



22c:196

## Security in a distributed system

---

EJ Jung

<http://www.cs.uiowa.edu/~ejjung/courses/196/>



## Course Personnel

---

- ◆ Instructor: **EJ Jung**
  - Office: MacLean Hall 201L
  - Office hours: Tue 1-2pm and Thu 10-10:50am
  - Email: include 22c:196 in the subject
  - Open door policy – don't hesitate to stop by!
- ◆ Watch the course website
  - Announcements, reading materials, lecture notes



## Prerequisites

---

- ◆ Required: 22c:021, 031, 118
  - Data structure, algorithms, computer networks
  
- ◆ Recommended:
  - Intro to cryptography
  
- ◆ Student questionnaire



## Background?

---

- ◆ Introduction to computer security?
  - Access control, Web security, sandboxing, firewalls?
  
- ◆ Cryptography?
  - Public-key and symmetric encryption, digital signatures, cryptographic hash, random-number generators?
  
- ◆ Computer networks?
  - Network architecture, application and transport layer protocols?
  
- ◆ Goals in this course?



## Grading

---

- ◆ Class participation (15% of the grade)
- ◆ Reviews (15% of the grade)
  - One or two papers a week
  - Half to one page review per week
- ◆ 1 hour presentation (20% of the grade)
  - Present the required readings or more
  - Pick your topic by Thursday, January 25
- ◆ Project (50% of the grade)
  - Individual
  - System design to the pseudo code level
  - Implementation is optional
- ◆ No extensions



## Example project

---

- ◆ Design a peer-to-peer file backup system
- ◆ Use reputation system to choose which peer to store the backup
- ◆ Pseudo code of each peer's decision and action



## Plagiarism

---

- ◆ UI CLAS policy at
  - [http://www.clas.uiowa.edu/students/academic\\_handbook/ix.shtml](http://www.clas.uiowa.edu/students/academic_handbook/ix.shtml)
- ◆ ACM's guideline at
  - <http://www.acm.org/pubs/plagiarism%20policy.html>
- ◆ No verbatim copying without quotation marks
  - unless you wrote it before



## Accommodation

---

- ◆ Contact me for any accommodation needed
  - class, assignment, test, schedule, etc.
- ◆ Make-up exams are only allowed for the occasions specified by CLAS
  - [http://www.clas.uiowa.edu/faculty/teaching/classroom\\_p&p/general\\_exam\\_p&p.shtml](http://www.clas.uiowa.edu/faculty/teaching/classroom_p&p/general_exam_p&p.shtml)



## Course Materials

---

- ◆ No required textbook
- ◆ Required readings
  - Links from the class homepage
  - Most of them are accessible through Ulowa InfoHawk
    - Can use [scholar.google.com](https://scholar.google.com) at school



## Main Themes of the Course

---

- ◆ Recurring ideas in security in distributed systems
  - Not to understand one paper or system
  - But to see the core of secure system design
  - Be able to apply these ideas yourself
- ◆ Challenges in distributed systems
  - Bandwidth
  - Synchrony
  - Trust on a stranger node



## What This Course is Not About

---

- ◆ Not a comprehensive course on computer security
- ◆ Not a course on ethical, legal or economic issues
  - No file sharing, DMCA, free speech issues
- ◆ No overview of cryptography
- ◆ Only some issues in systems security
  - No how to share files on Windows or Unix
  - No which firewall program is the best
- ◆ No language-based security



## List of topics – pick by Jan. 25

---

- ◆ Logical key hierarchy
- ◆ Merkle hash tree
- ◆ One-way key chain
- ◆ Threshold cryptography
- ◆ Distributed hash table
- ◆ Reputation systems
- ◆ Signature of viruses and worms
- ◆ Role-based access control
- ◆ Probabilistic Safety
- ◆ Dictionary attack
- ◆ Hash function and breaking them
- ◆ Trusted computing