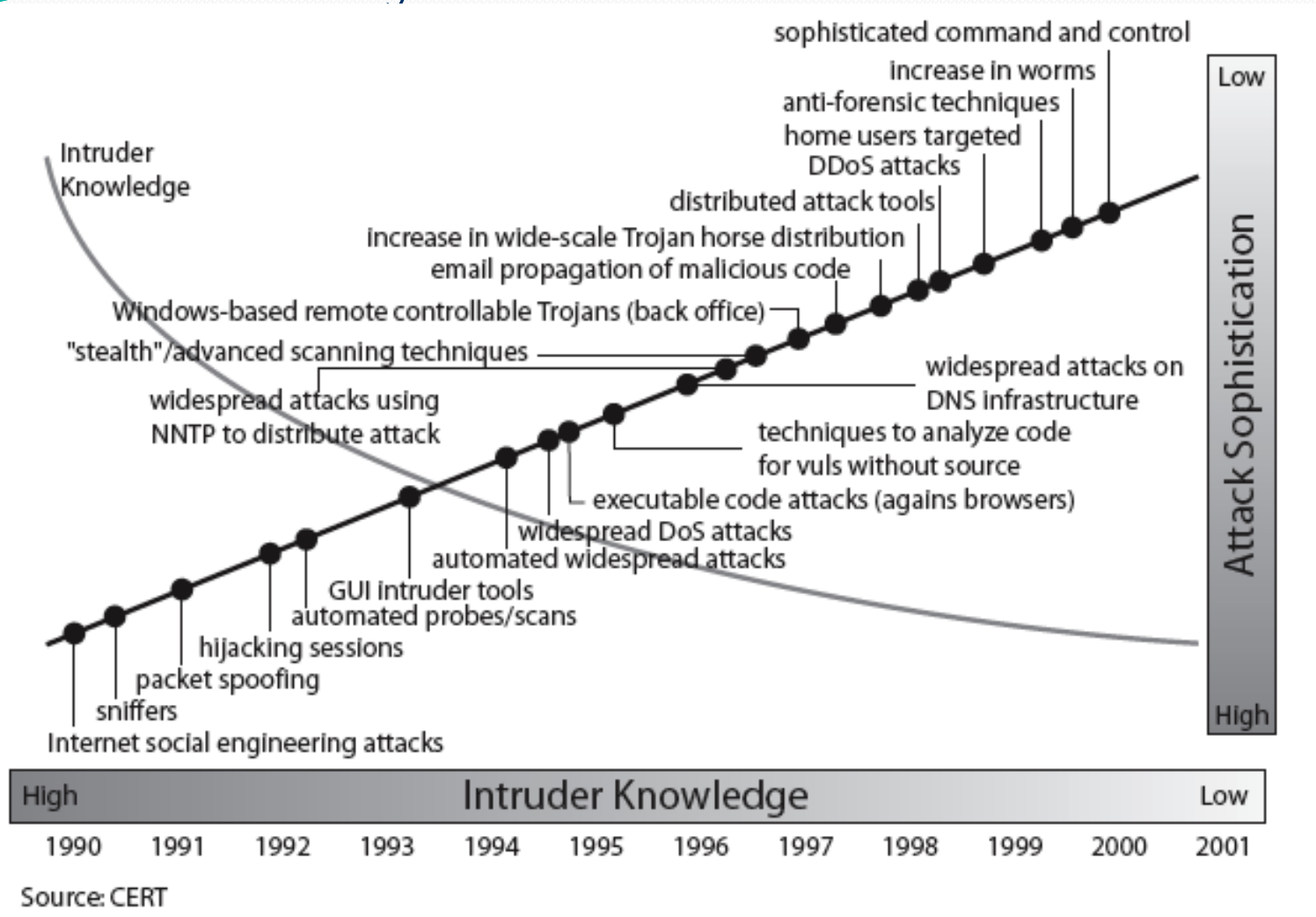
Computer Security - generic name for the collection of tools designed to protect data and to thwart hackers

Network Security - measures to protect data during their transmission

Internet Security - measures to protect data during their transmission over a collection of interconnected networks

Security is the measures to prevent, detect, and correct security violations that involve the transmission & storage of information

Security Trends



- growth in sophistication of attacks contrasting with decrease in skill & knowledge needed to mount an attack.

