CS 134
Elements of Cryptography and Computer & Network Security
Fall 2019

Instructor: Qi Alfred Chen

https://www.ics.uci.edu/~alfchen/teaching/cs134-2019-Fall

[lecture slides are adapted from previous slides by Prof. Gene Tsudik]

Today

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

CS 134 Background

- Classes: Tu/Th 2-3:20pm @ HSLH 100A
  - 4 discussion sessions:
    - W 8-8:50 AM SH 128
    - W 9-9:50 AM SH 128
    - W 1-1:50 PM PSCB 140
    - W 2-2:50 PM PSCB 140
- Senior-level undergraduate course
- Some overlap with CS 203 / NetSYS 240 (graduate)
- Offered yearly since 2002
- Last time offered Spring 2019

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 may not available ahead of class
- No drop after second week
- No [Pass/No-Pass] option

Contact Information

- Instructor: Qi Alfred Chen -- Just call me "Alfred"
  - Email: *alfchen@uci.edu*
  - Assistant Prof. in CS
  - Research area: **Cybersecurity**
    - Most interested in the attack side
      - Breaking things, especially real-world systems, are fun!
        - Past: Smartphone, network protocols, GUI, access control, …
        - Recent: Smart home, self-driving cars, smart traffic light, …
      - My attack demo videos on YouTube attracted **> 90,000 views** (as of this year) from all over the world (daily peak of **>17,000 views** ☺)
    - Also work on the defense side
      - Fixing problems are bigger contributions!
    - More details in my website: https://www.ics.uci.edu/~alfchen/
  - Office Hours:
    - Wednesdays, 4-5 PM, DBH 3204
    - More if needed, e.g., before midterm and/or final
    - Otherwise, by appointment: contact by email but try TA-s first

Contact Information

- TAs:
  - Yoshimichi Nakatsuka

    Contact: nakatsuy@uci.edu
  - Samuel Pangestu

    Contact: spangest@uci.edu
- Readers:
  - Takami Sato

    Contact: takamis@uci.edu
  - Ziwen Wan

    Contact: ziwen.wan@uci.edu

OFFICE HOURS: Thursday 5-6 PM (starting next week), ~~DBH 4011~~ICS2 214, 215, 216, 217

Please **only use Piazza** for questions to TA/readers; emails above are only for emergency use

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
  - Classes I will most likely miss
    - Oct 29: Security PI meeting
    - Nov 21: CPS PI meeting
- Course website:
  - check it regularly
  - news, assignments, grades and lecture notes (PDF) will all be posted there
- Read your email often

Class Info

- Course space: Canvas
  - https://canvas.eee.uci.edu/courses/19896
  - Only for email-based announcements
- Q&A space: Piazza
  - https://piazza.com/uci/fall2019/compsci134
  - Post all your questions here
- Grading: Gradescope
  - https://www.gradescope.com/courses/66307
  - Entry code in Piazza
  - Homeworks will be turned in here

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 (26%)
  - Time (tentative): Oct 31 Thursday, in class
- Final (26%)
  - Time: Dec 12 Thursday, 1:30-3:30pm
- 3 Homeworks (16% each)

BTW:

- I may or may not grade on a curve
- I do not hesitate assigning "C"-s and worse …
- This is a large class (>150 students)
- ~10% didn't pass in previous years, so study hard

Student Expectations

- Keep up with material covered in lectures!
  - browse lecture slides
    - Slides will be on-line the same day
- Attend all lectures
- 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 in your 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
- This is a big class and some of you will get unpleasant grades

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) me and TAs

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 (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

