

Welcome to CS 134 (formerly known as ICS 168): Elements of Cryptography and Computer + Network Security Winter 2007

<http://sconce.uci.edu/134>
(currently not available due to Bren Hall move)

1

ICS 134: background

- Senior-level undergraduate course
- Some overlap with ICS 268/243G (graduate courses)
- Offered yearly
 - AY01-02: Spring 2002
 - AY02-03: Fall 2002
 - AY03-04: Winter 2004
 - AY04-05:
 - Winter 2005
 - Summer 2005
 - AY05-06: Winter 2006
 - AY06-08: Winter 2007

2

Why take this course?

- Not required for any track or concentration
 - But listed as an option in two specializations
- Difficult course
- There'll be some weird math
- The instructor is a hard grader
- Lectures are not available ahead of time
- There is no 2nd chance if one messes up
- There is no drop after 2nd week
- Can't take it P/NP
- It's a difficult course...

3

Contact Information

- Instructor: Gene Tsudik
 - Email: gts@ics.uci.edu
 - Phone: x43410
 - Office: CS 458E (might change!)
 - Office Hours:
 - Wed: 4:00-5:00pm
 - Fri: 9:30-10:30am (no office hours tomorrow)
 - Else, by appointment: email, phone
- TA/Grader: Claudio Soriente
 - 2nd year PhD student, research in security
 - Email: csorient@uci.edu
 - Office Hours:
 - Discussion Section
 - 1 more hour TBD

4

Complaints about:

- Course content: to me
- Course grading: to me
- TA: to me
- Instructor, i.e., me:
 - ICS Undergraduate Associate Dean: Prof. Regan
 - or
 - ICS Dean: Prof. Richardson
- Life in general: ?

5

Prerequisites

- Ideally, at least 2 of:
 - Operating systems (143)
 - Distributed systems (148)
 - Computer networks (153)But might do with one...
- Design/Analysis of Algorithms (161)

6

Class Info

- Lecture format
 - Slides (not usually posted before class)
 - Maybe 1 or 2 guest lectures
 - 19 lectures total + midterm;
- Browse the course Web site often:
 - <http://sconce.uci.edu/134>**
 - check it regularly
 - News, grades and lecture notes (**in PDF**) will all be there
- Read your email, class mailing list:
 - 34170-W07@classes.uci.edu**

7

Course Textbooks/Readings

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:

Possibly, some research papers (will be made available on line)

8

Course Grading

- Midterm (25%)
and
- Final (25%)
and
- 3 home-works (15% each)
and
- 5% for attendance/participation/enthusiasm

BTW:

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

9

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
- Read your email regularly. No excuses!
- Exams and homework:
 - No collaboration of any sort
 - Violators will be prosecuted
 - An F in the course is guaranteed

10

Drop Policy

- Drop anytime during first 2 weeks...
- Thereafter, no drop
- Incompletes to be avoided at all costs
- But,...I have to graduate this quarter

11

and remember:

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

12

also:

- You might have fun...
- I certainly will make some mistakes
- I want your feedback!
- Please ask lots of questions

13

Today

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

14

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
- Trojans/Worms/Viruses
- Intrusion Detection

15

Focus of the class

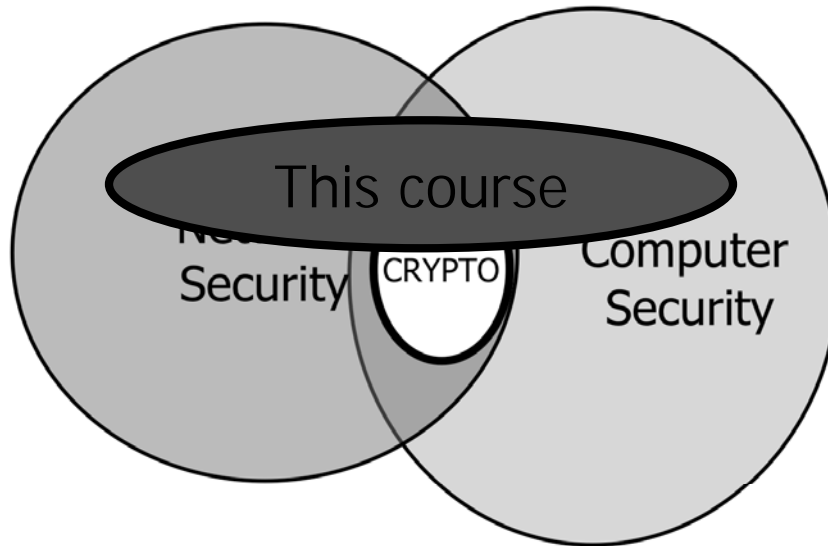
- Recognize security attacks/threats
- Learn basic defense mechanisms (crypto and otherwise)
- Appreciate how much remains to be learned after this course

BTW:

- You will certainly not become an expert
- You will (I hope) be interested to study further

16

Bird's eye view



17

Outline

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

18

Computer Security: The cast of Characters

Attacker or Adversary



Your computer



19

Network Security: the cast of characters



communication channel



EVE

20

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**

21

Terminology (security)

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

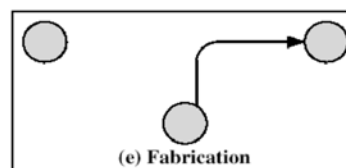
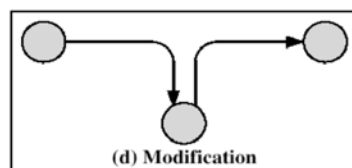
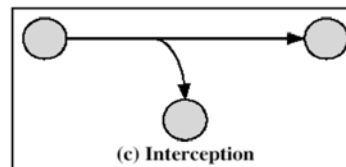
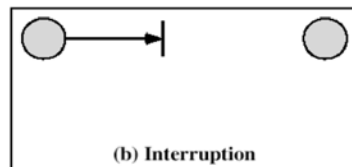
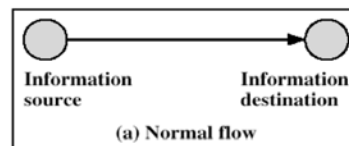
22

