IK2206 Säkerhet och datasekretess på internet 7,5 hp

Internet Security and Privacy

När kurs inte längre ges har student möjlighet att examineras under ytterligare två läsår.

Fastställande

Kursplan för IK2206 gäller från och med HT14

Betygsskala

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

Utbildningsnivå

Avancerad nivå

Huvudområden

Datalogi och datateknik,Elektroteknik

Särskild behörighet

IK1203 Nätverk och kommunikation eller motsvarande.

Knowledge in data communication and Internet technologies.

Undervisningsspråk

Undervisningsspråk anges i kurstillfällesinformationen i kurs- och programkatalogen.

Lärandemål

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.

Kursinnehåll

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.

Kurslitteratur

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

- SEM1 - Seminarier, 1,5 hp, betygsskala: P, F
- TEN1 - Tentamen, 4,5 hp, betygsskala: A, B, C, D, E, FX, F
- UPG1 - Rapport, 1,5 hp, betygsskala: P, F

Examinator beslutar, baserat på rekommendation från KTH:s handläggare av stöd till studenter med funktionsnedsättning, om eventuell anpassad examination för studenter med dokumenterad, varaktig funktionsnedsättning.

Examinator får medge annan examinationsform vid omexamination av enstaka studenter.

Övriga krav för slutbetyg

The examination is done partly as a written exam and partly in the form of a written and oral presentation of the project work.

Etiskt förhållningssätt

- Vid grupparbete har alla i gruppen ansvar för gruppens arbete.
- Vid examination ska varje student ärligt redovisa hjälp som erhållits och källor som använts.
- Vid muntlig examination ska varje student kunna redogöra för hela uppgiften och hela lösningen.