Vertiefungs- und Wahlpflichtmodule: Sicherheitstechniken in Kommunikationsnetzen

Modul-Bezeichnung MSc Curriculum 2012	überarbeitet: Mündemann, 20.4.13	Stufen nach Bloom	Sicherheitstechniken in Kommunikationsnetzen
englische Modulbezeichnung			Safety and security techniques in communication networks
Abkürzung			STK
Beschreibung erstellt	am		05.02.2013
	durch		Hanemann
Niveaustufe			Master
Studiensemester			2
Kreditpunkte			5
Status	Pflichtmodul		
	Wahlpflichtmodul		Wahlpflichtmodul
	Wahlmodul		
Häufigkeit des Angebotes			jedes Semester nach Bedarf der Hochschulen des VFH-Verbundes
Lehrsprache			Deutsch
Autoren			Prof. Dr. Hanemann (FH Lübeck)
Verantwortliche Hochschule			FH Lübeck
Fachverbunds-leiter(in)			Prof. Dr. Hanemann (FH Lübeck)
Verantwortliche(r) Lehrende(r) am Standort nach dem Meister-Geselle-Prinzip: ein Lehrender für alle Standorte	Beuth-Hs Berlin		Prof. Dr. Hanemann (FH Lübeck)
	FH Brandenburg		Prof. Dr. Hanemann (FH Lübeck)
	FH Emden / Leer		Prof. Dr. Hanemann (FH Lübeck)
	FH Lübeck		Prof. Dr. Hanemann (FH Lübeck)
	Ostfalia Hochschule Wolfenbüttel		Prof. Dr. Hanemann (FH Lübeck)
Lerngebiet			Vertiefung Mobile Computing, Vertiefung Software-Technologien
Erworbene Kenntnisse, Fertigkeiten, Kompetenzen	Formale, algorithmische, mathematische Kompetenzen	Wissen	Mathematischer Hintergrund von sicherheitsrelevanten Algorithmen zur Verschlüsselung und Authentifizierung
		Verstehen	
		Anwenden	
		Analysieren	
		Synthetisieren	
		Evaluieren, Bewerten	
	Analyse-, Design- und Realisierungs-Kompetenzen	Wissen	
		Verstehen	
		Anwenden	
		Analysieren	
		Synthetisieren	
		Evaluieren, Bewerten	
	Technologische Kompetenzen	Wissen	Bedeutung von sicherheitstechnischen Lösungen für die Medienübertragung einordnen
		Verstehen	Prinzipien und Funktionsweise der unterschiedlichen Authentifizierungs-Mechanismen verstehen
		Anwenden	unterschiedliche Authentifizierungs-Mechanismen anwenden
		Analysieren	unterschiedliche sicherheitstechnische Lösungen in Kommunikationsnetzen erkennen
		Synthetisieren	

		Evaluieren, Bewerten	
	Fachübergreifende Kompetenzen	Wissen	
		Verstehen	
		Anwenden	
		Analysieren	
		Synthetisieren	
		Evaluieren, Bewerten	
	Methodenkompetenzen	Wissen	
		Verstehen	
		Anwenden	
		Analysieren	
		Synthetisieren	
		Evaluieren, Bewerten	
	Projektmanagement-Kompetenz	Wissen	
		Verstehen	
		Anwenden	
		Analysieren	
		Synthetisieren	
		Evaluieren, Bewerten	
	Soziale Kompetenz und Selbstkompetenz	Wissen	
		Verstehen	
		Anwenden	
		Analysieren	
		Synthetisieren	
		Evaluieren, Bewerten	
Obligatorische Teilnahmevoraussetzungen (nach Prüfungsordnung)			
Fakultative Teilnahmevoraussetzungen			
Medien-/ Lernform			Multimedial aufbereitetes Online-Studienmodul zum Selbststudium mit zeitlich parallel laufender Online-Betreuung (E-Mail, Chat, Einsendeaufgaben u. a.) sowie Präsenzphasen.
Arbeitsaufwand / work load (jeweils in Zeitstunden summiert)	Pflicht-Präsenzstudium	Vorlesung, Übung, Labor, Seminar u.a.	
		Modulprüfung	0,5h
	Online-Studium (Chat, Audio- / Videokonf. u.a.) incl. studentische Lerngruppen und fakultative Präsenzen		8h
	Erarbeiten der Prüfungsvorleistungen		12h
	Eigenstudium einschl. Prüfungs-vorbereitung		129,5h
Summe Workload in Stunden			150h
Präsenzinhalte			In der ersten Präsenzveranstaltung werden Übungen mit den Schwerpunkten IPSec, SSL, SSH und SNMP durchgeführt. Die zweite Präsenzveranstaltung dient der Prüfungsvorbereitung
Präsenzart	obligatorisch		
	fakultativ		fakultativ
Präsenzteilnahme	erfordert physische Anwesenheit		

