



Zertifikatsprogramm - Z301

Grundlagen der Netzsicherheit

- Einführung
- Sicherheit von Rechnernetzen
- Zugriffsmanagement
- Klassische Netzwerke
- Moderne Netzwerke

Tobias Scheible, M.Eng.

Modul Z-301

Grundlagen der Netzsicherheit

Studienbrief 1: Einführung

Studienbrief 2: Sicherheit von Rechnernetzen

Studienbrief 3: Zugriffsmanagement

Studienbrief 4: Klassische Netzwerke

Studienbrief 5: Moderne Netzwerke

Autor:

Tobias Scheible, M.Eng.

1. Auflage

Hochschule Albstadt-Sigmaringen

© 2021 Hochschule Albstadt-Sigmaringen

Hochschule Albstadt-Sigmaringen
Zertifikatsprogramm
Poststraße 6
72458 Albstadt

Version 1.0.0

1. Auflage (2021-04-14)

Das Werk einschließlich seiner Teile ist urheberrechtlich geschützt. Jede Verwendung außerhalb der engen Grenzen des Urheberrechtsgesetzes ist ohne Zustimmung der Verfasser unzulässig und strafbar. Das gilt insbesondere für Vervielfältigungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Um die Lesbarkeit zu vereinfachen, wird auf die zusätzliche Formulierung der weiblichen Form bei Personenbezeichnungen verzichtet. Wir weisen deshalb darauf hin, dass die Verwendung der männlichen Form explizit als geschlechtsunabhängig verstanden werden soll.

Inhaltsverzeichnis

Einleitung zu den Studienbriefen	6
I. Abkürzungen der Randsymbole und Farbkodierungen	6
II. Zu dem Autor	8
III. Modullehrziele	9
IV. Literaturempfehlungen	10
V. Inhalte	10
Studienbrief 1 Einführung	11
1.1 Lernergebnisse	11
1.2 Advance Organizer	11
1.3 Rechnernetze Grundlagen	12
1.3.1 Netzwerke	12
1.3.2 Schichtenmodelle	22
1.4 Kryptografie Grundlagen	38
1.4.1 Hashfunktionen	38
1.4.2 Verschlüsselungsverfahren	43
1.4.3 Signaturen und Zertifikate	46
1.5 Informationssicherheit Grundlagen	49
1.5.1 Bedrohungen	49
1.5.2 Schutzziele	52
1.6 Zusammenfassung	53
1.7 Übungsaufgaben	53
Studienbrief 2 Sicherheit von Rechnernetzen	55
2.1 Lernergebnisse	55
2.2 Advance Organizer	55
2.3 Sicherheitskonzept	56
2.3.1 Strukturanalyse	56
2.3.2 Schutzbedarfsfeststellung	57
2.3.3 Auswahl und Anpassung von Maßnahmen	57
2.3.4 Basis-Sicherheitscheck	58
2.3.5 Weiterführende Sicherheitsmaßnahmen	58
2.3.6 Weitere Konzepte	59
2.4 Angriffe auf Netzwerke	61
2.4.1 Scans	61
2.4.2 Man-in-the-Middle	63
2.4.3 Denial-of-Service	64
2.4.4 Spezielle Hardware Tools	66
2.4.5 Physische Angriffe	69

2.5	Verteidigungsmaßnahmen	71
2.5.1	Separation von Netzen	71
2.5.2	Firewalls und Proxies	72
2.5.3	Virtual Private Network (VPN)	73
2.5.4	Intrusion Detection and Prevention Systems	74
2.5.5	Honeypots und Honeynets	74
2.6	Zusammenfassung	76
2.7	Übungsaufgaben	77
2.7.1	Laborumgebung	77
2.7.2	Übungen	78
Studienbrief 3 Zugriffsmanagement		81
3.1	Lernergebnisse	81
3.2	Advance Organizer	81
3.3	Authentifikation	82
3.3.1	Authentisierung	82
3.3.2	Authentifizierung	84
3.3.3	Autorisierung	90
3.4	Protokolle und Systeme	93
3.4.1	LDAP	93
3.4.2	RADIUS/Diameter	95
3.4.3	Kerberos	96
3.5	Zusammenfassung	99
3.6	Übungsaufgaben	100
Studienbrief 4 Klassische Netzwerke		101
4.1	Lernergebnisse	101
4.2	Advance Organizer	101
4.3	LAN/WAN	102
4.3.1	Netzzugangsschicht	102
4.3.2	Internetschicht	107
4.3.3	Transportschicht	111
4.3.4	Anwendungsschicht	113
4.4	WLAN	119
4.4.1	Technische Umsetzung	119
4.4.2	WLAN Sicherheitsarchitektur	121
4.4.3	Angriffe auf WLAN-Verbindungen	123
4.5	Bluetooth	128
4.5.1	Technische Umsetzung	128
4.5.2	Bluetooth-Sicherheitsarchitektur	129
4.5.3	Angriffe auf Bluetooth-Verbindungen	130
4.6	Mobilfunk	132
4.6.1	GSM und GPRS	132
4.6.2	UMTS	133
4.6.3	LTE	134

4.6.4	5G	135
4.6.5	Angriffsszenarien	136
4.7	Zusammenfassung	141
4.8	Übungsaufgaben	142
Studienbrief 5 Moderne Netzwerke		143
5.1	Lernergebnisse	143
5.2	Advance Organizer	143
5.3	Konzepte	144
5.3.1	Software-Defined Networking	144
5.3.2	Network Function Virtualization	146
5.3.3	Komponenten	147
5.4	Protokolle	149
5.4.1	Virtual Local Area Network	149
5.4.2	Generic Routing Encapsulation	149
5.4.3	OpenFlow	150
5.5	Zusammenfassung	151
5.6	Übungsaufgaben	152
Liste der Lösungen zu den Kontrollaufgaben		153
Verzeichnisse		159
I.	Abbildungen	159
II.	Beispiele	160
III.	Definitionen	160
IV.	Exkurse	160
V.	Kontrollaufgaben	161
VI.	Tabellen	161
VII.	Literatur	162
Stichwörter		167
Glossar		171

