

CS 5173/4173 Computer Security

Fall 2020

Dr. Song Fang

School of Computer Science
University of Oklahoma

About Instructor

- Dr. Song Fang,
 - Office: DEH 232
 - Email: songf@ou.edu
 - Office hour: TR 3:30pm – 5:00pm
 - Class meetings: TR 5:00pm – 6:15pm, Nielsen Hall 0170
 - Course website:
<https://www.cs.ou.edu/~songf/teaching/F20cs5173/index.html>

About TA

- Mr. Yan He,
 - TA office: DEH 115
 - Email: hey@ou.edu
 - Office hour: T 3:00 – 4:00 pm

Course Objectives

- Understanding of basic issues, concepts, principles, and mechanisms in computer security. E.g.,
 - Symmetric and public key cryptography
 - Hash functions
 - Authentication
 - Network security protocols
 - Other security issues
- 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

Prerequisites

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

Textbook

- Suggested 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.
 - Wenliang Du. *Computer Security: A Hands-on Approach. 1st Edition*, 2017.

Grading

- Quizzes: 10% (6 in total and the lowest will be dropped)
- Labs: 30% ([SEED labs](#)) (6 in total and the lowest **will not** be dropped)
- Midterm 1: 30% (25% for 5173)
- Midterm 2: 30% (25% for 5173)
- In-class presentation (CS 5173 only)

In-class Presentation

- A paper list will be provided on Canvas
- Two students form a team
- 20 minutes presentation + 5 QA
- Slides must be uploaded for grading as well
- Peer review (2 extra points for all students)

Policies on incomplete grades and late assignments

- Lab deadlines will be hard.
- Late submission will be accepted with a 15% reduction in grade each day they are late by (up to a maximum of 3 days).

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.

Mandatory Masking Policy – Fall 2020

- University Mandatory Masking Policy:
<https://www.ou.edu/coronavirus/masking-policy>
- Please make sure you are wearing your mask while in class.
 - If you do not have a mask or forgot yours, see the professor for available masks.
 - If you have an exemption from the Mandatory Masking Policy, please see the professor to make accommodations before class begins.
 - If and where possible, please make your professor aware of your exemption and/or accommodation prior to arriving in class.
- If a student is unable or unwilling to wear a mask and has not made an accommodation request through the ADRC, they will be instructed to exit the classroom.

Academic Integrity

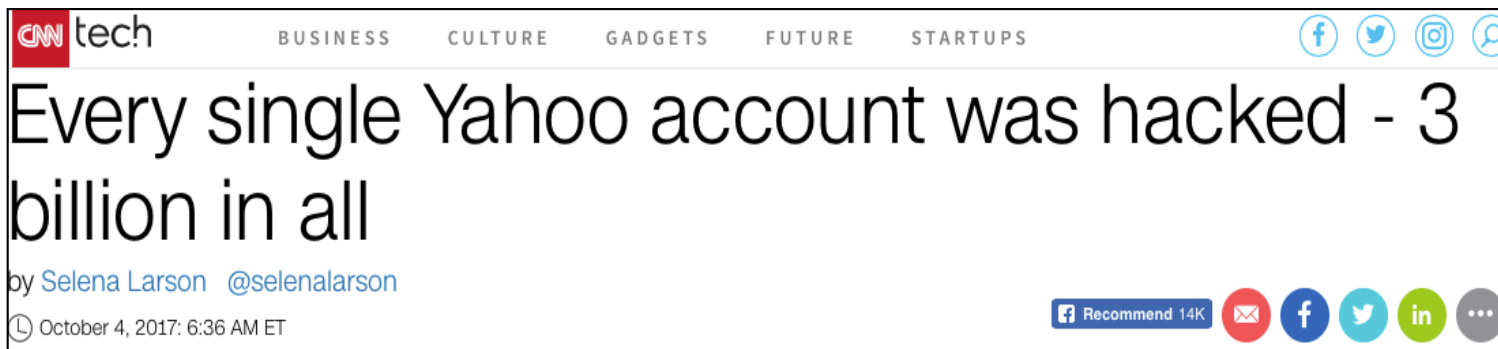
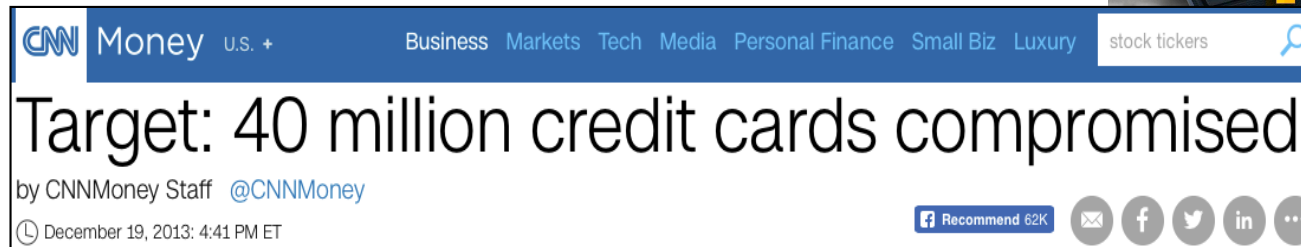
- A student must complete his/her tests, projects and assignments on his/her own. Example cheating behaviors include but not limited to: direct and indirect plagiarizing another student's work or online resources.
- For student's guide to Academic Integrity, please visit
<http://integrity.ou.edu/students.html>

