

CSCI-4971: Secure Software Principles
MR 12:00PM-1:50PM (AE 215)
Spring 2010

Contact Information

Course Website

<http://www.cs.rpi.edu/academics/courses/spring10/csci4971/>

Undergraduate TAs

Adam Comella	comela@cs.rpi.edu
Ryan Govostes	govosr@cs.rpi.edu
Alex Radocea	radoca@rpi.edu
Jay Smith	jaysmith@lavabit.com
Andrew Zonenberg	zonena@cs.rpi.edu

Graduate TA

Matt Edman
Lally 01A
(518) 276-8489
edmanm2@cs.rpi.edu

Overview

This hands-on course aims to introduce students to the technical skills necessary to examine security vulnerabilities in software systems including various operating systems and applications. It will primarily be taught in a laboratory setting where students can interact with a number of skilled Undergraduate TAs to develop expertise in identifying, generalizing, and exploiting implementation errors. By the end of the semester, students should be able to audit their own source code for security vulnerabilities, identify vulnerabilities in open and closed source third-party applications and develop proof-of-concept exploits. While the course will typically be case-oriented, it will have sufficient coverage of theoretical and fundamental principles of cryptography and general system security. We also expect to one or more guest lecturers throughout the semester.

Recommended Reading

There is no required textbook for this course. Instead, each lecture will have links to suggested references relevant to the topics discussed. References and additional reading material will also be added to the course website.

Grading

- 50% of your grade will be based on successful completion of the given tasks during a lab session.
- 25% of your grade will be based on lab reports written in the form of security advisories. The specific requirements for each lab report will be given to you prior to the end of a lab. Lab reports will typically be due at the start of the first class period after which they are assigned.
- 25% of your grade will be based on an end-of-semester project. The project will require students to choose an existing “real world” software application and use the skills acquired in this course to analyze the chosen application for security vulnerabilities. Further details will be given later in the semester. Students *must* have passing grade on the project to pass the class.

Mailing List

A mailing list called **ssp-discuss** has been set up for discussion amongst students in the course. Please see the following URL for instructions on how to subscribe to the mailing list:

<https://twiki.cs.rpi.edu/twiki/bin/view/LabstaffWeb/EcartisSubscription>

Please email one of the TAs if you have trouble subscribing.

Schedule

The tentative schedule below is intended to give you a rough idea of the topics that will be covered throughout the semester. The actual dates are likely to change during the course of the semester. If you have questions about a particular topic, please email the Undergraduate TAs listed for that topic.

Date	Topic	Type	Lead TAs
January 25	Unix Security	Lecture	Adam, Jay
January 28	Unix Security	Lab	Adam, Jay
February 1	Secure C Coding	Lecture	Alex, Andrew
February 4	Secure C Coding	Lab	Alex, Andrew
February 8	Secure C Coding	Lecture	Alex, Andrew
February 11	Secure C Coding	Lab	Alex, Andrew
February 15	<i>No Class – President’s Day</i>	—	—
February 18	x86 Assembly	Lecture	Andrew, Alex
February 22	x86 Assembly	Lab	Andrew, Alex
February 25	x86 Assembly	Lecture	Andrew, Alex
March 1	x86 Assembly	Lab	Andrew, Alex
March 4	Reverse Engineering	Lecture	Ryan, Alex
March 8	<i>No Class – Spring Break</i>	—	—
March 11	<i>No Class – Spring Break</i>	—	—
March 15	Reverse Engineering	Lab	Ryan, Alex
March 18	Reverse Engineering	Lecture	Ryan, Alex
March 22	Reverse Engineering	Lab	Ryan, Alex
March 25	Fuzzing	Lecture	Jay, Adam
March 29	Fuzzing	Lab	Jay, Adam
April 1	Guest Lecture: Dr. Dave Musser – <i>Proof-Carrying Code</i>	Lecture	—
April 5	Guest Lecture: Dr. Dave Musser – <i>Proof-Checking With Athena</i>	Lecture	—
April 8	Cryptography Review	Lecture	Matt, Andrew
April 12	Guest Lecture: Dr. Adam Young — <i>Cryptovirology</i>	Lecture	—
April 15	Windows Security	Lecture	Andrew, Jay
April 19	Windows Security	Lab	Andrew, Jay
April 22	Web Application Security	Lecture	Ryan, Adam
April 26	Web Application Security	Lab	Ryan, Adam
April 29	Web Application Security	Lecture	Ryan, Adam
May 3	Web Application Security	Lab	Ryan, Adam
May 6	Final Project Presentations	Lecture	—
May 10	Final Project Presentations	Lecture	—