CS 557: Software Secure Design and Analysis

Joshua D. Guttman
guttman@wpi.edu

Fuller Labs 311 Thursdays, 6–8:50

Class website is at URL `http://web.cs.wpi.edu/~cs557/f14/` and `http://web.cs.wpi.edu/~guttman/cs557_website/`

This syllabus in PDF format:
`syllabus.pdf`

Project previews in PDF and .html formats: `project_summaries.pdf`, `project_summaries.html`

Papers for readings in PDF format: `papers`

Main goals. This course is intended to provide both practical and theoretical understanding of software security. In particular, we will emphasize design and analysis.

This is in contrast with much of the work today on cyber security, which seems to provide an endless stream of "hacks" and "patches." A hack discovers and exploits some weakness in a system. A "patch" fixes the system at least enough to make that hack stop working. This is an endless cycle: The attacker will always eventually find a new hack.

This course will focus on how to design systems with solid security. That means:

- Determining what security goals the software needs to achieve to do its job for its users;
- Developing a view of the adversary's abilities and intent;
- Designing authentication, access control, and confidentiality mechanisms to ensure that the adversary cannot defeat the security goals;
- Implementing the mechanisms in a reliable way;

- Analyzing the design and the implementation, and testing both in an adversarial frame of mind.

Attacking systems is still an important step in finding out their strengths and weaknesses, but the designer has already chosen the game board.

In today's world, there are a variety of existing techniques and tools that can feed in to these steps. These include cryptography, cryptographic protocols, access control mechanisms, programming language choices, and support from operating system and hardware. We will explore all of these areas.

We will choose a lot of examples at different levels that are related to TLS, the Transport Layer Security protocol formerly known as SSL. The implementations of TLS have illustrated a lot of problems over the years; there has been strong recent work on a verified implementation; and it is a key tool to use in tying distributed components together securely.

Projects and grades. There will be four projects. Each project will be discussed during three separate weeks in class. We will introduce it and discuss the goals in one week. Teams will complete their design and implementation and give a brief overview in a subsequent week. Then, each team will become an *antiteam* to another group's project. The purpose is to learn how to look at design and code critically, and find problems. It's a kind of team sports.

Readings and summaries will be required periodically.

See `project_summaries.html`.

There will be no final exam.

Office Hours. My office is FL 137. My email address is `mailto:guttman@wpi.edu`. Please include "[cs557]" in the subject line. This helps me find and respond quickly to messages about this class.

I will work hard to respond quickly to email messages, so please feel free to send me quick questions. Please let me know early if issues seem to be arising.

In-person office hours are available on Thursdays by appointment. Virtual office hours are available via Skype (joshua.guttman); send email to arrange for a meeting.