Security 2: Introduction

Suman Jana

Columbia University

Course goals

- Deeper dive into computer security
  - Understanding security vulnerabilities and existing defenses
  - Learn how to build secure systems

How to think about security

- Security is an end-to-end property of the overall design/system
- You do not get security by sprinkling on crypto or by forcing people to change their passwords frequently
- Those can sometimes help—but bad guys go around strong security, not through it
- Security is a systems property

How to think about insecurity…

- The bad guys don’t follow the rules
- To understand how to secure a system, you have to understand what sort of attacks are possible
- Note that that is not the same as actually launching them. . .

Logistics

- No text book but assigned readings from different sources
- Grading
  - Three programming assignments in C/Python (30%)
  - Take home Midterm (20%)
  - Final project (45%)
  - Class participation (5%)
- Class webpage: http://sumanj.info/security_2.html

Prerequisites

- COMS W4181 is a prerequisite for this class—I assume that you know the material in it
- However—in this very bureaucratic university, SSOL does not enforce prerequisites
- A prerequisite is a warning: you are expected to know the material
- I will not ask anyone if they've taken 4181 or not But—I will not review encryption algorithms, firewalls, etc.
- If you have any doubts, see me

Late policy

- As noted, three programming assignments (PAs)
- PAs must be submitted electronically by the deadline
- PAs received later that day lose 5%, the next day 10%, two days late 20%, three days late 30%; after that, zero credit
- Exceptions granted only for unforeseeable events. Workload, day job, etc., are quite foreseeable.
- No grace period, no freebies
- Problems? See TAs/me before the due date

Contacting Me

- Feel free to drop in during (virtual) office hours.
- I’ll announce changes (if any) on my home page
- I’m amenable to meeting other times, by appointment.
- If you have any questions, please use email

Lectures

- I prepare slides for each class, and upload them shortly before class time
- Slides (and other information) are uploaded to my web page
- Well, occasionally they’re uploaded shortly after class. . .

Responsibility

- You’re all adults
- You’re all responsible for your own actions
- If there’s something missing, you have to tell me/TA ASAP

Programming assignments

- All programming homework must be done in C or C++ unless otherwise instructed. Don’t bother asking for exceptions.

- Turn in a single tar file, including a Makefile; if necessary, include test data and a README file with execution instructions

- All programs must compile and run on Linux on the Google Cloud machines; zero credit for programs that don’t compile. Note that this means you must be comfortable compiling and running code on Linux.

- Because most security problems are due to buggy code, there will be copious deductions for bugs

Project

- Teams of 3 (might change depending on the final class size)
- Pick teammates early by first 2-3 weeks of the class
- Ideally, you will pick projects one of the following two theme areas: automated vulnerability detection (e.g., fuzzing), and machine learning + security
- Talk to me early, I can help to pick a project topic that suits your skills and interests