Zürcher Hochschule
für Angewandte Wissenschaften

School of
Engineering

t.ISI - Internet-Sicherheit

Kursverantwortung:	Marc Rennhard, rema
Credits:	4
Schuljahr:	2011/2012
Zuletzt gespeichert:	12.12.2011 13:11

Lernziel:
Die Studierenden erhalten einen fundierten Einblick in die Grundlagen, Protokolle und Methoden der Internet-Sicherheit. Dadurch sind die Studierenden in der Lage, internetbasierte Anwendungen hinsichtlich Sicherheit zu analysieren und Sicherheitskonzepte für internetbasierte Anwendungen selbst aufzustellen und umzusetzen. Im Speziellen erhalten die Studierenden folgende Kompetenzen:

- Sie verstehen die Grundlagen der Kryptologie (Algorithmen, Einsatzzwecke, Resistenz gegenüber Angriffen)

- Sie kennen und verstehen die modernen Protokolle und Methoden zur Sicherung der Kommunikation im Internet und um den Zugriff auf Systeme und Anwendungen zu kontrollieren und können diese zweckmässig einsetzen

- Sie verstehen insbesondere die Möglichkeiten und Limiten dieser Protokolle und Methoden hinsichtlich der Sicherheit, die sie bieten

- Sie kennen Angriffsszenarien und können einzelne Attacken selbst durchführen

Lerninhalt:
Vorlesung:

Kryptologie (10 Lektionen): Secret- und Public-Key Cryptography, Authentisierung, Integrität, Digitale Signaturen, Zertifikate, PKI, Cryptanalysis

Methoden und Protokolle zur Sicherung von Internet-Applikationen (18 Lektionen): Layer 1 & 2 Sicherheit, Wireless LAN Sicherheit, Firewalls, End-to-End Sicherheit (SSL/TLS, IPsec), Virtual Private Networks, Authentisierungprotokolle (NTLM, Kerberos, Shibboleth), Access Control Mechanismen (DAC, MAC, RBAC), E-Mail Sicherheit (S/MIME, PGP)

Praktikum:

- Secret-Key Cryptography
- Public-Key Cryptography und Hash Functions
- Netzwerkattacken
- Firewalls & Portscans
- Intrusion Detetcion mit Snort und Prelude
- Apache Webserver Hardening und Digitale Zertifikate
- Access Control Mechanismen

Vorkenntnisse:

KT1 (Kommunkationstechnik 1)

Durchführung:

Unterrichtsart	Anzahl Lektionen pro Woche
Vorlesung	14*2
Übung/Praktika	7*4
Gruppenunterricht	
Blockunterricht	
Seminar	

Leistungsnachweise:

Laut Tabelle oder gemäss schriftlicher Festlegung des Dozierenden zu Semesterbeginn!

Anzahl	Art	Gewichtung
1	Modulendprüfung	80%
	Prüfungen während der Unterrichtszeit	
7	Bewertete Praktika	20%

Unterrichtssprache:

Deutsch

Unterrichtsunterlagen:

Vorlesungsfolien mit zusätzlichen, ausführlichen Kommentaren

Bemerkungen:

Nicht zwingend notwendig, aber zur Vertiefung geeignet: - Charlie Kaufmann, Radia Perlman, Mike Spencer, Network Security, Second Edition, Prentice Hall, 2002