OSI Security Architecture

- ITU-T X.800 “Security Architecture for OSI”
- Defines a systematic way of defining and providing security requirements
- X.800: a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers

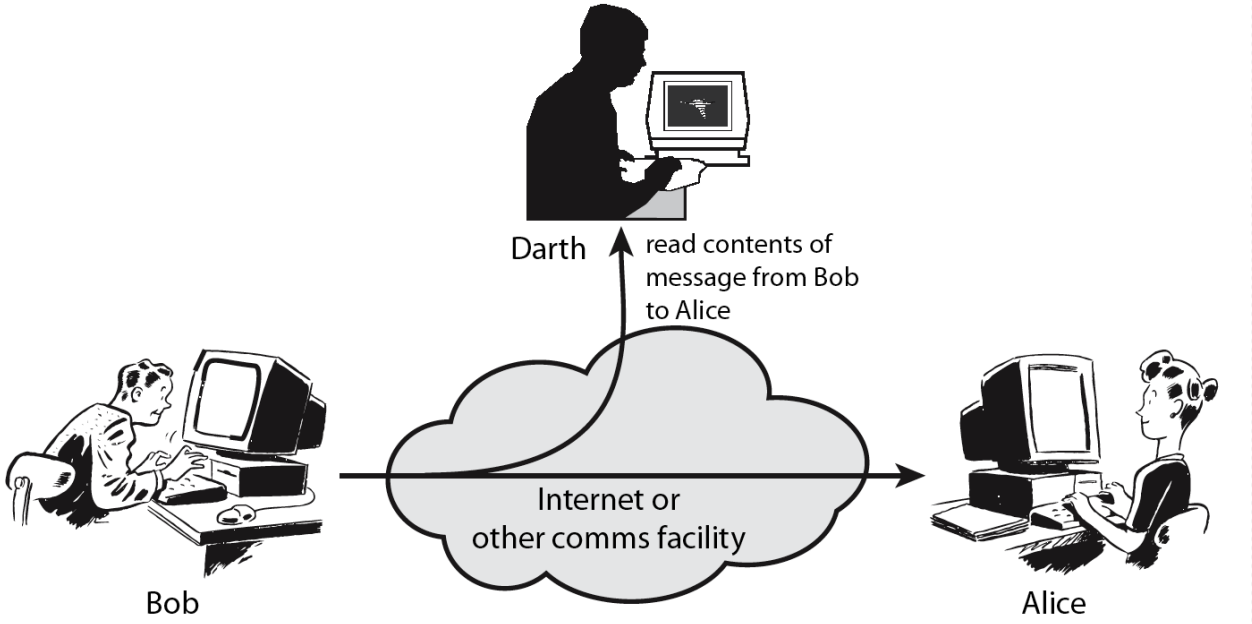
Information Security

- Considers 3 aspects:
  - **Security attack -** Any action that compromises the security of information owned by an organization.
  - **Security mechanism -** 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.

Security Attack

- any action that compromises the security of information
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
  - passive
  - active

