Zurich University of Applied Sciences

School of Engineering

t.ISI - Internet-Sicherheit

Person responsible for the course:	Marc Rennhard, rema
Credits:	4
Valid for:	2011/2012
Last saved:	31.08.2011 11:37

Learning objectives:

The students get a profound introduction to the foundations, protocols, and methods of Internet security. As a result, the students are able to analyze Internet-based applications with respect to security and they can design and implement their own security concepts for Internet-based applications. In particular, the students will learn the following competencies:

- They understand the basics of cryptology (algorithms, usage, resistance to attacks)

- They know and understand state-of-the-art protocols and methods to secure communications in the Internet and to control access to systems and applications and can apply them

- They especially understand the possibilities and limitations of these protocols and methods with respect to security

- They know attack scenarios and can carry out some attacks on their own

Course content:

Lecture:

Cryptology (10 lessons): Secret- and Public-Key Cryptography, Authentication, Integrity, Digital Signatures, Certificates, PKI, Cryptanalysis

Methods and Protocols to Secure Internet- Applications (18 lessons): Layer 1 & 2 Security, Wireless LAN Security, Firewalls, End-to-End Communication Security (SSL/TLS, IPsec), Virtual Private Networks, Authentication Protocols (NTLM, Kerberos, Shibboleth), Access Control Mechanisms (DAC, MAC, RBAC), e-Mail Security (S/MIME, PGP)

Lab:

- Secret-Key Cryptography
- Public-Key Cryptography and Hash Functions
- Network Attacks
- Firewalls & Portscans
- Intrusion Detection wth Snort and Prelude
- Apache Web Server Hardening and Digital Certificates
- Access Control Mechanisms

Previous knowledge:

KT1 (Kommunkationstechnik 1)

Teaching method:

Type of lesson:	Number of lessons per week:
Lecture	14*2
Tutorial/Practicum	7*4
Group teaching	
Block instruction	
Seminar	

Assessment:

According to the table or as specified in writing by the lecture at the beginning of the semester!

Number	Type	Weighting
1	End of term exam	80%
	Exam during the semester	
7	Rating of lab exercise results	20%

Language of instruction:

Deutsch

Instruction material:

Lecture slides with additional, detailed comments

Comments:

Not mandatory, but well-suited for additional insights: Charlie Kaufmann, Radia Perlman, Mike Spencer, Network Security, Second Edition, Prentice Hall, 2002