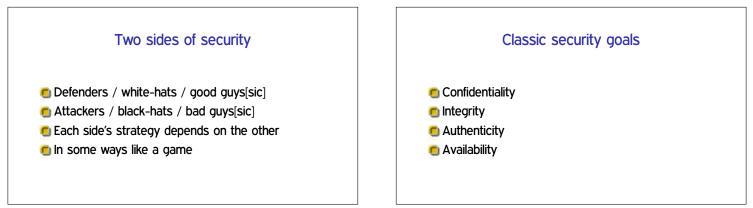
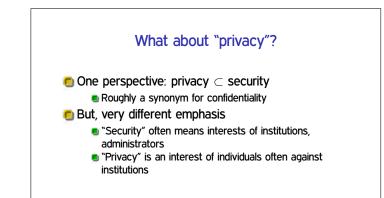
CSci 8271 Security and Privacy in Computing Day 1: Introduction and Logistics

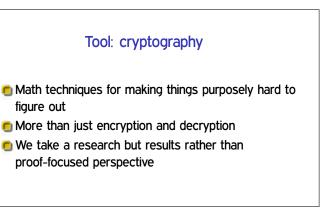
Stephen McCamant University of Minnesota

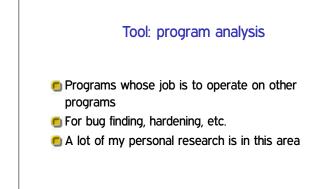
Introductions







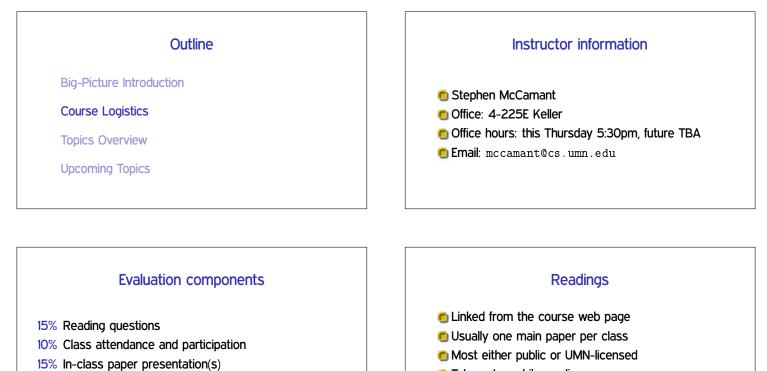




Applications

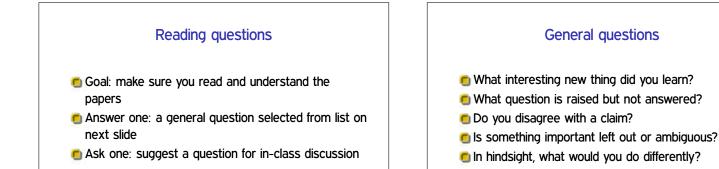
Security problems occur all over computer science

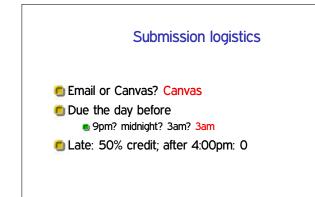
- Broad division: systems and networks
- E For 8271, mixture of standard and uncommon



- 10% Hands-on demo assignment
- 50% Research project

- 🖲 Take notes while reading
- Bring a copy (to refer to) to class
- Also: optional and background

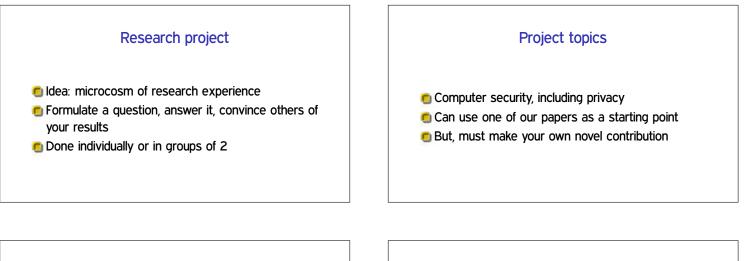




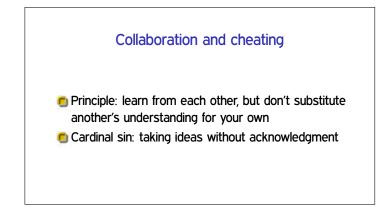
In-class discussion lead

- 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 Hands-on demo assignment Image: The goal of a seminar is discussion, not lecture Experience actually using an existing research tool Image: Image: Done individually Done individually Image: Aim is not to show off knowledge Find existing software, and get it to do something interesting Image: An interesting question > a straightforward answer Preparation in advance, short writeup, brief in-class demo



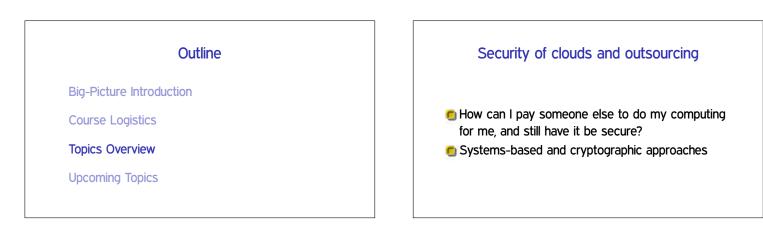




Course web site

Department web site is under csci8271
 Also linked from my home page ~mccamant
 Canvas page also available

🖲 Piazza?



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

Big-Picture Introduction

Course Logistics

Topics Overview

Upcoming Topics

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