CIS 5173/4173 Computer Security

Topic #1. Basic Security Concepts

Why This Course?

- Increased volume of security incidents



Why This Course?

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

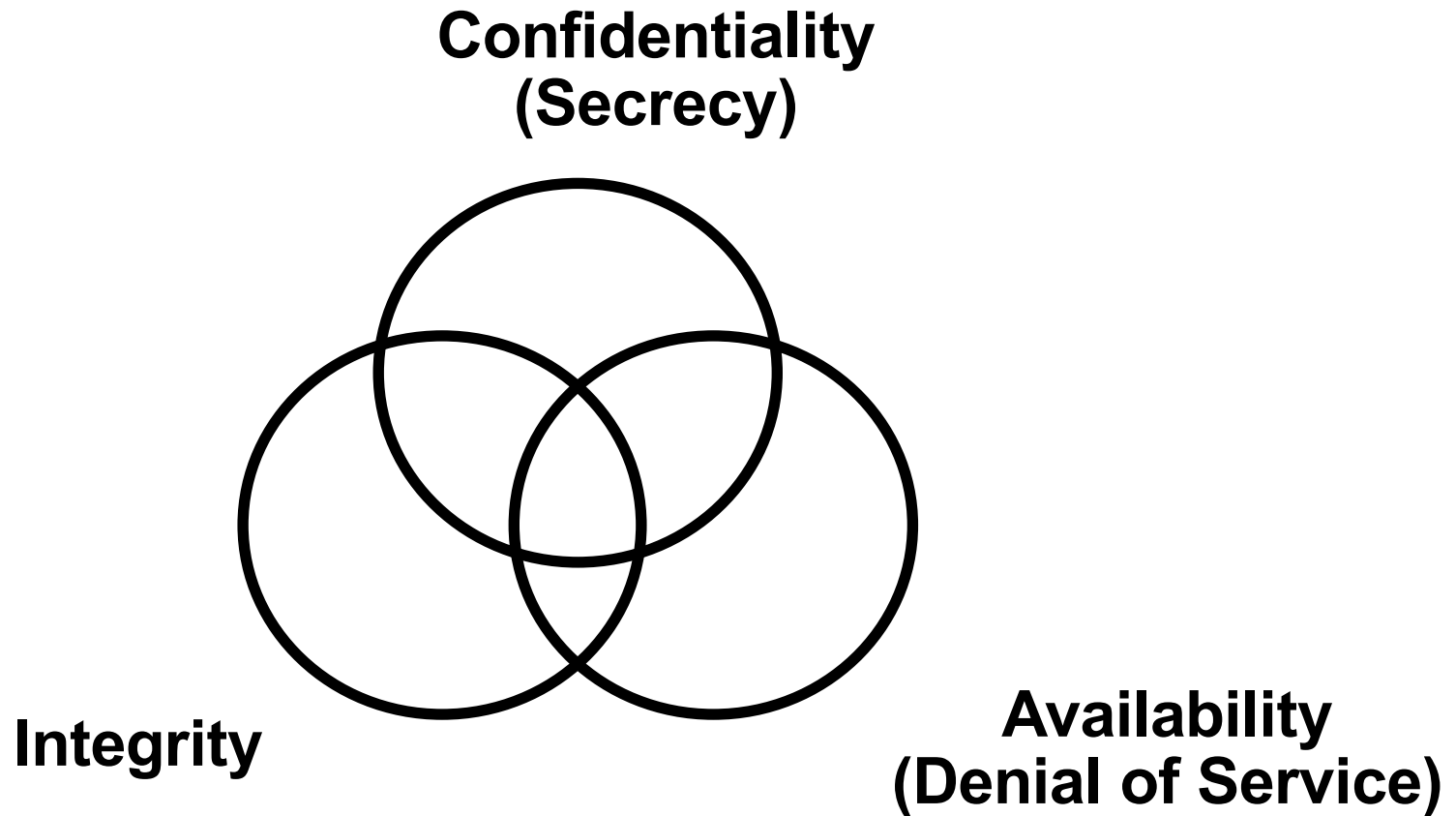
Contributing Factors

- 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 → Windows 8 → Windows 10
 - 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






