Content

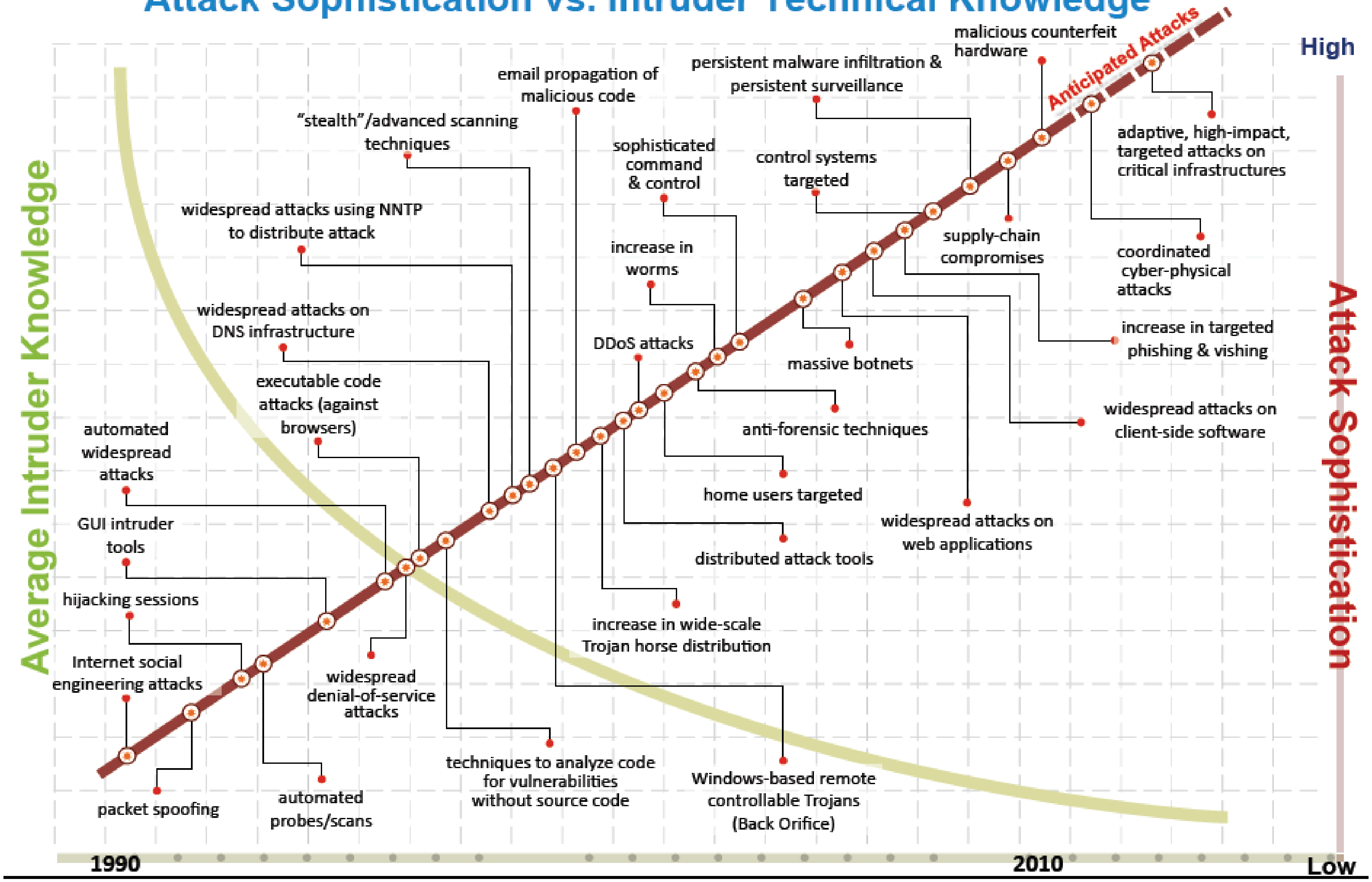
1. Introduction to Computer cybersecurity, Cryptography and Applications . Term Project
2. History and kinds of Cryptography and computer security applications
3. Number Theory and Modular Aritmetic.
4. Cryptographic Functions and Discrete logarithms problem
5. Fundamentals of Symmetric Encryption and DES Algorithm DES and 3DES
6. Cryptanalysis Methods, Differential and linear cryptanalysis methods.
7. Advanced Encryption Standard and Block encryption modes.

