CS 134:
Elements of Cryptography and Computer + Network Security
Winter 2015

sconce.ics.uci.edu/134-W15/

CS 134 Background

- 11:00-12:20 @ DBH 1500
- Discussions section – as needed (must register!)
- Senior-level undergraduate course
- Some overlap with CS 203 / NetSYS 240 (graduate)
- Offered since 2002
- Last time Winter 2014

Why (not) take this course?

- Not required for any track or concentration
  - listed as an option in two specializations
- Difficult course material
- There'll be some weird math
- Tough grading
- Lectures often not available ahead of time
- There is no second chance if you mess up
- There is no drop after second week
- No Pass / No-pass option

Contact Information

- Instructor: Gene Tsudik
  - Email: **gene.tsudik **AT* uci.edu***
  - Office: DBH 3228 (office hours only)
  - ICS1 458E otherwise (for urgent matters only)
  - Office Hours:
    - Mondays, 11-noon
    - More if needed, e.g., before finals or if out of town on Monday
    - Otherwise, by appointment: contact by email to set up
- TA: Tyler Kaczmarek
  - PhD student, research in security & privacy
  - Email: ***tkaczmar *AT* uci.edu***
  - Office Hours:
    - Wednesdays, 2-3pm @ ICS1 468
    - 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)
  - 2-3 guest lectures
  - 19 lectures total + midterm
- Course website:

  sconce.ics.uci.edu/134-W15/

  - check it regularly
  - news, assignments, grades and lecture notes (**in PDF**) will all be posted there
- Read your email

Course Textbooks/Readings

"Sort of" REQUIRED:

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 (25%)
- Final (25%)
- 3 Homeworks (15% each)
- 5% for attendance / participation / enthusiasm

BTW:
- I may or may not grade on a curve
- I will not hesitate giving C-s and worse…

Student Expectations

- Keep up with material
  - complete relevant readings before class
  - browse lecture slides
    - Slides will be on-line the same day, after class
- 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

Drop Policy

- Drop anytime during first 2 weeks…
  - Deadline – January 16
- Thereafter, no drop
- Incompletes to be avoided at all costs
- But,…I have to graduate this quarter ☺

and remember:

- This is not a course for wimps
- You don't have to be here
- This course is not required
- I am not flexible

However:

- You might have fun…
- I will certainly make mistakes – point them out!
- I want your feedback
- Please ask lots of questions

Complaints about:

- Course content: to me
- Course grading: to me
- TA: to me
- Instructor, i.e., me:
  - ICS Associate Dean of Student Affairs

    or
  - Computer Science Department Chair

Today

- Administrative stuff
- Course organization
- Course topics
- Gentle introduction

Course Topics – tentative and unsorted

- Security attacks/services
- Conventional cryptography
- Public Key cryptography
- Key Management
- Digital Signatures
- Secure Hash Functions
- Authentication + Identification
- Certification/Revocation
- Wireless/Mobile Net security
- DDOS attacks and trace-back
- IP security
- Firewalls
- SSL/TLS
- Kerberos, X.509
- Access Control (RBAC)
- E-cash, secure e-commerce
- Mobile code security
- WSN security
- RFID
- Trojans/Worms/Viruses
- Intrusion Detection