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

23

Some Classes of Security Attacks



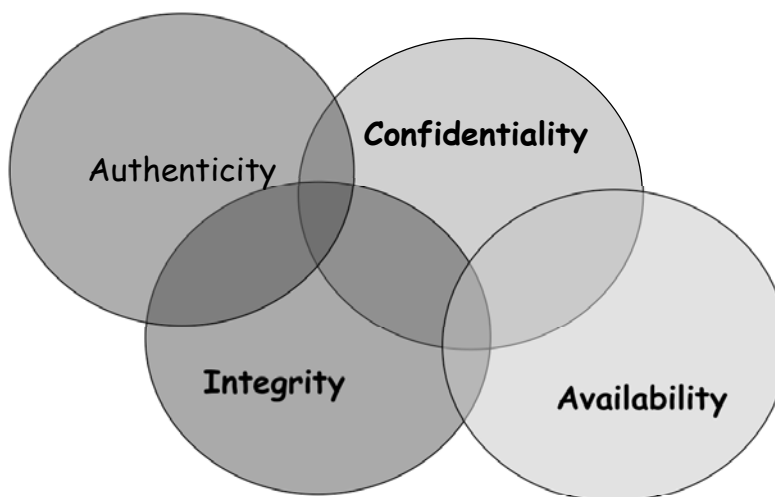
24

Security Attacks

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

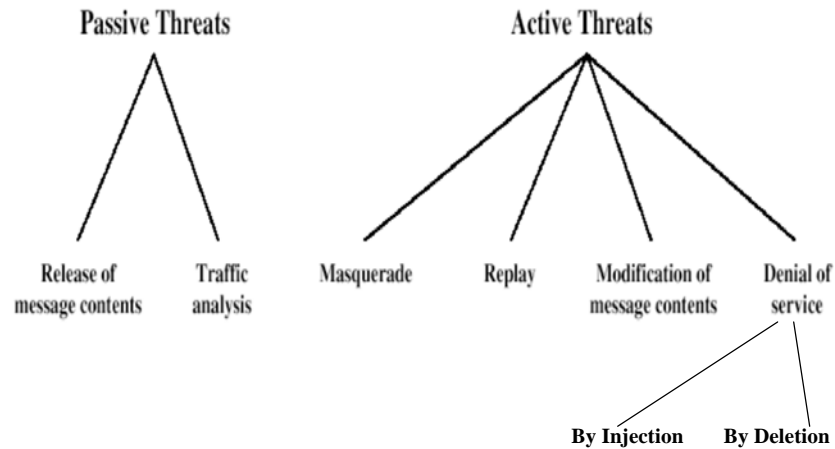
25

Main Security Goals



26

Security Threats threat vs attack?

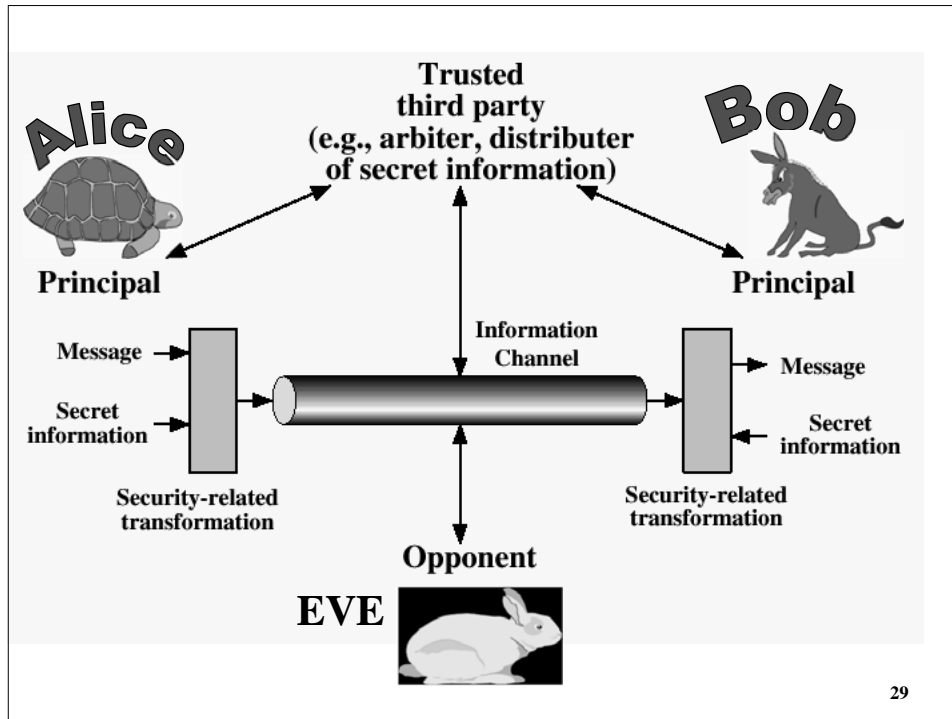


27

Example Security Services

- Confidentiality: to assure 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

28



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) → authenticate holders
- Policies (e.g., frequent password changes, separations of duty) → prevent insider attacks
- Physical Controls (doors, guards, etc.) → control access