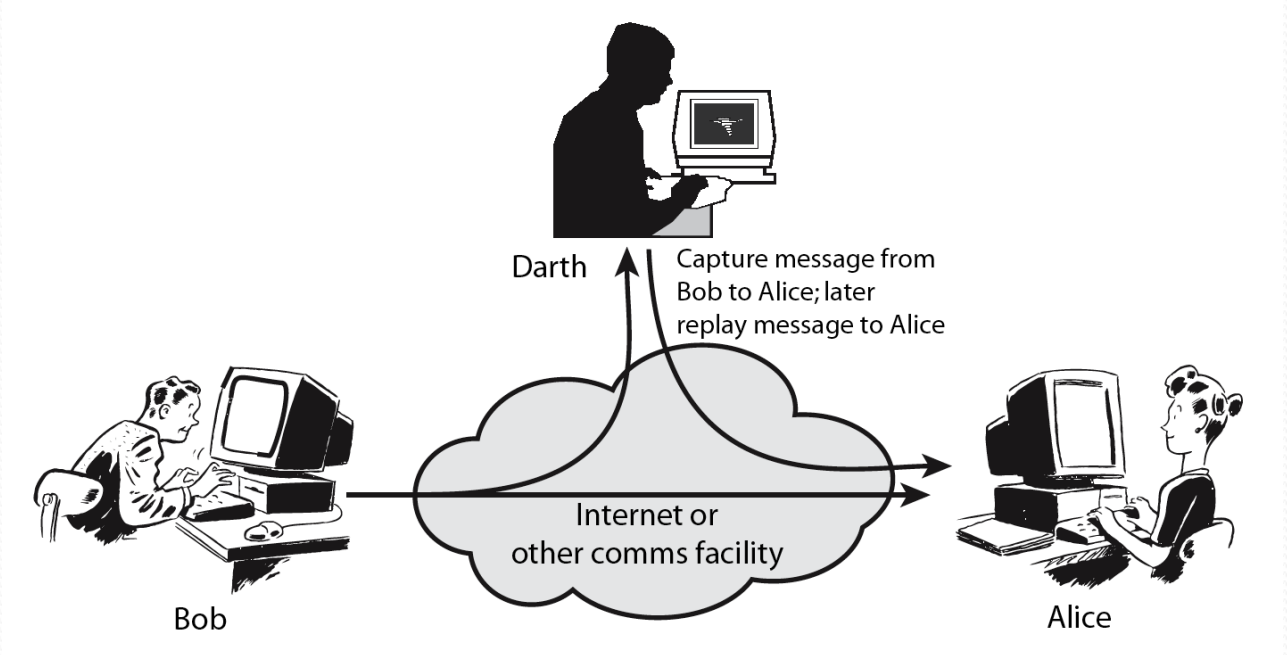
Passive Attacks



Passive Attacks attempt to learn or make use of information from the system but does not affect system resources.

- obtain message contents
- monitor traffic flows
- difficult to detect as they do not involve any alteration of the data
- measures are available to prevent their success

Active Attacks



Active Attacks attempt to alter system resources or affect their operation.

- masquerade of one entity as some other
- replay previous messages
- modify messages in transit

It is quite difficult to prevent active attacks absolutely, because of the wide variety of potential physical, software, and network vulnerabilities.

The goal is to detect active attacks and to recover from any disruption or delays caused by them.

Security Service

- enhance security of data processing systems and information transfers of an organization
- intended to counter security attacks
- using one or more security mechanisms
- often replicates functions normally associated with physical documents
  - Example:

    have signatures, dates;

    need protection from disclosure, tampering, or destruction; be notarized or witnessed;

    be recorded or licensed

Security Services (X.800)