Einleitung zu den Studienbriefen

I. Abkürzungen der Randsymbole und Farbkodierungen

Beispiel	B
Definition	D
Exkurs	E
Kontrollaufgabe	K
Übung	Ü

II. Zu dem Autor



Zunächst studierte Tobias Scheible Kommunikations- und Softwaretechnik an der Hochschule Albstadt-Sigmaringen und schloss sein Diplomstudium 2009 in der Fachrichtung Kommunikationstechnik ab. In seiner Diplomarbeit beschäftigte er sich mit der Erhebung von spezifischen Anforderungen an asynchrone Web Applications. 2017 schloss er sein Masterstudium Systems Engineering, das er berufsbegleitend absolvierte, ebenfalls an der Hochschule Albstadt-Sigmaringen ab. In seiner Masterthesis befasste er sich mit der automatisierten und benutzerzentrierten Sicherheitsbewertung von Web-Anwendungen.

Seine berufliche Laufbahn nach dem Studium begann er in der Marketingbranche, wobei er für die Konzeption und Entwicklung von Webprojekten und die Planung und Durchführung von Online-Marketing Kampagnen zuständig war.

Seit 2012 ist er als Sicherheitsforscher an der Hochschule Albstadt-Sigmaringen tätig. Dort arbeitete er zuerst als Modulentwickler im Forschungsprojekt Open Competence Center for Cyber Security und entwickelte Studieninhalte zu den Bereichen Cloud Computing und Internettechnologien. Danach engagierte er sich als Autor und e-Tutor im berufsbegleitenden Masterstudiengang Digitale Forensik und leitete im Bachelorstudiengang IT Security Praktika rund um das Thema Informationssicherheit und Digitale Forensik. Aktuell ist er im Forschungsprojekt SEKT tätig und beschäftigt sich mit der IT-Sicherheit von elektronischen Kommunikationssystemen in smarten textilen Produkten. Darüber hinaus ist er in der Weiterbildung als Dozent im Hochschulzertifikatsprogramm tätig.

Lehrveranstaltungen

- Internettechnologien *Hochschulzertifikatsprogramm*
- Einführung in die Informatik *Masterstudiengang Digitale Forensik*
- Internet Grundlagen *Masterstudiengang Digitale Forensik*
- Betriebssystemforensik *Masterstudiengang Digitale Forensik*
- Grundlagen der digitalen Forensik *Masterstudiengang IT GRC Management*
- Cloud Technologies and Cloud Security Architectures *Masterstudiengang IT GRC*
- Digitale Forensik *Bachelorstudiengang IT Security*
- Praktikum Cyber Security *Bachelorstudiengang IT Security*
- Industrieprojekt *Bachelorstudiengang IT Security*
- Praktikum IT Security 2 *Bachelorstudiengang IT Security*
- Seminar IT Security 2 *Bachelorstudiengang IT Security*
- Informationssicherheit Praktikum *Bachelorstudiengang Wirtschaftsinformatik*
- Digitale Rechnersysteme *Studium Initiale*
- Einführung Algorithmen und Programmierung *Studium Initiale*
- Wissenschaftliches Arbeiten *Studium Initiale*

III. Modullehrziele

Die Lehrveranstaltung „Grundlagen der Netzsicherheit“ gibt Ihnen einen Überblick über die eingesetzten Technologien von Rechnernetzen und zeigt die wichtigsten Merkmale und Eigenschaften von klassischen und modernen Datennetzen. Es werden die wichtigsten Sicherheitsprotokolle, die häufigsten Angriffe auf Netzwerke und die entsprechenden Verteidigungsmaßnahmen erläutert. Sie lernen die Funktionsweise und Sicherheitsarchitektur der drahtlosen Netzwerke WLAN, Bluetooth und Mobilfunk kennen. In Übungen im virtuellen Labor führen Sie selbst Angriffe durch, um im Anschluss Bedrohungsszenarien nachvollziehen und einordnen zu können.

Im ersten Studienbrief „Einführung“ werden Grundlagen in den Bereichen Rechnernetze, Kryptografie und IT-Sicherheit behandelt, um vorhandenes Wissen zu reaktivieren und einen gemeinsamen Ausgangspunkt für dieses Modul zu schaffen.

Im zweiten Studienbrief „Sicherheit von Rechnernetzen“ erlernen Sie generelle Sicherheitskonzepte für Netzwerke. Anhand von realitätsnahen Angriffsszenarien und relevanten Verteidigungsmaßnahmen werden Sicherheitseigenschaften von Netzwerktechnologien praxisorientiert vorgestellt.

Im dritten Studienbrief „Zugriffsmanagement“ wird ein Überblick über das Thema Zugriffssteuerung gegeben. Außerdem werden verschiedene Protokolle und Systeme behandelt, die einen wirksamen Schutz ermöglichen.

Im vierten Studienbrief „Klassische Netzwerke“ wird die Architektur der LAN/WAN-Netze anhand des Schichtenmodells vorgestellt. Darüber hinaus wird dargelegt, welche Angriffsarten auf welcher Ebene möglich sind. Zusätzlich werden die verbreitetsten Angriffsarten auf WLAN-Netzwerke behandelt und erläutert, welche Gegenmaßnahmen hier existieren. Anhand des Bluetooth Protokolls wird ein alternatives Funknetzwerk beschrieben. Außerdem gibt es einen Ausblick auf die verwendeten Sicherheitskonzepte der Mobilfunknetze und deren Weiterentwicklung.

