Advanced Topics in Computer Security: Principles of Security and Trust*

Joshua D. Guttman
guttman@wpi.edu FL 137

Higgins Laboratory 202
Tuesday, Thursday 4–5:20

September 18, 2012

Class website is at URL `http://web.cs.wpi.edu/~cs564/f12/`

This syllabus in PDF format:
`syllabus.pdf`

The paper summary sheet in PDF and .tex formats:
`paper_summary_sheet.pdf`, `paper_summary_sheet.tex`
(use these or else any other format you prefer, with the same questions.)

Directory of papers is at `papers`.

Schedule of readings is at `schedule.html` and `schedule.pdf`.

Paper summaries are in directory `paper_summaries/`.

CPSA Examples are available in the directory `cpsa_examples`.

A CPSA Exercise is in `exercise/cpsa_class_exercise.html`. The CPSA user documentation is at `cpsauser.html`.

*Listed this year as CS559, Topics in Theoretical Computer Science. This is also in effect the first version of the newly approved class, CS564, Advanced Topics in Computer Security.

Main goals. The purpose of this course is to give insight into the principles of security and trust. We focus on fundamental ideas and techniques to design and analyze mechanisms allowing mutually suspicious parties to interact and collaborate through distributed systems. The course will divide into four main parts.

First, we will examine cryptographic protocols, which are the main mechanism for achieving confidentiality and authentication (and many related goals) in distributed systems. Important protocols include SSL/TLS, SSH, IPSec and IKE. We will focus on how protocols break and why; how to analyze them to determine what security goals they achieve, using tools such as CPSA and ProVerif; and how to design new ones. In this part, we treat cryptography as a black box and focus on *structural* or *symbolic* analysis methods. *Part I Schedule: 23 Aug.–18 Sept.*

Second, we will study the foundations of cryptography. We will examine foundational aspects of block ciphers, cryptographic hashes, public key cryptography, digital signatures, zero-knowledge proofs, and secure multiparty computation. We will consider definitions of security for cryptographic primitives. We will identify key assumptions that justify primitives, and general constructions that can be used to build cryptographic operations from suitable building blocks. *Part II Schedule: 20 Sept.–11 Oct.*

Third, we will examine access control. Access control mechanisms are responsible for authorizing actions or else preventing them, depending on the principals who are performing the actions and the objects on which they are acting. Access control becomes especially challenging in distributed systems, when one principal may depend on other principals to feed reliable information to decisions, or may delegate parts of the decision to others. *Part III Schedule: 23 Oct.–6 Nov.*

Our fourth part will integrate the topics we have studied in the first three. We will consider:

- Cryptographic definitions of key distribution and authentication.
- Cryptographic and symbolic approaches to composing protocols. If two protocols are safe to run separately, are they still safe if both are used on the same network?
- If a security goal is proved using a symbolic method, how do we know that it is still satisfied when we consider cryptographic definitions of authentication and confidentiality?

  This is called "computational soundness."

- How can we relate access control and protocol behavior? For instance, a protocol should be able to deliver information to be used in access control decisions. Also, access control policies should be able to control when and how protocols are executed. How can we design mechanisms that combine protocols and access control?
- Can we design cryptographic primitives that build in certain access control mechanisms? ("Attribute-based encryption.")
- The Automated Teller Machine network uses devices that generate keys and apply cryptographic operations to protect user Personal Identification Numbers. Can a programmer outside the device force it to disclose its secrets? How can we design and verify devices that no adversary can manipulate to disclose its secrets? ("Hardware Security Modules.")

Part IV Schedule: 8 Nov. –13 Dec.

Readings. Our readings will be mainly research papers, with several chapters from Katz and Lindell's *Introduction to modern cryptography* to give the basics of cryptography. I will post URLs or place PDFs in our *myWPI* area for research papers.

Reports and Projects. Students will complete three small projects and lead 3–5 discussions during the semester.

Each project will include tool-supported analysis of a protocol, exploring variants of the protocol to determine which ones achieve which security goals. A short summary will describe the variants, their security properties, and the key differences. ProVerif and CPSA are relevant tools.

Each student will lead discussions of about 20 minutes on particular research papers. Before each discussion, the leader will fill out a *paper summary sheet*. The paper summary sheet has five questions. The goal is to answer each question in a few sentences (generally two or three); these answers concentrate a lot of information about the paper.

The summary sheet is due by email to me at 1 pm so that I can print copies to distribute.

During the discussion, the leader and the rest of the class will discuss which parts of the paper support the answers given; which parts contain supplementary details; and which parts have other key goals. Each student in the class should read every paper; highlighting or margin notes are needed to participate effectively in the discussion.

The discussion leader should write a revised summary at the end of the class.

Revised summaries will be posted as part of the class website.

There will be no final exam.

Office Hours. My office is FL 137. My email address is `mailto:guttman@wpi.edu`. Please include "[cs564]" in the subject line. This helps me find and respond quickly to messages about this class.

I will have office hours in the first half of the semester:

Tues. 5:20–6:00, immediately after class.

Thurs. 5:20–6:00, immediately after class.

Fri. 1–2, as needed.

I am also available at many other times; please send me email. When B term starts I will adjust my office hours. Please do not leave messages on my office phone; I use it rarely.