

t.ISI - Internet-Sicherheit

Kursverantwortung: Marc Rennhard, rema
verantwortliche OE:
ECTS: 4
Schuljahr: 2012/2013
Zuletzt gespeichert: 25.03.2013 18:52

Fachkompetenz:

-

Methodenkompetenz:

-

Sozialkompetenz:

-

Selbstkompetenz:

-

Lernziel:

Fast jedes IT-System hat heute gewisse Sicherheitsanforderungen, insbesondere wenn das System exponiert ist und über ein Netz (z.B. das Internet) erreicht werden kann. In diesem Modul werden die Grundlagen der IT-Sicherheit vermittelt, um IT-Systeme zu sichern und bezüglich Sicherheit zu analysieren. Im Speziellen erhalten die Studierenden folgende Kompetenzen:

- Sie verstehen die Grundlagen der Kryptologie (Algorithmen, Einsatzzwecke, Resistenz gegenüber Angriffen), welche die Basis für eine Vielzahl der modernen Sicherheitsmechanismen bietet.
 - Sie beherrschen die modernen Protokolle und Methoden zur Sicherung der Kommunikation und um den Zugriff auf Systeme und Anwendungen zu kontrollieren und können diese zweckmässig anwenden.
 - Sie verstehen insbesondere auch die Möglichkeiten und Limiten dieser Protokolle und Methoden hinsichtlich der Sicherheit, die sie bieten.
 - Sie beherrschen Angriffsverfahren auf Kommunikationsprotokolle und können Attacken selbst durchführen.
-

Lerninhalt:

Theorie Kryptologie (10 Lektionen):

- Secret- und Public-Key Cryptography
- Authentisierung, Integrität, Digitale Signaturen
- Zertifikate, Public Key Infrastructure

Theorie Methoden und Protokolle (18 Lektionen):

- Layer 1 & 2 Sicherheit, Wireless LAN Sicherheit
 - End-to-End Sicherheit (SSL/TLS, IPsec), Virtual Private Networks
 - Authentisierungsprotokolle (NTLM, Kerberos, Shibboleth)
-

- Firewalls, 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 Detektion mit Snort und Prelude
- Apache Webserver Hardening und Digitale Zertifikate
- Autorisierung in Linux

Vorkenntnisse:

KT1 (Kommunikationstechnik 1)

Durchführung:

Unterrichtsart	Anzahl Lektionen pro Woche
Vorlesung	14*2
Übung/Praktika	14*2
Blockunterricht	

Leistungsnachweise:

Laut Tabelle oder gemäss schriftlicher Festlegung des Dozierenden zu Semesterbeginn!

Bezeichnung	Art	Form	Umfang	Bewertung	Gewichtung
Leistungsnachweise während Unterrichtszeit	Bewertete Praktika	Schriftlich und mündlich	Alle Praktika	Punkte, die zur Punktzahl der Schlussprüfung addiert werden	20%
Semesterendprüfung	Prüfung	schriftlich	90 Minuten	Note	80%

Unterrichtssprache:

Deutsch

Unterrichtsunterlagen:

Vorlesungsfolien mit zusätzlichen, ausführlichen Kommentaren

Ergänzende Literatur:

Zur selbstständigen Vertiefung: Charlie Kaufmann, Radia Perlman, Mike Spencer, Network Security, Second Edition, Prentice Hall, ISBN 0130460192

Bemerkungen:

-