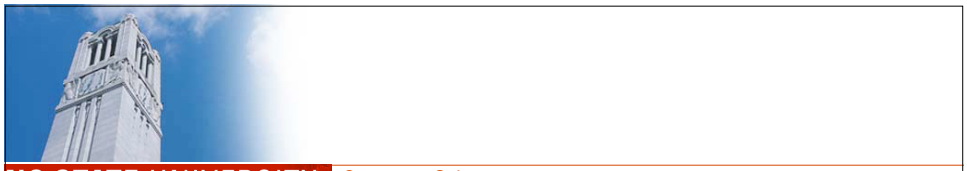


NC STATE UNIVERSITY Computer Science

CSC 774 -- Network Security

Topic 0. Basic Security Concepts

(For students who haven't taken CSC 574)

Information Security Problems

- Public, private, and government networks have been penetrated by unauthorized users and rogue programs
- Increased volume of security breaches attributed Computer Emergency Response Team (CERT) reports a tremendous increase in cracking incidents
- Insider attacks

Information Security Concerns

- Distributed Denial of Service (DDOS) attacks
- Worm attacks (e.g., code red)
- Monitoring and capture of network traffic
  - User IDs, passwords, and other information are often stolen on Internet
- Exploitation of software bugs
- Unauthorized access to resources
  - Disclosure, modification, and destruction of resources
- Compromised system used as hostile attack facility
- Masquerade as authorized user or end system
- Data driven attacks
  - Importation of malicious or infected code
- E-Mail forgery

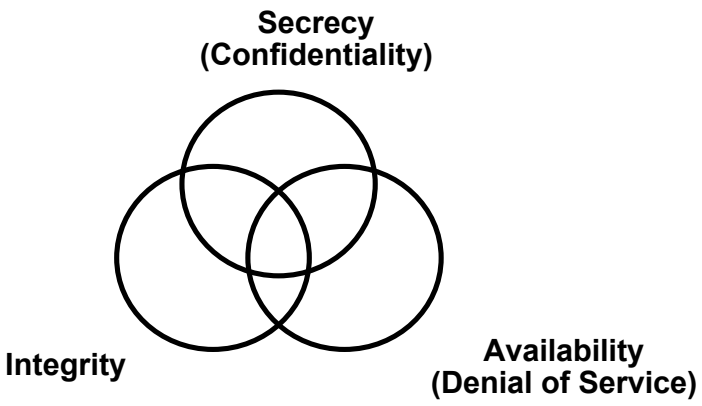
Contributing Factors

- Lack of awareness of threats and risks of information systems
  - Security measures are often not considered until an Enterprise has been penetrated by malicious users
- Wide-open network policies
  - Many Internet sites allow wide-open Internet access
- Vast majority of network traffic is unencrypted
  - Network traffic can be monitored and captured

Contributing Factors (Cont'd)

- Lack of security in TCP/IP protocol suite
  - Most TCP/IP protocols not built with security in mind
  - Work is actively progressing within the Internet Engineering Task Force (IETF)
- Complexity of security management and administration
- Exploitation of software (e.g., protocol implementation) bugs
  - Example: Sendmail bugs
- Cracker skills keep improving

Security Objectives



Security Objectives

- Secrecy — 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 provided by the system

- Note the use of improper rather than unauthorized
- Authorized users are accountable for their actions

Commercial Example

- Secrecy — An employee should not come to know the salary of his manager
- Integrity — An employee should not be able to modify the employee's own salary
- Availability — Paychecks should be printed on time as stipulated by law

Military Example

- Secrecy — The target coordinates of a missile should not be improperly disclosed
- Integrity — The target coordinates of a missile should not be improperly modified
- Availability — When the proper command is issued the missile should fire

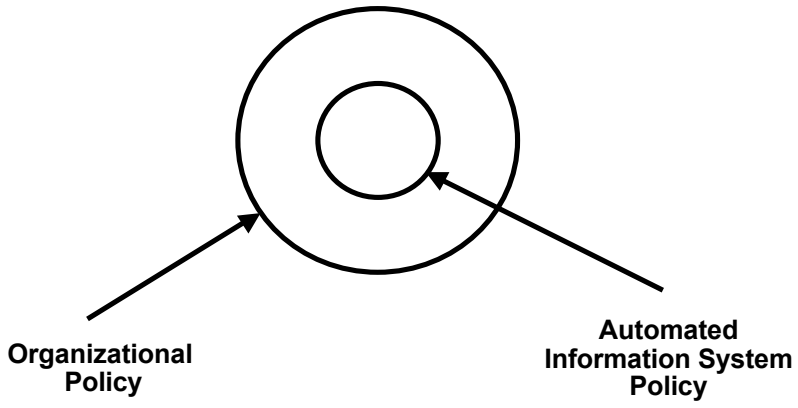
A Fourth Objective

- Securing computing resources — Prevent/detect/deter improper use of computing resources including
  - Hardware Resources
  - Software resources
  - Data resources
  - Network resources

