CIS 6930 Emerging Topics in Network Security

Dr. Yao Liu

yliu@cse.usf.edu
http://www.cse.usf.edu/~yliu/
About Instructor

• Dr. Yao Liu, Assistant Professor of Computer Science and Engineering Department
  – http://www.cse.usf.edu/~yliu/
  – yliu@cse.usf.edu
  – 813-974-1079
  – Office: ENB 336
  – Office hours:
    • MW 11:00pm – 12:30pm
Course Objectives

• Learn advanced issues, concepts, principles, and mechanisms in network security, e.g.,
  – Secret sharing
  – Broadcast authentication protocols
  – Group key management
• Learn recent research advances in network security
• Prepare for graduate research in network security
Prerequisites

• It would be helpful to you if you have a rudimentary understanding of computer networks and security.
Text

• No required textbook
• Research papers listed on the course website
• Suggested textbook
Course Mechanics

• Slides will be provided
• But be prepared to
  – Take notes, and
  – Participate in class discussion
• Course website:
  – http://www.cse.usf.edu/~yliu/Emerging%20Topics/teaching.html
  – For course materials, e.g., slides, homework files, papers, etc.
  – Will be updated frequently
Grading

• Homework assignment (15%)
• Summaries of reading papers (30%)
• In-class paper presentation (20%)
• Course research project (25%)
• quiz (10%)
Grading (Cont’d)

• The final grades are computed according to the following rules:
  – A+: $\geq 99\%$  A: $\geq 97\%$ and $< 99\%$  A-: $\geq 95\%$ and $< 97\%$
  – B+: $\geq 85\%$ and $< 95\%$  B: $\geq 80\%$ and $< 85\%$  B-: $\geq 75\%$ and $< 80\%$
  – C+: $\geq 66\%$ and $< 75\%$  C: $\geq 63\%$ and $< 66\%$  C-: $\geq 60\%$ and $< 63\%$
  – D+: $\geq 56\%$ and $< 60\%$  D: $\geq 53\%$ and $< 56\%$  D-: $\geq 50\%$ and $< 53\%$
Policies on incomplete grades and late assignments

• Homework, paper summaries, project deadlines will be hard.
• Late submission will be accepted with a 15% reduction in grade each day they are late by.
• Once a homework solution is posted or the paper is discussed in class, submissions will no longer be accepted.
Academic Integrity

• The university policies against academic dishonesty will be strictly enforced.
• Graduate students who are caught cheating will get an FF for this course.
Course Outline

• Topic 1: Basic concepts of network security
  – Encryption, decryption, hash functions, DES, public key, authentication techniques, etc.

• Topic 2: Advanced network security primitives
  – Secret sharing
  – Group Key Management
  – Broadcast authentication
Course Outline

• Topic 3: Emerging research topics
  – Implantable Medical Device Security
  – Security and Privacy Vulnerabilities of In-Car Wireless Networks
  – Wireless Electronic Warfare: Jamming and anti-jamming techniques
  – Location Based Access Control
  – Power grid security
  – RFID security
  – Smart phone security
  – ......
Research Paper

• Small team -- at most three students per group
• Proposal, interim report, and final report
  – Proposal due: Feb/20/16
  – Interim report: March/27/16
  – Final submission due: midnight EST, April/20/16
• The instructor will be available to discuss your topic during the office hours
• You should start thinking about team and topic now
Example Topics

• Topics include but not limited to:
  – Security in Virtual Computing Clouds
  – Security in Mobile Ad-hoc Networks
  – Smart phone security
  – Power Grids Security
  – Vulnerability Analysis
  – Intrusion Detection
  – Authentication
  – DNS Security
  – Digital Watermarking
  – New techniques (e.g., security of Bitcoins)
In-class presentation

• Each student will be assigned of one paper to present in the class

• Paper presentation will start on February 10\textsuperscript{th}, and follows the alphabetic order on your last name.
  – Pratik Adhav
  – Saeed Alahmari
  – Radha Aluru
  – Geol Gladson Battu
A Brief Review of Basic Security Concepts
Security Objectives

Secrecy
(Confidentiality)

Integrity

Availability
(Denial of Service)
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
Commercial Example

• Secrecy — 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

• 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
Security Mechanisms

• In general three types
  – Prevention
  – Detection
  – Tolerance

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

Ease of Use

Functionality

COST
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
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