Im letzten Studienbrief „Moderne Netzwerke“ wird ein Ausblick auf flexible und softwaregesteuerte Netzwerktechniken gegeben. Anhand von verschiedenen Konzepten und Protokollen werden die Grundlagen erklärt und der konkrete Einsatz mit Beispielen erläutert. Abschließend werden die hier relevanten Sicherheitskonzepte aufgegriffen.

Nach erfolgreichem Abschluss des Moduls haben Sie Kenntnisse über die wichtigsten Merkmale und Eigenschaften von klassischen und modernen Netzwerken und können die verwendeten Sicherheitskonzepte einordnen. Des Weiteren können Sie die Funktionsweise und Sicherheitseigenschaften von klassischen und modernen Netzwerktechnologien exemplarisch anwenden.

IV. Literaturempfehlungen

Das Modul wurde so realisiert, dass die Studienbriefe genügend Materialien in Form von Hinweisen, Übungen und Abbildungen bieten, um selbstständig und ohne weitere Literatur bearbeitet werden zu können. Zusätzlich erfolgen immer wieder Verweise auf frei verfügbare externe Quellen, um spezifische Aspekte näher zu erläutern oder mit individuellen Beispielen zu verdeutlichen.

Darüber hinaus können Sie aus dem Netzwerk der Hochschule Albstadt-Sigmaringen (auch per VPN) auf folgende eBooks kostenfrei zugreifen:

- IT-Sicherheit für TCP/IP- und IoT-Netzwerke : Grundlagen, Konzepte, Protokolle, Härtung | Steffen Wendzel | Springer Vieweg, Wiesbaden | ISBN 9783864914898 | <https://doi.org/10.1007/978-3-658-22603-9>
- Netzsicherheit : Grundlagen & Protokolle; mobile & drahtlose Kommunikation; Schutz von Kommunikationsinfrastrukturen | Günter Schäfer; Michael Roßberg | dpunkt.verlag, Heidelberg | ISBN 9783864901157 | <https://ebookcentral.proquest.com/lib/hsalbsig-ebooks/detail.action?docID=1764755>
- IT-Sicherheit: Konzepte - Verfahren - Protokolle | Claudia Eckert | De Gruyter, Oldenbourg | ISBN 9783110551587 | <https://www.degruyter.com/viewbooktoc/product/490352>
- Kryptographie und IT-Sicherheit | Stephan Spitz; Michael Pramateftakis; Joachim Swoboda | Springer Vieweg, Wiesbaden | ISBN 9783834881205 | <https://doi.org/10.1007/978-3-8348-8120-5>

Darüber hinaus können die folgenden Bücher zur Unterstützung hinzugezogen werden:

- Computernetzwerke | Andrew S. Tanenbaum; David J. Wetherall | Pearson, München | ISBN 9783868941371 | <https://www.pearson-studium.de/computernetzwerke.html>

Zusätzlich kann noch die folgende Online-Quelle zur Unterstützung genutzt werden:

- IT-Grundschutz des BSI - NET: Netze und Kommunikation | https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompodium/bausteine/NET/NET_Uebersicht_node.html

V. Inhalte

Elemente, die als *Exkurs* gekennzeichnet sind, gehen über die eigentliche Zielsetzung des Modul hinaus, verdeutlichen aber den Zusammenhang und stellen einen Praxisbezug her. Diese Elemente sind daher *nicht prüfungsrelevant*.

Studienbrief 1 Einführung



1.1 Lernergebnisse

Sie können grundlegende Begriffe der Netzwerktechnik erklären und einordnen. Sie besitzen das Wissen, um kryptografische Konzepte einzuordnen und können verschiedene Algorithmen und Protokolle situationsbezogen einschätzen. Darüber hinaus sind Sie in der Lage, die Kernelemente der IT-Sicherheit zu erläutern.

1.2 Advance Organizer

Dieser erste Studienbrief legt die Grundlagen für das weitere Verständnis des Themas Netzsicherheit. Die Inhalte werden nicht in den Online-Vorlesungen behandelt, sondern dienen im Selbststudium zur Wiederholung bzw. Reaktivierung des Wissens aus den Bereichen Rechnernetze, Kryptografie und IT-Sicherheit. In den folgenden Studienbriefen werden diese Grundlagen mit konkreten Anwendungsszenarien verknüpft.

Studienbrief 2 Sicherheit von Rechnernetzen



2.1 Lernergebnisse

Sie können einerseits die für Netzwerke relevanten Sicherheitskonzepte beschreiben und andererseits die dafür bedeutsamen Bereiche identifizieren. Sie kennen die häufigsten Angriffsarten auf Netzwerke und ihre Auswirkungen. Außerdem können Sie die Konzepte hinter typischen Verteidigungsmaßnahmen darstellen.

2.2 Advance Organizer

In diesem Studienbrief werden die Sicherheitsprinzipien von Rechnernetzen behandelt, auf denen die weiteren Studienbriefe aufbauen. Hierzu werden diese exemplarisch erklärt und später in komplexeren Szenarien aufgegriffen.

Studienbrief 3 Zugriffsmanagement



3.1 Lernergebnisse

Sie können die wichtigsten Begriffe und Konzepte in diesem Themenbereich einordnen und wiedergeben. Sie wissen, welche Protokolle und Systeme für die Realisierung verwendet werden. Zusätzlich können Sie anhand von Beispielen den konkreten Einsatz beschreiben.

