Course Syllabus for CSE 334/434: Software System Security

Gang Tan

Aug 28th, 2012

Course description. An introduction to the state of the art of software-security research. This course surveys common software vulnerabilities, including buffer overflows, format string attacks, cross-site scripting, and botnets. The course also discusses common defense mechanisms, including static code analysis, reference monitors, language-based security, secure information flow, and others.

Prerequisites. For undergraduate students: CSE 109: Systems Programming and CSE 262: Programming Languages

Time and location. TTh 2:35-3:50pm; PA 466

Instructor and TA. Gang Tan, PL 329, 610-7583737, gtan@cse.lehigh.edu. Office hours: Weds 1:30-3pm or by appointment.

Course Website. A public website is at http://www.cse.lehigh.edu/~gtan/teaching/cse334434f12/. Homeworks, readings, and schedule are announced there. Course supplemental materials will be posted in CourseSite (coursesite.lehigh.edu).

Textbook. No textbooks are required for this course.

Major topics covered.

1. Security fundamentals
2. C vulnerabilities: buffer overflows, format string attacks, ...
3. Web application security
4. Reference monitors; software-based fault isolation
5. Program verification; symbolic evaluation
6. Secure information flow
7. Java security
8. Malware; DDoS; botnets

Accommodations for Students with Disabilities. If you have a disability for which you are or may be requesting accommodations, please contact both your instructor and the Office of Academic Support Services, University Center C212 (610-758-4152) as early as possible in the semester. You must have documentation from the Academic Support Services office before accommodations can be granted.

Attendance. Attendance is expected. Students who have legitimate reasons for absence have to inform the instructor **before the fact**. You are responsible for all materials presented in class whether present or not.

Readings. Readings will be announced on the public course website.

Homework. You will periodically receive homework assignments that are to be turned in and will be graded. You may discuss the homework with other students in the class, but you must do your own work; you may not copy someone else's solution.

Assignments and their due dates will be announced on the course website.

Late Homework. If you submit your homework within three days of the due date, we will deduct 20% of your score. Within a week, we will deduct 40%. We will not accept homework submissions after a week. Timely grading of late homework is not guaranteed.

Exams. There will be no midterm exams. We will have a final exam. Students may opt to do a final research project instead of the final exam.

Missed Exams. Make-up for missed exams will only be granted on a case-by-case basis.

Grading. For CSE 334 students: Homework 50%; Final exam/final project 40%; Class participation 10% .

For CSE 434 students: Homework 40%; Paper presentation 15%; Final exam/final project 40%; Class participation 5% .

Academic Integrity. Academic integrity is crucial for the pursuit of knowledge. Please refer to Lehigh's policy of academic integrity (http://www.lehigh.edu/~inprv/academic_integrity.html) for reference.

Technology use. The purpose of this course is to help students understand basic software security problems and counter measures. The knowledge should not in any way be used by students to exploit vulnerabilities inside Lehigh or outside. Please check out Lehigh's "Policies on the Use of Computer Systems and Facilities" (http://www.lehigh.edu/security/computepolicy.html) for acceptable use of Lehigh's network and information technology.

Feedback. The success of this course need a mutual communication between course staff and students. We welcome your feedback on anything related to the course, such as course material we covered, teaching techniques, and difficulties in finishing the homework and project. We need your input!