CSC650 Secure Networked Systems

Introduction

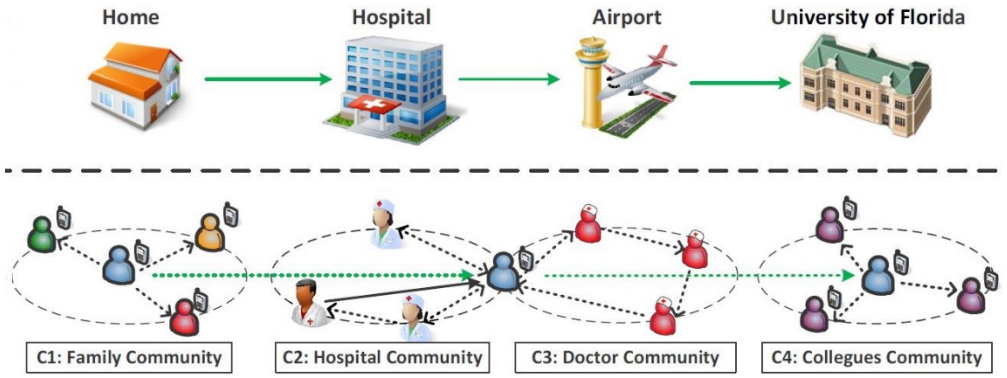
Professor Hao Yue

Spring 2016

Welcome!

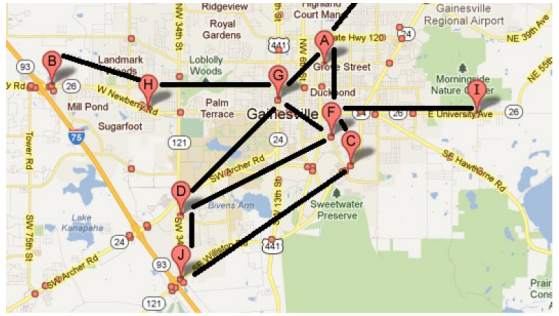
Who am I

Hao Yue
Assistant Professor
Email: haoyue@sfsu.edu
Homepage: TBA



Research Interests:

- Wireless Networks
- Mobile Computing
- Computer and Network Security
- Internet of Things



Past

If he had anything confidential to say, he wrote it in cipher, that is, by so changing the order of the letters of the alphabet, that not a word could be made out. If anyone wishes to decipher these, and get at their meaning, he must substitute the fourth letter of the alphabet, namely D, for A, and so with the others.

-- Suetonius, Life of Julius Caesar

Now

- Security stories in the past 24 hours
  - A serious security flaw was found in eBay, which could leave buyers and sellers vulnerable to hack attacks
  - Vulnerability discovered in Children's Internet-connected toy
  - Nokia released a new Internet-of-Thing security tool to monitor and control all the components on a network
  - J. P. Morgan announced it is planning to invest a half-billion dollars in security
  - …

Course Overview

- This course introduces the fundamental concepts on computer security and standard security mechanisms and protocols.
- Topics will include Secret Key Cryptography, Public Key Cryptography, Authentication, Network Security, Intrusion Detection, DDoS, Web Security, DES, RSA, IPsec, SSL/TLS, and other emerging topics (as time permits).

Learning Outcome

- Students successfully completing this course will
  - Have basic knowledge on cryptography and standard network security mechanisms
  - Gain hands-on experience in implementing security mechanisms and building secure systems

General Info

- Instructor: Hao Yue
- Class Time/Location: Tuesday, 7:00PM – 9:45PM, TH429
- Office: TH930
- Office Hours: Wednesday 11:00AM-12:00PM and 5PM-6PM, or by appointment
- Email: haoyue@sfsu.edu
- TA: TBA

Class Time

- One class is divided into three sessions

  Session 1: 7:00-7:50PM

  Break: 7:50-8:00PM

  Session 2: 8:00-8:50PM

  Break: 8:50-9:00PM

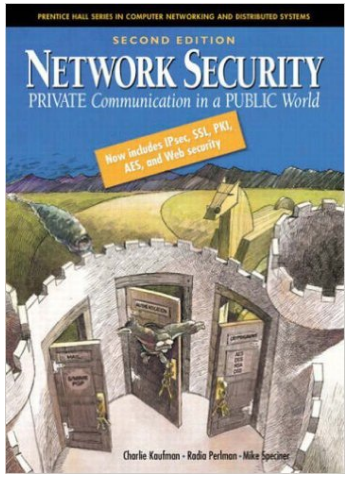
  Session 3: 9:00-9:45PM

You need to know

- Operating Systems
- Computer Networks
- C/C++ programming language
- Please contact the instructor if you have questions regarding the concerns about whether your background is suitable for the course.

