Introduction to Security

CSS 322 – Security and Cryptography

Contents

- Terminology and Trends
- Security Services, Mechanisms and Attacks
- Who’s Who in Network Security

Terminology and Scope

- Computer Security
  - "Collection of tools designed to protect data and thwart hackers" in computer systems
- Network Security
  - Measures "to protect data during their transmission"
- Internet Security
  - Measures to protect data during their transmission over collection of interconnected networks (e.g. an internet)

- There is a lot of overlap between the above!
- This course will focus on Internet Security

Security Trends

- Reported vulnerabilities in applications, operating systems and network software have grown significantly in past 10 years
- Security incidents reported have also grown at exponential rate
  - See CERT website for latest statistics (www.cert.org)
- Attacks are becoming more sophisticated, but easier to perform
  - The Internet (and computers on Internet) has enabled these changes, and become target of attack

Aspects of Security

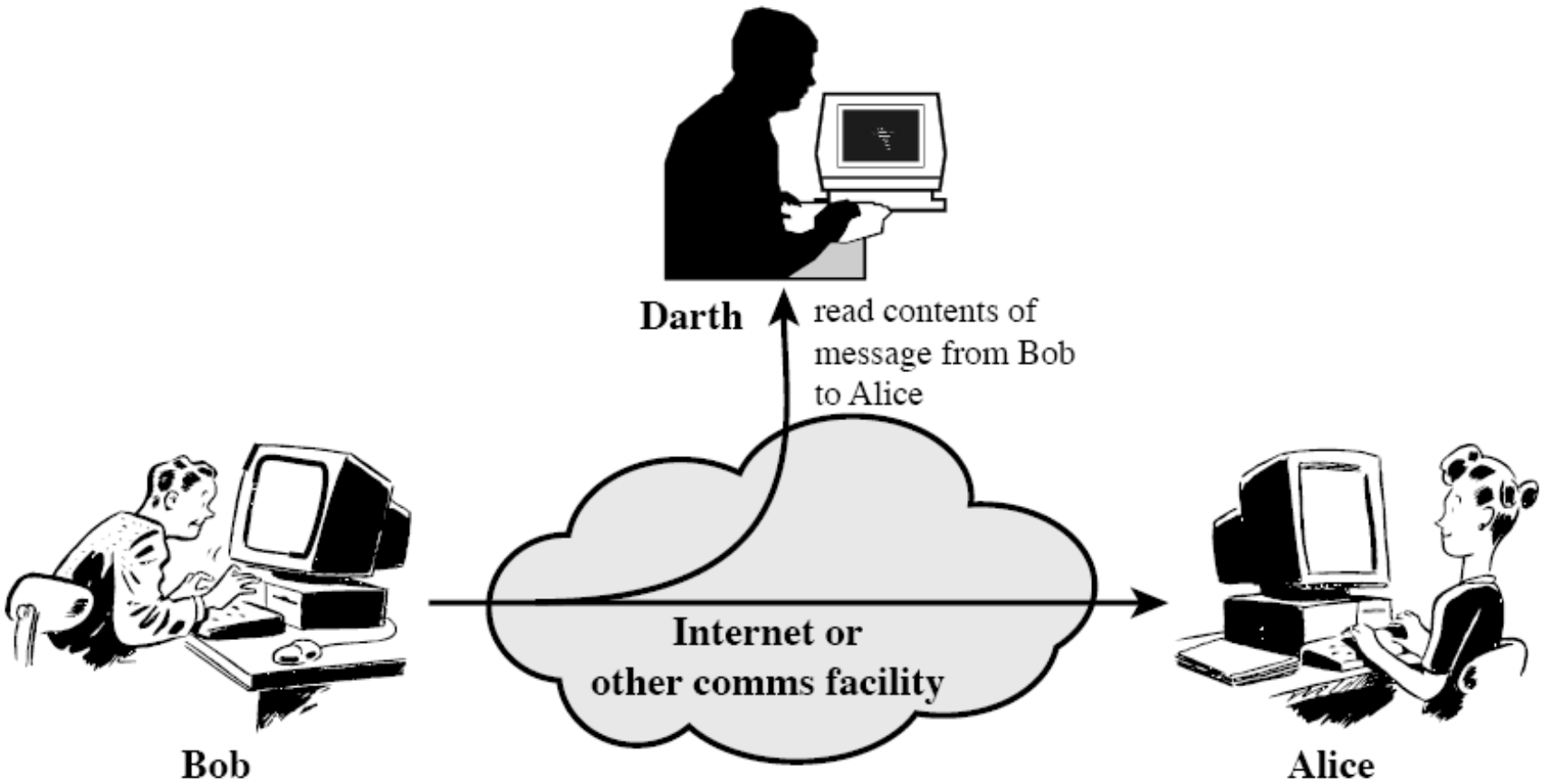
- Need a systematic approach to describing requirements and characteristics of computer/network security
  - ITU-T X.800 Security Architecture for OSI provides conceptual description of a security architecture
  - X.800 focuses on 3 aspects of security

