Computer and Network Security

Dr. Yao Liu

About Instructor

- Dr. Yao Liu,
  - Office: ENB 336
  - Phone: 813-974-1079
  - Email: yliu@cse.usf.edu
  - URL: http://www.cse.usf.edu/~yliu/
  - Office hour: MW 1:30am – 3:00pm
  - Class meetings: MW 09:30pm - 10:45pm

About TA

- Mr. Xiaoshan Wang
  - Office: ENB 213
  - Email: xiaoshanwang@mail.usf.edu
  - Office hour: Tuesday 2:00pm - 4:00pm

Course Objectives

- Understanding of basic issues, concepts, principles, and mechanisms in network security. E.g.,
  - Cryptography
  - Authentication
  - Classic security standards like Kerberos , IPsec and Internet key management
- Be able to determine appropriate mechanisms to protect computer and networked systems.

Course Outline

- Basic Security Concepts
  - Confidentiality, integrity, availability
  - Security terms, security mechanisms
- Cryptography
  - Basic number theory
  - Secret key cryptography
  - Public key cryptography
  - Hash function
  - Key management

Course Outline (Cont’d)

- Identification and Authentication
  - Basic concepts of identification and authentication
  - User authentication
  - Authentication protocols
- Network and Distributed Systems Security
  - Public Key Infrastructure (PKI)
  - Kerberos
  - IPsec
  - Internet key management

Projects

- Research projects:
  - Project proposal
  - Project report
  - Project demo/presentation
- You are expected to explore issues beyond what’s included in lectures by yourselves

Prerequisites

- It is highly desirable that you have successfully finished introductory computer programming courses.
- Prior knowledge of networking fundamentals is recommended.

Textbook

- Required textbook
  - Charlie Kaufman, Radia Perlman, and Mike Speciner, *Network Security: Private Communication in a Public World, 2nd Edition*, Prentice Hall, ISBN: 0-13-046019-2.

On-line Resources

- WWW page: http://www.cse.usf.edu/~yliu/Network%20Security/teaching.html
- For course materials, e.g., lecture slides, homework files, papers, tools, etc.
  - Will be updated frequently. So check frequently.

Grading

- Assignments 20%, project 20%, midterm 20%, final 30%, quiz 10%
- Tests are open-book and open-notes.
- The final grades are computed according to the following rules:
  - A+: >= 95%; A: >= 85% and < 95%;
  - A-: >= 80% and < 85%; B+: >= 75% and < 80%;
  - B: >= 70% and < 75%; B-: >= 66% and < 70%;
  - C+: >= 63% and < 66%; C: >= 60% and < 63%;
  - C-: >= 56% and < 60%; D: >= 53% and < 56%;
  - E: >= 50% and < 53%; F: < 50%.
-

Policies on incomplete grades and late assignments

- Homework and project deadlines will be hard.
- Late homework will be accepted with a 15% reduction in grade each day they are late by.
- Once a homework assignment is discussed in class, submissions will no longer be accepted.

Policies on Absences and Scheduling Makeup Work

- Make-up exams will not normally be permitted. Exceptions will be made if a student presents a police report or a doctor's note that show some emergency situation.
- Events such as going on a business trip or attending a brother's wedding are not an acceptable excuse for not taking an exam at its scheduled time and place.

Academic Integrity

- An FF grade will be assigned to a student who is caught cheating for this class. Example cheating behaviors include but not limited to: direct and indirect plagiarizing another student’s work or online resources, and modifying incorrect test and homework answers for regrading.

CIS 6930/4930 Computer and Network Security

Topic #1. Basic Security Concepts

Why This Course?

- Increased volume of security incidents
- Security threats
  - Malware: Virus, worm, spyware
  - Spam
  - Botnet
  - DDoS attacks
  - Phishing
  - …

