

CRYPTOGRAPHY AND NETWORK SECURITY

UNIT 1

Unit 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

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

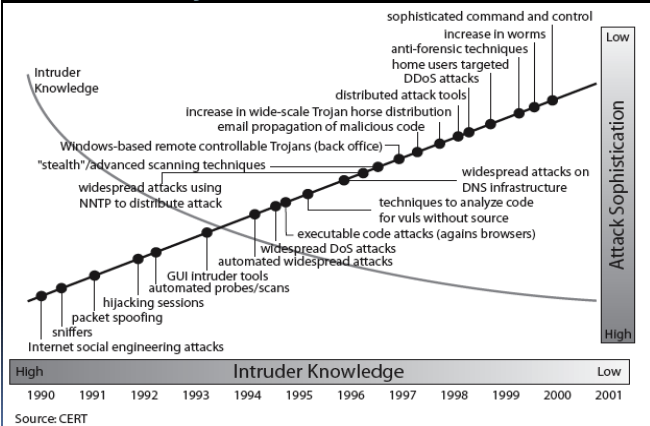
- **Computer Security** - generic name for the collection of tools designed to protect data and to thwart hackers
- **Network Security** - measures to protect data during their transmission
- **Internet Security** - measures to protect data during their transmission over a collection of interconnected networks
 - note boundaries between them are blurred.

Aim of Course

- our focus is on **Internet Security**
- which consists of measures to deter, prevent, detect, and correct security violations that involve the transmission & storage of information



Security Trends



OSI Security Architecture

- ITU-TX.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



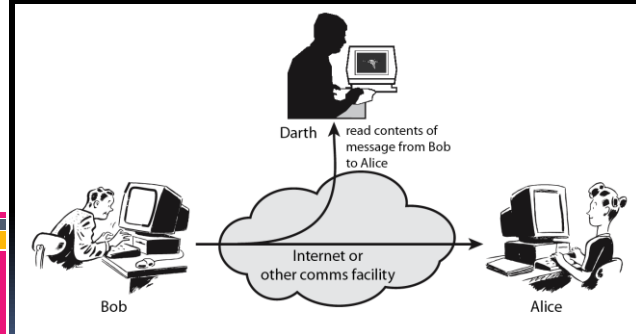
Aspects of Security

1. Security Attack: Any action that compromises the security of information owned by an organization.
2. Security Mechanism: A process (or a device incorporating such a process) that is designed to detect, prevent, or recover from a security attack.
3. Security service: A processing or communication service that enhances the security of the data processing systems and the information transfers of an organization.
 - The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.

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
- Often *threat* & *attack* used to mean same thing
- Have a wide range of attacks
- Can focus of generic types of attacks
 - passive
 - active

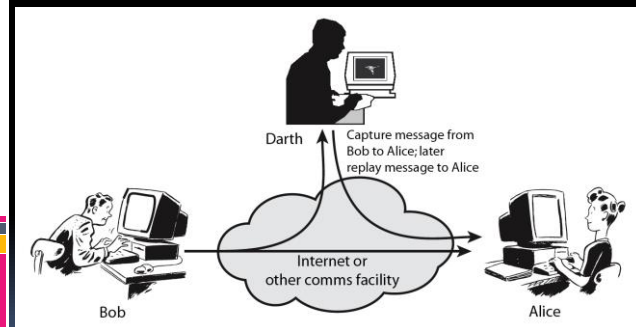
Passive Attacks



Passive Attacks

- "passive attacks" attempt to learn or make use of information from the system but does not affect system resources.
- By eavesdropping on, or monitoring of, transmissions to:
 - + obtain message contents or
 - + monitor traffic flows
- Are difficult to detect because they do not involve any alteration of the data.

Active Attacks



Active Attacks

- “active attacks” attempt to alter system resources or affect their operation.
- By modification of data stream to:
 - + masquerade of one entity as some other
 - + replay previous messages
 - + modify messages in transit
 - + denial of service
- it is quite difficult to prevent active attacks absolutely, because of the wide variety of potential physical, software, and network vulnerabilities.
- Instead, 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
 - which, for example, have signatures, dates; need protection from disclosure, tampering, or destruction; be notarized or witnessed; be recorded or licensed

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 (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

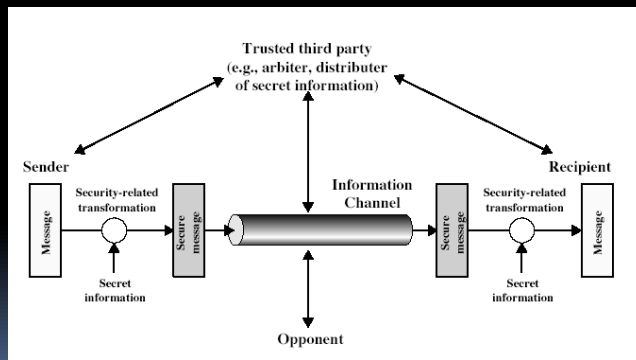
Security Mechanism

- 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
- Hence our focus on this topic

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

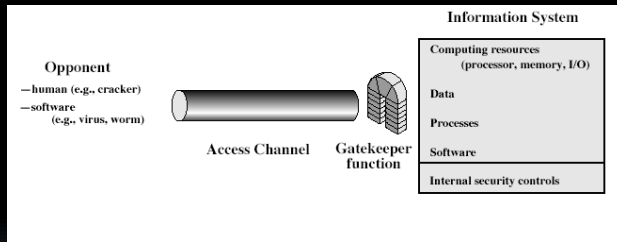
Model for Network Security



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



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 may be useful to help implement this model

Summary

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