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

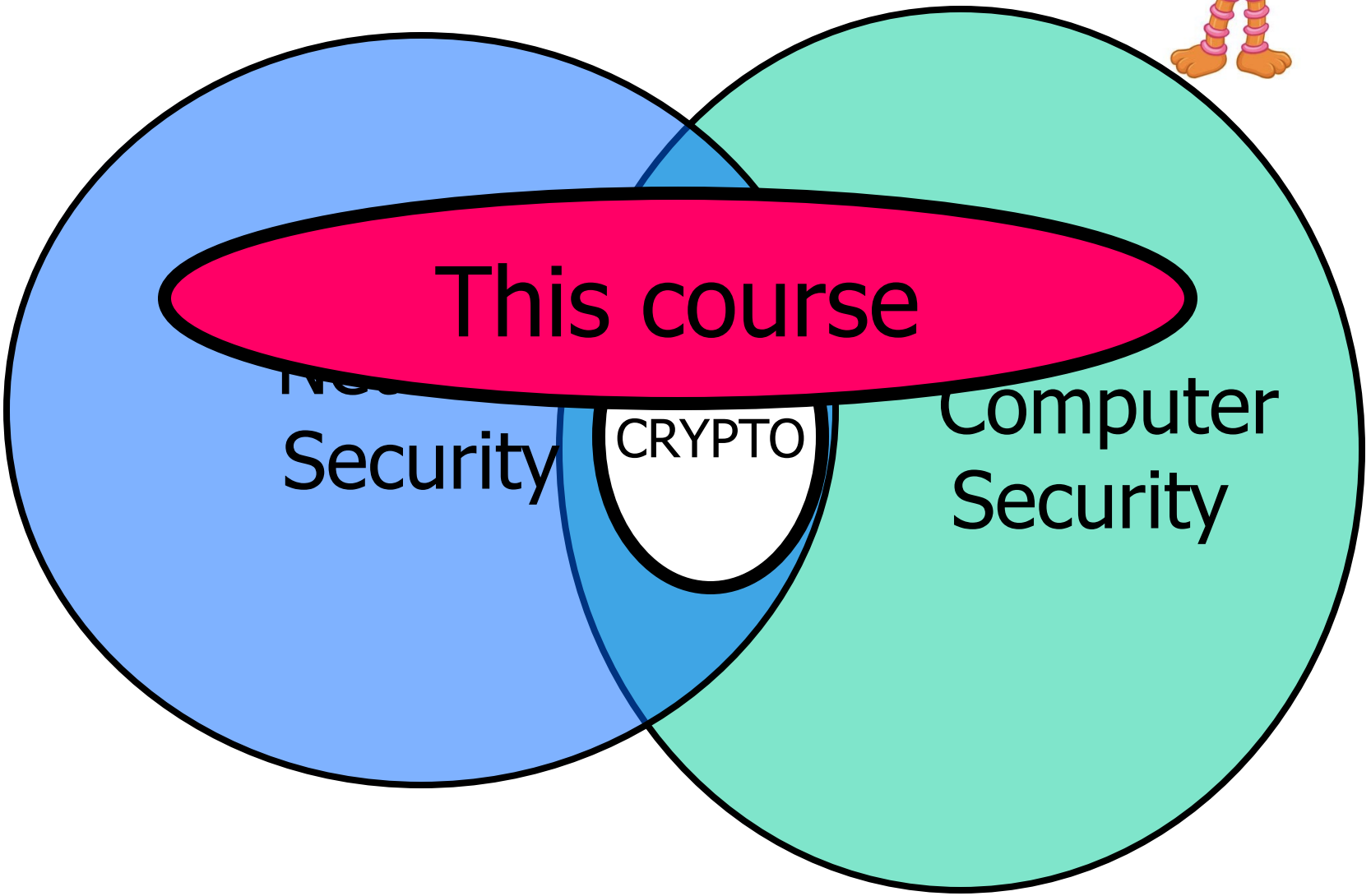
Focus of the Class

- 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 (or a Mr. Robot-type)
- You might be interested to study the subject further

Bird's eye view



Outline

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

Computer Security: The Cast of Characters

Attacker or Adversary

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

Your Computer/Phone/Tablet

Your data: financial, health records, intellectual property …

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)

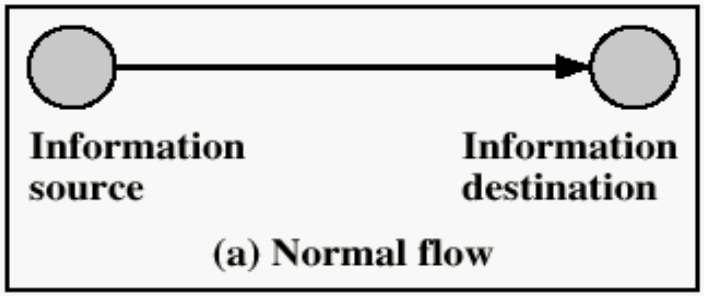
- **Access Control & Authorization**
- **Accountability**
- **Intrusion Detection**
- **Physical Security**
- **Tamper-Resistance**
- **Certification & Revocation**

