Security

Note:

These slides are created using information from.

Network Security Essentials by William Stallings

Computer Networking, A top-down approach by James F.Kurose and Keith W.Ross

Maximum Security by Anonymous

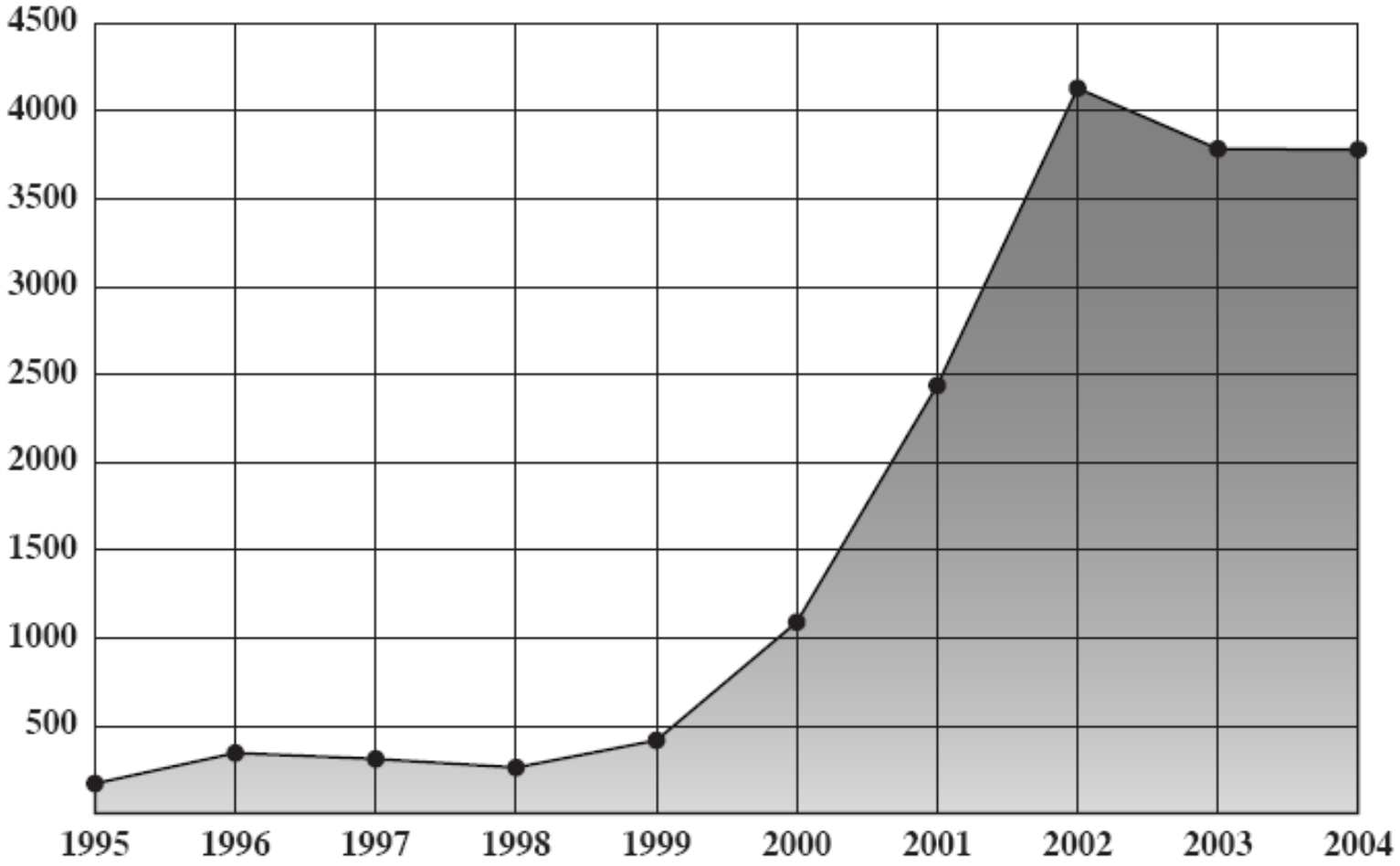
Lectures and Notes from my teacher Svend Mortensen

Chapter 1 – Introduction

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our own readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable.