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

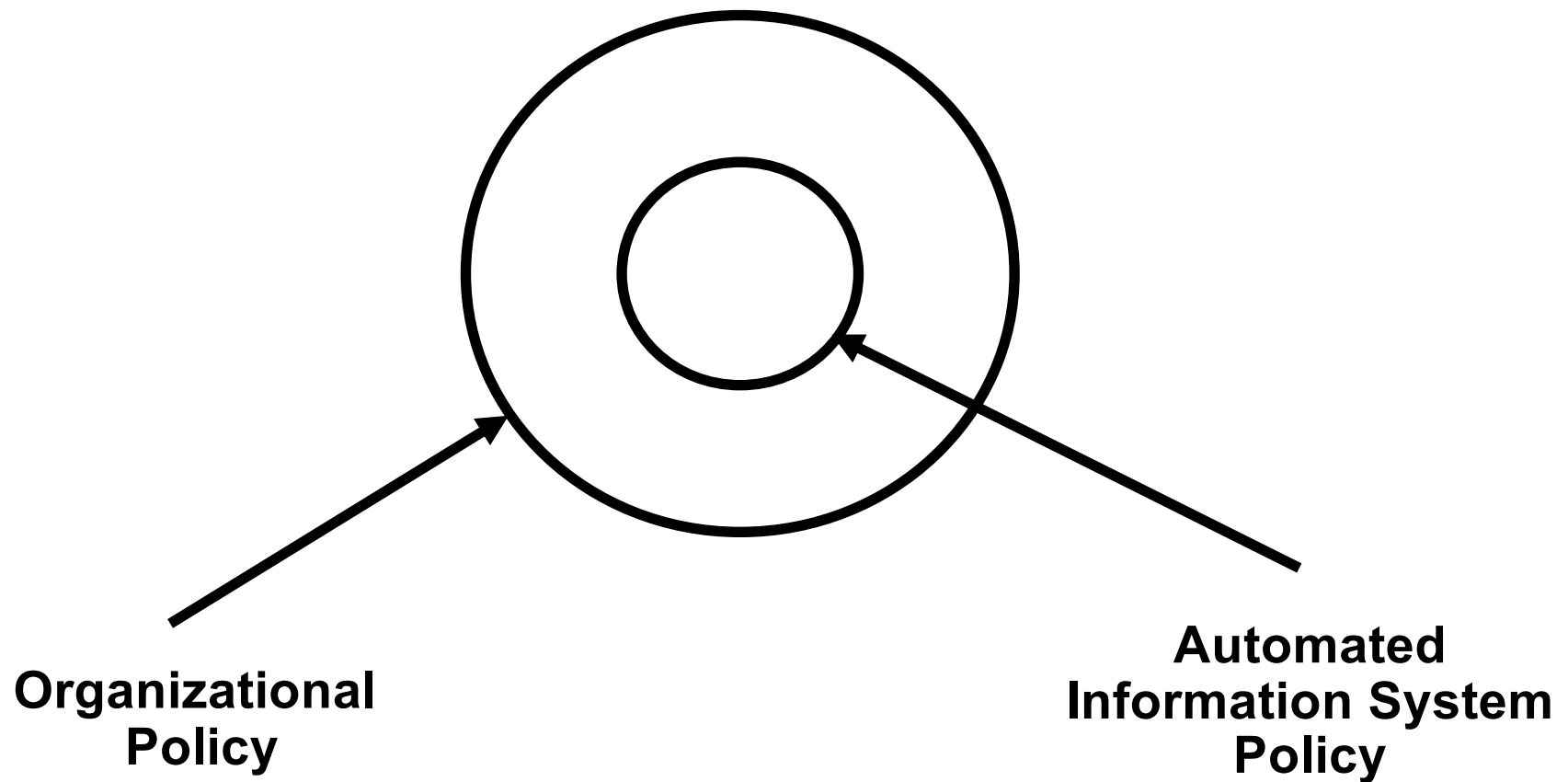
Military Example

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

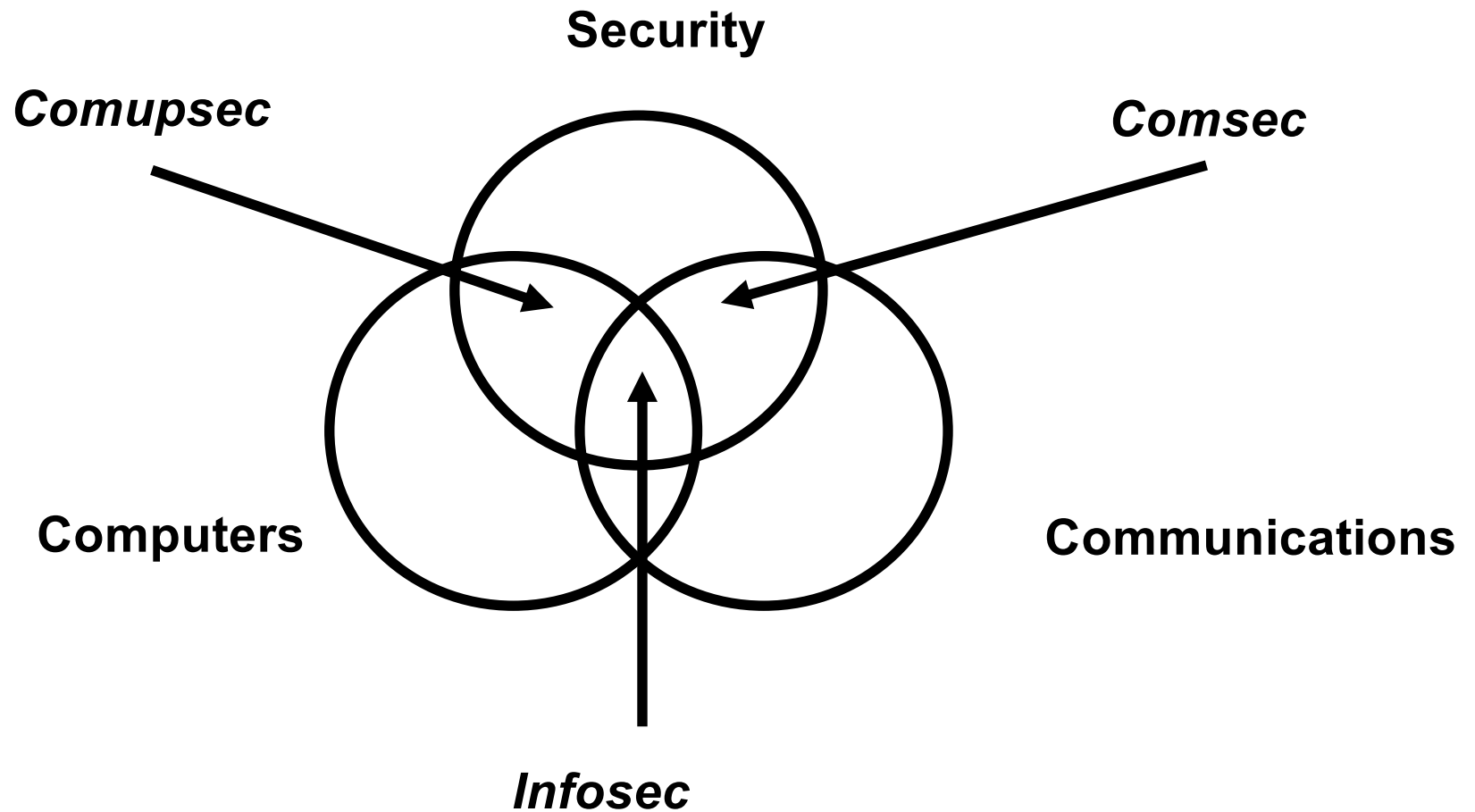
Achieving Security

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

Security 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 authentication 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

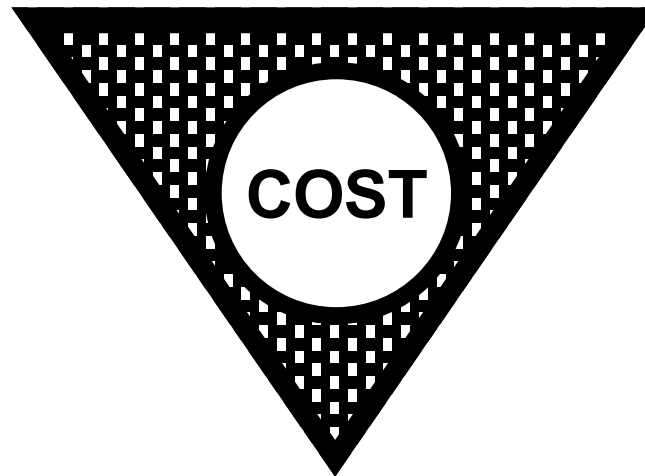
Security Assurance

- **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



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