3.2 Advance Organizer

In diesem Studienbrief werden die Methodiken in den Bereichen Authentifikation, Identity und Secret Management beschrieben und erläutert, wie damit Zugänge gesteuert werden können. Dieser Aspekt wird später bei den Angriffsszenarien vertieft.

Studienbrief 4 Klassische Netzwerke



4.1 Lernergebnisse

Sie können die Architektur von LAN/WAN-Netzen anhand des Schichtenmodells beschreiben und wissen, auf welcher Schicht welche Art von Angriffen zu erwarten ist. Sie wissen, welche Angriffe auf WLAN-Netze durchgeführt werden können und wie Sicherheitskonzepte in diesem Bereich aufgebaut sind. Sie können den Aufbau des Bluetooth Protokolls beschreiben und darlegen, welche Angriffsszenarien hier relevant sind. Außerdem können Sie die verschiedenen Mobilfunkstandards und die dazugehörigen Sicherheitsfunktionen einordnen.

4.2 Advance Organizer

Dieser Studienbrief beschreibt die etablierten Netzwerktechniken und verknüpft das Wissen aus den vorherigen Studienbriefen mit diesen Konzepten. Die Realisierung der Netzsicherheit wird durch Methoden der offensiven Sicherheit in den Bereichen LAN, WLAN und Bluetooth verdeutlicht.

Studienbrief 5 Moderne Netzwerke



5.1 Lernergebnisse

Sie können die Grundlagen und Konzepte von modernen und flexiblen Netzwerken erläutern. Zudem können Sie darstellen, welche Protokolle eingesetzt werden und sie können erläutern, wie konkrete Anwendungsszenarien aussehen. Darüber hinaus können Sie die Methoden zur Absicherung von modernen Netzwerken einordnen.

5.2 Advance Organizer

Dieser Studienbrief gibt einen Ausblick auf die Konzepte und Protokolle von modernen Netzwerken. Es wird gezeigt, wie diese in Rechenzentren, Cloud-Umgebungen und großen Unternehmen eingesetzt werden. Hierbei wird auch aufgezeigt, welche neuen Aspekte der Netzwerksicherheit sich daraus ergeben.

Verzeichnisse

I. Abbildungen

Abb. 1.1:	Zwei verbundene Rechner	12
Abb. 1.2:	Zwei Clients sind mit einem Server verbunden	14
Abb. 1.3:	Schema einer Ring-Topologie	15
Abb. 1.4:	Schema einer Bus-Topologie	15
Abb. 1.5:	Schema einer Stern-Topologie	16
Abb. 1.6:	Schema eines Punkt-zu-Punkt-Netzes	17
Abb. 1.7:	Ein Switch in einem Netzwerk	18
Abb. 1.8:	Gliederung der verschiedenen Netztypen	21
Abb. 1.9:	Schema der Kommunikationsarten Unicast, Multicast und Broadcast	22
Abb. 1.10:	Beispiel eines Schichtenmodells	23
Abb. 1.11:	ISO/OSI 7-Schichten Referenzmodell	25
Abb. 1.12:	Vergleich der Referenzmodelle	27
Abb. 1.13:	TCP/IP-Protokollstapel	28
Abb. 1.14:	Beispiel einer ARP-Anfrage	29
Abb. 1.15:	Ping per ICMP	31
Abb. 1.16:	TCP Drei-Wege-Handschlag	33
Abb. 1.17:	URI-Aufbau	36
Abb. 1.18:	URL-Aufbau	36
Abb. 1.19:	Beispiel zweier Hashfunktionen mit unterschiedlichen Eingabestrings	39
Abb. 1.20:	Ablauf Hash-based Message Authentication Code (HMAC)	42
Abb. 1.21:	ECB Penguin - ECB-Modus vs. verkettetem Modus [9]	44
Abb. 1.22:	Abstrahiertes Verfahren des Diffie-Hellman-Schlüsselaustauschs	46
Abb. 2.1:	„Erstellung der Sicherheitskonzeption im Informationssicherheitsmanagement“ [12, S. 36]	56
Abb. 2.2:	Beispielhafte Darstellung einer Defense-in-Depth Strategie“ [13]	60
Abb. 2.3:	Man-in-the-Middle	63
Abb. 2.4:	Beispielhafte Darstellung eines DoS-Angriffes	65
Abb. 2.5:	Lan Tap Pro	67
Abb. 2.6:	Packet Squirrel von Hak5	67
Abb. 2.7:	WiFi Pineapple Nano in Form eines größeren USB WiFi-Adapters	68
Abb. 2.8:	WiFi Deauther mit Akku und Display	69
Abb. 2.9:	Bluetooth, WiFi, GSM und UMTS Störsender	69
Abb. 2.10:	Beispielhafte Darstellung einer Separation	71
Abb. 2.11:	Nur bestimmte Verbindungen werden von der Firewall zugelassen	72
Abb. 2.12:	Getunnelte Verbindungen per VPN	73
Abb. 2.13:	T-Pot Aufbau [16]	75
Abb. 2.14:	Oracle VM VirtualBox Startbildschirm	77
Abb. 3.1:	Ablauf einer Authentifikation	82
Abb. 3.2:	transparente RFID-Zugangskarte	85
Abb. 3.3:	Zugang per Fingerabdruckscanner	86