1. Security Attack
   - Any action that attempts to compromise the security of information or facilities
2. Security Mechanism
   - A method of preventing, detecting or recovering from an attack
3. Security Service
   - Uses security mechanisms to enhance the security of information or facilities in order to stop attacks

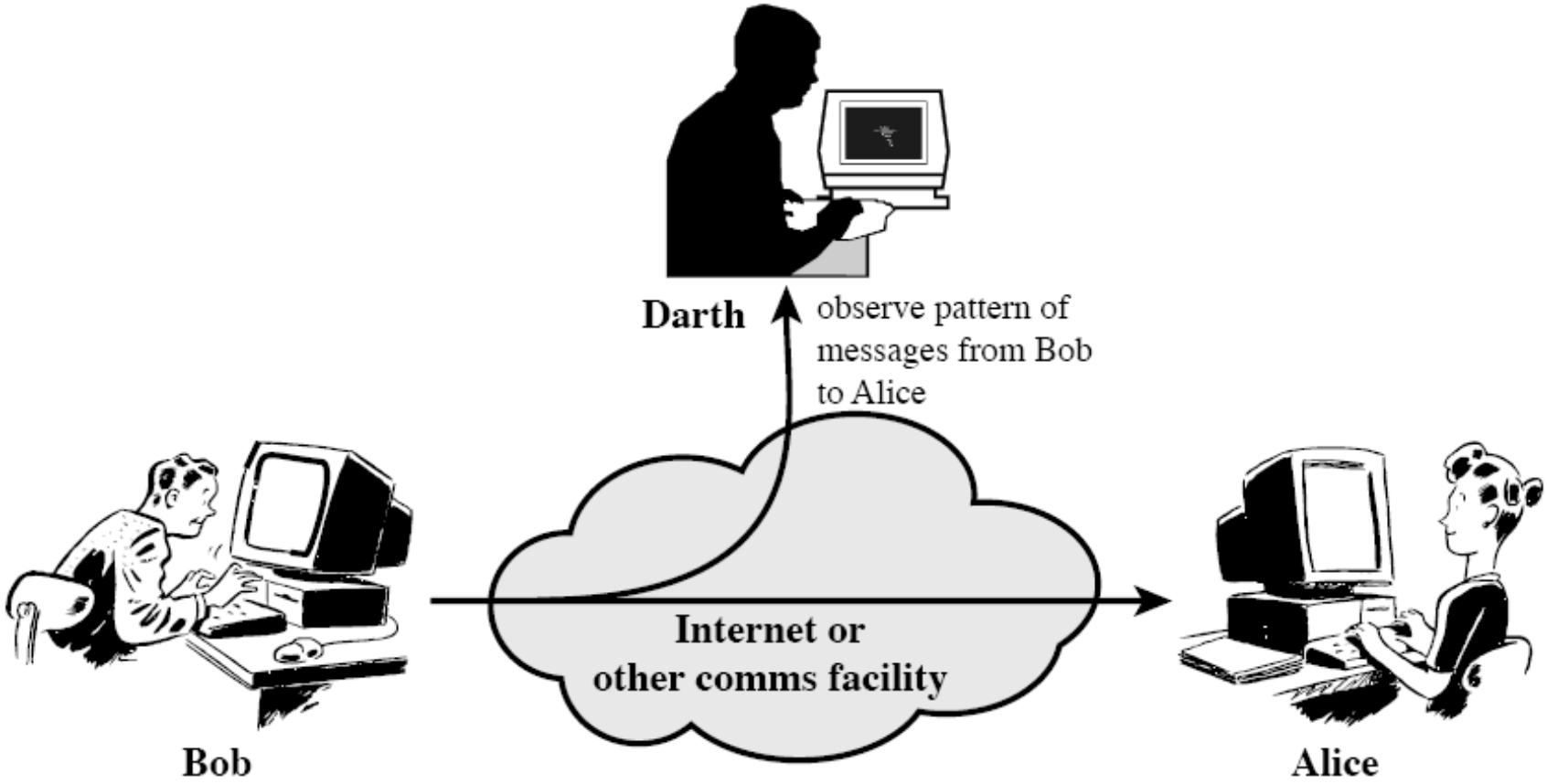
Security Attacks

- Passive Attacks
  - Make use of information, but not affect system resources
  - Eavesdropping or monitoring transmissions of information
    - Release message contents
    - Traffic analysis
  - Relatively hard to detect, but easier to prevent
- Active Attacks
  - Alter system resources or operation. Four sub-types:
    - Masquerade: pretend to be someone else
    - Replay: retransmission of captured information
    - Modification: change message contents
    - Denial of service: reduce the availability of resources
  - Relatively hard to prevent, but easier to detect
    - (Ability to detect may act as a deterrent or prevent attacks)

