CS 134
Elements of Cryptography and Computer & Network Security
SPRING 2023

Instructor: Gene Tsudik

https://sprout.ics.uci.edu/cs134s23.html

https://canvas.eee.uci.edu/courses/55238

https://piazza.com/uci/spring2023/cs134

Today

- Administrative Stuff
- Course Organization
- Course Topics
- Gentle Introduction
- Basics of Cryptography

CS 134 Background

- Classes: Tu/Th 11:00am-12:20am
- Senior-level undergraduate course
- Some overlap with CS 203 / NetSys 240 (graduate)
- Offered yearly since 2002
- Last time offered Fall 2022 (Prof. A. Chen)

Why (not) take this course?

- Difficult course material
- There will be some unusual math
  - e.g., number theory, group theory
- Tough grading
  - might work hard and still wind up with a "C"
- Mean instructor
- Lecture slides sometimes unavailable before class
- No second chance if you mess up (only 10 weeks!)
- No drop after second week

Contact Information

- Instructor: **Gene Tsudik**
  - Email: ***gene.tsudik@uci.edu***
  - *CS Professor (since 2000)*
  - *Research: Security, Privacy, Applied Cryptography in the context of:*
    - *IoT/CPS, Hardware, UI-s, Internet, Wireless Networks, Attacks, etc*
  - Office Hours:
    - Mondays 10am-noon
    - More if needed, e.g., before midterm and/or final
    - Otherwise, by appointment: contact by email, but try the TA first

- TA:
  - **Elina van Kempen**
    - 2nd year CS PhD student (security/cryptography)
    - Contact: evankemp@uci.edu
    - Office Hours: TBD

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)
  - ~19 lectures total (including midterm)
  - possibly some guest lectures
- Read your email often

Class Info

- Course space: Canvas
  - *https://canvas.eee.uci.edu/courses/55238*
- Q&A space: Piazza
  - *https://piazza.com/uci/spring2023/cs134*
  - *Access Code: Cryptomorphology*
  - Post all your questions there

Course Textbooks/Readings

OPTIONAL (BUT RECOMMENDED):

Network Security: Private Communication in a Public World, 2nd edition
Charlie Kaufman, Radia Perlman, Mike Speciner
Prentice Hall – 2002 – ISBN: 0130460192

OPTIONAL:

Cryptography : Theory and Practice, 3rd edition
Douglas R. Stinson
CRC Press – 2005 – ISBN: 1584885084

Also:
Cryptography and Network Security, 4th edition
William Stallings
Prentice Hall – 2006 – ISBN: 0131873164

Course Grading

- Midterm (30%)
- Final (30%)
- Two home-works (20% each)

BTW:
- I may or may not grade on a curve
- I do not hesitate to assign C-s and lower…
- ~10% didn't pass in prior years, so PLEASE work hard

Student Expectations

- Keep up with material covered in lectures!
  - read lecture slides
  - slides will be on-line the same day
- Attend all lectures (but I won't take attendance)
  - It will likely influence your grade!
  - Generally viewed as the aspect that **most contributes to learning!**
- No excuses for not reading your email!
- Exams and homework:
  - No collaboration of any sort
  - Violators will be dealt with harshly
  - An **F** in the course is guaranteed if caught
  - A note placed in your official academic file

Drop Policy

- No late drops except for documented emergencies
- Incompletes to be avoided at all costs
- But, what if: 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

13

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 constructive feedback
- Please ask questions and challenge (within reason) both me and TA

14

Complaints about:

- Course content: to me
- Course grading: to me
- TAs/Readers: to me
- Instructor, i.e., me:
  - ICS Associate Dean of Student Affairs (M. Gopi)

    or
  - Computer Science Department Chair (T. Givargis)

Course Topics: Tentative & Unsorted

Will be covered

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

We may also touch 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 this course

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

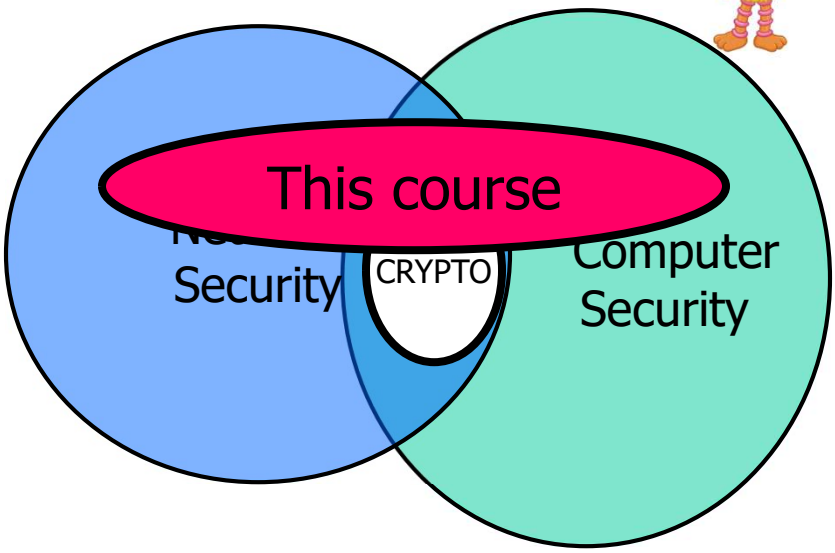
BTW:

