CIS700:
Hardware Support for Security

Professor Milo Martin

http://www.cis.upenn.edu/~milom/cis700-Spring05/

Why Am I Teaching This Course?

Security is important
- Lots of reasons why

Security is hard
- No silver bullet
- Much deeper than stopping buffer overflows

My expertise
- Computer architecture and related issues
- Not (yet) a security expert

Key question
- Can hardware support improve the security of computing systems?

This course
- We'll explore this question

Who are you?

What is your experience?

Your background?

Your interest in this course?

Computer Security

Computer security is a broad field
- Traditional computing systems issues
- Cryptography
- Physical security
- Law enforcement and public policy
- Psychology and economics

Goals
- Main goal: "thwart attacks"
- Privacy, authentication, detection, forensics, digital rights management (DRM), attack preemption

Security Engineering

Is there such a thing as a secure system?

Security is all about tradeoffs
- Cost vs security
  - of attack, of countermeasure, value of item protected
- Usability vs security
- Risk management
- Pragmatism, not proofs

Must consider "big pictures" issues
- Unexpected attacks (for example, social engineering)
  - Home security analogy
  - Three lightbulbs story
  - Flying vs driving analogy

Again, key question: can hardware be part of the solution?
- Change the engineering tradeoffs?

Course Format

Glorified reading and discussion group
- We'll read 30-40 papers over the semester
- Goal: vigorous in-class discussion

Reading analysis before each class
- Answer a few questions about the readings
- Due at 10:00am the day of class
- Keeps you honest on the reading; gets us thinking

Short essays
- 2-3 short essays answering a big-picture question about what we've talked about
- Looking for deep insight

(FYI: Each aspect, 33% of your course grade)

Who Should Take This Course?

Targeted for PhD students actively researching either

- Computer architecture
- Security
- (Or maybe just general systems)

Minimum, should have substantial background in either:

- Computer architecture and hardware issues (501 as a minimum)
- Computer security (coursework or experience)

Also, past experience reading "systems" papers a must

- If you've never read an academic research paper before, look out
- We're going to do a lot of reading

Disclaimer: What I Know (and Don't Know)

Computer hardware

- I know a thing or two about a thing or two

Computer security

- Lots of informal knowledge, not really an expert (yet)

How do they fit together?

- I don't know (yet)
- Can't yet give you the "big picture"
- Haven't yet read all the papers we'll be reading

Result: course will evolve as we go

General Course Topics

Security background

- Focusing on "Security Engineering"
- Readings from Anderson's book

Hardware-based:

- Cryptographic smart cards and co-processors
- Dynamic information-flow tracking
- Buffer-overflow prevention
- Secure information processing
- Reducing runtime overheads of secure programming languages
- Fast cryptography
- Fine-grain memory protection
- Tamper resistant systems
- Code injection prevention
- Various "trusted" computing initiatives

Many low-level software issues covered (by necessity)

Course Readings

Anderson's book for background

- Some at course beginning
- Some spread throughout course

Many conference papers

- Architecture conferences: ISCA, ASPLOS, MICRO, HPCA
- Systems and security conferences: SOSP, Usenix

Reading list will evolve

- We'll touch on lots of topics
- How long we spend on each topic will vary
- Based on class input, dynamically adjust as course proceeds

Next Time

Readings from Anderson's "Security Engineering"

- Preface, Forward
- Chapters 1 & 2
- Copies outside 3rd floor CIS office by end of today
- Purchase book for next week

Answer these questions (10:00am Wed):

- Q1: In what ways are the disciplines of security engineering and computer engineering similar? In what ways are these different?
- Q2: How could the identify-friend-or-foe (IFF) system described in 2.2.2 be modified to prevent the described attack?
- Q3: What didn't you understand about the reading

Come ready to discuss