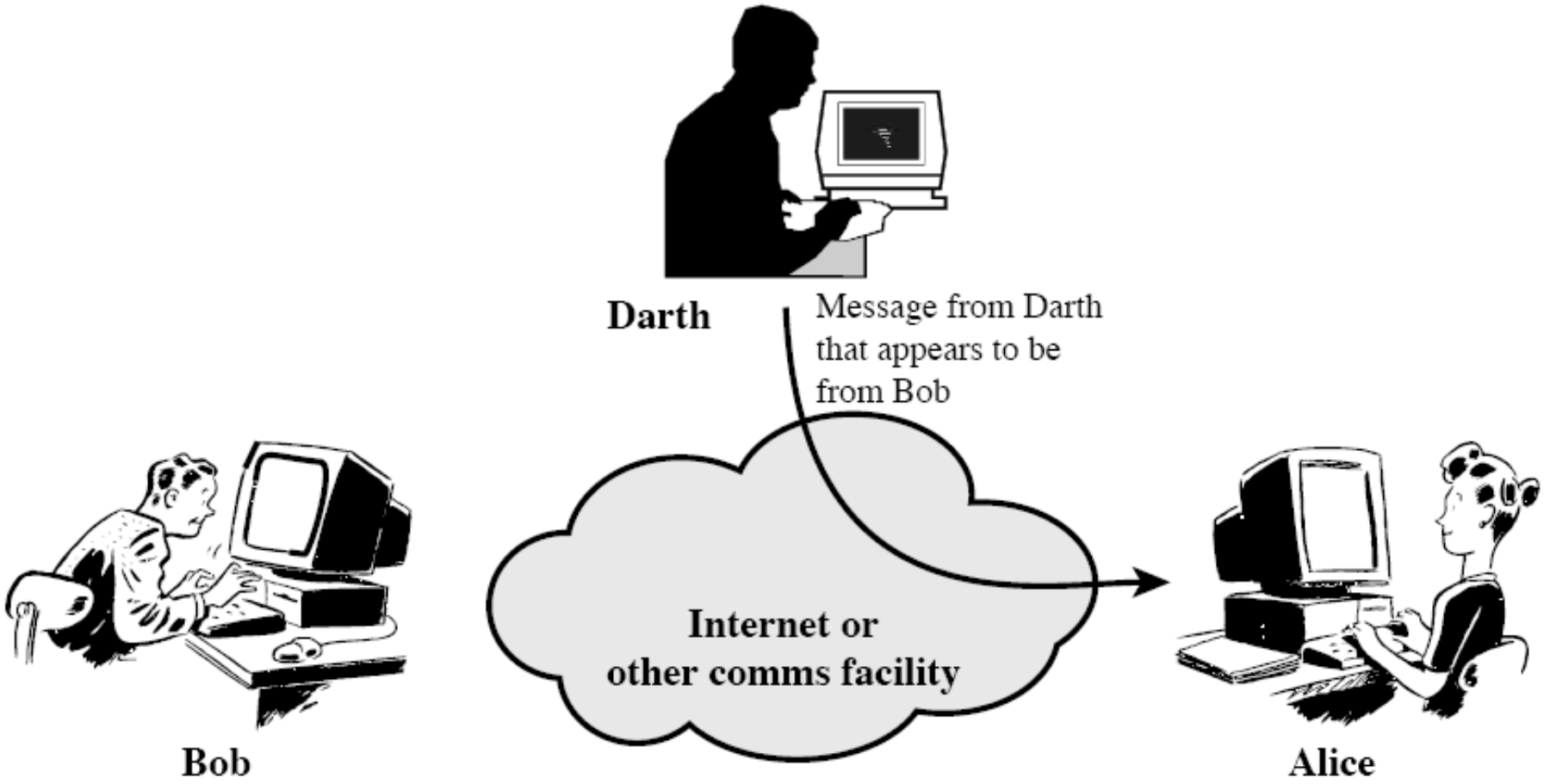
Passive: Release Message Contents



Passive: Traffic Analysis