8. Hash Functions and Applications
9. Fundamentals of Public key Cryptosystems and RSA
10. Diffie-Hellman key exchange and El-Gamal encryption algorithms
11. Elliptic Curve Cryptosystems, Midtern Exam.
12. Fundamentals of Quantum Cryptography.
13. Computer Security and applications of cryptographic protocols
14. Digital Signatures and Applications

Information security requirements

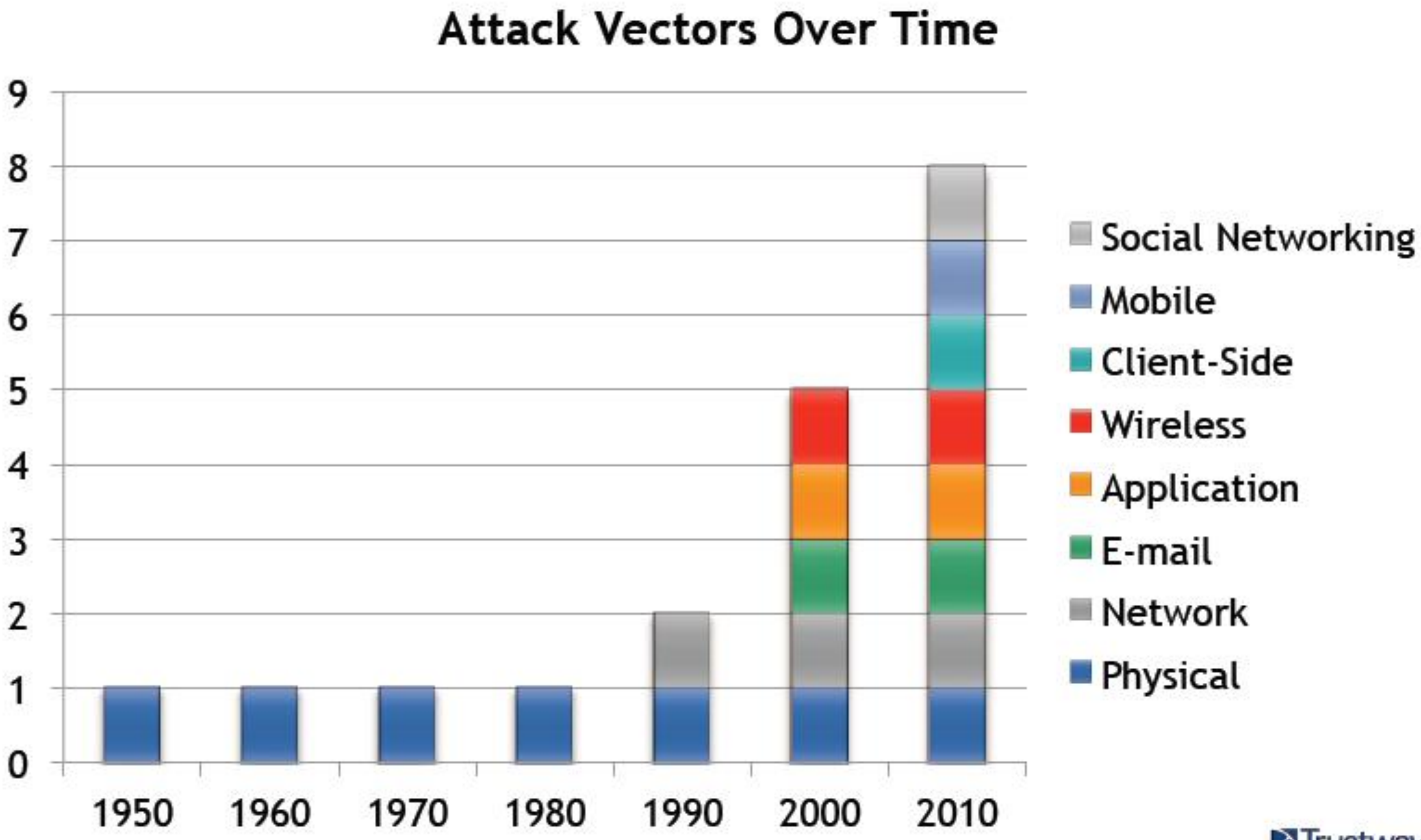
- Information Security requirements have changed in recent times
- traditionally provided by physical and administrative mechanisms
- computer use requires automated tools to protect files and other stored information
- use of networks and communications links requires measures to protect data during transmission

Attack Sophistication vs. Intruder Technical Knowledge



Carnegie Mellon University

Attack Vector Evolution



- ITU-T X.800 “Security Architecture for OSI”
- defines a systematic way of defining and providing security requirements
- for us it provides a useful, if abstract, overview of concepts we will study

Aspect of Security

- consider 3 aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**

Security Attacks

- any action that compromises the security of information owned by an organization
- information security is about how to prevent attacks, or failing that, to detect attacks on information-based systems
- often *threat* & *attack* used to mean same thing
- have a wide range of attacks
- can focus of generic types of attacks
  - passive
  - active

Threat

- An event, the occurrence of which could have an undesirable impact on the well-being of an asset.