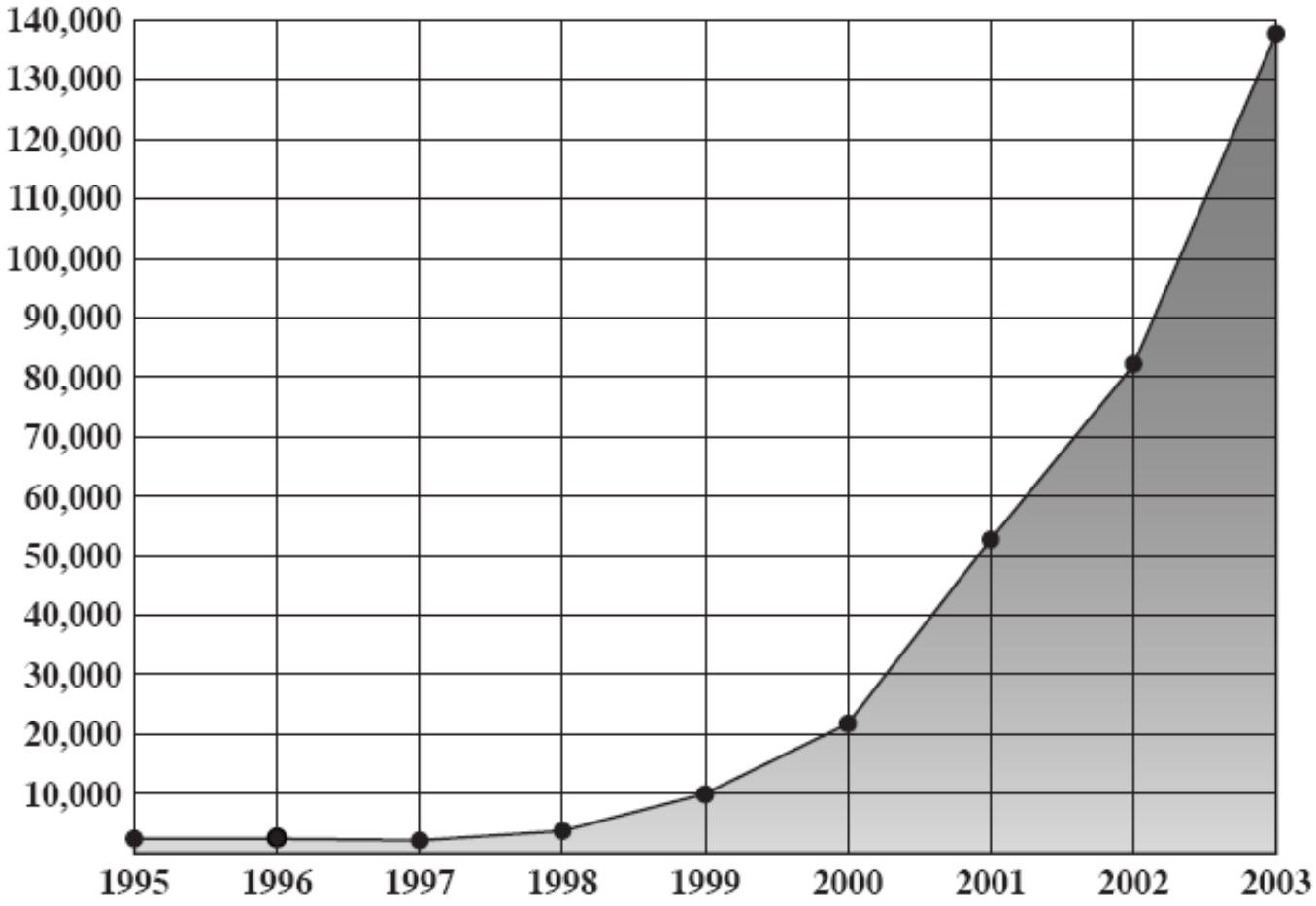
***—The Art of War,* Sun Tzu**

CERT statitics



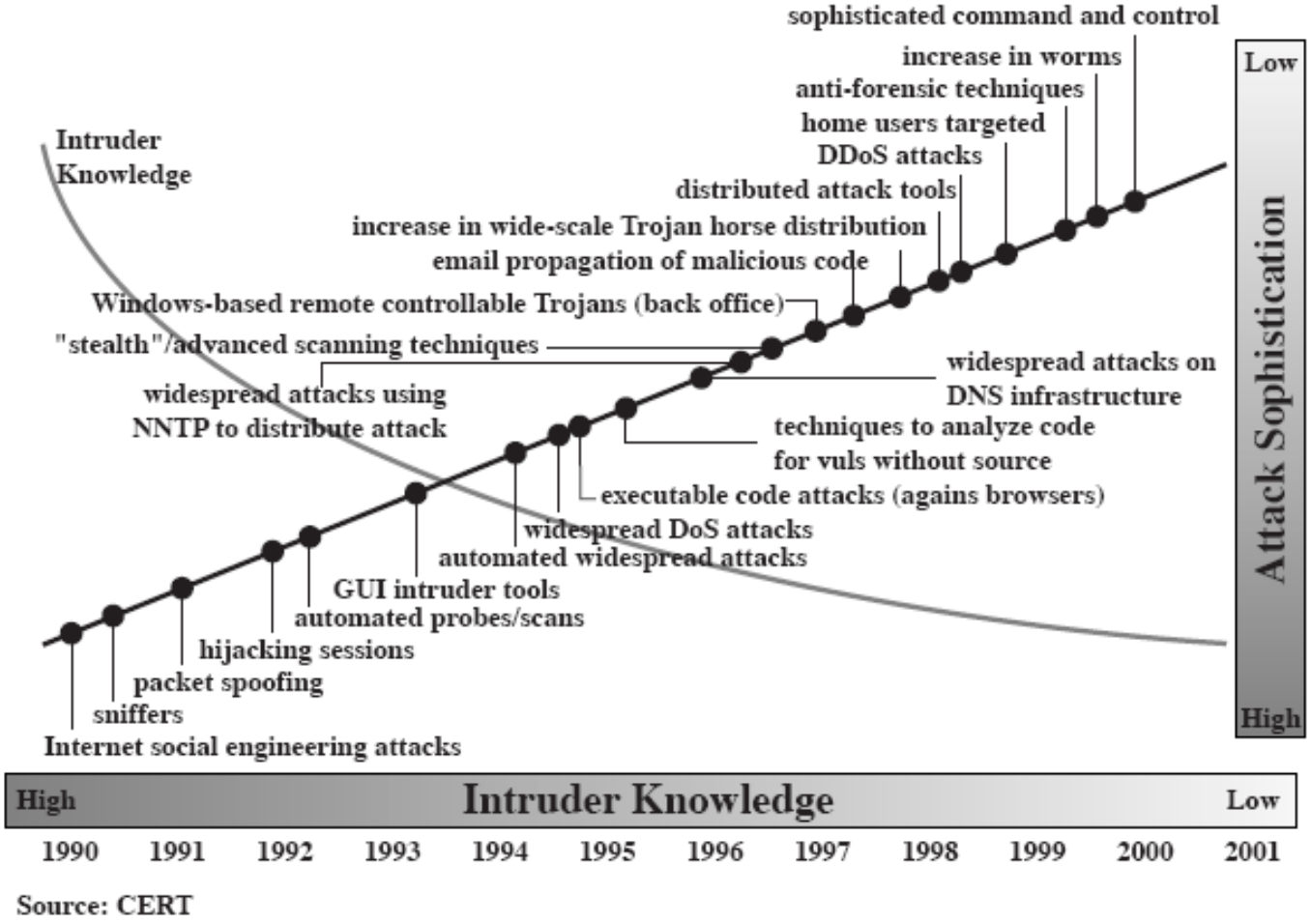
(a) Vulnerabilities reported

CERT statitics - incidents



(b) Incidents reported

Trends in attack sophistication



Source: CERT

Figure 1.2 Trends in Attack Sophistication and Intruder Knowledge

Background

- 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

Definitions

- **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

Information security

- Assets
- Threats
- Attacks
- Vulnerabilities
- Controls

Security Components

Also known as security goals, objectives, etc.

- Primary Security Goals (CIA-properties)
  - Confidentiality
  - Integrity
  - Availability

Security Components

- Other goals frequently listed
  - Authenticity
    - Requests or information are authentic and authenticated
    - Resources (both hardware and software) are genuine
- Accountability/Non-Repudiation
  - Actions can be traced back to a single entity
    - People can be made responsible for their actions
- Privacy (privacy families defined by Common Criteria)
  - Pseudonymity, unlinkability, anonymity, unobservability
  - Usually in conflict with authentication and accountability
  - But latest crypto allows for privacy-friendly authentication + accountability

Confidentiality

- Preventing unauthorized observation of information or resources (keeping secrets secret)
  - War-plans, business strategies, client confidentiality (doctors, priests, lawyers, banks)
- Particularly important in military information security
  - Security models, policies and mechanisms developed to enforce the need-to-know principle
- Confidentiality can be ensured with cryptography
  - A cryptographic key is used to scramble (encrypt) data so that unauthorized entities cannot read it