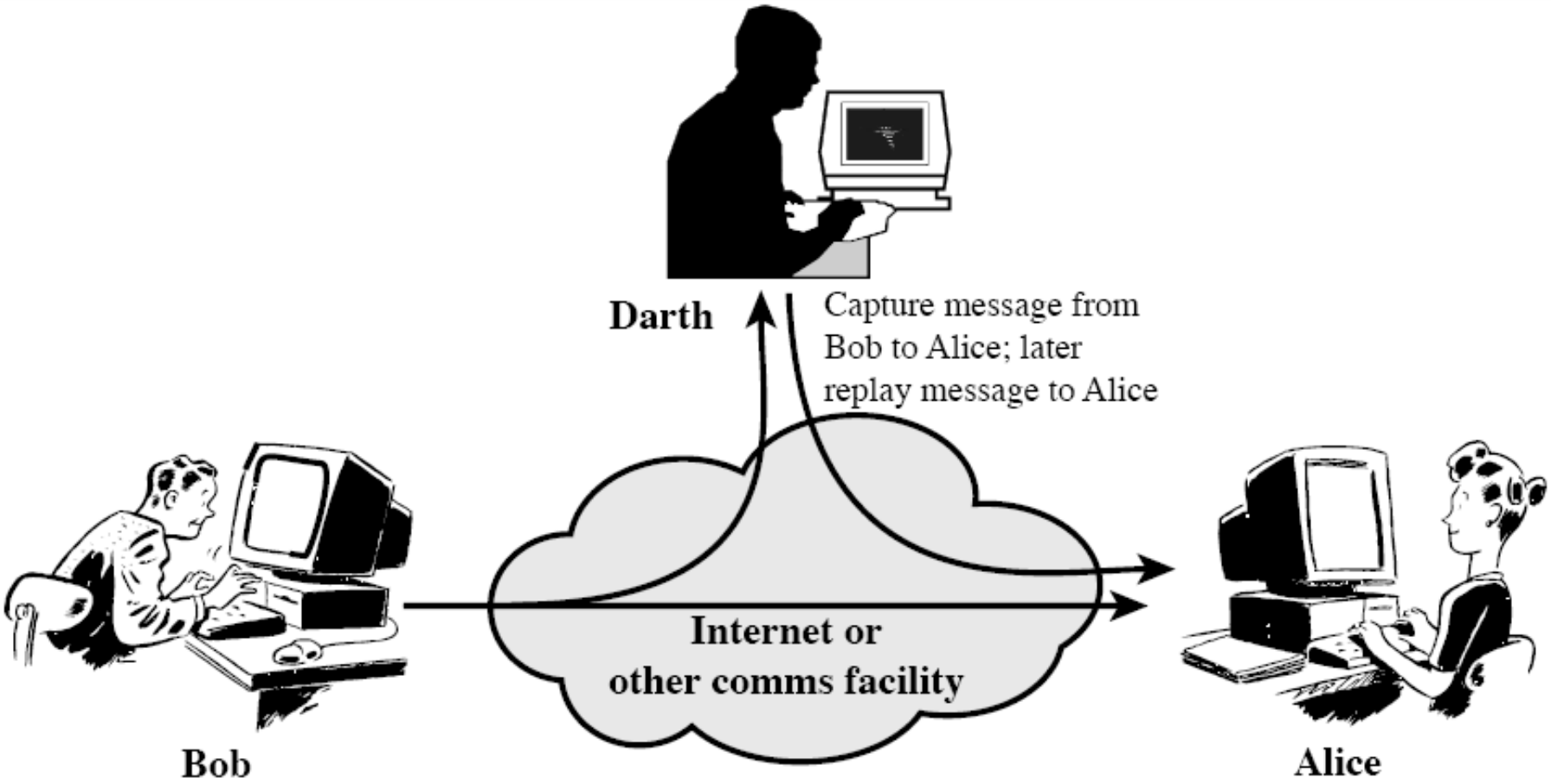
Active Attack: Masquerade



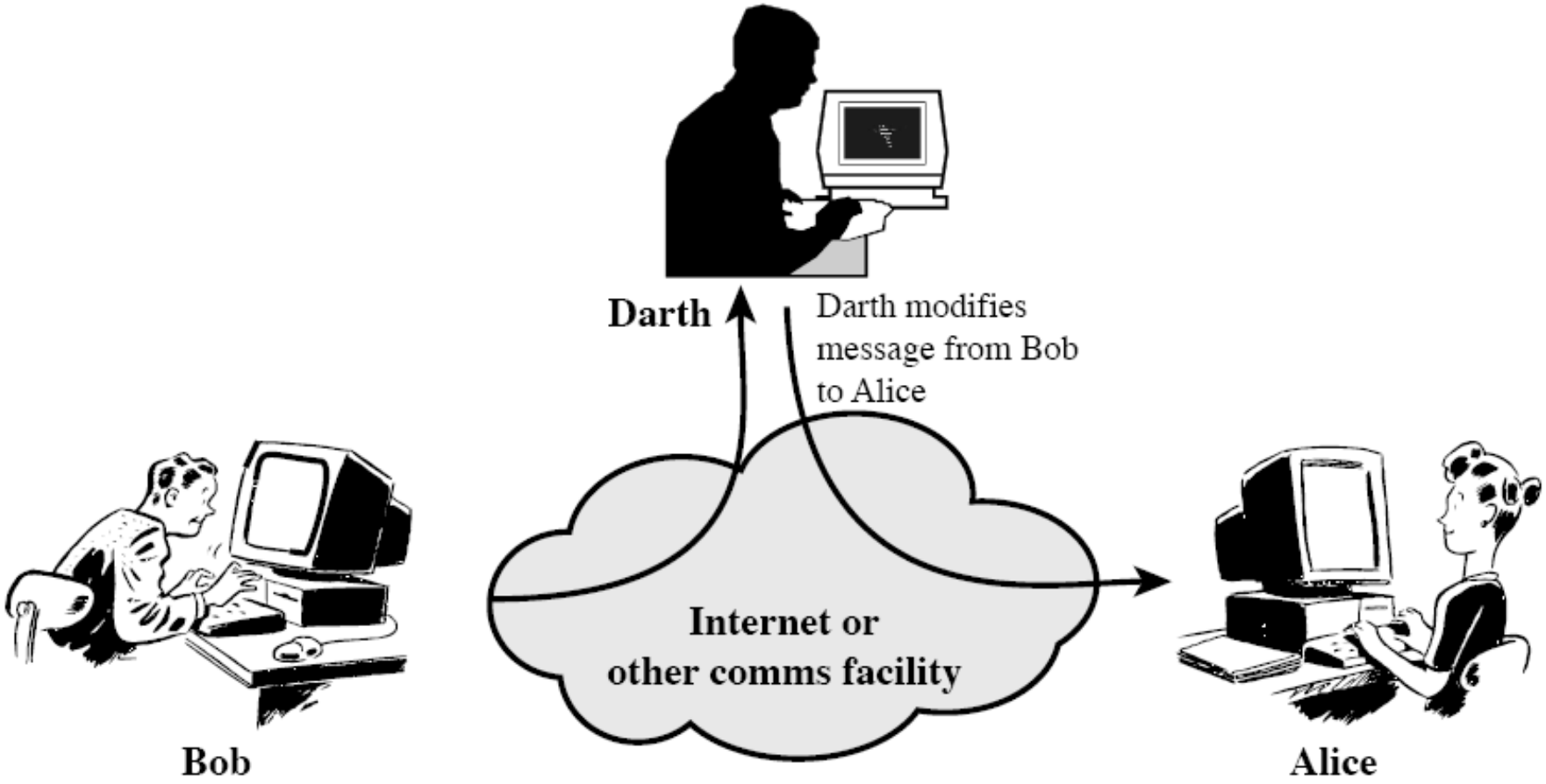
“On the Internet, nobody knows if you’re a dog”

“On the Internet, nobody knows you’re a dog.”