Abb. 3.4: „Benötigte Zeit für Brute-Force-Angriff“ [18]	87
Abb. 3.5: Übersicht auf der Website <i>Have I Been Pwned</i> [19]	88
Abb. 3.6: Ablauf einer Zwei-Faktor-Authentisierung (2FA)	90
Abb. 3.7: Funktionsweise des Kerberos Protokolls	97
Abb. 4.1: Sniffing-Angriff - abfangen von Ethernet Frames	103
Abb. 4.2: Getunnelte Verbindung per VPN	109
Abb. 4.3: Unterbrechung und Umleitung der Verbindung	139
Abb. 4.4: 5G Störsender [39]	140
Abb. 5.1: Beispiel zweier virtualisierter Netzwerke	144
Abb. 5.2: Aufbau der OpenDayLight Plattform [41]	146
Abb. 5.3: Floating IP Anwendungsszenario	148

II. Beispiele

Beispiel 1.1: Kabelloses Netzwerk (WLAN)	16
Beispiel 1.2: DNS Telefonbuch Vergleich	37
Beispiel 2.1: WhatsApp	64
Beispiel 2.2: Produktionsbetrieb	71
Beispiel 2.3: T-Pot	75
Beispiel 3.1: Adobe Hack	88
Beispiel 3.2: Angriff auf die Wasserversorgung	92
Beispiel 4.1: WLAN Karte	124
Beispiel 4.2: REVOLTE	135
Beispiel 4.3: Twitter CEO Jack Dorsey	138
Beispiel 5.1: Anuket	147

III. Definitionen

Definition 1.1: Kryptografie	38
Definition 1.2: Hashfunktion	38

IV. Exkurse

Exkurs 1.1: Überseekabel	21
Exkurs 1.2: Verifikation in der IT-Forensik	40
Exkurs 1.3: Argon2 Algorithmus	41
Exkurs 1.4: Security & Safety	49
Exkurs 2.1: Penetrationstest	58
Exkurs 2.2: Shodan	63

V. Kontrollaufgaben

Kontrollaufgabe 1.1:	Topologie	16
Kontrollaufgabe 1.2:	Schichtenmodell	24
Kontrollaufgabe 1.3:	WLAN	27
Kontrollaufgabe 1.4:	IP-Adressen	30
Kontrollaufgabe 1.5:	Hash-Verfahren	41
Kontrollaufgabe 1.6:	Verschlüsselung	45
Kontrollaufgabe 1.7:	Schutzziele	53
Kontrollaufgabe 2.1:	Risikoanalyse	60
Kontrollaufgabe 2.2:	Scans	63
Kontrollaufgabe 2.3:	Scans	66
Kontrollaufgabe 2.4:	Hardware Tools	69
Kontrollaufgabe 2.5:	Separation von Netzen	71
Kontrollaufgabe 2.6:	IDS & IPS	74
Kontrollaufgabe 3.1:	Risikoanalyse	84
Kontrollaufgabe 3.2:	Risikoanalyse	86
Kontrollaufgabe 3.3:	Risikoanalyse	88
Kontrollaufgabe 3.4:	Risikoanalyse	88
Kontrollaufgabe 3.5:	Risikoanalyse	92
Kontrollaufgabe 4.1:	ARP-Spoofing	104
Kontrollaufgabe 4.2:	MAC-Filter	107
Kontrollaufgabe 4.3:	IP-Fragmentierung	109
Kontrollaufgabe 4.4:	WireGuard	111
Kontrollaufgabe 4.5:	TCP-Verbindung	112
Kontrollaufgabe 4.6:	SYN-Cookie	113
Kontrollaufgabe 4.7:	DHCP Starvation Attack	115
Kontrollaufgabe 4.8:	DNS	118
Kontrollaufgabe 4.9:	WPA2 und WPA3	122
Kontrollaufgabe 4.10:	Probe Requests	125
Kontrollaufgabe 4.11:	Schlüsselextraktion	131
Kontrollaufgabe 4.12:	SMS fälschen	137
Kontrollaufgabe 4.13:	IMSI-Catcher	140
Kontrollaufgabe 5.1:	Risikoanalyse	145
Kontrollaufgabe 5.2:	Risikoanalyse	148
Kontrollaufgabe 5.3:	VLAN und VXLAN	150

VI. Tabellen

Tabelle 1.1:	Beschreibung der einzelnen Schichten des ISO/OSI-Modells	26
Tabelle 1.2:	Beispiele einiger fester Ports	34
Tabelle 4.1:	Angriffe auf die Zugriffskontrolle	124

Tabelle 4.2: Angriffe auf die Geheimhaltung und die Vertraulichkeit	125
Tabelle 4.3: Angriffe auf die Integrität	125
Tabelle 4.4: Angriff auf die Authentifizierung	126
Tabelle 4.5: Angriffe auf die Verfügbarkeit	127