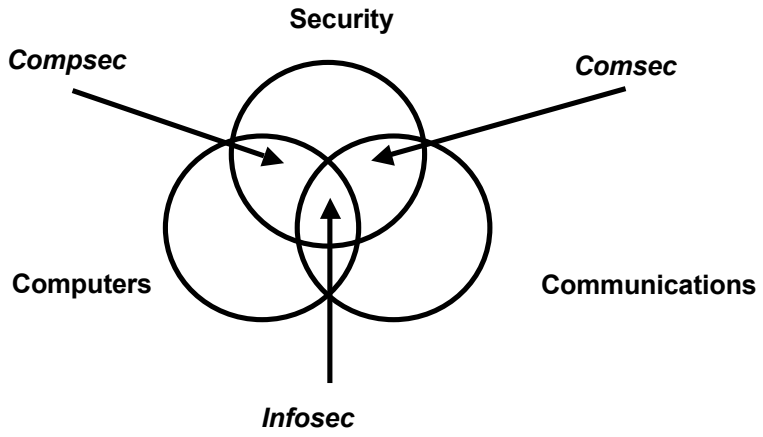
Achieving Security

- Security policy — What?
- Security mechanism — How?
- Security assurance — How well?

Security Policy



Compusec + Comsec = Infosec



Security Mechanism

- Prevention — Access control
- Detection — Auditing and intrusion detection
- Tolerance — Practicality

Good prevention and detection both require good authentication as a foundation

Security Mechanism

- Security mechanisms implement functions that help *prevent*, *detect*, and *respond* to security attacks
- Prevention is more fundamental
  - Detection seeks to prevent by threat of punitive action
  - Detection requires that the audit trail be protected from alteration
- Sometime detection is the only option, e.g.,
  - Accountability in proper use of authorized privileges
  - Modification of messages in a network
- Security functions are typically made available to users as a set of *security services* through APIs or integrated interfaces
- Cryptography underlies (almost) all security mechanisms

Security Services

- Confidentiality: protection of any information from being exposed to unintended entities.
  - Information content.
  - Parties involved.
  - Where they are, how they communicate, how often, etc.
- Authentication: assurance that an entity of concern or the origin of a communication is authentic - it's what it claims to be or from
- Integrity: assurance that the information has not been tampered with

Security Services - Cont'd

- Non-repudiation: offer of evidence that a party is indeed the sender or a receiver of certain information
- Access control: facilities to determine and enforce who is allowed access to what resources, hosts, software, network connections
- Monitor & response: facilities for monitoring security attacks, generating indications, surviving (tolerating) and recovering from attacks

Security Services - Cont'd

- Security management: facilities for coordinating users' service requirements and mechanism implementations throughout the enterprise network and across the internet
  - Trust model
  - Trust communication protocol
  - Trust management infrastructure

Security Assurance

- How well your security mechanisms guarantee your security policy
- Everyone wants high assurance
- High assurance implies high cost
  - May not be possible
- Trade-off is needed.

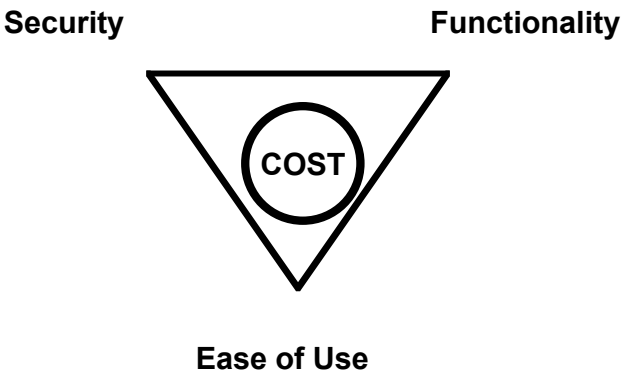
Security by Obscurity

- Security by obscurity says that if we hide the inner workings of a system it will be secure
- It is a bad idea
- Less and less applicable in the emerging world of vendor-independent open standards
- Less and less applicable in a world of widespread computer knowledge and expertise

Security by Legislation

- Security by legislation says that if we instruct our users on how to behave we can secure our systems
- It is a bad idea
- For example
  - Users should not share passwords
  - Users should not write down passwords
  - Users should not type in their password when someone is looking over their shoulder
- User awareness and cooperation is important, but cannot be the principal focus for achieving security

Security Tradeoffs



Threat-Vulnerability-Risk

- Threats — Possible attacks on the system
- Vulnerabilities — Weaknesses that may be exploited to cause loss or harm
- Risk — A measure of the possibility of security breaches and severity of the ensuing damage
- Requires assessment of threats and vulnerabilities

Risk Management

- Risk analysis
  - Mathematical formulae and computer models can be developed, but the underlying parameters are difficult to estimate.
- Risk reduction
- Risk acceptance
  - Certification
    - Technical evaluation of a system's security features with respect to how well they meet a set of specified security requirements
  - Accreditation
    - The management action of approving an automated system, perhaps with prescribed administrative safeguards, for use in a particular environment

Instructional Objectives

- Be able to explain the following concepts.
  - Security
  - three goals of information security
  - examples of attacks against the goals of information security
  - security policy
  - security mechanism
  - security assurance
  - typical security services
    - confidentiality, authentication, integrity, non-repudiation, access control, monitor & response, security management).