ECE543/444
Computer Network Security

Yu Cheng
Illinois Institute of Technology
Spring 2023

ILLINOIS INSTITUTE OF TECHNOLOGY

Course Framework

Instructor

- Prof. Yu Cheng, cheng@iit.edu; (312) 567-7996; Siegel Hall 320
- TA: Suyang Wang, swang133@hawk.iit.edu
- Office Hours: 3:30pm-4:30pm, Tuesday/Thursday, or by appointment

Course Description

- This course studies computer network security by covering topics such as fundamental cryptographic algorithms; protocol design and analysis for secure communications over Internet; efficient key management infrastructure; strong password protection; attack and security models; practical security protocols in application layer, transport layer, network layer, and link layer.

Pre-Requisites

- Basic Operational Mathematics, background knowledge of Internet (ECE 407/408)

Text Book

- "*Network Security: Private Communications in a Public World*" 2nd edition, by Charlie Kaufman, Radia Perlman, and Mike Speciner, Prentice Hall.
- Some extra notes added

What This Course is About

- Focus on network protocols
  - network communications (long distance)
  - key distribution over network (chicken & egg)
- Cryptography, especially practical issues and intuition
  - mathematic principles; practical application; intuition for design
- How to design a secure protocol
  - Perspectives from good guy and bad guy
- Recognizing snake oil and common flaws
  - In-depth thinking required; conditions for security
- Conceptual overview of standards
- Representative practical applications and protocols
- Possible research topics

How and Why

Course Outline

Part I: Introduction	
Overview of security issues over the Internet	Chapter 1
Basic framework and methodology for network security	Chapters 2 and 9
Part II: Cryptographic Algorithms	
Secret key cryptography	Chapters 3 and 4
Hashes and message digests	Chapter 5
Public key algorithms	Chapter 6
Midterm Examination	
Part III: Identity and Credential Protection in Internet	
Key management infrastructure	Chapter 15
Strong password protocols	Chapter 12
Protocols for credential management	Chapters 11 and 16
Part IV: Security in Practical Applications/Protocols	
Application layer (Email)	Chapters 20 and 21
Transport layer (SSL) and network layer (IPSec)	Notes
Link layer (Wireless Network Security)	Notes
Security in 5G cellular networks	Notes (Gest speaker)
Final Examination	

Assignment and Grading

Homework assignments

- Submit before the specified deadline
  - NO LATE assignments accepted without prior instructor consent

Grading system

Homework Assignments	15 points
Paper reading project	20 points
RSA implementation project	15 points
Midterm Exam	25 points
Final Exam (Comprehensive)	25 points
Engagement bonus (by Quiz)	5 points

A student will directly receive an “E” score, if the student

- does not submit at least 50% of the homework assignments (e.g., at least 3 submissions in 6 assignments)
- does not do the required course project
- does not take the midterm exam
- does not take the final exam
- use a published or submitted paper as course project (“Cheating”)
- use a similar project report from a previous course (“Cheating”)

Course resources

- http://blackboard.iit.edu – assignments, assignment solutions, additional distributes

- **Some general things**
  - Stick to the deadlines. Grading policies will be strictly applied
  - Copy, plagiarism, or cheating will directly result in the “E” grade and will be reported to related university office
  - Arguments for score upgrading with personal reasons (not based on performance), after exam or the submission due date, will not be considered and will be passed to the department

How to get good grades (high motivation + hard work)

- Regularly attend the classes
- Refresh timely after each lecture
- Independently work on the homework problems
- Seriously deal with the course projects

Future Networking Research Lab (FunLab)

- Wireless network performance analysis and protocol design
- Machine learning, cloud computing and big data
- Internet and wireless network security
- Next-generation Internet architecture, protocols, and management

- Graduated thesis students joined AT&T, Juniper, InterDigital, Google, Qualcomm, United Technologies Research Center, Shanghai Jiaotong University, Southeastern University

Funded by NSF CAREER AWARD (2011), Trustworthy Computing, NeTS, and ECCS

http://www.ece.iit.edu/~yucheng/