Security Engineering, 16:332:507 (S), 3 credits

Instructor: Janne Lindqvist

Course Catalog Description:
This class teaches essential principles, techniques, tools, and methods for systems security engineering. Students work in small collaborative design teams to propose, build, and document a project focused on securing systems. Additional assignments include creating several small projects. Students document their work through a series of written and oral proposals, progress reports, and final reports. Covers the basics of security engineering, usability and psychology, human factors in securing systems, mobile systems security, intersection of security and privacy, security protocols, access control, password security, biometrics, and topical approaches such as gesture-based authentication.

Pre-Requisite Courses:
None

Pre-Requisite by Topic:
1. Data Structures and Algorithms
2. Familiarity with Operating Systems

Textbook & Materials:
Ross Anderson, "Security Engineering: A Guide to Building Dependable Distributed Systems, 2nd Edition", Wiley, October 2008.

Topical scientific publications in security engineering.

Overall Educational Objective:
To introduce students to security engineering: how to think and analyze security from systems perspective. To create a foundation for further study and professional practice in security engineering.

Course Learning Outcomes:
A student who successfully fulfills the course requirements will have demonstrated:

1. An ability to analyze security and privacy of systems.
2. An ability to conduct user-centered design for security engineering.
3. An ability to understand programming constraints with systems security.
4. An understanding of limitations and advantages of security protocols, biometric systems, password authentication and various alternative systems.

How Course Outcomes are Assessed:
Practical home work assignments 30%, midterm 30%, final project 40%

Topics Covered in Classes:
Topic 1: Course Introduction. What is Security Engineering? How security engineering overlaps and is distinct from other fields of engineering. Examples: banking, hospital and home. (1 week)
Topic 2: Security Protocols: Fundamentals, design and analysis. Modern protocols. Human aspects and ceremonies in protocols. Changing the environment. (1 week)
Topic 3: Usability and Psychology: Usable Security and Privacy: Attacks based on psychology. Insights from psychology research. System issues. (2 weeks)
Topic 4: Mobile Device Security. Mobile platform security. Mobile app distribution and security. Mobile OS security. Privacy issues with apps. (2 weeks)
Topic 5: Password Authentication: Difficulties with reliable password entry. Difficulties with remembering the password. Password research. Measuring password security (2 weeks)
Topic 6: Access Control: Groups and Roles, Access Control Lists, Sandboxing Virtualization (1 week)
Topic 7: Biometric Systems and Alternatives Topic: Handwritten signatures, Face recognition, Fingerprints, Voice Recognition, User-Generated gestures (2 weeks)
Topic 8: Evaluating Security: Assurance, Economic Incentives, Evaluation (1 week)
Topic 9: Recent Topics in Security Engineering: Topics chosen on a yearly basis (2 weeks)

Computer Usage:
Using practical security software.

Laboratory Experiences:
No laboratory experiences.

Prepared by:
J. LINDQVIST

Date: April, 2014, Updated September, Updated October, 2014. This revision, October 2015.