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

Course syllabus for IK2206 valid from Autumn 2018

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

IK1203 Networks and Communications or equivalent.

Knowledge in data communication and Internet technologies.

Language of instruction

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

Intended learning outcomes

The aim of the course is to give the students in depth knowledge of techniques used to create secure communication protocols. The students shall after the course 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 digests
- use message integrity codes
- explain the principles for public key encryption
- choose appropriate techniques for authentication
- explain the design of Internet standards such as: Kerberos, IPsec, SSL and PKI
- evaluate a complex application and identify how security related issues are solved and how this will impact the security of the application.

Course contents

The course is based on a set of lectures and a project work. The lectures cover the following areas:

- basics of cryptography and information theory, substitution, mono- and poly-alphabetic, home-phonic and, transposition ciphers
- properties and implementation of block ciphers, modes of operations, properties of message digests and how to provide integrity
- public-key encryption, RSA, Diffie-Hellman and, digital signatures
- authentication of users, passwords, biometrics, hand shake to provide a private and integrity protected communication channel
- communication protocols used on the Internet: Kerberos, IPsec, SSL, PKI etc.

In the project work the students will learn more about a particular technology or application domain such as bank security, link layer security, biometrics, quantum cryptography etc. Each student will write a short overview of the subject and prepare a tutorial presentation.

Course literature

There are two alternatives textbooks:

1. **Cryptography and Network Security: Principles and Practice, International Edition: Principles and Practice**, 6/E. William Stallings. Pearson, 2013. ISBN-10: 0273793357, ISBN-13: 9780273793359.
2. **Network Security Essentials: Applications and Standards, International Edition: Applications and Standards**, 5/E. William Stallings. Pearson, 2013. ISBN-10: 0273793365, ISBN-13: 9780273793366.

Note that for alternative 1. the chapters related to intrusion detection and firewalls are provided as online material. A six-month subscription for access to online resources is included with each book. Alternative 2. has only brief coverage of authentication, and needs to be complemented with other resourcees, including material from lectures.

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.