- You certainly won't become an expert (or a Mr. Robot-type)
- You might be interested to study the subject further

17

Bird's eye view





18

Outline for today

- Players/actors/entities
- Terminology
- Attacks, services and mechanisms
- Security attacks
- Security services
- Methods of defense
- Model for network security

19

Computer Security: The Cast of Characters

Attacker or Adversary



Can be:
individuals, groups, organizations, nations (including software, or even hardware, acting on their behalf)

Your Computer/Phone/Tablet and IoT devices



Your data: financial, health records, intellectual property …



20

Network Security: The Cast of Characters



communication channel





Alice **Bob**

Eve(sdropper)

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)

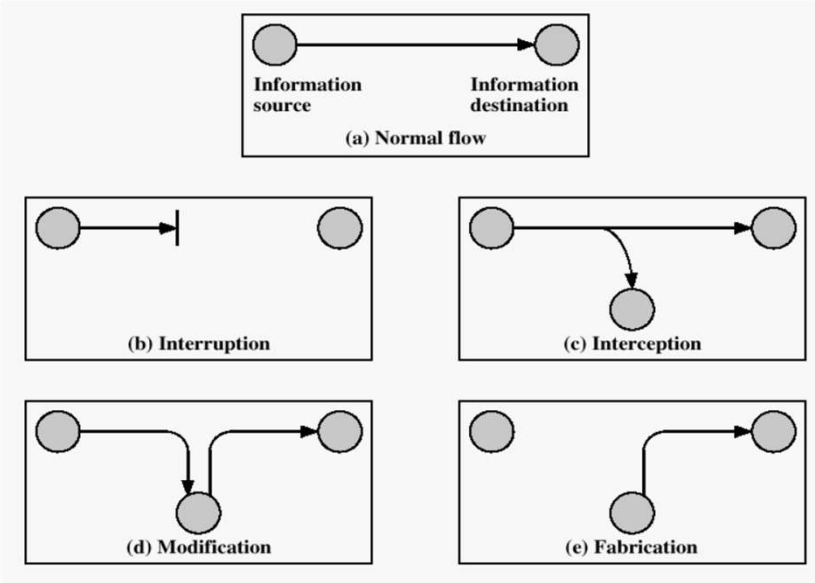
- **Access Control & Authorization**
- **Accountability**
- **Intrusion Detection**
- **Physical Security**
- **Tamper-Resistance**
- **Certification & Revocation**

Attacks, Services and Mechanisms

- **Security Attack:** an action (or event) that aims to compromise (undermine) security of information or resource
- **Security Mechanism:** a measure (technique or method) designed to detect, prevent, or recover from, a security attack
- **Security Service:** something that enhances security. A "security service" makes use of one or more "security mechanisms"

- Examples:
  - ***Security Attack:*** Eavesdropping (aka Interception)
  - **Security Mechanism:** Encryption
  - **Security Service:** Confidentiality

Some Classes of Security Attacks



25

25

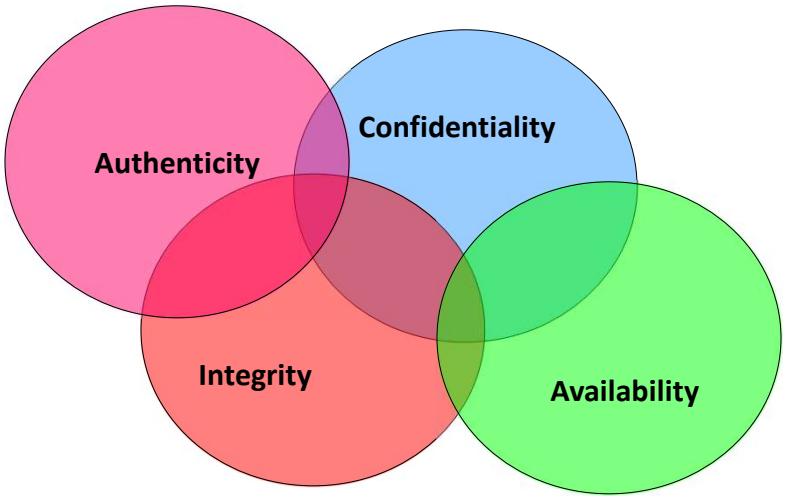
Security Attacks

- **Interruption:** attack on availability
- **Interception:** attack on confidentiality
- **Modification:** attack on integrity
- **Fabrication:** attack on authenticity

