Cryptography and Network Security

What is Security ?

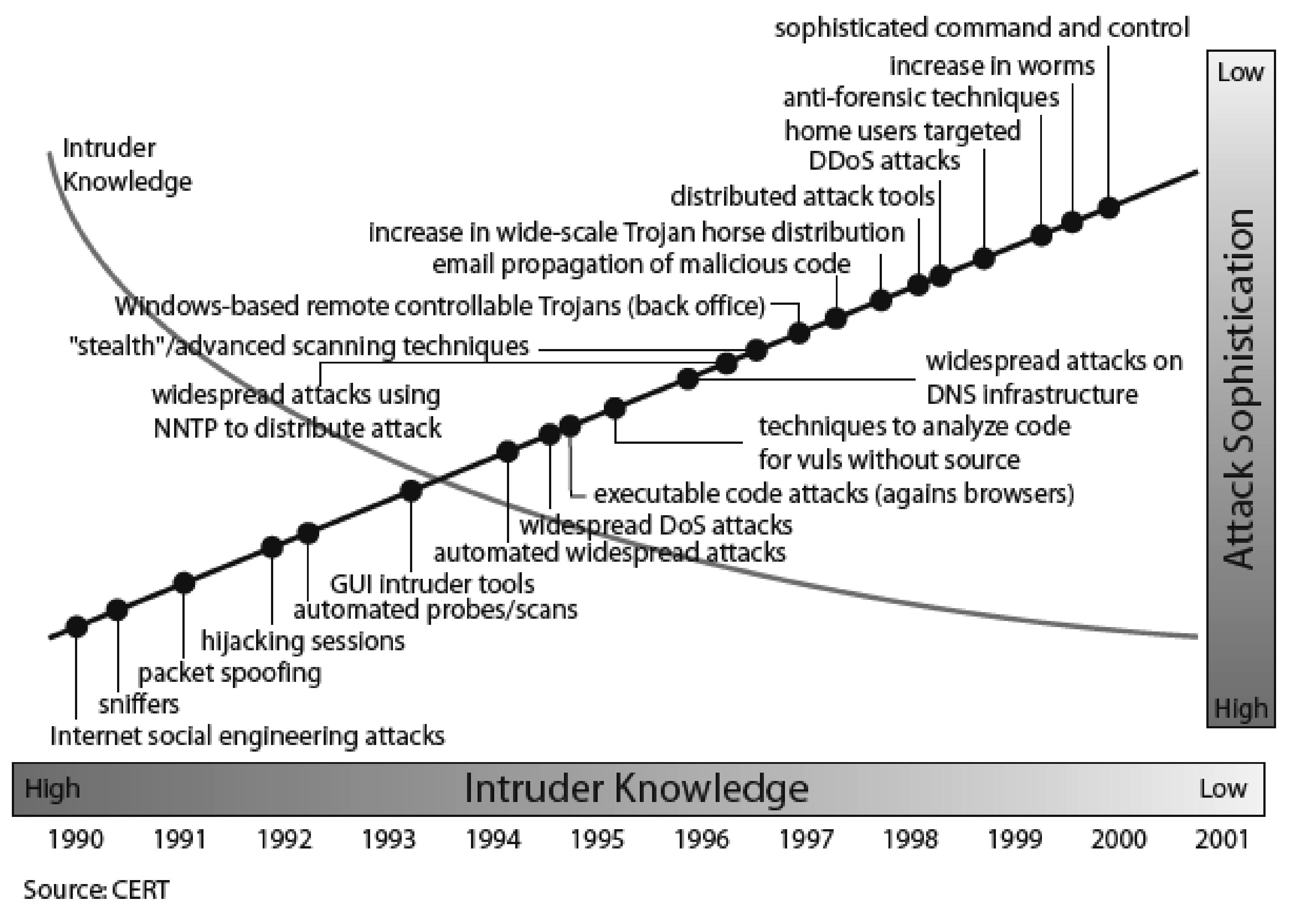
Computer Security - generic name for the collection of tools designed to protect data and to thwart hackers

