CS 134
Elements of Cryptography and Computer & Network Security
Fall 2016

Instructor: Karim ElDefrawy

/uci_compsci134/compsci134_main.htm

(short version http://goo.gl/tJ08Pq)
Today

- Administrative Stuff
- Course Organization
- Course Topics
- Gentle Introduction
- Basics of Cryptography (Crypto)
CS 134 Background

- Classes: Wednesday 7:00pm-9:50pm @ HG 1800
- Discussions section – as needed (must register!)
- Senior-level undergraduate course
- Some overlap with CS 203 / NetSYS 240 (graduate)
- Offered since 2002
- Last time Winter 2016 (by Gene Tsudik)
Why (not) take this course?

- Not required for any track or concentration
  - listed as an option in two specializations
- Difficult course material
- There will be some unusual math (e.g., number theory, group theory)
- Tough grading
- Lectures may not always be available ahead of class
- There is no second chance if you mess up
- There is no drop after second week
- No Pass/No-Pass option
Contact Information

- **Instructor:** Karim ElDefrawy
  - Email: *keldefra* AT *uci.edu*
  - Office: ICS1 468A *(office hours only)*
  - Office Hours:
    - Wednesday, 5:30pm-7pm
    - More if needed, e.g., before finals or if out of town on Wednesday
    - Otherwise, by appointment: contact by email to set up

- **TA:** Norrathep (Oak) Rattanavipanon
  - PhD student, research in security & privacy
  - Email: *nrattana* AT *uci.edu*
  - Office Hours:
    - Tuesday 11am-noon and Friday 3-4pm @ ICS1 468A
    - More if needed
Prerequisites

Ideally, at least 2 of:

– Operating Systems (CS 143A)
– Distributed Systems (CS 131)
– Computer Networks (CS 132)

AND:

– Design/Analysis of Algorithms (CS 161)
Class Info

• Lecture format
  – lecture slides (not always posted before class)
  – ~10x2 lectures total (including midterm and final)

• Course website: https://goo.gl/tJ08Pq
  • check it regularly
  • news, assignments, grades and lecture notes (in PDF) will all be posted there

• Read your email
Course Textbooks/Readings

OPTIONAL (BUT RECOMMENDED):

Charlie Kaufman, Radia Perlman, Mike Speciner

OPTIONAL:

Cryptography : Theory and Practice, 3rd edition
Douglas R. Stinson

Also:
Cryptography and Network Security, 4th edition
William Stallings
Course Grading

- Midterm (26%)
- Final (26%)
- 3 Homeworks (16% each)

BTW:
- I may or may not grade on a curve
- I do not hesitate giving C-s and worse ...
- This is a large class (95 students)
- ~12% didn’t pass in previous years so study hard
Student Expectations

• Keep up with material covered in lectures!
  – complete relevant readings before class
  – browse lecture slides
  • Slides will be on-line the same day, before class most of the time

• Attend lectures

• No excuses for not reading your email!

• Exams and homework:
  – No collaboration of any sort
  – Violators will be prosecuted
  – An F in the course is guaranteed if caught
Drop Policy

- Drop anytime during first 2 weeks ...
  - Deadline – Wednesday, October 5th
- Thereafter, no drop
- Incompletes to be avoided at all costs
- But, ... I have to graduate this quarter. Should have planned better.
And remember:

- This is **not** an easy course and **you do not** have to be here.
- This is a big class and **chances are some** will **not pass** (~12% in previous years).
- This **course is not required** for any track.
However:

- You might have fun ... security and crypto are very "interesting" topics (require a special mindset)
- I will certainly make mistakes – point them out!
- I want your feedback
- Please ask questions and challenge me!!!
Complaints about:

• Course content: to instructor
• Course grading: to instructor
• TA/Reader: to instructor
• Instructor, i.e., me:
  – ICS Associate Dean of Student Affairs (T. Givargis)
    or
  – Computer Science Department Chair (A. Nicolau)
Course Topics – Tentative and Unsorted