  - Authorized entities have access to a cryptographic key so that they can restore (decrypt) data to its original form
- Access control mechanisms protect data from unauthorized access
- Confidentiality may extend to protect knowledge about the
- existence of information or resources

Integrity

- Preventing unauthorised modification of information or resources
  - Data integrity pertains to the content of the information
  - *Origin integrity pertains to the source of the information*
    - *Origin integrity implies* ***authentication*** of the source of the information
- Two classes of integrity mechanisms:
  - Prevention mechanisms
    - *Prevents data from being modified in unauthorized ways.*
  - Detection mechanisms
    - *Detects unauthorized modification of data*
- Integrity is often more important than confidentiality in commercial information systems

Availability

- Availability means that the systems information and resources are available to authorized users when they need them
- Attacks against availability
  - *Denial-of-Service* (DoS)
- Availability is difficult
- Difficulties in ensuring availability include:
  - Difficult to distinguish between high load and DoS

Threat

- A threat is a potential violation of security
  - Often a three step process
    - threat -> vulnerability **->** attack (exploit)
- Four classes of threats:
  - Disclosure (unauthorised access to information)
  - Deception (acceptance of false data)
  - Disruption (interruption or prevention of correct operation)
  - Usurpation (unauthorised control of (part of) the system)
- Five ways to deal with the effects of exploits:
  - Prevention (remove all vulnerabilities)
  - Deterrence (making exploits difficult – *but not impossible*)
  - Deflection (make other targets relatively more attractive)
  - Detection (as they happen or after the fact – *forensics*)
  - Recovery (restore the system to a usable state)