26

26

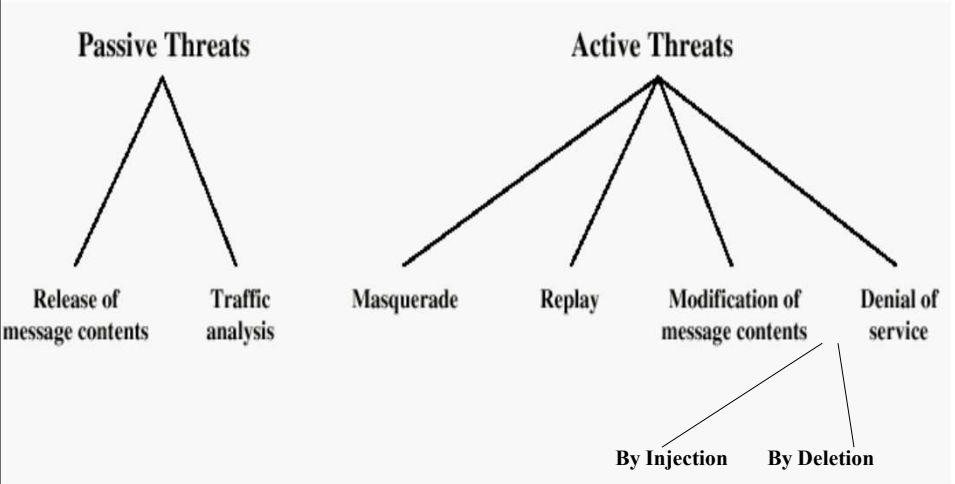
Main Security Goals



27

27

Security Threats



28

28

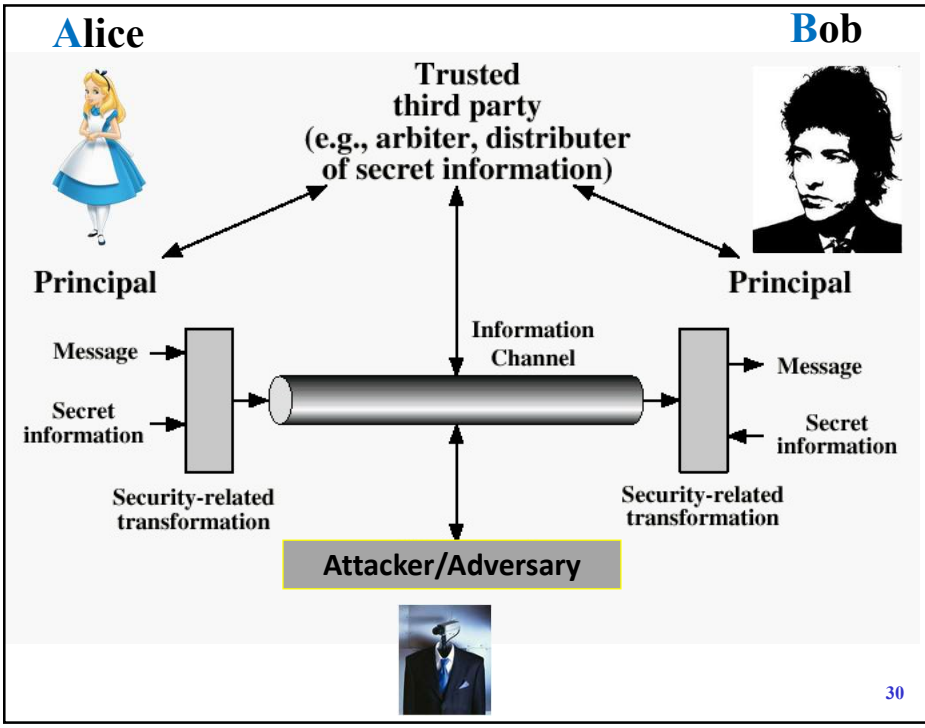
Sample Security Services

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

  Examples of attacks on Availability:

  - Denial of Service (DoS) Attacks
    - e.g., against DNS server, "smart" home camera, or bank web server
  - Malware (ransomware) that deletes or encrypts files

29



30

Some Methods of Defense

- **Cryptography** → confidentiality, authentication, identification, integrity, etc.
- **Software Controls** (e.g., in databases, operating systems) → protect system from users and users from each other
- **Hardware Controls** (e.g., smartcards, badges, biometrics) → authenticate holders (users)
- **Policies** (e.g., frequent password changes, separation of duty rules) → prevent insider attacks
- **Physical Controls** (doors, guards, moats etc.) → physical access controls

End of Lecture 1

Any urgent questions?