

Information Systems Security

Security Concerns

- | Monitoring and capture network traffic
- | Exploitation of software bugs
- | Unauthorized access to resources
- | Masquerade as authorized user or end system
- | E-mail forgery
- | Malicious attacks
- | Etc.

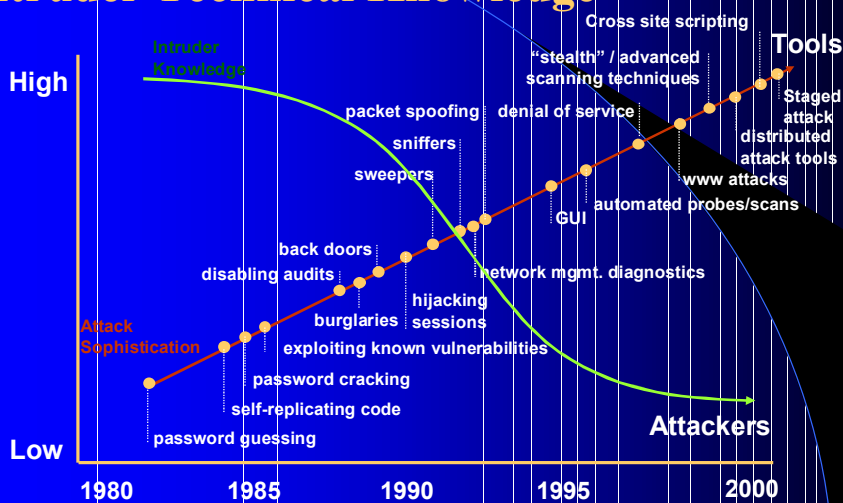
Contributing Factors

- | Increased Internet Usage
- | Lack of awareness of threats and risks
- | Wide-open network policies
- | Unencrypted network traffic
- | Complexity of security measurements and administration
- | Software bugs
- | Availability of cracking tools

CSCE 727 - Farkas

3

Attack Sophistication vs. Intruder Technical Knowledge



Copyright: CERT, 2000
CSCE 727 - Farkas

4

Security Objectives

- | **Confidentiality:** prevent/detect/deter improper **disclosure** of information
- | **Integrity:** prevent/detect/deter improper modification of information
- | **Availability:** prevent/detect/deter improper **denial of access** to services

Military Example

- | **Confidentiality:** target coordinates of a missile should not be improperly disclosed
- | **Integrity:** target coordinates of missile should be correct
- | **Availability:** missile should fire when proper command is issued

Commercial Example

- | **Confidentiality:** patient's medical information should not be improperly disclosed
- | **Integrity:** patient's medical information should be correct
- | **Availability:** patient's medical information can be accessed when needed for treatment

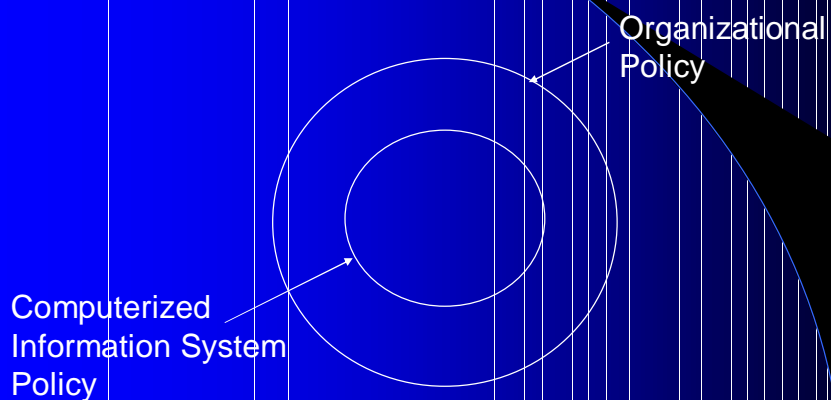
Fourth Objective

- | **Securing computing resources:** prevent/detect/deter improper use of computing resources
 - Hardware
 - Software
 - Data
 - Network

Achieving Security

- | Policy
 - What to protect?
- | Mechanism
 - How to protect?
- | Assurance
 - How good is the protection?