Services, Mechanisms, Attacks

- need systematic way to define requirements
- consider three aspects of information security:
  - **security attack**
  - **security mechanism**
  - **security service**

Security Service

- is something that enhances the security of the data processing systems and the information transfers of an organization
- intended to counter security attacks
- make use of one or more security mechanisms to provide the service
- replicate functions normally associated with physical documents
  - eg have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

Security Mechanism

- a mechanism that is designed to detect, prevent, or recover from a security attack
- no single mechanism that will support all functions required
- however one particular element underlies many of the security mechanisms in use: **cryptographic techniques**
- hence our focus on this area

Security Attack

- 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
- have a wide range of attacks
- can focus of generic types of attacks
- note: often *threat* & *attack* mean same

Security Attacks

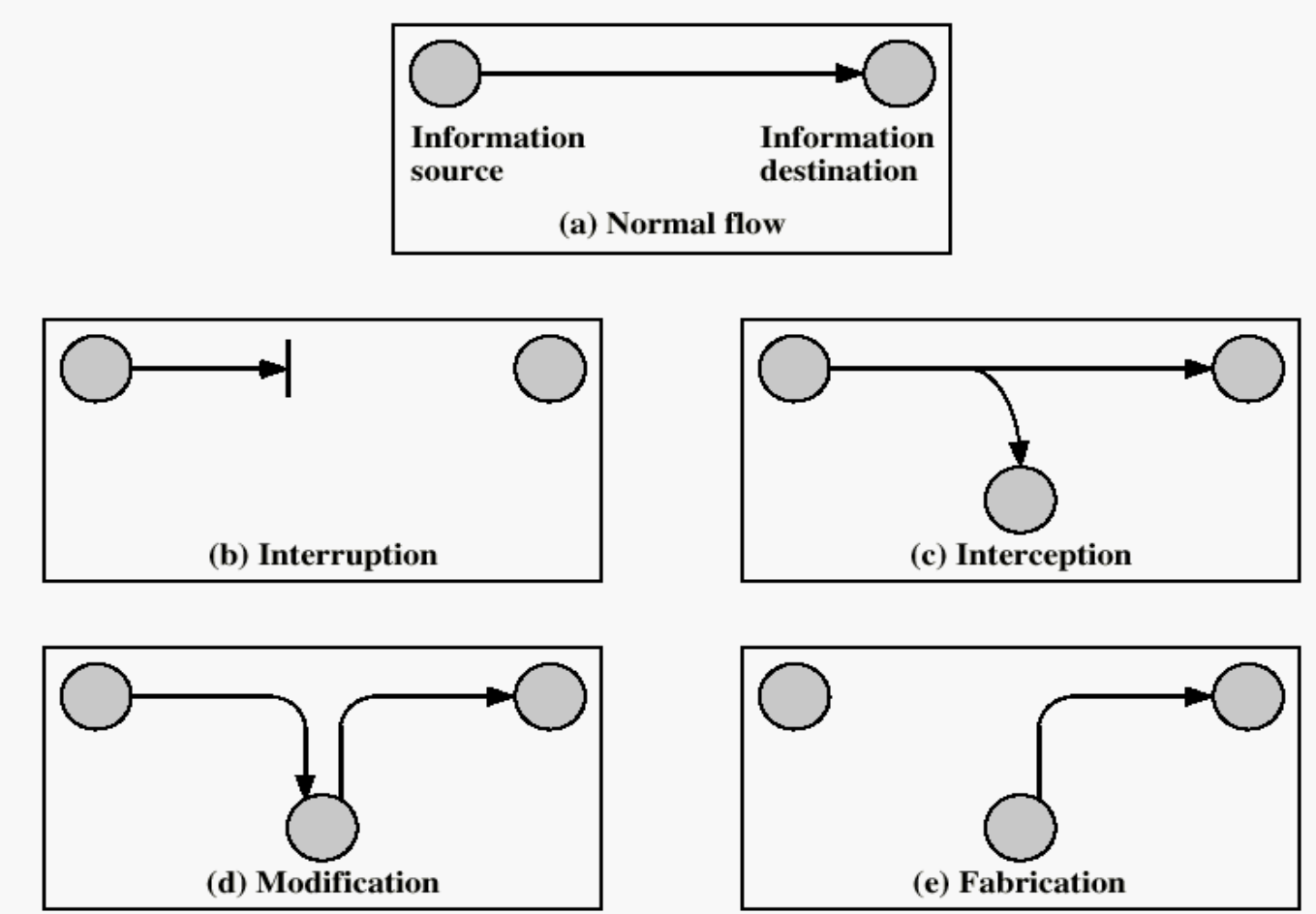


Figure 1.1 Security Threats

Attackers

- Insiders
  - Disgruntled employees
  - Guests, consultants, contract workers …
- Crackers (*hackers*)
  - Technically knowledgeable programmers
  - Script-Kiddies (*cracker wannabes*)
- Spies (*industrial and military*)
  - Technical knowledge, technical means, many resources
- Criminals (*thieves, organized crime*)
  - Technical knowledge, technical means, many resources
- Terrorists

