FEP3300 Advanced Networked Systems Security 8.0 credits

Säkra nätverkssystem, fortsättningskurs

This is a translation of the Swedish, legally binding, course syllabus.

If the course is discontinued, students may request to be examined during the following two academic years

Establishment

Course syllabus for FEP3300 valid from Spring 2012

Grading scale

Education cycle

Third cycle

Specific prerequisites

Eligible students should be already prepared by a basic course on network security, systems security, or Internet security. Preparation on most of, or all if possible, among data networks, operating systems, wireless networks, Internet-working, is presumed. If equivalent knowledge was acquired through a different path, the students should contact the instructor to obtain his agreement. Following the companion “Networked Systems Security” course is not a strict requirement, but it is strongly encouraged for continuity and best results.

Language of instruction

The language of instruction is specified in the course offering information in the course catalogue.

Intended learning outcomes

The course intends to enhance and extend the crisp understanding of fundamental concepts and technologies related to the security of modern networked systems. It builds on the preparation of students through the Networked Systems Security course (EP2500/EP3200). It seeks to hone the ability to deal with open-ended, real-world engineering problems, as well as prepare for independent work on related topics.

At the end of the course, students shall be able to:

(i)Comprehend, analyze, and identify vulnerabilities, threats, and attacks against a variety of modern or emerging networked systems.

(ii)Define precisely security properties and requirements for networked systems security solutions.

(iii)Design and analyze security protocols, mechanisms, and architectures that safeguard the network operation against attacks.

(iv)Comprehend and analyze qualitatively and quantitatively the overhead of security mechanisms, and refine their designs, in order to ensure the effectiveness and efficiency of the secured networked systems.

(v)Identify, analyze, and apply best practices for security schemes deployed widely or currently advancing towards standardization for networked systems.

This course is planned for advanced MSc and entry level PhD students. It naturally complements its companion course, “Networked System Security.” offering the opportunity to deal with security and privacy problems in a deeper and hands-on manner. The mix of advanced, motivated MSc students and PhD students can be beneficial for both.

Especially for PhD designed additional assignment problems, dedicated recitation slots, individual consultation with the teaching team; and to the extent possible personalization of the project objectives, to align them to the study plan of the PhD student.

Course contents

The course content will be updated and detailed at the start of the course each year. Basically, the course will work on security, including privacy, for a spectrum of networked systems: (i) Internet and TCP/IP networks, (ii) Cellular data and voice networks, (iii) Wireless local and personal area networks, (iv) Internet of Things and embedded systems, (v) Wireless Sensor Networks, and (vi) Mobile ad hoc and hybrid networks, such as vehicular communication systems. While the first three types of networked systems have been the predominant ones, and shall get significant attention, the course will shift the balance and present more cutting edge technologies and up and coming, future systems in the research literature.

The emphasis, throughout the course, shall be on honing the student’s understanding of concepts and technologies, on common security requirements across various systems, on how features of each system determine the state-of-the-art of security solutions and on how design decisions should be made for effective and efficient security solutions. The course is project oriented, and it gives the opportunity for students to deal with real-world or research

oriented problems, and prepare themselves for further work towards a Licentiate or MSc thesis, or PhD or other research work, and also work in the industry, on any topic related to network and system security.

Disposition

The course is structured around weekly lectures. A set of assignments including a project are mandatory and they are graded. Students are supported via extensive office hours, held by the instructor and the teaching assistants throughout the course. All material and instruction shall be in English.

Course literature

Updated yearly reading list from the research and technical literature; reference to the reading material (textbooks) of the NSS course.

Examination

Based on recommendation from KTH's coordinator for disabilities, the examiner will decide how to adapt an examination for students with documented disability.

The examiner may apply another examination format when re-examining individual students.

Assignments and project outcomes will be graded, they are all mandatory for successfully completing the course, and they will result in a single final grade.

Other requirements for final grade

Requirements for final grades: they are in the letter scale, A-F. Pass/fail for PhD students.

Ethical approach

- All members of a group are responsible for the group's work.
- In any assessment, every student shall honestly disclose any help received and sources used.
- In an oral assessment, every student shall be able to present and answer questions about the entire assignment and solution.