VII. Literatur

- [1] Steffen Wendzel. *IT-Sicherheit für TCP/IP- und IoT-Netzwerke - Grundlagen, Konzepte, Protokolle, Härtung*. Springer-Verlag, Berlin Heidelberg New York, 2018.
- [2] The Internet Standards Process. <https://tools.ietf.org/html/bcp9>. Letzter Zugriff: 08.02.2021.
- [3] Larry L. Peterson and Bruce S. Davie. *Computernetze - eine systemorientierte Einführung*. Dpunkt-Verlag, Köln, 2008.
- [4] Jürgen Scherff. *Grundkurs Computernetzwerke - Eine kompakte Einführung in Netzwerk- und Internet-Technologien*. Springer-Verlag, Berlin Heidelberg New York, 2010.
- [5] DE-CIX Frankfurt statistics. <https://www.de-cix.net/en/locations/germany/frankfurt/statistics>. Letzter Zugriff: 08.02.2021.
- [6] Luigi Lo Iacono Christoph Sorge, Nils Gruschka. *Sicherheit in Kommunikationsnetzen*. Oldenbourg Wissenschaftsverlag, München, 2013.
- [7] Einwegfunktion. <https://de.wikipedia.org/wiki/Einwegfunktion>. Letzter Zugriff: 16.02.2021.
- [8] Joachim Swoboda Stephan Spitzer, Michael Pramateftakis. *Kryptographie und IT-Sicherheit: Grundlagen und Anwendungen*. Springer Fachmedien Wiesbaden, 2011.
- [9] The ECB Penguin. <https://blog.filippo.io/the-ecb-penguin/>. Letzter Zugriff: 17.02.2021.
- [10] Claudia Eckert. *IT-Sicherheit - Konzepte - Verfahren - Protokolle*. Walter de Gruyter GmbH und Co KG, Berlin, 7. edition, 2012.
- [11] IT-Grundschatz-Bausteine. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschatz/IT-Grundschatz-Kompodium/IT-Grundschatz-Bausteine/Bausteine_Download_Edition_node.html. Letzter Zugriff: 16.02.2021.
- [12] Bundesamt für Sicherheit in der Informationstechnik (BSI). BSI-Standard 100-2 - IT-Grundschatz-Vorgehensweise. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschatzstandards/BSI-Standard_1002.pdf?__blob=publicationFile. Letzter Zugriff: 02.03.2021.
- [13] Moving Beyond “Blinky Box” Security to Defense-in-Depth Security. <https://ussignal.com/blog/moving-beyond-blinky-box-security-to-defense-in-depth-security>. Letzter Zugriff: 09.04.2021.

- [14] Heise Medien GmbH und Co. K. iX extra - Security. <https://www.heise.de/ix/downloads/05/2/7/7/6/8/3/1/ix.2019.10.extra.pdf>. Letzter Zugriff: 05.03.2021.
- [15] Ronald Eikenberg. Hackerangriff auf WhatsApp. <https://www.heise.de/security/meldung/Hackerangriff-auf-WhatsApp-1974342.html>. Letzter Zugriff: 09.03.2021.
- [16] T-Pot GitHub. <https://github.com/telekom-security/tpotce>. Letzter Zugriff: 05.03.2021.
- [17] Norbert Pohlmann. *Cyber-Sicherheit - Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung*. Springer-Verlag, Berlin Heidelberg New York, 2019.
- [18] Passwort gegen Brute-Force-Angriff. <https://www.mahr-edv.de/passwort-gegen-brute-force-angriff>. Letzter Zugriff: 09.04.2021.
- [19] Have I Been Pwned. <https://haveibeenpwned.com>. Letzter Zugriff: 09.04.2021.
- [20] Hackerangriff auf Trinkwasser: Immer gleiches Passwort, Windows 7 und Teamviewer. <https://www.heise.de/news/Hackerangriff-auf-Trinkwasser-Nur-ein-Passwort-Windows-7-und-Teamviewer-5053320.html>. Letzter Zugriff: 11.04.2021.
- [21] LDAP und OpenLDAP - Installation und Betrieb unter Linux. <https://www.minux.de/fileadmin/mediapool/pdf/ldap.pdf>. Letzter Zugriff: 16.03.2021.
- [22] WLAN sichern mit Radius - Individuelle Authentifizierung mit Freeradius unter Linux. <https://www.heise.de/ct/artikel/WLAN-sichern-mit-Radius-1075339.html>. Letzter Zugriff: 16.03.2021.
- [23] Erweiterte Zugangskontrolle fürs LAN - Schlüsselgewalt. <https://www.heise.de/select/ix/2018/5/1524882983171288>. Letzter Zugriff: 06.04.2021.
- [24] Patrick-Benjamin Bök, Andreas Noack, Marcel Müller, and Daniel Behnke. *Computernetze und Internet of Things - Technische Grundlagen und Spezialwissen*. Springer Fachmedien Wiesbaden, Wiesbaden, 2020.
- [25] Private Auskunft - DNS mit Privacy und Security vor dem Durchbruch. <https://www.heise.de/select/ct/2018/14/1530492966691096>. Letzter Zugriff: 01.04.2021.
- [26] WLAN-Sicherheit: Eine Liste mit Angriffstechniken auf 802.11 und 802.1X. <https://www.computerweekly.com/de/ratgeber/WLAN-Sicherheit-Eine-Liste-mit-Angriffstechniken-auf-80211-und-8021X>. Letzter Zugriff: 30.03.2021.
- [27] Wer vertraut dem Blauzahn? https://www.syss.de/fileadmin/dokumente/Publikationen/2018/P6200082_HBJ-Cybersecurity_11-2018_10.pdf. Letzter Zugriff: 29.03.2021.