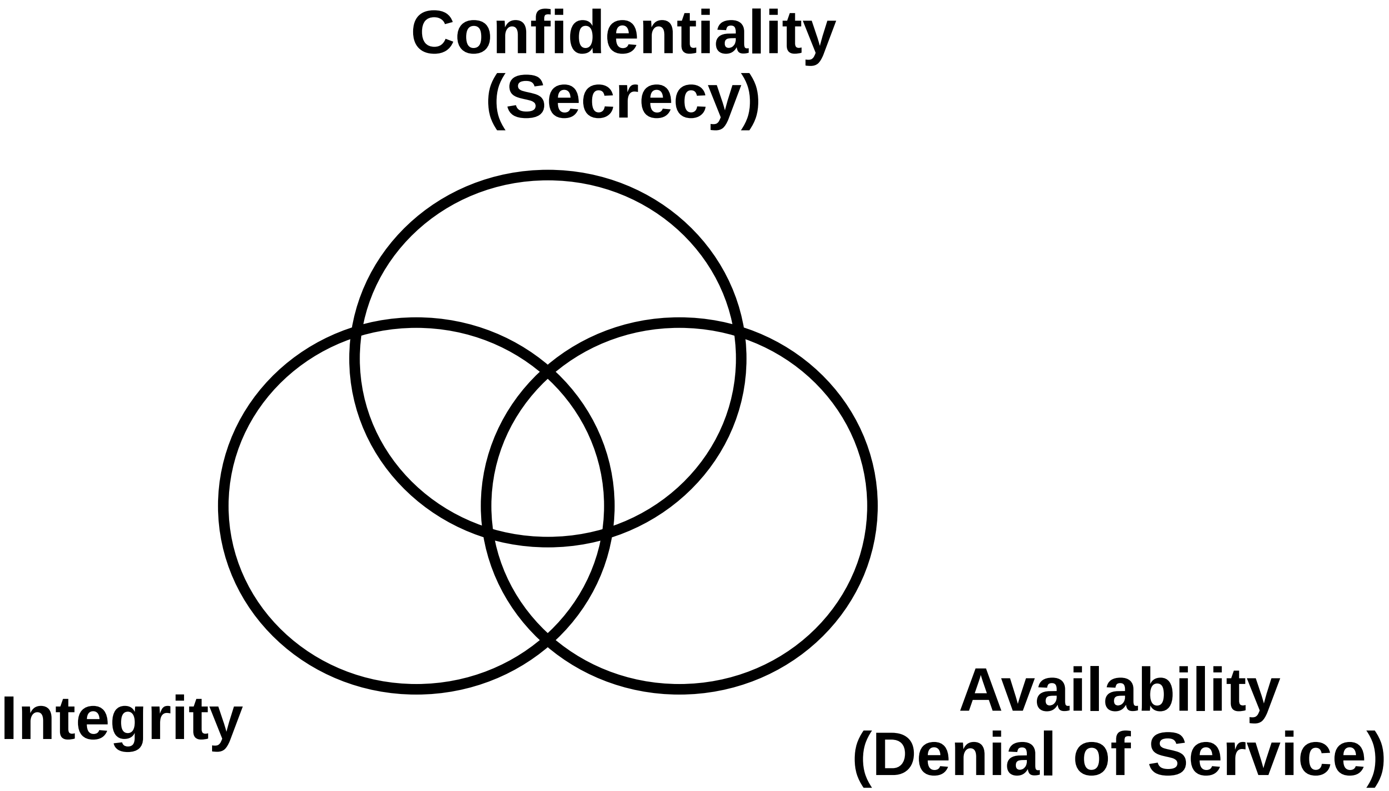
Contributing Factors

- 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
  - The situation is getting better, but …
- (Historical) Reluctance to invest in security mechanisms
  - The situation is improving
    - Example: Windows 95 → Windows 2000 → Windows XP → Windows XP SP2 → Windows Vista → Windows 7
  - But there exists legacy software
- Wide-open network policies
  - Many Internet sites allow wide-open Internet access

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
  - Security is not just encryption and authentication
- Software vulnerabilities
  - Example: buffer overflow vulnerabilities
  - We need techniques and tools to better protect software security
- Cracker skills keep improving

Security Objectives



Confidentiality
(Secrecy)

Integrity

Availability
(Denial of Service)

Security Objectives (CIA)

- Confidentiality — Prevent/detect improper disclosure of information
- Integrity — Prevent/detect improper modification of information
- Availability — Prevent/detect improper denial of access to services provided by the system
- These objectives have different specific interpretations in different contexts

Commercial Example

- Confidentiality — An employee should not 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