Authentication - assurance that the communicating entity is the one claimed

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

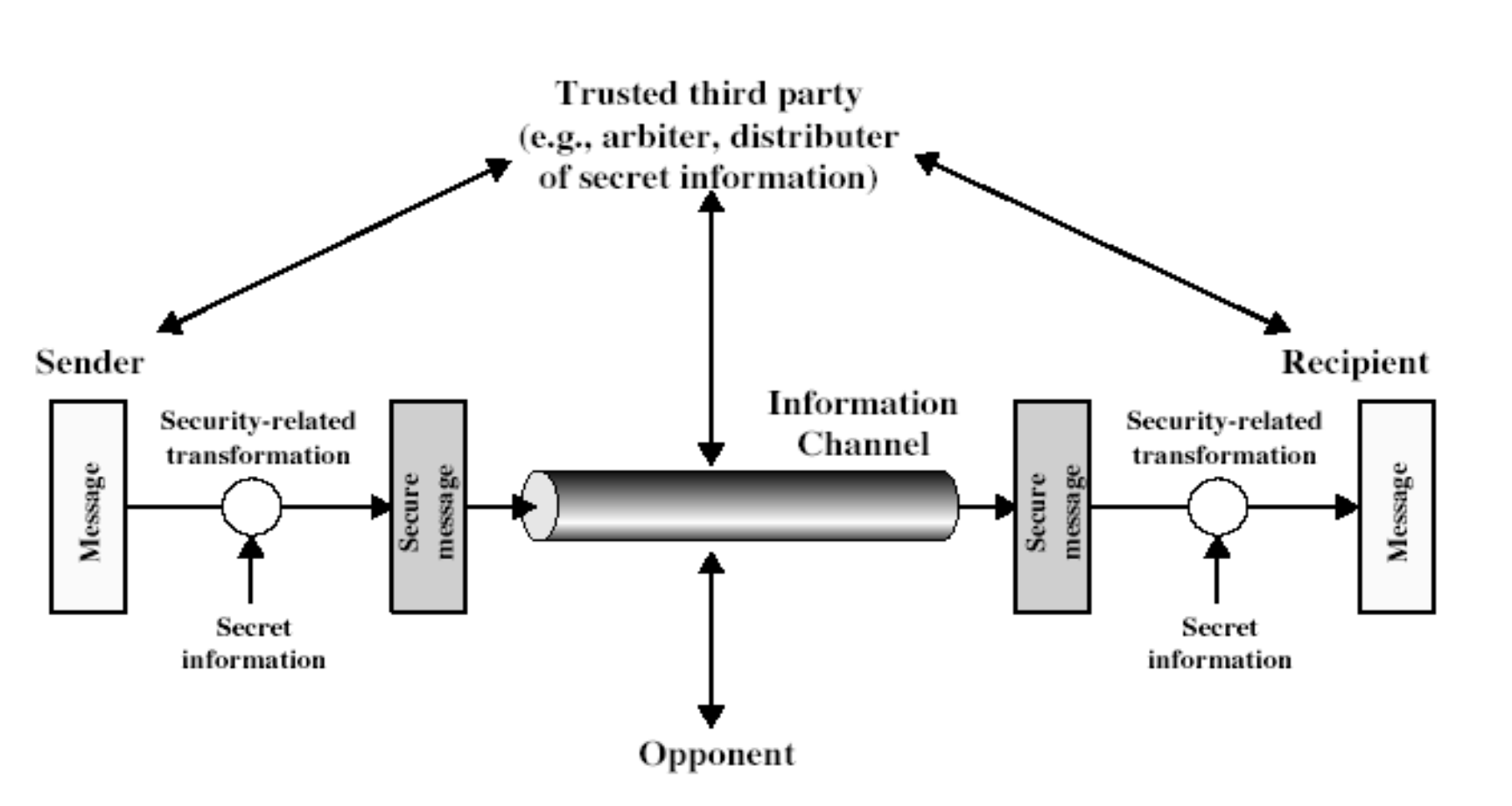
Non-Repudiation - protection against denial by one of the parties in a communication

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 techniques / cryptographic algorithms**
- Security Mechanism (X.800)

  - encipherment, digital signatures, access controls, data integrity, authentication exchange, traffic padding, routing control, notarization

