

Vorlesung
Sicherheit:
Fragen und Lösungsansätze

Dr. Thomas P. Ruhroth

TU Dortmund, Fakultät Informatik, Lehrstuhl XIV

Vorlesungswebseite (bitte notieren):

http://www-secse.cs.tu-dortmund.de/secse/pages/teaching/ws14-15/sfl/index_de.shtml

Ergebnisse des Fragebogen

Infos

- Männlich: 22
- Weiblich 4
- Anrede:
 - **Sie: 1**
 - Du: 15
 - Egal: 8
 - Enth: 1
- Besuch der Vorlesung
 - Pflicht: 7
 - Sicher: 15
 - Mal sehen: 6
-
- Studiengänge:
 - Ba Inf: 9
 - Ma Inf: 1
 - Ma Stat: 1
 - Datenwissenschaften: 6
 - Inf: 6
 - Ba Ang. Inf: 3

Sprachen und Sicherheitssysteme

	Experte	Mittler Erfh	Grundkennt.	Keine Erfah.	Nie gehört
Java	2	18	9	2	0
C	0	4	13	8	0
C++	1	2	11	11	1
C#	1	5	5	10	4
Email-Verschl	0	4	4	15	4
VPN	0	3	5	14	5
Java Sec	0	0	0	16	10
Sec Progr	0	0	6	15	5

Begriffe

	Sehr gut	gut	naja	falsch	ka
Asymmetrische Verschlüsselung	5	9	0	1	11
Authentifikation	5	6	4	2	9
Nonce	1	0	0	0	25
Hashfunktion	3	9	4	1	9
Körper	3	5	7	1	10

Erwartungen:Vorlesung Misserfolg

- Kein Bezug zur Realität/ Zu theoretische (7)
- Übungsblätter zu schwierig/zeitaufwendig (4)
- Dozentenwechsel/ Krankheit/ Sterben (3)
- Überforderung/Nicht erfüllbare Erwartung (3)
- Wissenslücken werden nicht geschlossen/ Nichts lernen/
Nicht verstehen (2)
- Schlechte Note/ Durchfallen (2)
- Ich lasse mich überraschen
- Sehr trocken
- Schlechte Folien
- Zu Schnell

Bemerkung

- Aufwand größer als 3 SWS
 - Die SWS beschreiben nur die Präsenzzeiten (Vorlesung und Übung)!
 - Keine Vorlesung kann nur durch den Besuch der Vorlesungen und Übungen bestanden werden!

Inhalt

- Grundlagen der Sicherheit/ Überblick (5)
- Praxisbezug/ Aktuelle Beispiele (2)
- Verfahren zum Finden von Backdoors/Prüfen von Software
- TLS
- Basiswissen Verschlüsselung
- Spaß
- Klar definiert aber realitätsnah
- Vorbereitung fürs weitere Studium

Dozent

- Erklärt verständlich/ interessant (5)
- Nicht krank werden (3)
- Motivation (2)
- Beantwortet Fragen (2)
- Beispiele (2)
- Gleiches Verhalten wie in Lsys (2)
- Locker und entspannt mit genügend Leistungsdruck (2)
- Weiter so wie in der ersten Vorlesung
- Kompetenz
- Hohe rhetorische Fähigkeiten
- Einfühlungsvermögen in die Gruppe
- Freundlich

0. Organisatorisches (Update 1)

Prüfungen

Modulprüfung: **mündliche Prüfung** (25-35 Minuten)

Leistungsnachweise:

- Diplom-Studierende nach DPO 2001 erhalten einen unbenoteten Schein durch erfolgreiche Teilnahme an der Prüfung.
 - Die Teilnahme an den Übungen und die Abgabe von Hausübungen sind freiwillig.
- Bachelor-Studierende benötigen für die **Zulassung** zur Prüfung/Klausur einen Leistungsnachweis über die **erfolgreiche Teilnahme an den Übungen.**

Heimübungen

- Zwei Arten:
 - Leistungspunktaufgaben
 - Bearbeitungspunktaufgaben

Leistungspunktaufgaben (LP)

Leistungspunktaufgaben entsprechen den Aufgaben wie Sie sie kennen:

- Richtigkeit wird Bewertet
- Vollständige Bearbeitung
- Lösungen sind eindeutig

Nachteil:

- Oft zu strukturiert => Denken wird nicht gefördert
- Sicher zu lösen => Wiederholung aber keine Herausforderung

Bearbeitungspunktaufgaben (BP)

- Freiere Gestaltung der Aufgabe
 - Aufgabe kann über den Stoff hinausgehen
 - Punkte für „glaubhafte Beschäftigung“ mit dem Stoff
 - Punkte für eine gute Lösung
 - Lösungsvorschläge aus den Abgaben
- Nachteile:
 - In der Regel keine Musterlösungen möglich