Means of Attackers

- Insiders
  - Knowledge of system configuration, network topologies, processes,…
  - Only computing resources provided by organization
- Crackers (*hackers*)
  - Able to adapt tools to configuration of target
  - Able to write new tools/exploits
  - Few computing resources (apart from bot-nets)
- Script-Kiddies (*cracker wannabes*)
  - Can only use tools provided by others

Means of Attackers

- Spies (*industrial and military*)
  - Technical knowledge, rich computing resources, other resources
- Criminals (*thieves, organized crime*)
  - Technical knowledge, technical means, many resources
- Terrorists
  - Probably between spies and script-kiddies, but nothing is known

OSI Security Architecture

- 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

Security Services

- **X.800** defines it as: a service provided by a protocol layer of communicating open systems, which ensures adequate security of the systems or of data transfers
- **RFC 2828** defines it as: a processing or communication service provided by a system to give a specific kind of protection to system resources
- X.800 defines it in 5 major categories

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

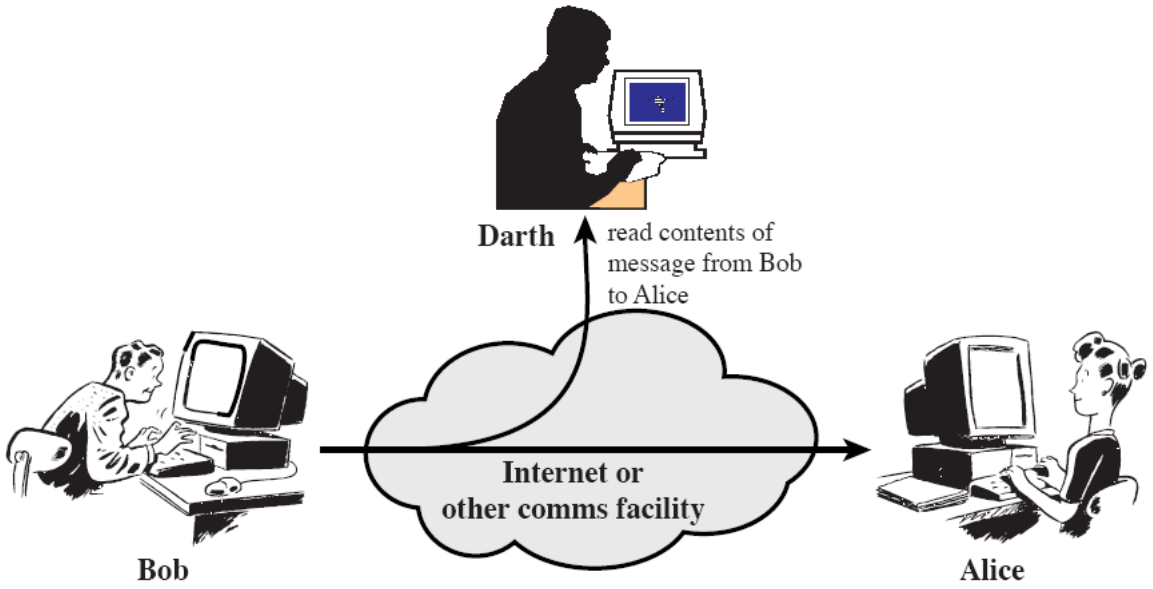
Security Mechanisms (X.800)

- 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

Classify Security Attacks as

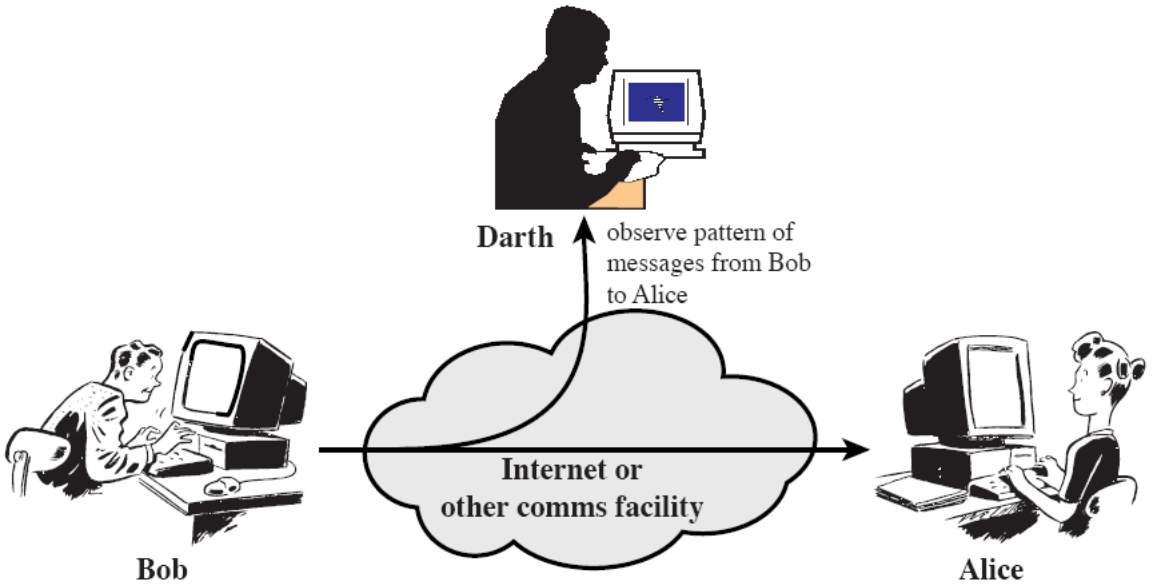
- **passive attacks** - eavesdropping on, or monitoring of, transmissions to:
  - obtain message contents, or
  - monitor traffic flows
- **active attacks** – modification of data stream to:
  - masquerade of one entity as some other
  - replay previous messages
  - modify messages in transit
  - denial of service