Course Materials

- Textbook
  - Network Security: Private Communication in a Public World, 2nd Edition, by Charlie Kaufman, Radia Perlman and Mike Speciner
- Course slides, assignments, and other materials will be made available on iLearn.



Grading

- Grading will be distributed as follows:
  - 10% Attendance and Quizzes
  - 15% Homework Assignments
  - 20% Course Projects
  - 25% Midterm Exam
  - 30% Final Exam
- Final scores will be converted to letter grades based on a class curve
- You get the grade that you earn, so be sure that you earn a grade you like.

Grading

- Assignments
  - Three homework assignments. Each counts for 5% of the final grade.
  - Two project assignments. Each counts for 10% of the final grade.
- Exams
  - One closed-book, closed-notes midterm and one take-home final exam
- Attendance and Quizzes
  - Five roll-calls. Each counts for 1% of the final grade.
  - Quizzes count for 5% of the final grade in total
- Class Participation
  - Students actively participating in class will receive up to 5 bonus points in the final grade

Lateness

- All assignments are due at the beginning of class
- Late submission within 48 hours of the deadline is allowed, for 75% of the credits
- Students with legitimate reasons should contact the instructor before the deadline to ask for an extension
  - Unless the problem is apocalyptic, don't give me excuses
- Start to work on the assignments as early as possible

Academic Integrity

- As scientists and engineering, we must trust each other to make progress
- Academic dishonesty, whether from *cheating, copying, fabricating results* or through *any other dishonest practice* will not be tolerated
- Refer to the link http://cs.sfsu.edu/plagarism.html for the department policy on plagiarism/cheating
- I take this very seriously – you should too.

What is security?

- Security is the protection of the items you value, called assets
- Assets of computer systems

Hardware

Software

Data

Security Goals

C-I-A Triad

- Confidentiality: information or resources can only be accessed and viewed by authorized parties
- Integrity: information or resources can be modified only by authorized parties
- Availability: information or resources accessible to authorized parties at appropriate times

Threats

- A threat is a set of circumstances that has the potential to cause loss or harm to a system
  - An ability of an attacker
  - E.g., eavesdrop on a communication channel
- A threat model is a collection of threats that deemed important for a particular system
  - A collection of attacker(s) abilities
  - E.g., A powerful attacker can read and modify all communications and generate messages on a communication channel

Vulnerabilities

- A vulnerability is a weakness that may be exploited to cause a threat
  - E.g., easy-to-guess password

- Sources of a vulnerability
  - Bad software or hardware
  - Bad design or requirements
  - Bad policy
  - System misuse
  - …

Attacks

- An attack occurs when someone attempts to exploit a vulnerability
  - Passive attacks (e.g., eavesdropping, traffic analysis)
  - Active attacks (e.g., message modification, message replay, Denial of Service)

- A compromise occurs when an attack is successful

Participants and Adversaries

- Participants are expected system entities
  - Computers, agents, people, enterprises, …
  - Depending on context referred to as: servers, clients, users, entities, hosts, routers, …
- An adversary is anyone attempting to launch an attack
- Could users be adversaries?

Trust

- Trust refers to the degree to which an entity is expected to behave
- A trust model describes, for a particular environment, who is trusted to do what.
- We make trust decisions every day…

Security Model

- A security model is the combination of a trust and threat models that address the set of perceived risks
  - Every design must have security model
- The single biggest mistake seen in use of security is the lack of a coherent security model
- This class is going to talk a lot about security models
  - What are the threats?
  - Who are our adversaries?
  - Who do we trust and to do what?

A Security Model Example

- Assume we have a University website that hosts courses through the web (e.g., iLearn)
  - Syllabus, other course information
  - Assignments submissions
  - Online Grading
- In class: elements of the security model
  - Participants (Trusted)
  - Adversaries
  - Threats