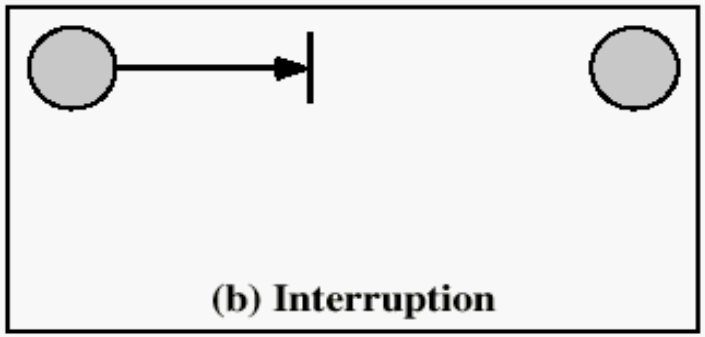
Attacks, Services and Mechanisms

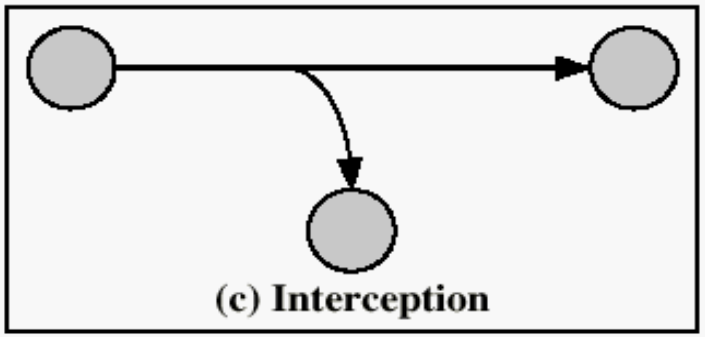
- **Security Attack:** an action (or event) that aims to compromise (undermine) security of information or resource
- **Security Mechanism:** a measure (technique or method) designed to detect, prevent, or recover from, a security attack
- **Security Service:** something that enhances security. A "security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

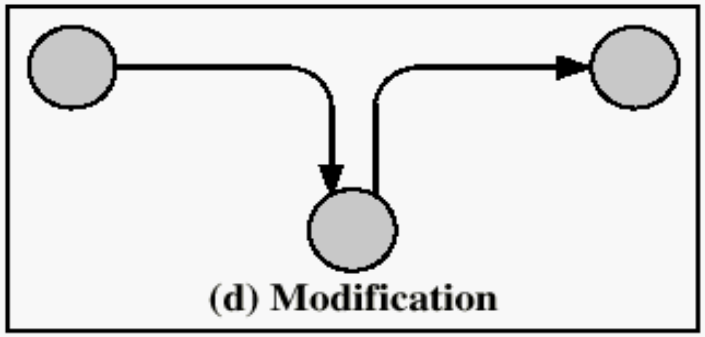
- Examples:
  - ***Security Attack:*** Eavesdropping (aka Interception)
  - **Security Mechanism:** Encryption
  - **Security Service:** Confidentiality