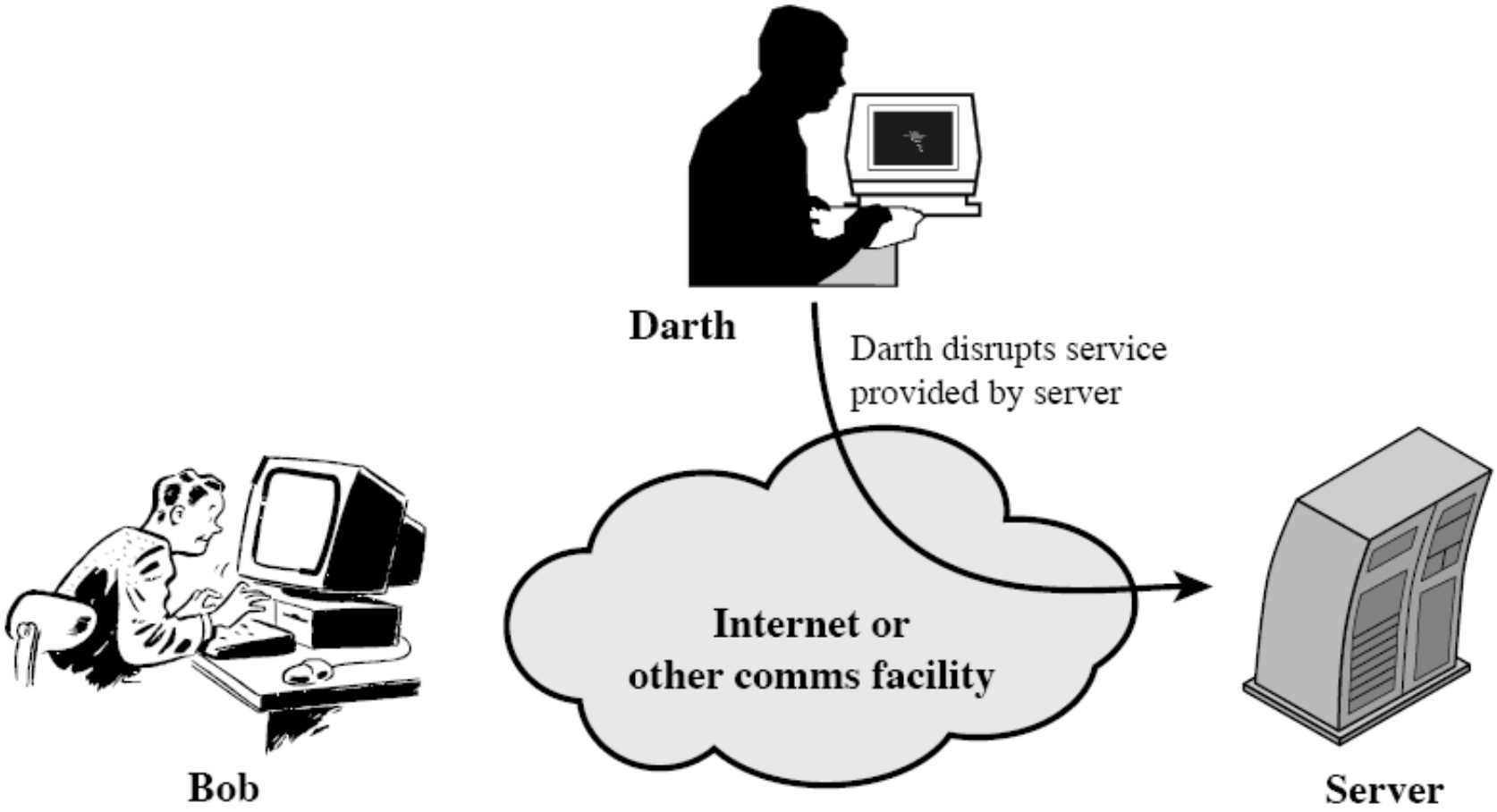
Active Attack: Replay



Active Attack: Modification



Active Attack: Denial of Service



Security Services

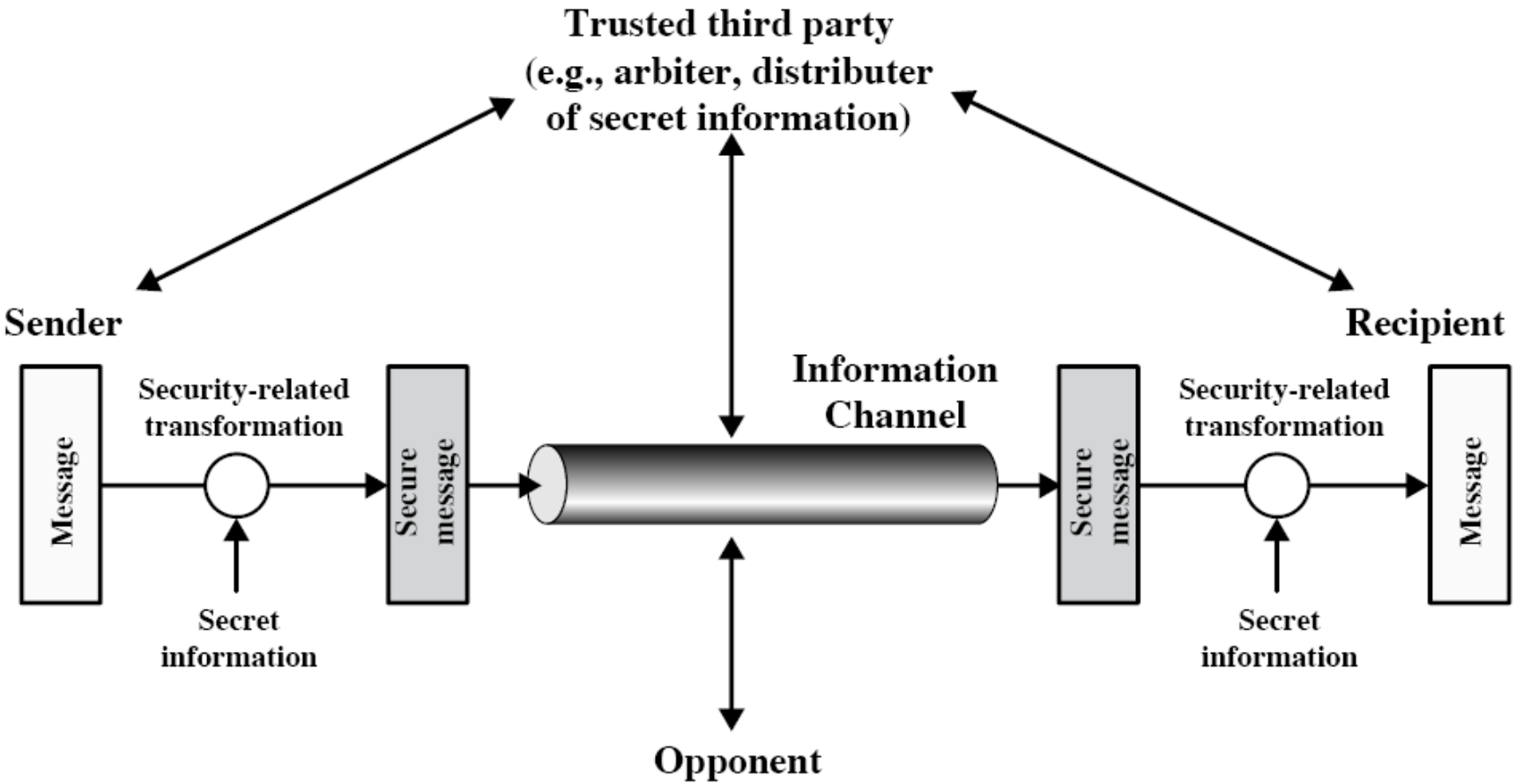
- RFC2828:
  - “A processing or communication service that is provided by a system to give a specific kind of protection to system resources”
- Can be classified as:
  - *Authentication*: assure that the communication and the communicating entities are authentic, e.g. a warning signal is real; a person is who they claim to be
  - *Access Control*: limit and control access to computers, network resources and applications
  - *Data Confidentiality*: protect data from passive attacks; privacy of communications