  [ISC^2]

- Any circumstances or event that has the potential to cause harm to a system or network" .That means, that even the existence of a(n unknown) vulnerability implies a threat by definition.

  [CERT]

Vulnerability

- A feature or bug in a system or program which enables an attacker to bypass security measures.

  [Schultz Jr.]

- An aspect of a system or network that leaves it open to attack.

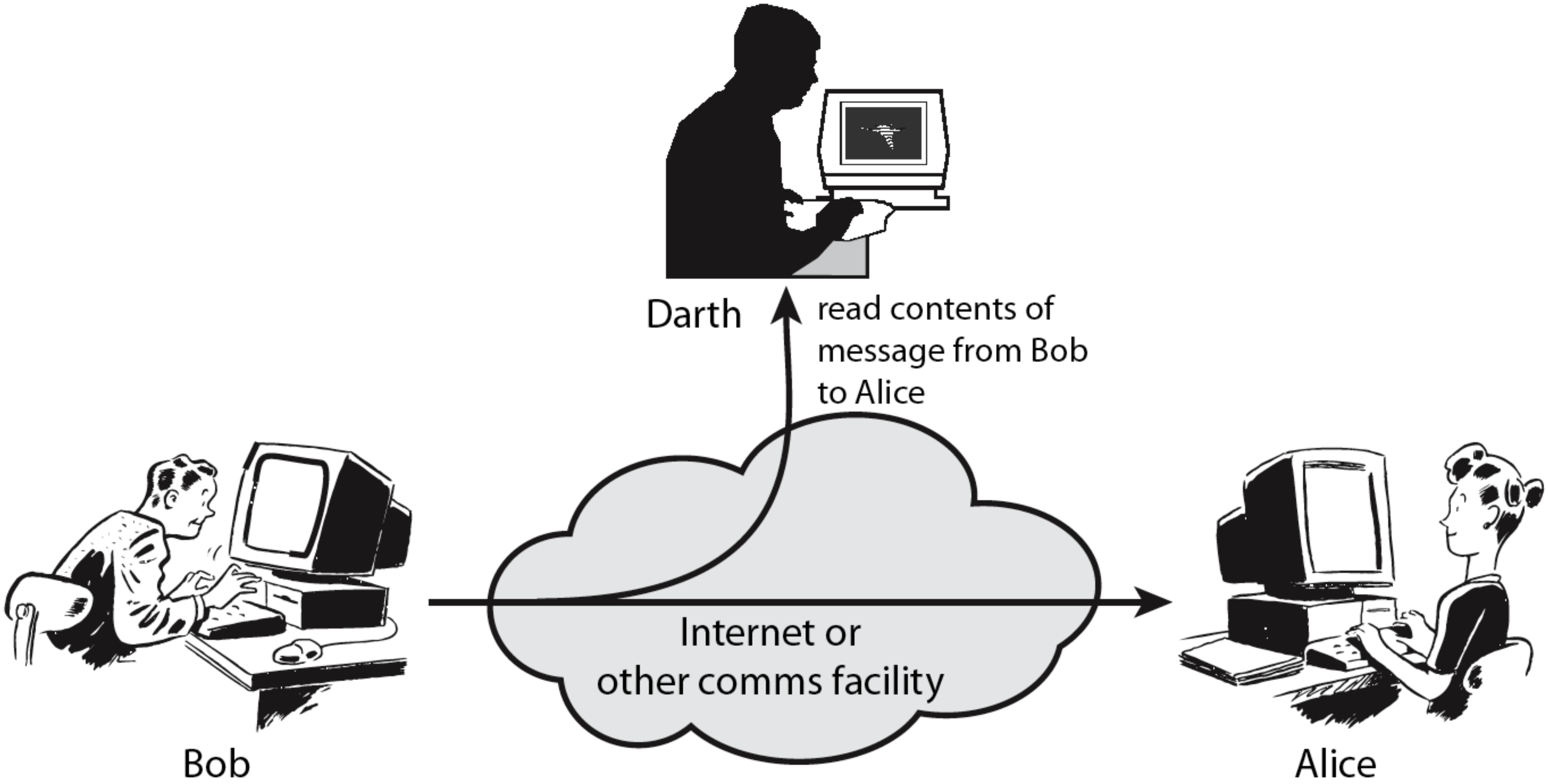
  [CERT]

- Absence or weakness of a risk-reducing safeguard. It is a condition that has the potential to allow a threat to occur with greater frequency, greater impact or both.