	per web-Konferenz möglich		Die Vermittlung der Präsenzinhalte ist per Webkonferenz möglich.
Prüfungsvorleistungen	Präsenzteilnahme		
	Online-Teilnahme		
	Einsendeaufgaben		Erfolgreiche Bearbeitung von Einsendeaufgaben
	Hausarbeit / Projektarbeit		
Teilleistungsnachweise			
Prüfungsform	Klausur	(120 Min)	Klausur (120 min)
	Mündliche Prüfung	(30 Min)	
	Hausarbeit mit Kolloquium	(30 Min)	
Benotung			
Literatur			Wolfgang Böhmer, "VPN - Virtual Private Networks", 2. Auflage, Hanser, 2005 James Kurose, Keith Ross, "Computernetzwerke", 6. Auflage, Pearson Studium, 2012 Claudia Eckert, "IT- Sicherheit", 7. Auflage, Oldenbourg Verlag, 2011
Weitere Hinweise			
Studieninhalte des Moduls (Allgemeines zum Modul / Zusammenfassung)			
Kapitelüberschriften / Überschriften der Lerneinheiten			LE 1: Netzwerk Management 1. Überblick 2. Simple Network Management Protocol (SNMP) 3. Protokoll-Spezifikation 4. Lesen und Setzen von Instanzen 5. RMON 6. Zusammenfassung
			LE 2: Angriffe aus dem Internet 1. Überblick 2. Typische Angriffsarten der Schichten 1 und 2 3. Typische Angriffsarten der Schicht 3 4. Typische Angriffsarten der Schicht 4 5. Typische Angriffsarten der höheren Schichten 6. Tools und Referenzen 6.1. Nessus 6.2. Wireshark 6.3. Snort 6.4. Nmap 6.5. Tripwire 6.6. Referenzen 7. Zusammenfassung
			LE 3: Abwehr von Angriffen 1. Überblick 2. Firewall 3. IDS 4. Honeypot 5. Zusammenfassung
			LE 4: Sicherheitsprotokolle 1. Überblick 2. Sicherheitsprotokolle im OSI-Modell 3. Grundlegende Verfahren 4. SSL / TLS 5. IPsec 6. SSH 7. Andere Anwendungen 8. Zusammenfassung

		LE 5: Dienstgüte im Internet 1. Überblick 2. Dienstgüte-Faktoren 3. Bekämpfung von Stauproblemen 4. Techniken zur Verkehrsflusskontrolle 5. Netzwerkmodelle 5.1. IntServ 5.2. DiffServ 6. Realisierungen 7. Zusammenfassung
		LE 6: Ressource Reservation Protocol 1. Überblick 2. RSVP in Host und Router 3. Reservierungs-Stil 4. Soft State 5. Service Parameter 6. RSVP Nachrichten und Objekte 7. Zusammenfassung
		LE 7: Multiprotocol Label Switching 1. Überblick 2. MPLS Prinzip 3. Label Switched Path 4. Forwarding Equivalence Class 5. MPLS-Header 6. Generalized MPLS 7. Zusammenfassung
		LE 8: Single Sign On (SSO) 1. Überblick 2. Grundlagen der Authentifizierung 3. Lösungsansätze für einheitliche Authentifizierung 4. Überblick über verschiedene Implementierungen von SSO 4.1. Kerberos 4.2. Public-Key-Infrastruktur 4.3. Central Authentication Service 4.4. OpenID 4.5. Liberty Alliance Project 4.6. Shibboleth 4.7. Security Assertion Markup Language 4.8. Weitere SSO Lösungen 5. Zusammenfassung