Model for Network Security

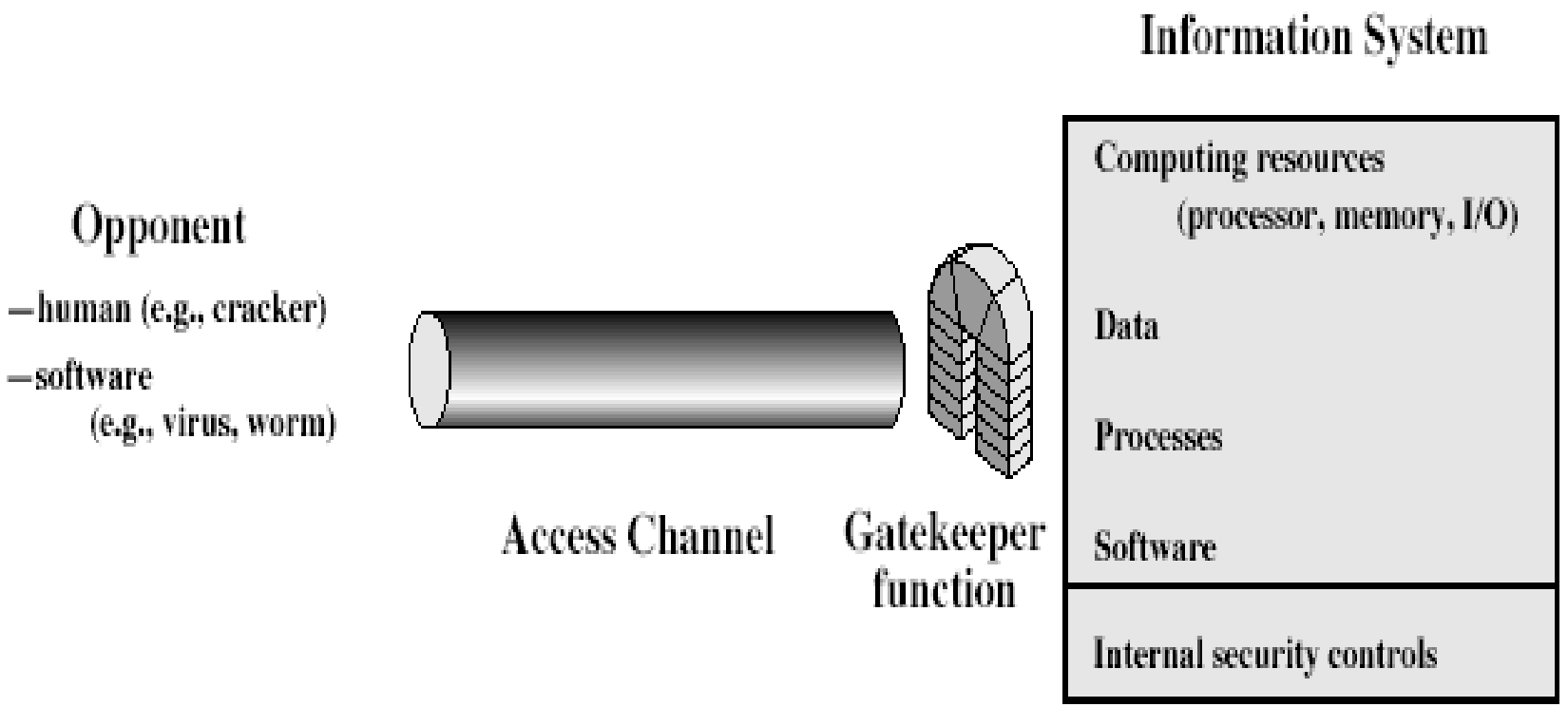


Model for Network Security

- To follow the security model it requires to:

1. design a suitable algorithm for the security transformation (e.g. encryption)
2. generate the secret information (keys) used by the algorithm (e.g. key generation, key scheduling)
3. develop methods to distribute and share the secret information (e.g. key distribution algorithms)
4. specify a protocol enabling the principals to use the transformation and secret information for a security service (e.g. security protocols)

Model for Network Access Security



Model for Network Access Security

- This model requires to:

1. select appropriate gatekeeper functions to identify users (authentication)

2. implement security controls to ensure only authorised users access designated information or resources (access control)

What is Cryptography?

- The primary goal of cryptography is to secure important data on transit or data on store

- Confidentiality ensures that no one can read the message except the authorized receiver, even if that data is transferred through an insecure medium
- Integrity assures that the received message has not been altered in any way from the original message sent.
- Authentication establishes identity, entity or message authentication.
- Non-repudiation proves that the sender really sent this message

What is Cryptography?

- The primary goal of cryptography is to secure important data on transit or data on store

- Confidentiality ensures that no one can read the message except the authorized receiver, even if that data is transferred through an insecure medium
- Integrity assures that the received message has not been altered in any way from the original message sent.
- Authentication establishes identity, entity or message authentication.
- Non-repudiation proves that the sender really sent this message

Types of Cryptography

- Encryption Algorithms

  Symmetric Key/Private Key : The encryption key and decryption key are easily derivable from each other

  - Block Cipher : Fixed blocks of data

  – Data Encryption Standard (DES), Triple DES, Advanced Encryption Standard (AES)

  - Stream Cipher : Block Size = 1

  – eStream Winners Trivium, Grain, MICKEY, Rabbit

  Asymmetric Key/Public Key : Infeasible to determine the decryption key, d from the encryption key, e

  – Diffie- Hellman, RSA, Elliptic Curve Cryptography

- HASH Function for Authentication
- Cryptanalysis and Attacks

  Algebraic Analysis

  Linear Cryptanalysis, Differential Cryptanalysis

  Algorithmic / Structural Analysis

  Man-in-the-Middle Attack, Related Key Attack

  Side Channel Analysis

  Power Attack, Timing Attack, Fault Analysis etc.

- Network Security ?