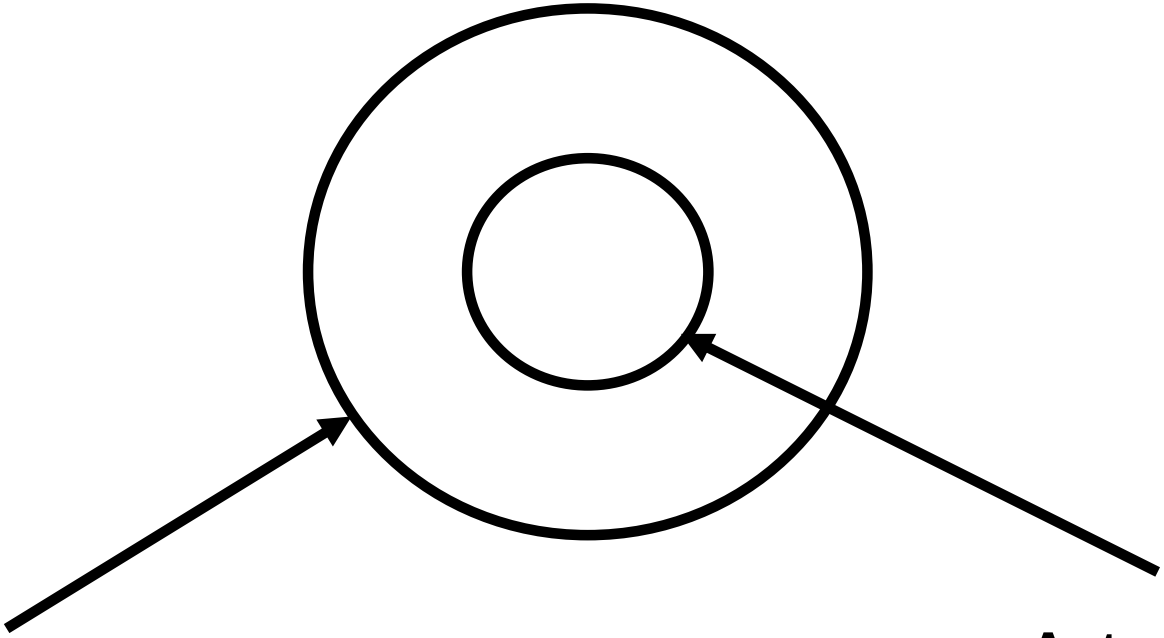
Military Example

- Confidentiality — 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

Achieving Security

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

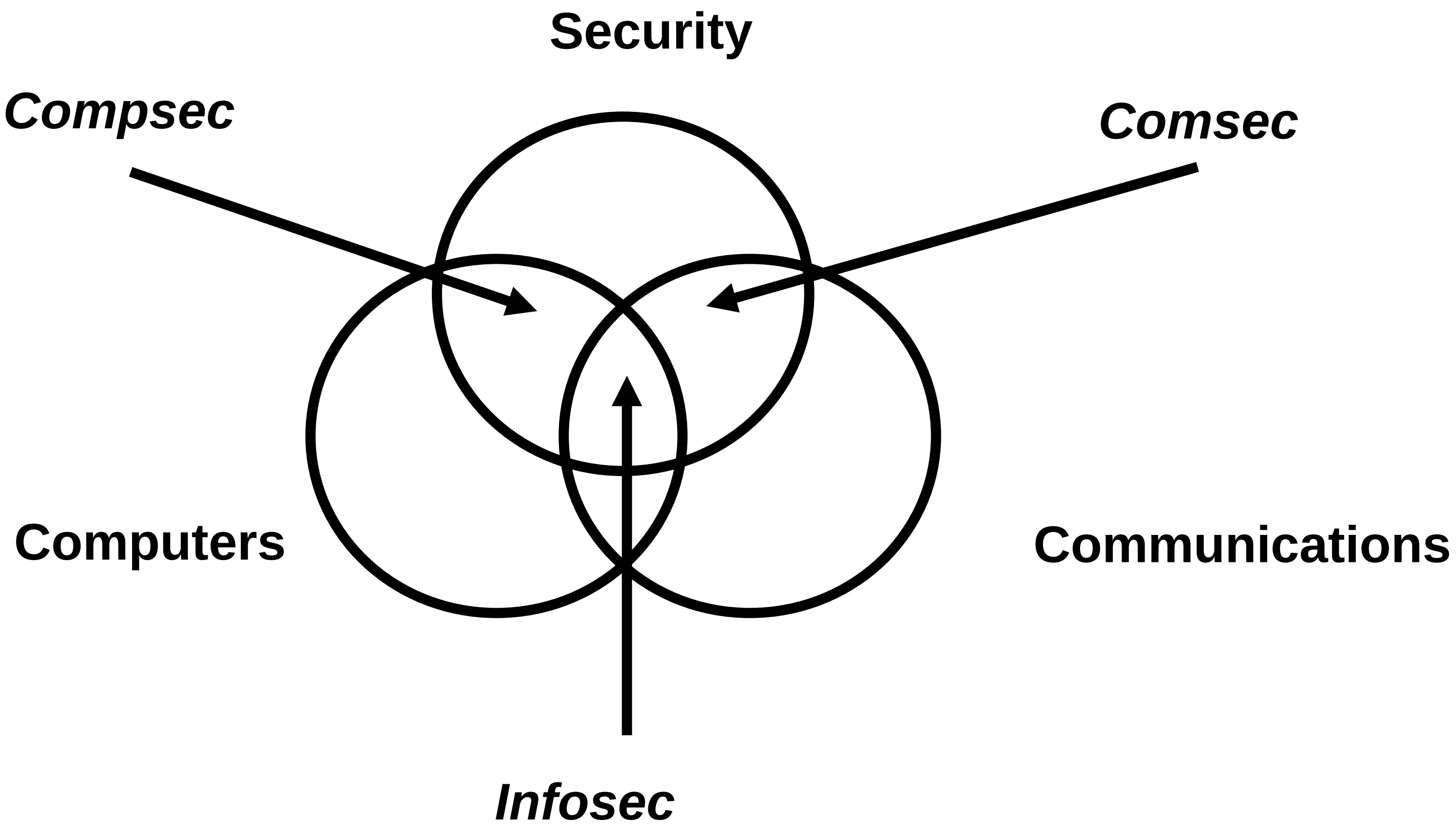
Security Policy



Organizational
Policy

Automated
Information System
Policy

Compusec + Comsec = Infosec



Security Mechanisms

- In general three types
  - Prevention
    - Example: Access control
  - Detection
    - Example: Auditing and intrusion detection
  - Tolerance
    - Example: Byzantine agreement

