CSci 8271
Security and Privacy in Computing
Day 1: Introduction and Logistics

Stephen McCamant
University of Minnesota

Introductions

Outline

Big-Picture Introduction

Course Logistics

Topics Overview

What is computer security?

- Keep "bad things" from happening
- Distinguished by presence of an adversary

Two sides of security

- Defenders / white-hats / good guys[sic]
- Attackers / black-hats / bad guys[sic]
- Each side's strategy depends on the other
- In some ways like a game

Classic security goals

- Confidentiality
- Integrity
- Authenticity
- Availability

What about "privacy"?

- One perspective: privacy $\subset$ security
  - Roughly a synonym for confidentiality
- But, very different emphasis
  - "Security" often means interests of institutions, administrators
  - "Privacy" is an interest of individuals often against institutions

Tool: cryptography

- Math techniques for making things purposely hard to figure out
- More than just encryption and decryption
- We take a research but results rather than proof-focused perspective

Tool: program analysis

- Programs whose job is to operate on other programs
- For bug finding, hardening, etc.

Applications

- Security problems occur all over computer science
- Broad division: systems and networks
- For 8271, mixture of standard and uncommon

Outline

Instructor information

- Stephen McCamant
- Office: 4-225E Keller
- Office hours: Monday 10-11am, Tuesday 2-3pm, or by appointment
- Email: `mccamant@cs.umn.edu`

Evaluation components

15% Reading questions
10% Class attendance and participation
15% In-class paper presentation(s)
10% Hands-on demo assignment
50% Research project

Readings

- Linked from the course web page
- Usually one main paper per class
- Most either public or UMN-licensed
- Take notes while reading
- Bring a copy (to refer to) to class
- Also: optional and background

Reading questions

- Goal: make sure you read and understand the papers
- Answer one: a general question selected from list on next slide
- Ask one: suggest a question for in-class discussion

General questions

- What interesting new thing did you learn?
- What question is raised but not answered?
- Do you disagree with a claim?
- Is something important left out or ambiguous?
- In hindsight, what would you do differently?

Submission logistics

- Email or Moodle?
- Due the day before
  - 6pm, midnight, or 6am?
- Late: 50% credit; after 2:30pm: 0

In-class presentation

- One, maybe two per student, scheduled in advance
- Can also promote an optional or chosen-by-you relevant paper
- Prepare 25 minutes of slides, but expect questions

Class participation

- The goal of a seminar is discussion, not lecture
- I expect everyone to contribute
- Aim is not to show off knowledge
  - An interesting question > a straightforward answer

Hands-on demo assignment

- Experience actually using an existing research tool
- Done individually
- Find existing software, and get it to do something interesting
- Preparation in advance, short writeup, brief in-class demo

Research project

- Idea: microcosm of research experience
- Formulate a question, answer it, convince others of your results
- Preferred group size of 2

Project topics

- Computer security, including privacy
- Can use one of our papers as a starting point
- But, must make your own novel contribution

Project goals

- Innovative
- Scholarly
  - Put in context of related work
- Appropriately evaluated
  - Able to convince a skeptic
- Well presented

Project results

- Report: about 10 pages, in the format of a conference paper
- In-class presentation: 25 minutes

Collaboration and cheating

- Principle: learn from each other, but don't substitute another's understanding for your own
- Cardinal sin: taking ideas without acknowledgment

Course web site

- Department web site under `csci8271`
  - Also linked from my home page `~mccamant`
- Moodle page also exists

Outline

Big-Picture Introduction

Course Logistics

Topics Overview

Security of and in the cloud

- Finding and exploiting co-residency
- Oblivious storage across a pair of cloud providers

Anonymous payment / Bitcoin

- The dangers of double-spending attacks
- True anonymity with zero-knowledge techniques

Binary hardening

- Control-flow integrity for off-the-shelf binaries
- Detecting and blocking return-oriented programming

Infrastructure paranoia

Could our CPUs, compilers, etc., have hidden back doors? How could we even tell?

Smartphone security

Android and iOS get avoid some desktop problems by design, but also introduce new dangers.

Anonymous overlays / Tor

How can we communicate anonymously on the Internet, when every packet has your IP address on it?

(Anti-)censorship techniques

Can we communicate even when/how a government doesn't want us to?

Botnets and spam

Economic and software ecosystems built on "efficient" fraud. How do they work and is there anything we can do to stop them?

Web application security

The web has a complicated distributed trust model, and processing is all based on string parsing. What could go wrong?

Side-channel snooping

Attacks that get information they shouldn't by going outside the usual sources. Like looking at the size of encrypted packets or the voltage on a power supply.

Differential privacy

Provably protecting statistical disclosures with automatically-added noise.

Bug hunting

Searching for vulnerabilities ("fuzzing") in large code bases.

Medical and voting applications

Domains with real-world implications, where hardware matters.

Non-traditional attacks

In which either the attack or the victim is something other than the usual computer.