

t.ISI - Internet-Sicherheit

Kursverantwortung:	Marc Rennhard, rema
Credits:	4
Schuljahr:	2010/2011
Zuletzt gespeichert:	14.02.2011 08:47

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 Studierende folgende Kompetenzen:

- Sie verstehen die Grundlagen der Kryptologie (Algorithmen, Einsatzzwecke, Resistenz gegenüber Angriffen)
 - Sie kennen und verstehen die modernen Protokolle zur Sicherung der Kommunikation im Internet und können diese zweckmässig einsetzen
 - Sie verstehen insbesondere die Möglichkeiten und Limiten dieser Protokolle hinsichtlich der Sicherheit, die sie bieten
 - Sie kennen Angriffsszenarien auf Protokolle und Applikationen und können Attacken selbst durchführen
-

Lerninhalt:

Vorlesung:

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

Sichere Internetprotokolle (14 Lektionen): Layer 1 & 2 Sicherheit, Wireless LAN Sicherheit, Firewalls, IPSec, SSL/TLS, Authentisierungsprotokolle (NTLM, Kerberos), E-Mail Sicherheit (S/MIME, PGP)

Aktuelle Sicherheitsprobleme mit Anwendungen im Internet (4 Lektionen): Typische Attacken (SQL Injection, Cross-Site Scripting, Buffer Overflows), Gegenmassnahmen

Praktikum:

- Secret-Key Cryptography
- Public-Key Cryptography und Hash Functions
- Netzwerkattacken
- Firewalls & Portscans
- Java Cryptography Architecture
- Apache Webserver Hardening und Digitale Zertifikate
- Attacken auf Webapplikationen

Vorkenntnisse:

KT1 (Kommunikationstechnik 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