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

Upcoming Topics

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.
- A lot of my personal research is in this area

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: this Thursday 5:30pm, future TBA
- 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 Canvas? Canvas
- Due the day before
  - 9pm? midnight? 3am? 3am
- Late: 50% credit; after 4:00pm: 0

In-class discussion lead

- One per student, scheduled in advance
- Can also promote an optional or chosen-by-you relevant paper
- Prepare 5 slides/5 minutes overview to start discussion
- Also be ready to go with topics to go more in depth into

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
- Done individually or in groups 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: 12+5 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 is under `csci8271`
  - Also linked from my home page `~mccamant`
- Canvas page also available
- Piazza?

Outline

Big-Picture Introduction

Course Logistics

Topics Overview

Upcoming Topics

Security of clouds and outsourcing

- How can I pay someone else to do my computing for me, and still have it be secure?
- Systems-based and cryptographic approaches

Blockchains and smart contracts

- Can your transactions be private if the ledger is public?
- Software engineering when bugs have direct monetary cost

Smartphone and app 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?

Web application security

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

Measuring privacy loss

Using math to define how computations reveal information or allow inferences.

(Anti-)censorship techniques

Can we communicate even when/how an ISP or government doesn't want us to?

Architectural side channels

Instruction-level timing and other low-level CPU details can reveal information unintentionally.

Naming and PKI

Systems like DNS and HTTPS certificates are central, but depend on a lot of centralized trust.

Embedded applications

Domains with real-world implications, where hardware matters, like medical devices and cars.

Physical side channels

Information leakage or unexpected attacks made possible by the physical world.

Subverted infrastructure

Could our CPUs, compilers, etc., have hidden back doors? Is there anything we could do about it?

Security of machine learning

The power of machine learning is leading it to be widely adopted, but it also makes new kinds of attack possible.

Applied cryptanalysis

In practice, the security of cryptographic systems can be broken by both mathematical and implementation problems.

Malice in the network

Malware, botnets, and spam form economic and software ecosystems built on "efficient" fraud. How do they work and is there anything we can do to stop them?

Passwords

Passwords are an authentication mode that users and researchers both love to hate, but they don't seem to be going away. Maybe we can make them less bad.

Bug hunting

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

Outline

Reading for Thursday

- "Why do Nigerian Scammers Say They are from Nigeria?"
  - Cormac Herley, Workshop on the Economics of Information Security (WEIS) 2012