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



Source: CERT

- 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

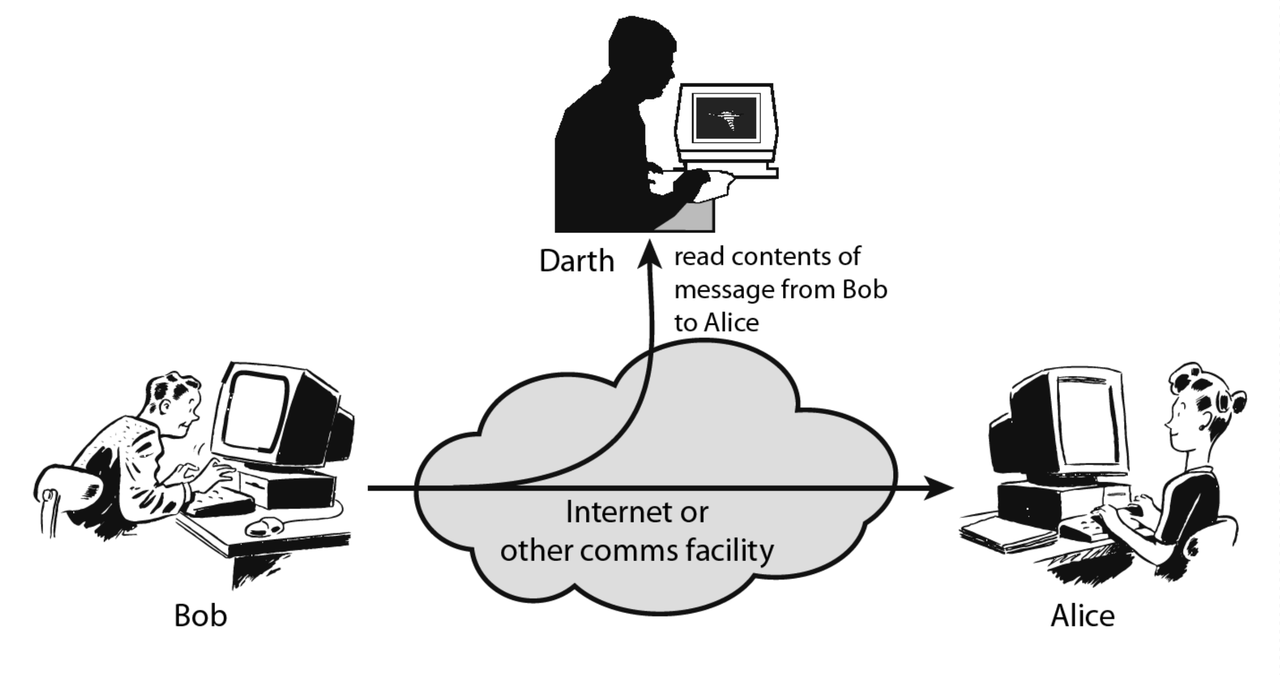
Information Security

- 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

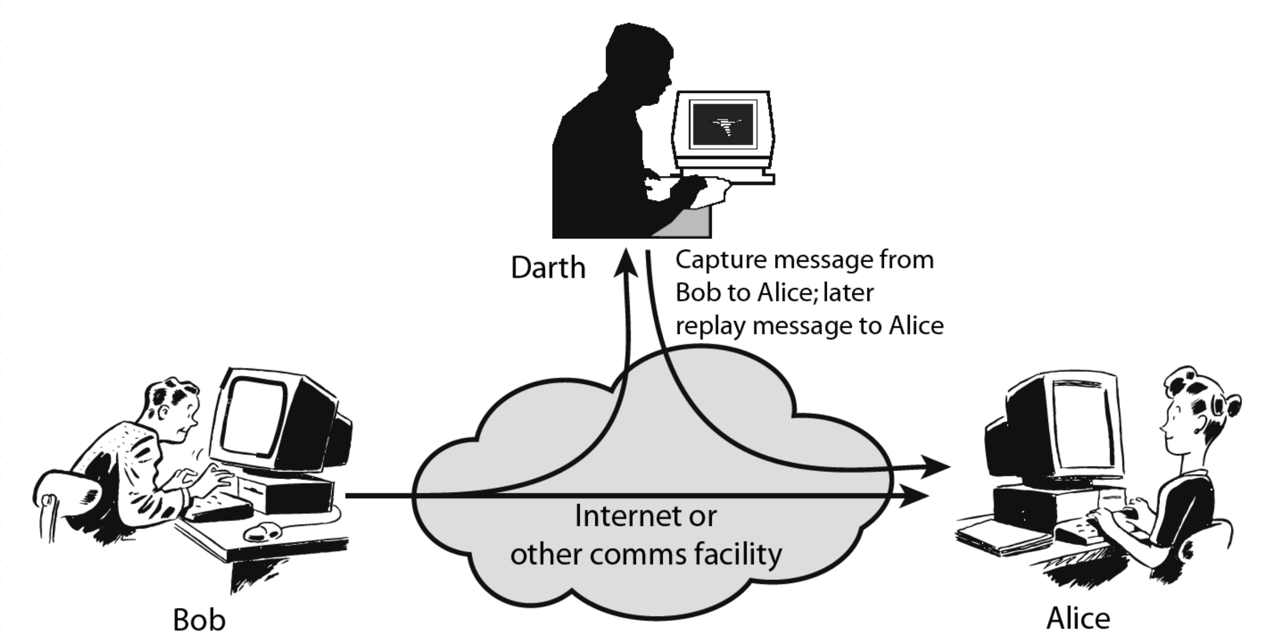
Passive Attacks


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

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


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

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.