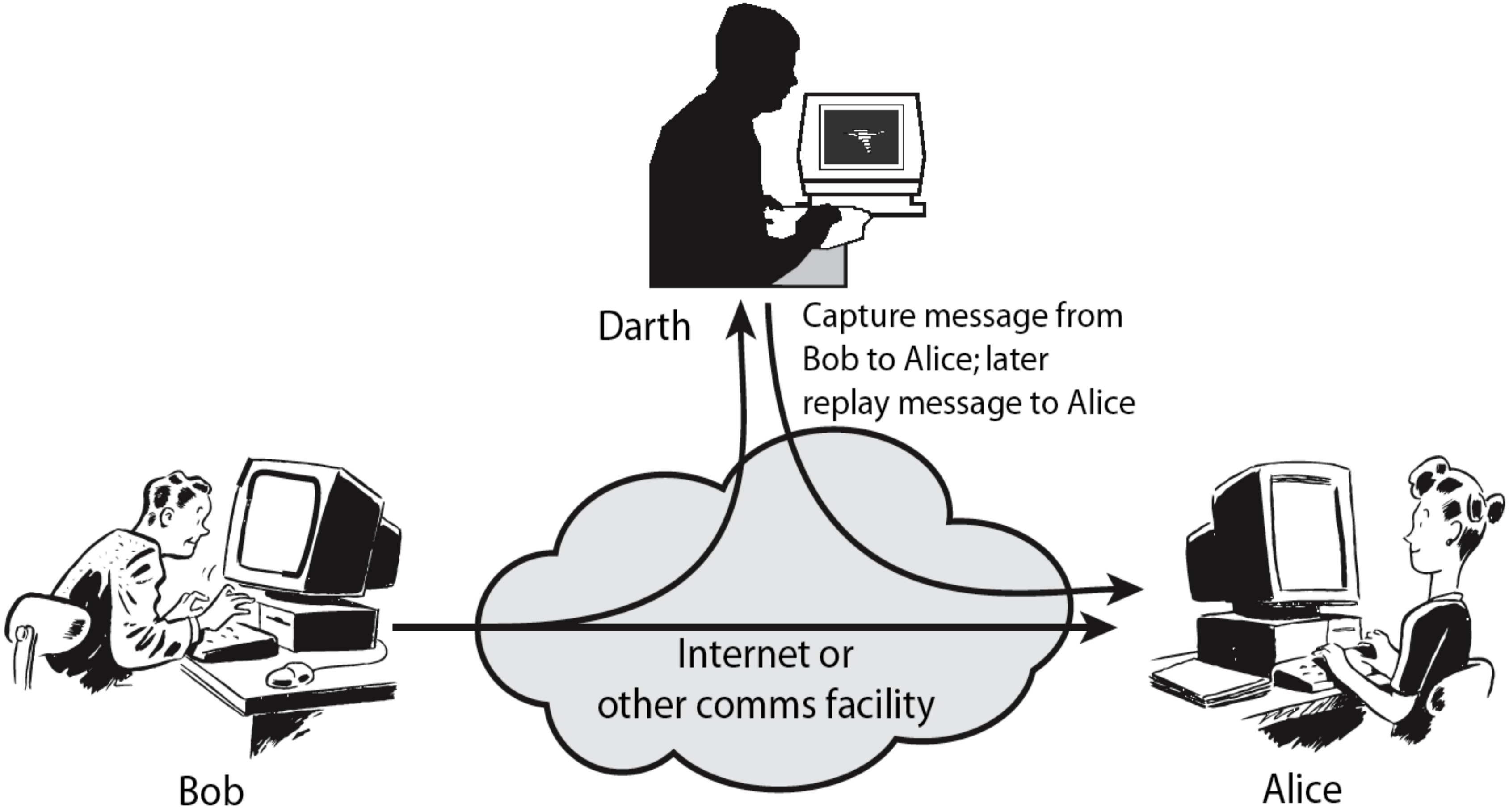
Threat and Attack

- Threat;
  - A potential for violation of security,
  - exists when there is a circumstance, capability, action or event
  - Posibble danger that might exploit a vulnerability
- Attack;
  - An assault on system security that derives from an intelligent threat

