**Course Title: Computer Systems Security**

## Syllabus

- Introduction, Threat Models
- Mobile Phone Security
- Anomaly Detection with Machine Learning
- Wireless security
- smart grid security
- Forensics
- system security
- Security Awareness

## Grading

| ACTIVITIES | PERCENTAGES |
|---|---|
| Mid Term | 20% |
| Final Exam | 35% |
| Final Project and Presentation | 25% |
| Homework (small projects) and Class Participation | 20% |

## Description

This course studies the design and implementation of secure IT and Industrial systems. Lectures cover threat models, attacks that compromise security, and techniques for achieving security, based on recent research papers.

Apart from reference books, each lecture will cover a paper in systems security. The paper should be read before lecture.

We'll discuss the paper in class. Please interrupt, ask questions, and point out mistakes.

### Hands-on

Each class will have a Hands-on session.

### Assignments

There are 4 labs and a final project in this course. Labs will look like real-world systems, in some respects: There are many interacting parts written in different languages. We'll look at / write Python, Javascript, etc…

There will be a final project at the end of the course (groups of 2–3 people), and presentations during the last week of class. Think of projects you'd like to work on as you're reading papers. Either attack or defense-oriented projects are possible. It is ok to combine this project with other class projects or your own research.

Lab exercises will be graded on the correctness based on both the lab assignment and whether they fulfill the specifications imposed by the grading / checking scripts.

### Turn-In Policy

You are required to turn in each lab.

### Collaboration

You are welcome to discuss the labs with other students, but you should complete all assignments on your own, and you should carefully acknowledge all contributions of ideas by others, whether from classmates or from sources you have read. Final projects will be in groups, where you should collaborate.

### Warning About Security Work / Research

You will learn how to attack systems so that you know how to defend them. Just because something is technically possible, doesn't mean it's legal.

## References


- Network Security (2nd edition) by Kaufman, Perlman, and Speciner. ISBN 0130460192.
- Menezes, van Oorschot, and Vanstone. Handbook of Applied Cryptography. CRC Press.
- Network Security Essentials by Stallings
- William Stallings and Lawrie Brown
- Applied Information Security: A Hands-on Approach, by David Basin, Patrick Schaller, and Michael Schlapfer.

+

- Research papers for each topic.