Passive attacks 1



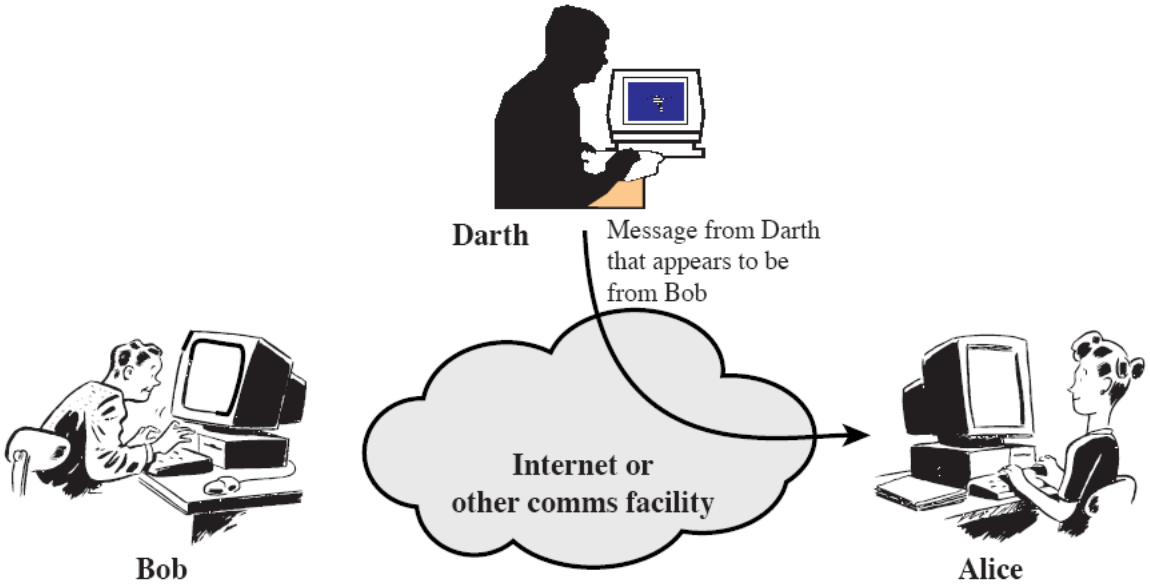
(a) Release of message contents

Passive attacks 2



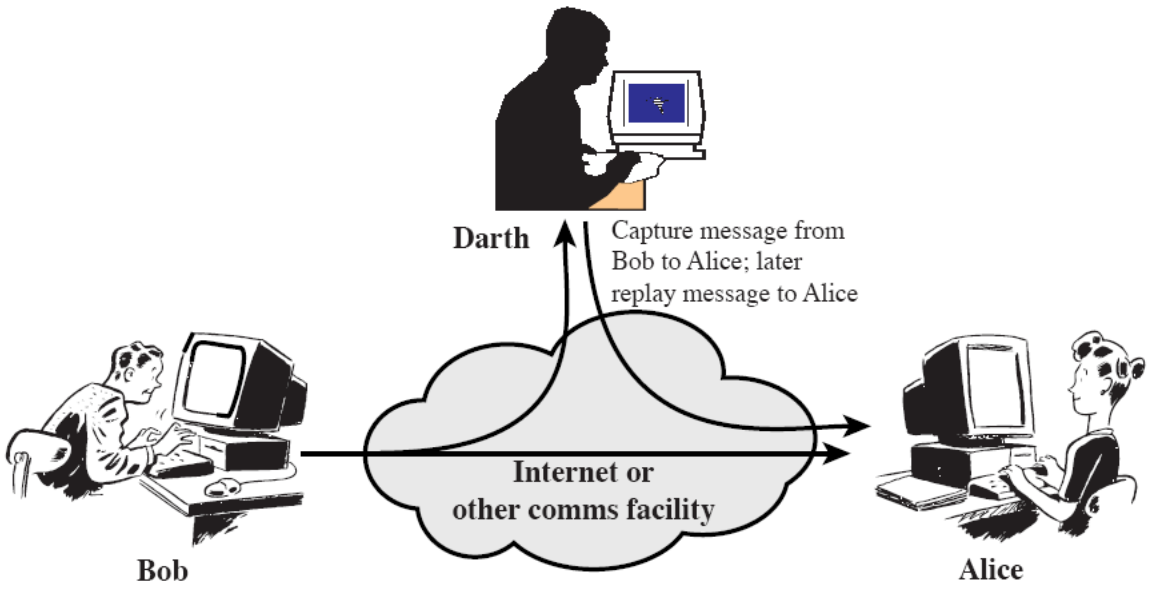
(b) Traffic analysis

Active attacks



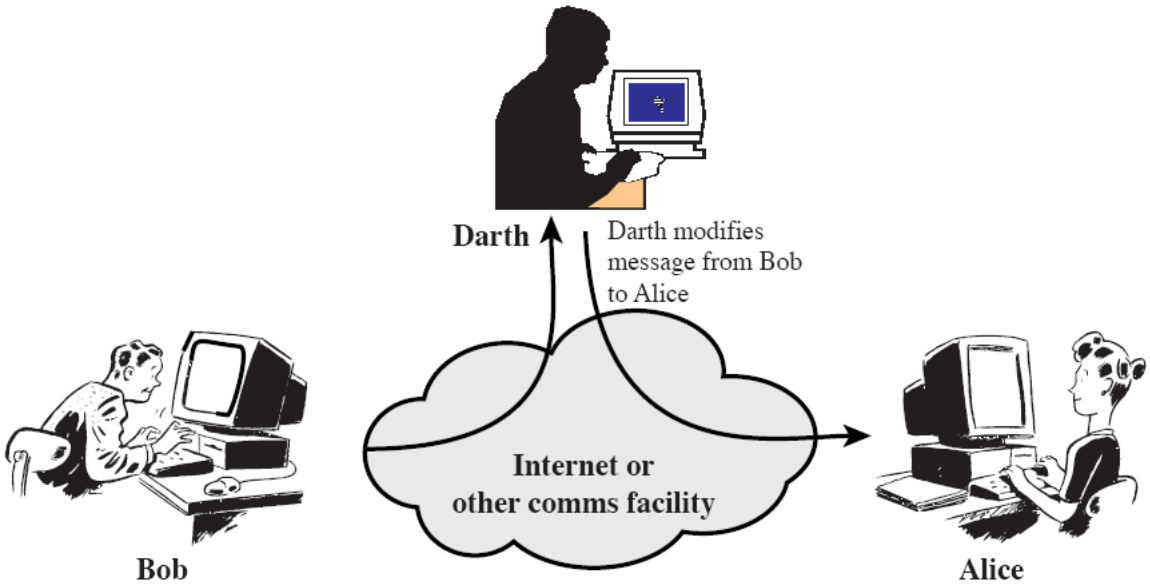
(a) Masquerade

Active attacks 2



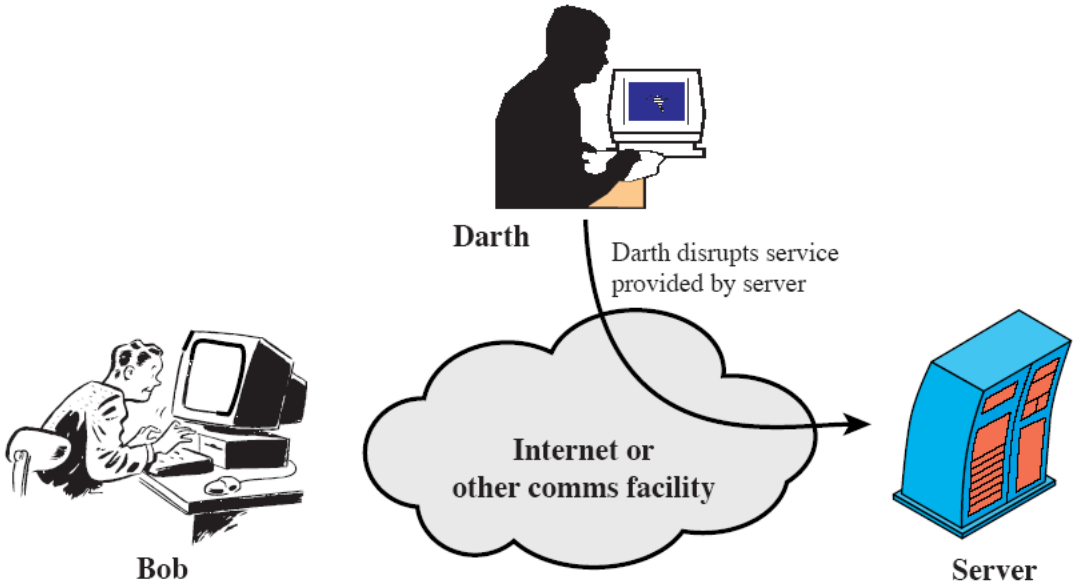
(b) Replay

Active attacks 3



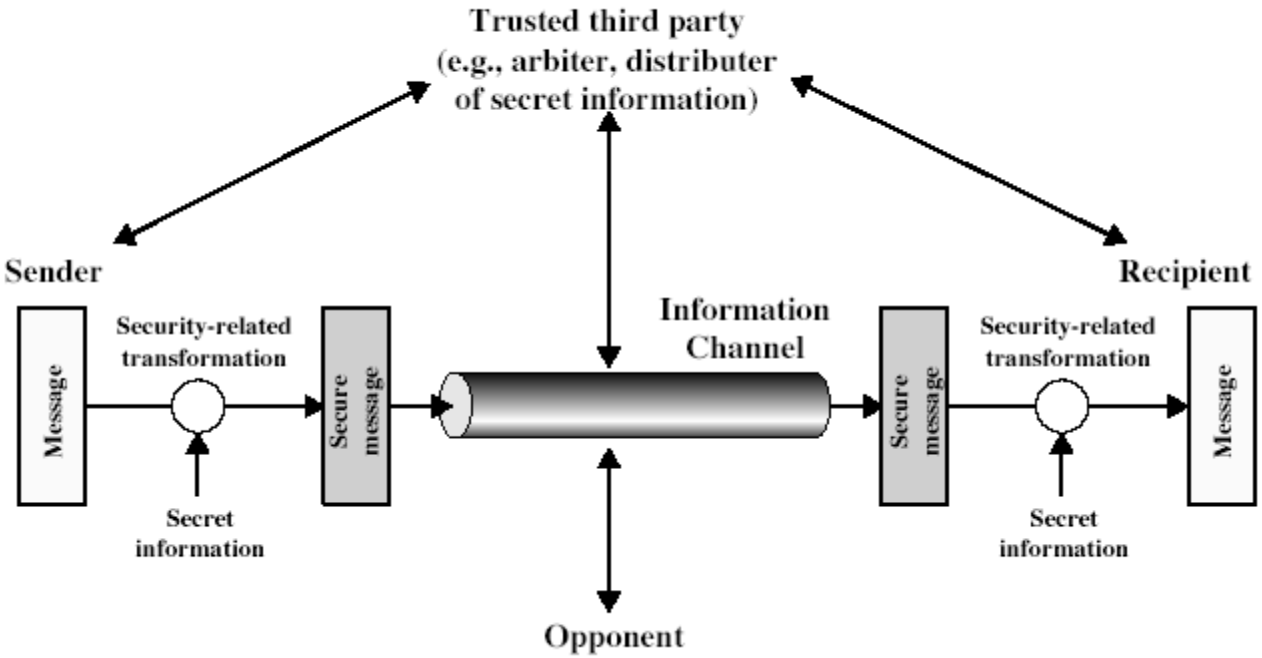