Security Policy



Security Mechanism

- | Prevention
- | Detection
- | Tolerance/Recovery

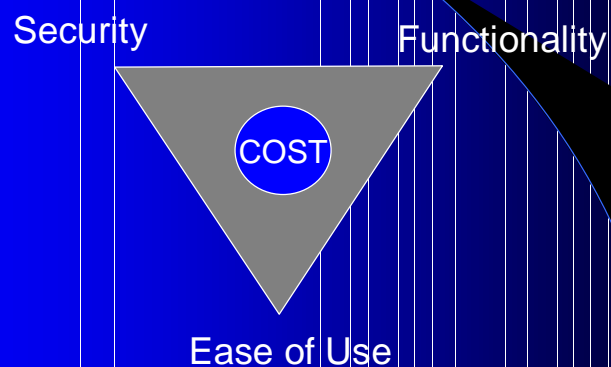
Security by Obscurity

- # Hide inner working of the system
- # Bad idea!
 - Vendor independent open standard
 - Widespread computer knowledge

Security by Legislation

- Instruct users how to behave
- Not good enough!
 - Important
 - Only enhance security
 - Targets only some of the security problems

Security Tradeoffs



Threat, Vulnerability, Risk

- § **Threat:** potential occurrence that can have an undesired effect on the system
- § **Vulnerability:** characteristics of the system that makes it possible for a threat to potentially occur
- § **Attack:** action of malicious intruder that exploits vulnerabilities of the system to cause a threat to occur
- § **Risk:** measure of the possibility of security breaches and severity of the damage

Types of Threats

- § Errors of users
- § Natural/man-made/machine disasters
- § Dishonest insider
- § Disgruntled insider
- § Outsiders

Types of Attack

- § **Interruption** – an asset is destroyed, unavailable or unusable (*availability*)
- § **Interception** – unauthorized party gains access to an asset (*confidentiality*)
- § **Modification** – unauthorized party tampers with asset (*integrity*)
- § **Fabrication** – unauthorized party inserts counterfeit object into the system (*authenticity*)
- § **Denial** – person denies taking an action (*authenticity*)

Computer Crime

- | Any crime that involves computers or aided by the use of computers
- | U.S. Federal Bureau of Investigation: reports uniform crime statistics

Computer Criminals

▮ **Amateurs:** regular users, who exploit the vulnerabilities of the computer system

- Motivation: easy access to vulnerable resources

▮ **Crackers:** attempt to access computing facilities for which they do not have the authorization

- Motivation: enjoy challenge, curiosity

▮ **Career criminals:** professionals who understand the computer system and its vulnerabilities

- Motivation: personal gain (e.g., financial)

Methods of Defense

▮ **Prevent:** block attack

▮ **Deter:** make the attack harder

▮ **Deflect:** make other targets more attractive

▮ **Detect:** identify misuse

▮ **Tolerate:** function under attack

▮ **Recover:** restore to correct state

Traditional security methods:
prevent, deter

Information Security Planning

- | Organization Analysis
- | Risk management
- | Mitigation approaches and their costs
- | Security policy
- | Implementation and testing
- | Security training and awareness

Cryptography

- Secret-Key Encryption
- Public-Key Encryption
- Cryptography Protocols

Insecure communications



Encryption and Decryption



Breakable versus Practically breakable

Unconditionally secure: impossible to decrypt. No amount of ciphertext will enable a cryptanalyst to obtain the plaintext

Computationally secure: an algorithm that is not breakable in practice based on worst case scenario

Breakable: all algorithms (except one-time pad) are theoretically breakable

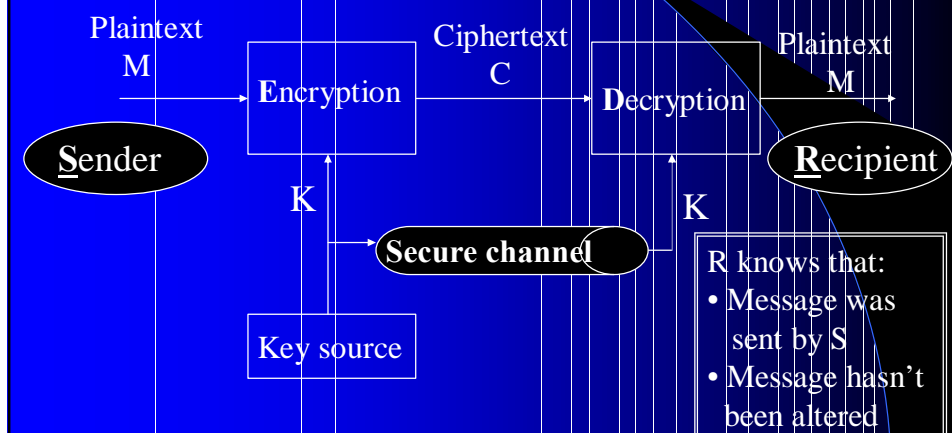
Protocols to solve problems

- | Key distribution
- | Digital Signatures
- | Electronic Voting
- | Contract Signing (read only)