- [28] Das stille Ende einer Revolution. <https://www.computerworld.ch/technik/telekommunikation/stille-ende-revolution-2609312.html>. Letzter Zugriff: 25.03.2021.
- [29] 2G/GSM-Abschaltung: Das sagen Telekom, Vodafone & O2. <https://www.pcwelt.de/news/2G-GSM-Abschaltung-Das-sagen-Telekom-Vodafone-02-10935096.html>. Letzter Zugriff: 25.03.2021.
- [30] A Practical-Time Attack on the A5/3 Cryptosystem Used in Third Generation GSM Telephony. <https://eprint.iacr.org/2010/013>. Letzter Zugriff: 26.03.2021.
- [31] Sicherheitslücke im Mobilfunk: UMTS-Verschlüsselung mittels SS7 umgangen. <https://www.heise.de/security/meldung/Sicherheitsluecke-im-Mobilfunk-UMTS-Verschlueselung-mittels-SS7-umgangen-2503376.html>. Letzter Zugriff: 26.03.2021.
- [32] Andriy Luntovskyy and Dietbert Gütter. *Moderne Rechnernetze - Protokolle, Standards und Apps in kombinierten drahtgebundenen, mobilen und drahtlosen Netzwerken*. Springer-Verlag, Berlin Heidelberg New York, 2020.
- [33] Call Me Maybe: Eavesdropping Encrypted LTE Calls With REVOLTE. https://revolte-attack.net/media/revolte_camera_ready.pdf. Letzter Zugriff: 26.03.2021.
- [34] Black Hat 2019: 5G Security Flaw Allows MiTM, Targeted Attacks. <https://threatpost.com/5g-security-flaw-mitm-targeted-attacks/147073/>. Letzter Zugriff: 26.03.2021.
- [35] Sicherheitslücke in 3G und 4G auch noch in 5G vorhanden. <https://www.funke.de/markt-trends/sicherheitsluecke-in-3g-und-4g-auch-noch-in-5g-vorhanden.162471.html>. Letzter Zugriff: 26.03.2021.
- [36] SMS-Hijacking: Zweifaktor-Schutz trivial ausgehebelt. <https://www.heise.de/news/SMS-Hijacking-Zweifaktor-Schutz-trivial-ausgehebelt-5994414.html>. Letzter Zugriff: 23.03.2021.
- [37] How Twitter CEO Jack Dorsey's Account Was Hacked. <https://www.wired.com/story/jack-dorsey-twitter-hacked/>. Letzter Zugriff: 23.03.2021.
- [38] Cloning 3G/4G SIM Cards with a PC and an Oscilloscope: Lessons Learned in Physical Security. <https://www.blackhat.com/us-15/briefings.html#cloning-3g-4g-sim-cards-with-a-pc-and-an-oscilloscope-lessons-learned-in-physical-security>. Letzter Zugriff: 23.03.2021.
- [39] Spätestens Desktop hohe Leistung 5G 4G 3G WiFi 2.4G WIFI GPS DCS PCS lojack Signal störsender. <https://www.jammer-shop.com/de/der-neueste-5G-desktop-signal-storsender.html>. Letzter Zugriff: 25.03.2021.
- [40] Was ist OpenDaylight? <https://www.ip-insider.de/was-ist-opendaylight-a-605887/>. Letzter Zugriff: 18.03.2021.

-
- [41] LITHIUM OVERVIEW. <https://www.opendaylight.org/what-we-do/current-release/lithium>. Letzter Zugriff: 11.04.2021.
- [42] LF Networking Launches Anuket, an Open Source Project to Accelerate Infrastructure Compliance, Interoperability and 5G Deployments. <https://www.lfnetworking.org/announcement/2021/01/27/lf-networking-launches-anuket-an-open-source-project-to-accelerate-infrastructure-compliance-interoperability>. Letzter Zugriff: 16.03.2021.
- [43] Generic Routing Encapsulation (GRE). <https://whatis.techtarget.com/de/definition/Generic-Routing-Encapsulation-GRE>. Letzter Zugriff: 18.03.2021.
- [44] Was ist OpenFlow? <https://www.ip-insider.de/was-ist-openflow-a-605856/>. Letzter Zugriff: 18.03.2021.

Stichwörter

- 2FA, 90
- 2G, 132
- 3G, 133
- 4G, 134
- 5G, 135
- 802.11, 119

- Address Resolution Protocol, 28
- AES, 44
- Angreifertypen, 50
 - Cracker, 50
 - Cyber-Terrorismus, 51
 - Hacker, 50
 - Kriminelle, 51
 - Mitarbeiter, 51
 - Skriptkiddie, 50
 - Wirtschaftsspione, 50
- Angriffsarten, 51
 - aktive Angriffe, 51
 - externe Angriffe, 51
 - interne Angriffe, 51
 - passive Angriffe, 51
- Anwendungsschicht, 35
- Application Layer, 35
- ARP, 28
 - Cache-Flooding, 104
 - Filter, 105
 - Spoofing, 103
- Authentifikation, 82
- Authentifizierung, 84
- Authentisierung, 82
- Authentizität, 52

- Bedrohung, 50
- Biometrie, 85
- Bluetooth, 128
 - MitM-Angriff, 131
 - Schlüsselextraktion, 131
 - Tracking, 130
- Bridge, 18
- Broadcast, 22

- Brute-Force, 86
- BSI, 49

- Certification Authority, 47
- Client, 13
- Client-Server-Modell, 14

- DDoS, 65
 - DDoS, 65
- Defense-in-Depth, 59
- DES, 43
- Detaillierter Scan, 62
- DHCP, 114
 - DHCP-Snooping, 116
 - Rogue-Server, 115
 - Starvation Attack, 115
- DHCP Starvation Attack, 115
- Diameter, 95
- Dienst, 13
- Diffie-Hellman, 46
- Distributed Logical Router, 147
- DMZ, 71
- DNS, 36, 114
 - Amplification Attacks, 114
 - Cache Poisoning, 114
 - DNS over HTTPS, 116
 - DNS over Quic, 116
 - DNS over TLS, 115
 - DNSSEC, 115
- DNS Amplification Attacks, 114
- DNS Cache Poisoning, 114
- Domain, 35
- Domain Name System, 36
- DoS, 64

- Ethernet, 26

- Firewall, 72
- Floating IP, 147

- GAN, 21
- Generic Routing Encapsulation, 149

- GPRS, 132
- GRE, 149
- GSM, 132

- Hacking Hardware, 66
 - Lan Tap Pro, 66
 - Packet Squirrel, 67
 - Störsender, 69
 - WiFi Deauther, 68
 - WiFi Pineapple, 68
- Hash, 38
 - Einwegfunktion, 39
 - Kollision, 39
- HMAC, 42
- Honeynet, 74
- Honeypot, 74
- hping3, 65
- Hub, 17

