Security & Privacy: *Syllabus & Schedule*

CS 55: Fall 2014

For the lectures, each topic will link to lecture notes, which should be available by classtime the day of the lecture. Notes for guest lectures will be provided when possible.

These notes will complement what's presented in class. Given my writing disability, the notes are also there to help you interpret my poor handwriting!

You will be responsible for the lecture notes, the material presented during the lectures, and the assigned reading.

The schedule below may be updated during the term as necessary.

CS55 Class Schedule for Fall 2014

Overture: What's the problem?

Reading (everyone):

- S&M, Chapter 1 and chapter 6 sections 6.0-6.3.
- Aleph One. The classic stack-smashing paper. Hard to read due to typography, but useful.
- Exploiting Format String Vulnerabilities, Sections 1,2,3, and 5 in particular.
- SANS, 2014 CWE/SANS Top 25 Most Dangerous Software Errors. Skim, paying attention to the types of errors
- Original Fuzz testing report, by Bart Miller, providing lots of examples of this very effective testing scheme.

Lecture notes:

- **01 - Introduction, logistics, course overview**
- **02 - Basics and Blunders**

Foundations: Information Security Principles

Reading (everyone):

- S&M, Chapters 2 and 3

- The Orange Book. Read the preface, intro, Sec 5, Sec 6, Sec 8, Sec 10, the Appendices, and Glossary are all worth reading. Skim the rest.
- Read Saltzer and Schroeder, Section 1A, with section 1B optional.
- Read Schell.

Graduate reading:

- Bell and LaPadula. (the seminal lattice model for secrecy).
- Mclean. (a critique of the lattice approach.)

Lecture notes:

- **03 - Access Control and Information Flow**
- **04 - The Orange Book and its relevance then and now**

Foundations: Cryptography

Reading (everyone):

- S&M, Chapter 7
- Neal Koblitz's article on math and cryptography
- NIST-recommended key lengths, sections 5.6.2 and 6-6.1.

Graduate reading:

- R. Kohlas and U. Mauerer. "Reasoning About Public-Key Certification: On Bindings Between Entities and Public Keys.". IEEE Journal on Selected Areas in Communications, 2000. (You can find more, including the one in which he fumes about PGP, **here**.)
- J. Marchesini, S.W. Smith. **"**Modeling Public Key Infrastructure in the Real World**."** Public Key Infrastructure: EuroPKI 2005. (our follow-up)
- S. Garfinkel and R. Miller. "Johnny 2: A User Test of Key Continuity Management with S/MIME and Outlook Express". Symposium on Usable Privacy and Security. 2005.

Lecture notes:

- **05 - Symmetric Cryptography**
- **06 - Public Key Cryptography**

Identity

Reading (everyone):

- S&M, Chapter 9,10.
- Sasse "Red-Eye Blink, Bendy Shuffle, and the Yuck Factor: A User Experience of Biometric Airport Systems"
- Sean's keyjacking paper

Graduate reading:

- Bird

Lecture notes:

- **07 - Authentication and Cryptography and Authenticating Humans**
- **08 - Public Key Infrastructures (PKI's)**

Attacks against cryptography

Reading (everyone):

- S&M, Chapter 8.
- The Dole and Goldberg/Wagner papers
- Kocher's timing paper
- Mining your Ps and Qs paper

Graduate reading:

Aim to understand the discussion, focus less on the proofs.

- Hastad's "On Using RSA with Low-Exponent in a Public Key Network"
- Kohlas & Maurer's "Reasoning About Public-Key Certification: On Bindings Between Entities and Public Keys"

Lecture notes:

- **09 - Breaking (or working around) Cryptography**

=> All material to this point will be covered on the Midterm Exam: Friday 18 October, 2014

Operating Systems and Hardware

Reading (everyone):

- S&M, Chapter 4; Chapter 5; Chapter 6.4-6.6;

- Spafford's paper on the Morris Worm
- Short article on recent malware: *How a browser worm slithered across a huge number of Tumblr accounts*
- D'Cunha et. al. *Programming Language Security: A Survey for Practioners.*
- Ken Thompson's "Trusting Trust" (Turing award winner)

Graduate reading:

- Sabelfield and Myer's paper on information flow
- Geer, et.al., "CyberInsecurity: The Cost of Monopoly"
- Karger and Kurth, """Increased Information Flow Needs for High-Assurance Composite Evaluations"

Lecture notes:

- **10 - Operating Systems Security and Malware**
- **11 - Hardware-based security, formal evaluation**

Virtualization and Networking Security

Reading (everyone):

- Govindavajhala and Appel's paper on light bulbs
- The insecurity of WEP

Graduate reading:

-

Lecture notes:

- **12 - Virtualization and security**
- **13 - Networks and Security**

Economics of Security

Reading (everyone):

- S&M, Chapter 14, 18; 11.1-11.2.
- Blueprint for a science of cyber security
- "Why Information Security is Hard---an Economic Perspective."

- "EMV: Why payment systems fail"

Graduate reading:

- Petitcolas, et. al.
- The Joux paper on hash concatenation

Lecture notes:

- **14 - Don't worry, it's in the cloud!**
- **15 - Money, Time, and Property. Clashing cultures (e.g., SCADA and IT Security), and Legal Aspects.**
- Current Bitcoin exchange rate

People

Reading (everyone):

- When password security questions aren't secure.
- Original Bitcoin Paper

Graduate reading:

- "Critical infrastructure cyber security: are economic incentives adequate?"

Lecture notes:

- **16 - People and security**

Privacy

Reading (everyone):

- **S&M**, Chapter 12.1-12.2, 12.4-12.5, 13.
- Johnson and Kapadia, "From Chaum to Tor and Beyond: A Survey of Anonymous Routing Systems"
- A taxonomy of privacy, just skim
- "I've got nothing to hide" ... oh really?

Graduate reading:

- Felten and Schneider

Lecture notes:

- **17 - Privacy and anonymity**

Finale: Project Presentations & Last 2 Days Of Class

- 4 minutes for each project
- Presentation Schedule v2

Encore!

- **Final Exam: 3:00-5:00PM, Monday 24 Nov. , Kemeny 008**

Back to CS55 Home Page **Charles C. Palmer** ccpalmer <at> dartmouth.edu

Document last modified: 16 November, 2014

Document last modified: 16 November, 2014