(c) Modification of messages

Active attacks 4



(d) Denial of service

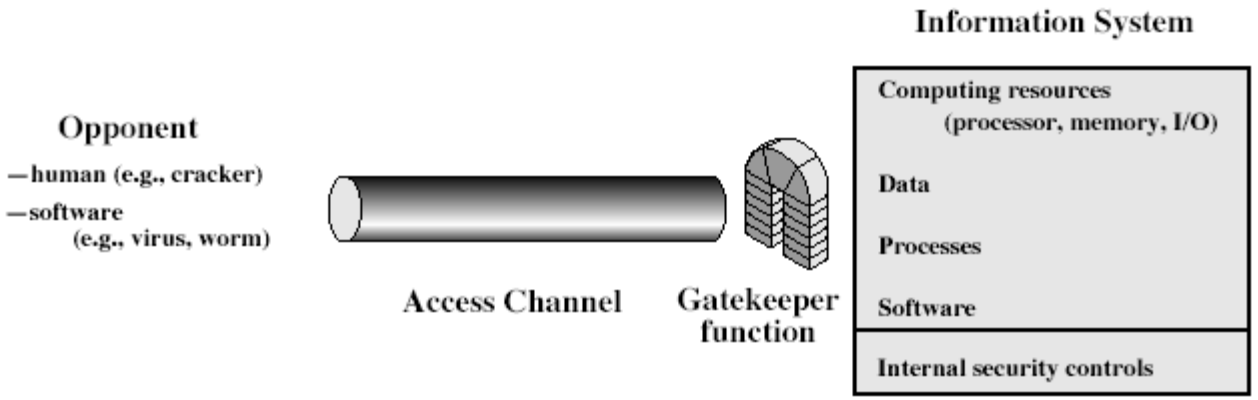
Model for Network Security



Model for Network Security

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

Model for Network Access Security



Model for Network Access Security

- using this model requires us to:
  - select appropriate gatekeeper functions to identify users
  - implement security controls to ensure only authorised users access designated information or resources
- trusted computer systems can be used to implement this model

Summary

- have considered:
  - computer, network, internet security
  - security services, mechanisms, attacks
  - X.800 standard
  - models for network (access) security