~~CS38~~ CS55: Security and Privacy, Fall 2011

Course goals and overview

Goals of the course

Successful completion of this course will mean you have learned how to think carefully about the security and privacy attributes of the systems and policies that you encounter in your work and personal life, whether they are computerized or not. While you should gain a broad understanding and a healthy skepticism of systems security and privacy, we also hope that you will learn how to build more secure systems rather than just becoming adept at finding security failures.

Course overview

Today's networked world highlights the importance of computer security and privacy. Not only is it easier for people to break into systems half way around the world, it is also easier to summon up once-private details about users using a simple web search. While it is clear that systems need to be secured and peoples' privacy must be protected, it is less clear *how* to do so. In fact, it is hard, if not impossible, to measure how secure a system is or even how much better (or worse) a system's security is after making some change. And in today's world of electronic convenience, it is surprisingly difficult to remain private. As just one example, it's hard to not use a social networking service such as Facebook, but employers are now digging into the personal profiles of their (potential) employees, sometimes costing them a job!

How then should we go about designing secure and privacy-enhancing systems? Grappling with a *defense in depth* strategy, it turns out, is part art, part science and part mathematics. In this course, we will cover a breadth of these topics including:

- **Cryptography**, the nuts and bolts of security. Cryptography gives us the equivalent of padlocks for securing systems. We will survey the best padlocks available, and the latest advances in electronic "lock picking." We will also discuss when cryptography can make systems more secure, and when it's more like putting steel doors on a grass hut.

- **System modeling**. Padlocks are of no use unless you know which doors to lock! We may model the system as having two doors, and use our padlocks on those two doors. We will look at ways in which to model systems, and study how models can fall short. "Did you realize the attacker could unscrew the hinges of the doors?" Oops.

- **Implementation security**. Even though our system should be secure in theory, in practice many systems will have implementation bugs. For example, systems today continue to be vulnerable to *buffer overflow* attacks.

- **Multidisciplinary**. Security and privacy are **multidisciplinary** challenges. It's not just about the cool technology, it's also about social systems, economics, and public policy.

- **Economics of security.** And, speaking of economics, what is the relationship between economic forces and security & privacy? Do price breaks take precedence over behavior that is arguably less secure or private? Is that free WiFi really FREE?

- **Humans as the weakest link**. Why try breaking into computers when you can simply ask the user for his or her password (e.g., by pretending to be a sysadmin over the phone)? Sometimes security mechanisms are simply too complicated for users to understand—indeed, users fall prey to phishing attacks for this very reason. How can we make secure systems more usable and immune to human error?

- How to take a **systems' perspective** on security & privacy. In the end, we must examine the system as a whole and apply defense in depth using various techniques in our security & privacytoolkit.

- **The need for privacy**. Why should we care? Is privacy only for people who have "something to hide?"

- **The Cloud.** With all the talk about "the cloud", what effect does it have on security and privacy? Does it make things better, or ...

- **Privacy-enhancing technologies**. We will look at systems such as anonymizing networks, their (il)legitimate uses, and recent advances in balancing these uses.

This course is heavily based on the course designed by Prof. Sean Smith and evolved by Apu Kapadia. Much of the material used in this course was either produced by Sean (e.g., the textbook) or assembled by the two of them. The instructor is deeply indebted to these two outstanding educators.

Background

The instructor is a adjunct professor who is an IBM Research Division employee, leading the Research Division's Cybersecurity efforts focusing on government concerns. Before that he led the Research Division's Security & Privacy departments at the Thomas J. Watson Research Center in for several years, beginning when he founded the "Ethical Hackers" team for IBM. He is also past Research Director and Senior Technical Advisor for the Institute for Information Infrastructure Protection (the I3P). Managed by Dartmouth College, the I3P is a consortium of leading universities, national laboratories and nonprofit institutions dedicated to strengthening the cyber infrastructure of the United States. If for some reason you want to know more, see his web page at IBM Research or you can find him on google+.

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

Document last modified: 17 July, 2011