  - *Data Integrity*: assure data sent is not duplicated, modified, inserted, replayed, deleted, …
  - *Nonrepudiation*: prevent sender or receiver from denying a message has been sent
  - *Availability Service*: protect system so it is available for intended purpose

Security Mechanisms

- Techniques available for implementing services to prevent or detect attacks
- Selected X.800 mechanisms (and examples):
  - Encipherment/encryption (symmetric and public key)
  - Access Control (firewall)
  - Data Integrity (message digests, digital signatures)
  - Authentication Exchange (certification authorities)
  - Notarisation (signatures, timestamps, witnesses)
- We cover these mechanisms in later topics

Model for Network Security

- Simple model of most security systems we will cover



Who's Who in Security

- Standards
  - ITU, ISO and IEC: International standards including OSI
  - IETF: Internet standards
  - NIST: US standards
  - TISI: Thai Industrial Standards Institute
- Certification
  - (ISC)2: Certified Information System Security Professional (CISSP)
  - SANS: GIAC Security Engineer
  - CompTIA: Security+
- Warning and Response
  - CERT (Computer Emergency Response Team)
    - US-CERT, ThaiCERT, …
- Certificates
  - Verisign, Entrust, CAcert, …
- Products and Solutions
  - RSA, Cisco, Juniper, Symantec, McAfee, …