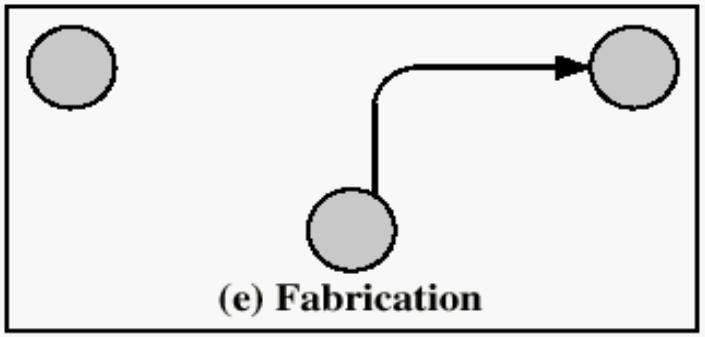
Some Classes of Security Attacks







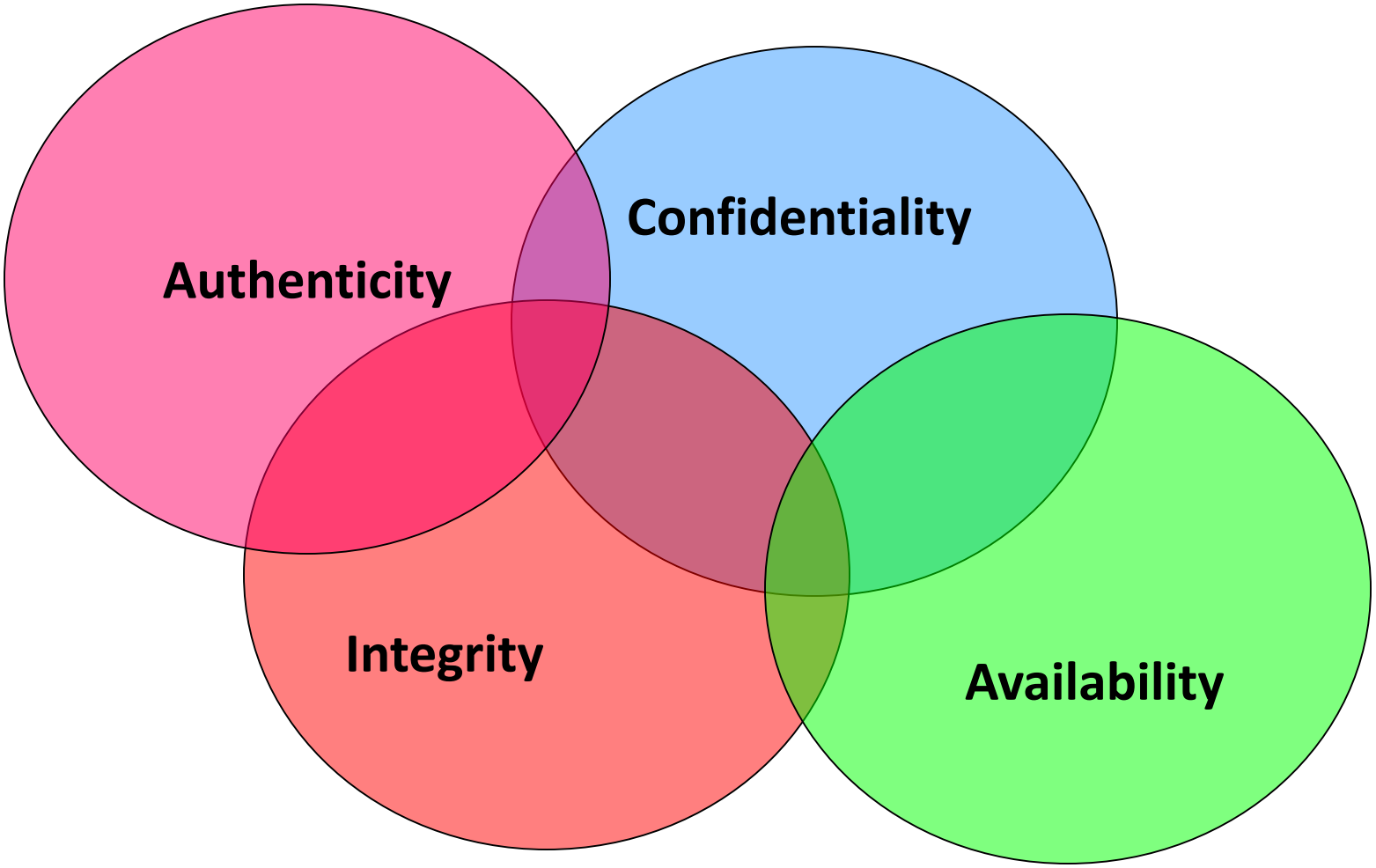




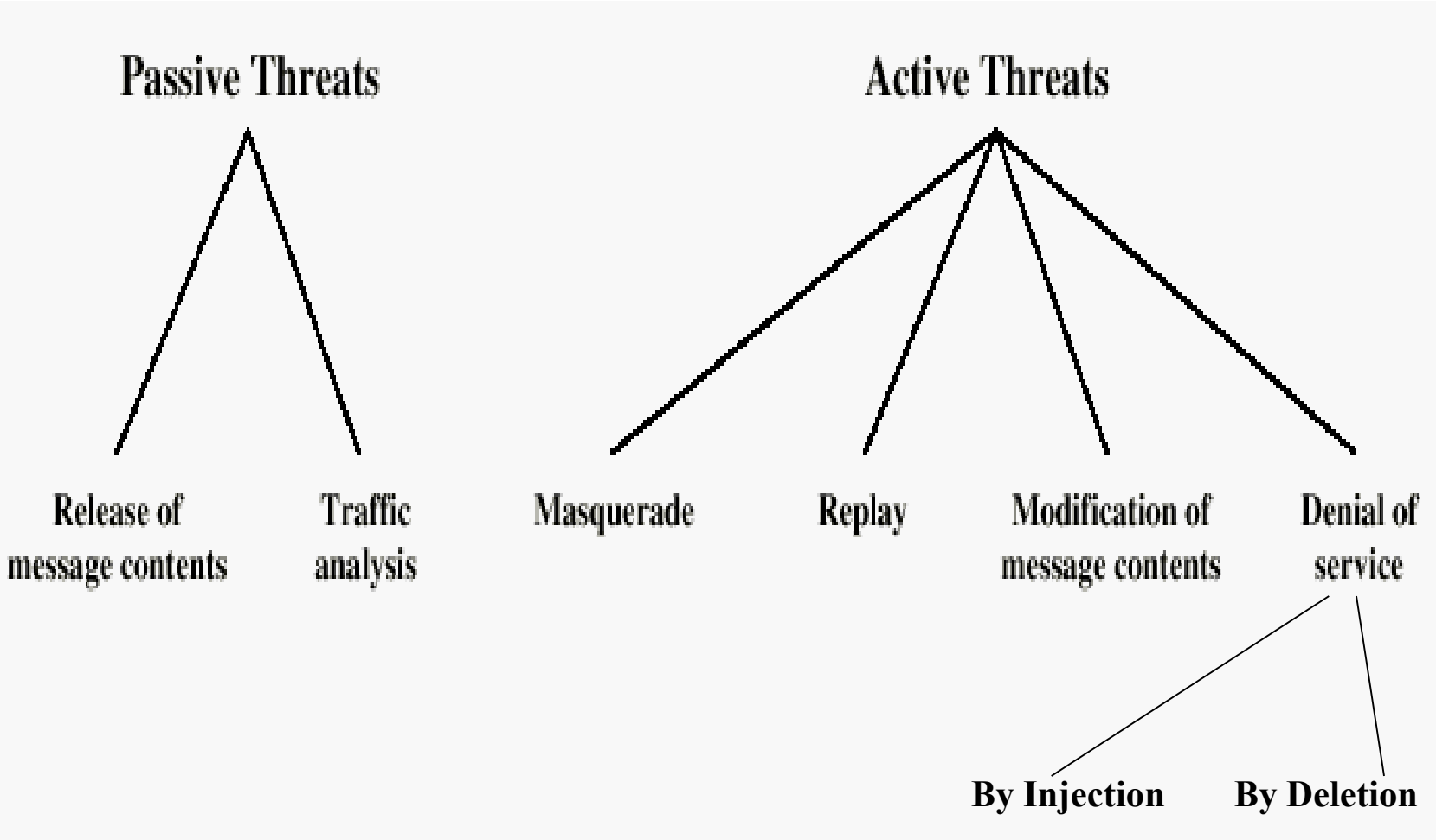
Security Attacks

- **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 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 a DNS name server or Bank Web server
  - Malware (ransomware) that deletes or encrypts files

Alice

Bob

Trusted
third party
(e.g., arbiter, distributer
of secret information)

Principal

Principal

Message

Secret
information

Information
Channel

Message

Secret
information

Security-related
transformation

Security-related
transformation

Attacker/Adversary

Some Security Mechanisms

- **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?