IK2206 Internet Security and Privacy 7.5 credits

Säkerhet och datasekretess på internet

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

Establishment

Grading scale

A, B, C, D, E, FX, F

Education cycle

Second cycle

Main field of study

Computer Science and Engineering, Electrical Engineering

Specific prerequisites

Knowledge of computer networks, 6 credits, equivalent to completed course EP1100/IK1203/IK2218/EP2120.

English skills corresponding to the upper secondary course English B/English 6.

Intended learning outcomes

After passing the course, the student should be able to:

- explain the principles behind encryption using shared keys

- motivate the design principles for block ciphers
- choose suitable modes of operations for block ciphers
- explain the principles of message hashing
- use message integrity codes
- explain the principles for public key encryption
- choose appropriate techniques for authentication
- explain the design of standardized technologies for secure communication such as Kerberos, IPsec, SSL/TLS and PKI
- account for threats to and weaknesses in common internet applications such as email and the web
- design, implement and evaluate a secure application according to the client-server model

in order to gain in-depth knowledge of the technologies used to create secure communication protocols.

Course contents

- Basics of cryptography and information theory: substitution, mono- and poly-alphabetic, home-phonic and, transposition ciphers.
- Block ciphers: properties and implementation of block ciphers and their uses.
- Asymmetric encryption: RSA, Diffie-Hellman. Properties and uses.
- Hash algorithms and digital signatures. Properties of message hashing and how integrity and authenticity can be ensured.
- Public key systems and certificates.
- Authentication of users: passwords, biometrics and multi-factor authentication.
- Authentication protocols for establishing private and privacy-protected communication, principles and properties. Basics of Kerberos.
- Network security, firewalls and virtual private networks. IPsec.
- Web security: attacks, phishing and web code injection. Secure web communication with SSL/TLS.
- Email security: attacks and spam. Methods for secure email, S/MIME and PGP.
- Design and implementation of secure applications supporting authenticated, privacy-protected and confidential communication using the Java application programming interface.

Examination

- PROA - Project, 1.5 credits, grading scale: P, F
- UPGA - Assignment, 1.5 credits, grading scale: P, F
- TENA - Examination, 4.5 credits, grading scale: A, B, C, D, E, FX, F

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.

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

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.