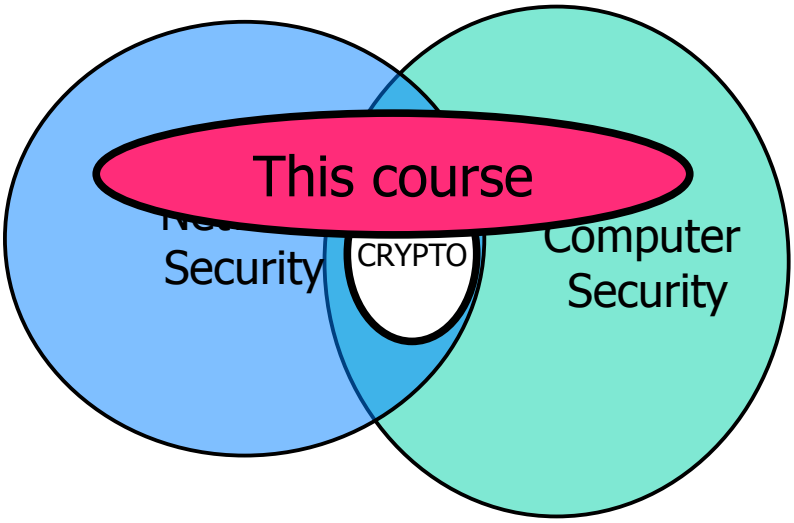
Focus of the class

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

BTW:

- You certainly won't become an expert
- You might be (I hope) interested to study the subject further

Bird's eye view



Outline

- The players
- Terminology
- Attacks, services and mechanisms
- Security attacks
- Security services
- Methods of Defense
- A model for network Security

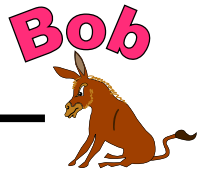
Computer Security: The cast of Characters

Attacker or Adversary

Your computer

Network Security: the cast of characters

communication channel



EVE

Terminology (crypto)

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

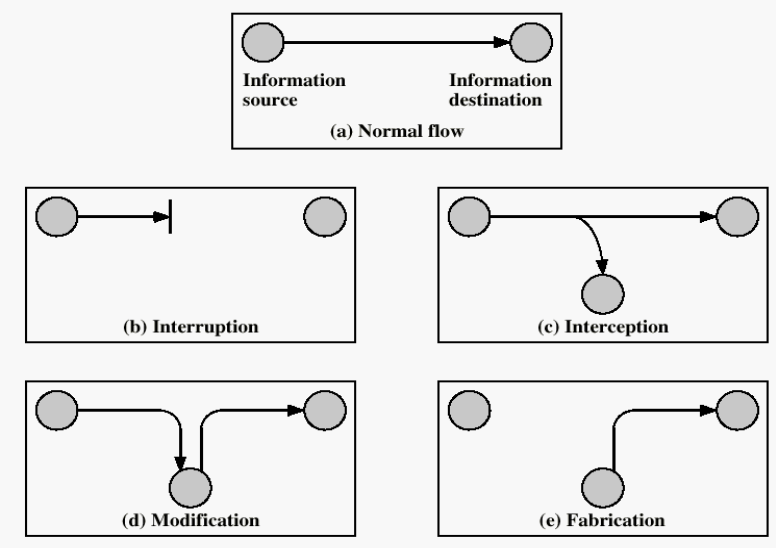
Terminology (security)

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

Attacks, Services and Mechanisms

- **Security Attack:** Any action that aims to compromise the security of information
- **Security Mechanism:** A measure 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