CSCE 727 - Farkas

27

Key Distribution: Conventional Encryption



CSCE 727 - Farkas

28

Key Distribution: Asymmetric-Key Exchange

- | Needs reliable channels
- | Without server
 - Broadcasting
 - Publicly available directory
- | With server
 - Public key distribution center
 - Certificates

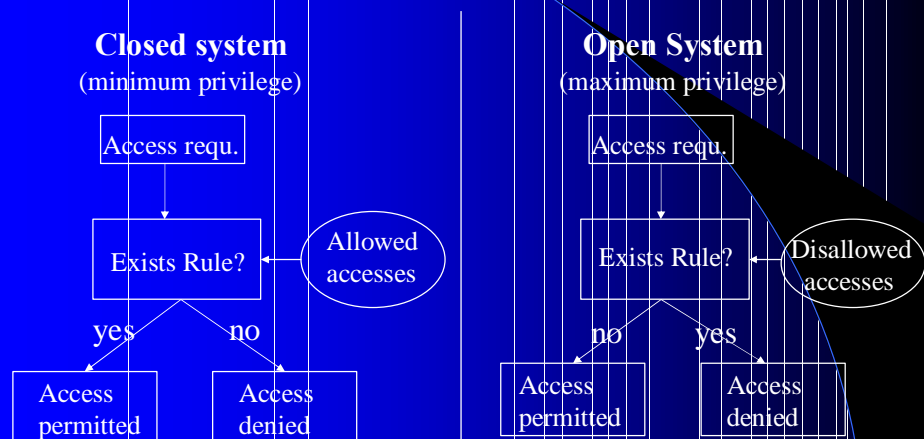
Identification and Authentication

- | *Person/group/code/system*: to be authenticated
- | *Distinguishing characteristic*: differentiates the entities to be authenticated
- | *Proprietor/system owner/administrator*: responsible for the system
- | *Authentication mechanism*: verify the distinguishing characteristic
- | *Access control mechanism*: grant privileges upon successful authentication

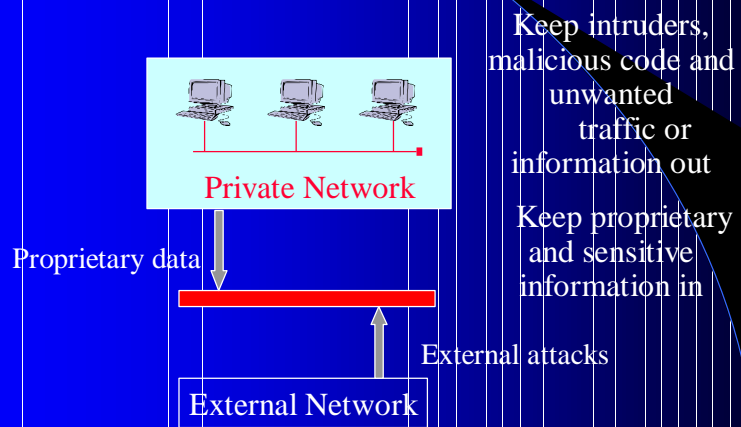
Access Control

- | **Access control:** ensures that all *direct* accesses to object are authorized
- | Protects against accidental and **malicious** threats by regulating the *reading, writing and execution* of data and programs
- | Need:
 - Proper *user identification and authentication*
 - Information specifying the *access rights is protected* from modification

Closed v.s. Open Systems



Firewall Objectives



Intrusion Management

- ▮ **Intrusion Prevention:** protect system resources
- ▮ **Intrusion Detection:** (second line of defense) discriminate intrusion attempts from normal system usage
- ▮ **Intrusion Recovery:** cost effective recovery models

Anomaly versus Misuse