Good prevention and detection both require good <u>authentication</u> as a foundation

Security Services

- Security functions are typically made available to users as a set of security services through APIs or integrated interfaces
- Confidentiality: protection of any information from being exposed to unintended entities.
  - Information content.
  - Parties involved.
  - 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

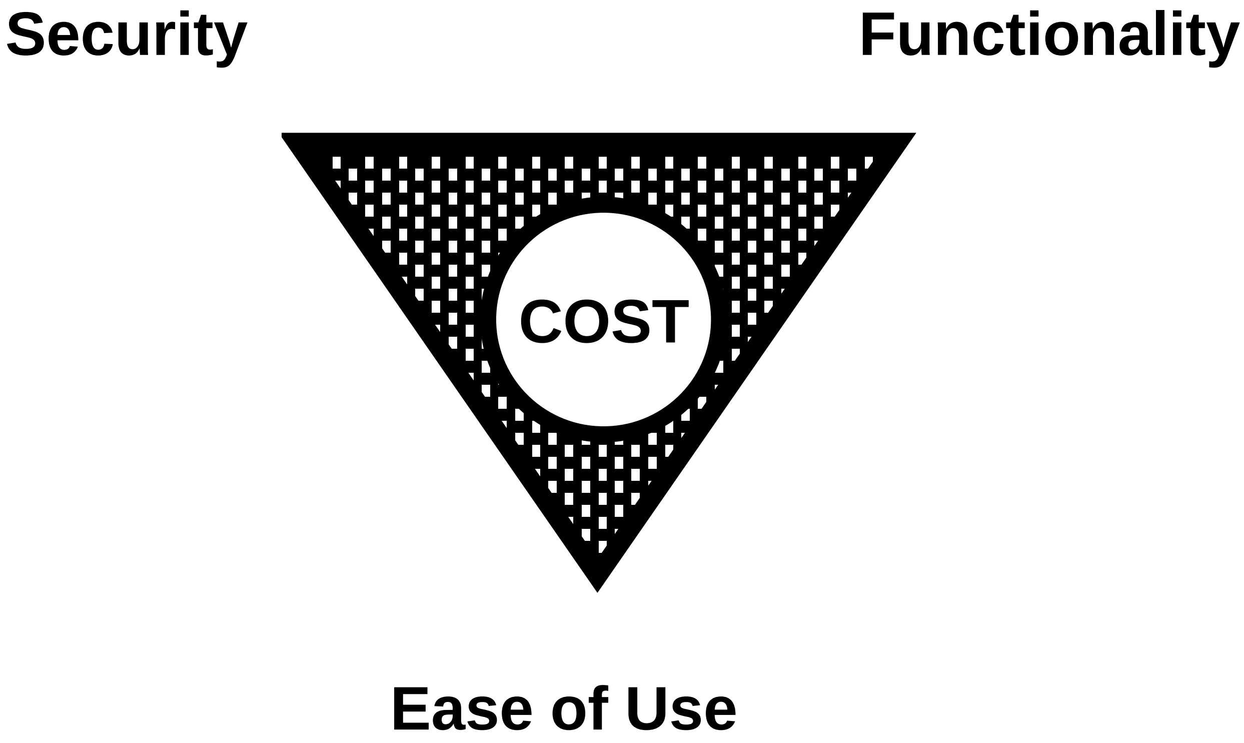
Security Services (Cont’d)

- 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 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 Tradeoffs



Security

Functionality

COST

Ease of Use

Security by Obscurity

- Security by obscurity
  - If we hide the inner workings of a system it will be secure
- More and more applications open their standards (e.g., TCP/IP, 802.11)
- 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
- 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

Threat-Vulnerability

- Threats — *Possible* attacks on the system
- Vulnerabilities — Weaknesses that may be exploited to cause loss or harm
- Requires assessment of threats and vulnerabilities

Threat Model and Attack Model

- Threat model and attack model need to be clarified before any security mechanism is developed
- Threat model
  - Assumptions about potential attackers
  - Describes the attacker’s capabilities
- Attack model
  - Assumptions about the attacks
  - Describe how attacks are launched