Passive Attacks


Darth
read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Active Atacks


Darth
Capture message from Bob to Alice; later replay message to Alice
Internet or other comms facility
Bob
Alice

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
  - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Properties of Security Services

- Authentication
- Access control
- Data confidentiality
- Authorization
- Data integrity
- Nonrepudation

Security Services

- X.800:

  “a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers”

- RFC 2828:

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

Security Services(X800)

- **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

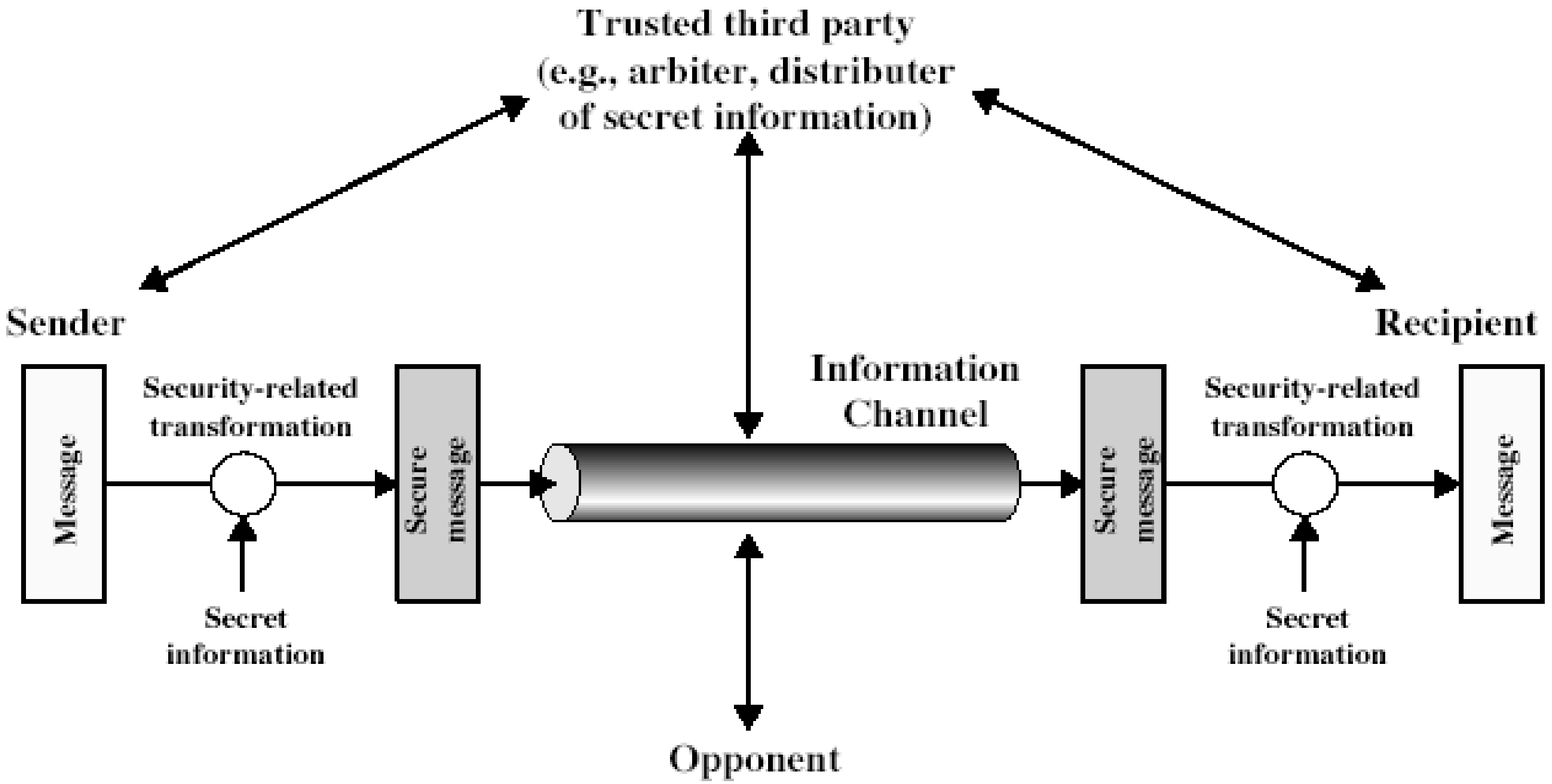
Security Mechanism

- 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**
- hence our focus on this topic