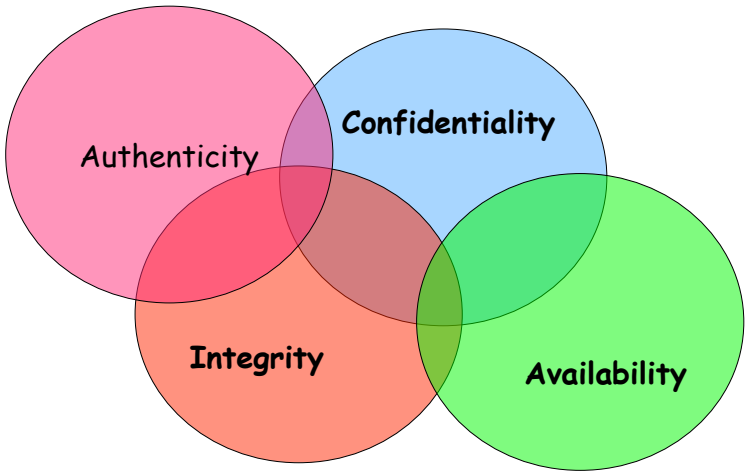
Some Classes of Security Attacks



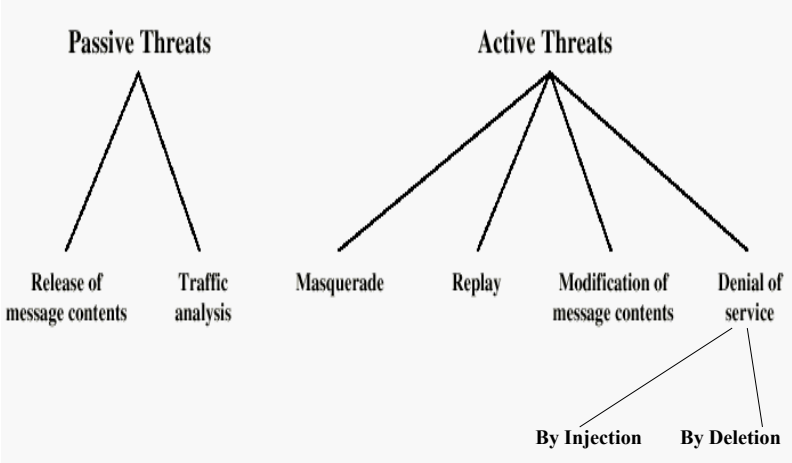
Security Attacks

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

Main Security Goals

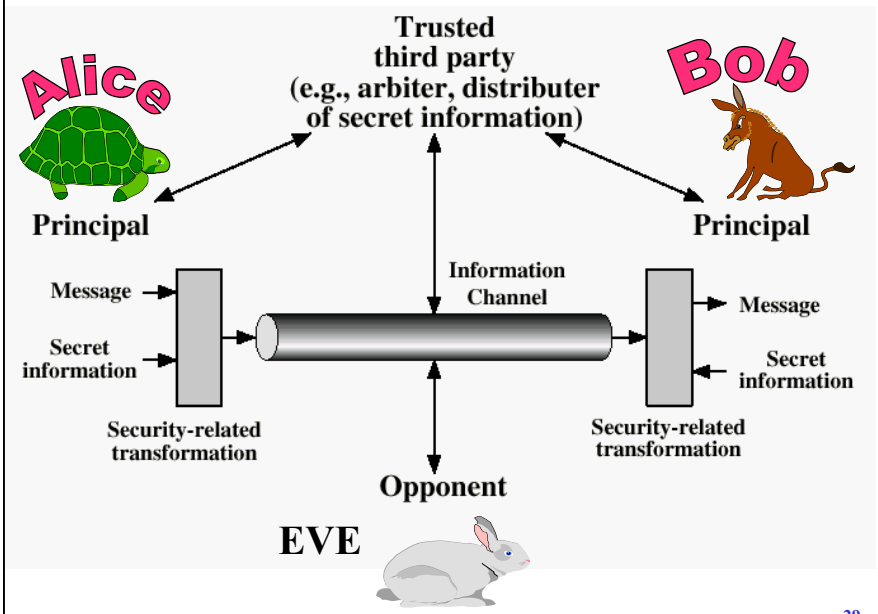


Security Threats
threat vs attack?



Example Security Services

- Confidentiality: to assure information privacy
- 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 permanence, non-erasure
  - Denial of Service Attacks
    - e.g., against a name server
  - Viruses that delete files



Some Methods of Defense

- Cryptography → confidentiality, authentication, identification, integrity, etc.
- Software Controls (e.g., in databases, operating systems) → protect users from each other
- Hardware Controls (e.g., smartcards, badges) → authenticate holders (users)
- Policies (e.g., frequent password changes, separations of duty) → prevent insider attacks
- Physical Controls (doors, guards, etc.) → control access