Will be covered

- Security attacks/services
- Conventional Cryptography
- Public Key Cryptography
- Key Management
- Digital Signatures
- Secure Hash Functions
- Authentication & Identification
- Certification/Revocation

May be touched upon

- Wireless/Mobile Net security
- DDOS attacks and trace-back
- Internet Protocol (IP) security
- Firewalls
- SSL/TLS
- Kerberos, X.509
- Access Control (RBAC)
- E-cash, secure e-commerce
- RFID security
- Trojans/Worms/Viruses
- Intrusion Detection
Focus of the Class

• Recognize security attacks/threats
• Learn basic defense mechanisms (cryptographic and other techniques)
• Appreciate how much remains to be learned after this course

BTW:
• You certainly won’t become an expert (neither a Mr. Robot)
• You might be (I hope) interested to study the subject further
Bird’s eye view

This course

Network Security

CRYPTO

Computer Security
Outline

• The players/actors
• Terminology
• Attacks, services and mechanisms
• Security attacks
• Security services
• Methods of defense
• A model for network security
Computer Security: The Cast of Characters

Attacker or Adversary

Can be: individuals, organizations, nations ...

Your Computer/Phone/Tablet

Your data: financial, health records, intellectual property ...
Network Security: The Cast of Characters

Alice

communication channel

Eve(sdropper)

Bob
Terminology (Cryptography)

• Cryptology, Cryptography, Cryptanalysis
• Cipher, Cryptosystem, Encryption scheme
• Encryption/Decryption, Encipher/Decipher
• Privacy/Confidentiality, Authentication, Identification
• Integrity
• Non-repudiation
• Freshness, Timeliness, Causality
• Intruder, Adversary, Interloper, Attacker
• Anonymity, Unlinkability/Untraceability
Terminology (Security)

- Access Control & Authorization
- Accountability
- Intrusion Detection
- Physical Security
- Tamper-Resistance
- Certification & Revocation
Attacks, Services and Mechanisms

• **Security Attack:** Any action (or event) that aims to compromise (undermine) the security of information

• **Security Mechanism:** A measure (technique or method) designed to detect, prevent, or recover from, a security attack

• **Security Service:** something that enhances the security of data processing systems and information transfers. A “security service” makes use of one or more “security mechanisms”

• Example:
  - **Security Attack:** Eavesdropping (Interception)
  - **Security Mechanism:** Encryption
  - **Security Service:** Confidentiality
Some Classes of Security Attacks

(a) Normal flow

(b) Interruption

(c) Interception

(d) Modification

(e) Fabrication
Security Attacks

• **Interruption**: attack on availability
• **Interception**: attack on confidentiality
• **Modification**: attack on integrity
• **Fabrication**: attack on authenticity
Main Security Goals

- Authenticity
- Confidentiality
- Integrity
- Availability
Security Threats: Threat vs Attack?

Passive Threats
- Release of message contents
- Traffic analysis

Active Threats
- Masquerade
- Replay
- Modification of message contents
- Denial of service

By Injection
By Deletion
Example Security Services

- **Confidentiality:** to assure information privacy and secrecy
- **Authentication:** to assert who created or sent data
- **Integrity:** to show that data has not been altered
- **Access control:** to prevent misuse of resources
- **Availability:** to offer access to resources, permanence, non-erasure

Examples of attacks on Availability:

- Denial of Service (DoS) Attacks
  - e.g., against a name server
- Malware that deletes or encrypts files
Some Methods of Defense

• Cryptography $\rightarrow$ confidentiality, authentication, identification, integrity, etc.

• **Software Controls** (e.g., in databases, operating systems) $\rightarrow$ protect users from each other

• **Hardware Controls** (e.g., smartcards, badges) $\rightarrow$ authenticate holders (users)

• **Policies** (e.g., frequent password changes, separations of duty) $\rightarrow$ prevent insider attacks

• **Physical Controls** (doors, guards, etc.) $\rightarrow$ control physical access