Security Mechanism(X.800)

- 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

Security model for networks

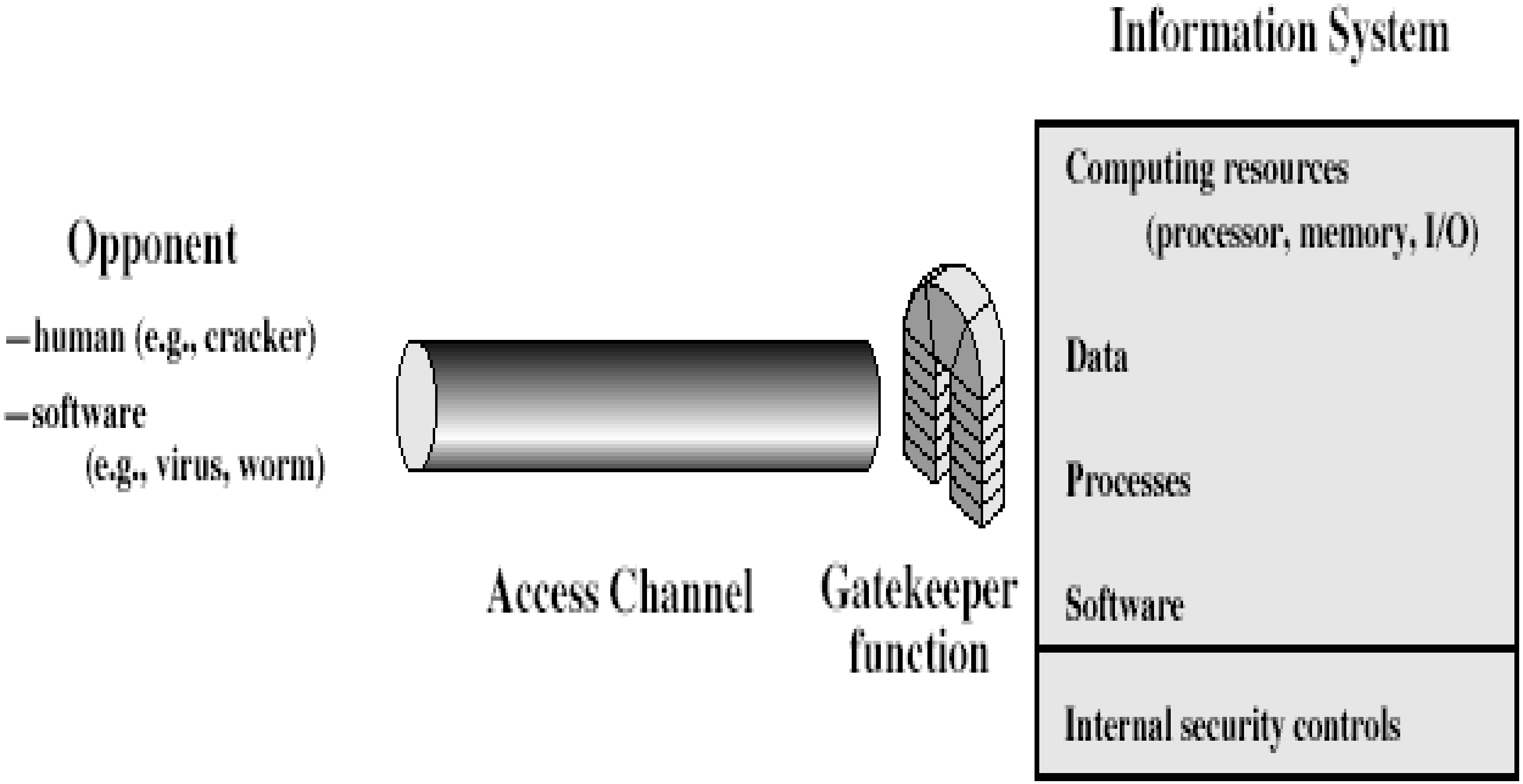


ıe

Model for Network Security

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

Model for Network Access Security



Opponent

- human (e.g., cracker)
- software (e.g., virus, worm)

Access Channel

Gatekeeper function

Information System

Computing resources (processor, memory, I/O)

Data

Processes

Software

Internal security controls

Model for Network Access 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

- specify a p 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

- trusted computer systems may be useful to help implement this model protocol enabling the principals to use the transformation and secret information for a security service