- ICMP, 31
 - Ping of Death, 108
 - Smurf-Angriff, 108
- IDS, 74
- IEEE 802.1AE, 106
- IEEE 802.1X, 106
- IMSI-Catcher, 139
- Integrität, 52
- Internet Control Message Protocol, 31
- Internet Layer, 30
- Internet Protocol, 30
- Internet Service Providern, 19
- Internetknoten, 19
- Internetschicht, 30
- IP, 30
 - IPv4, 30
 - IPv6, 31
- IP-Adresse Version 6, 31
- IPS, 74
- IPSec, 109
- IT-Grundschutz, 49, 56

- Kerberos, 96

- LAN, 20
- LDAP, 93

- LDAPS, 94
- Link Layer, 25
- LTE, 134

- MAC, 27
- MAC-Spoofing, 102
- MACsec, 106
- MAN, 21
- Man-in-the-Middle, 63
- MD5, 40
- Media-Access-Control-Adresse, 27
- Message Authentication Code, 42
- MFA, 90
- Mobilfunk, 132
- Modem, 18
- Multi-Faktor Authentifizierung, 90
- Multicast, 22

- Netzbetreiber, 19
- Netztopologieplan, 57
- Netzwerk Virtualisierung, 144
- Netzwerkplan, 57
- Netzzugangsschicht, 25
- NFV, 146
- NMAP, 61

- OpenDaylight, 145
- OpenFlow, 150
- OpenVPN, 110
- OPNFV, 147
- Overlay-Netz, 147

- PAN, 20
- Passwort, 84
- Penetrationstest, 58
- Point-to-Point Protocol, 29
- Ports, 33
- PPP, 29
- Protokoll, 13
- Proxy, 72

- RADIUS, 95
- Recognition, 61
- RFC, 12
- RIPEMD, 41
- Risiko, 50

- Risikoanalyse, 58
- Rogue-DHCP-Server, 115
- Router, 18
- RSA, 45
- Scan, 61
 - ICMP-Echo-Ping, 62
 - Null-Scan, 62
 - TCP-SYN-Scan, 62
- Schichtenmodelle, 22
 - ISO/OSI, 24
 - TCP/IP, 24
- Schlüsselaustausch, 45
- Schutzziele, 52
- Schwachstelle, 50
- SDN, 144
- Server, 13
- SHA, 40
- Sicherheitskonzept, 56
- Signatur, 47
- SIM, 137
- SIM-Swapping, 137
- SMS, 136
- Sniffing, 102
- Software-Defined Networking, 144
- Splitter, 18
- Spoofing, 63
 - ARP-Spoofing, 64
 - DNS-Spoofing, 64
 - IP-Spoofing, 64
- SS7, 138
- SSID, 120
- SSL, 116
- Switch, 18
- TCP, 32, 113
 - Desynchronisation, 112
 - Hijacking-Angriff, 112
 - Reset-Attacken, 112
 - Spoofing, 112
 - SYN-Cookies, 113
- Teardrop Attack, 107
- TLS, 34, 116
- Topologie, 14
 - Bus-Topologie, 15
 - Punkt-zu-Punkt-Topologie, 16
 - Ring-Topologie, 14
 - Stern-Topologie, 15
- Transmission Control Protocol, 32
- Transport Layer, 31
- Transport Layer Security, 34
- Transportschicht, 31
- Trust Center, 47
- UDP, 33
- UMTS, 133
- Underlay-Netz, 147
- Unicast, 22
- Uniform Resource Identifier, 36
- Uniform Resource Locator, 36
- URI, 36
- URL, 36
- User Datagram Protocol, 33
- Verbindlichkeit, 52
- Verfügbarkeit, 52
- Verschlüsselung, 43
 - asymmetrisch, 44
 - symmetrisch, 43
- Vertraulichkeit, 52
- Verzeichnisbaum, 93
- Verzeichnisdienst, 93
- Virtual Local Area Network, 149
- VLAN, 149
- VPN, 73
- VXLAN, 149
- WAN, 21
- War Driving, 123
- WEP, 122
- WireGuard, 110
- WLAN, 26, 119
 - Probe Requests, 123
 - SSID, 120
 - War Driving, 123
- WPA, 122
- WPA2, 122
- WPA3, 122
- ZenMAP, 61

Zero Trust, [59](#)

Zertifikat, [47](#)

Zugangskarte, [84](#)

Zurechenbarkeit, [52](#)

Zwei-Faktor-Authentisierung, [90](#)

Glossar

2FA	Zwei-Faktor-Authentisierung
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
BSI	Bundesamt für Sicherheit in der Informationstechnik
CIX	Commercial Internet eXchange
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DLR	Distributed Logical Router
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial-of-Service
EIAM	Enterprise Identity and Access Management
GAN	Globe Area Network
GRE	Generic Routing Encapsulation
GSM	Global System for Mobile Communication
HMAC	Hash-based Message Authentication Code
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPS	Intrusion Prevention System
ISP	Internet Service Provider
IXP	Internet Exchange Point
LAN	Local Area Network
LDAP	Light weight Directory Access Protocol
LTE	Long Term Evolution
MAC	Media-Access-Control
MAC	Message Authentication Code

MAN	Metropolitan Area Network
MFA	Multi-Faktor-Authentifizierung
MitM	Man-in-the-Middle-Angriff
NFV	Network Function Virtualization
NIC	Network Interface Card
NV	Netzwerk Virtualisierung
PAN	Personal Area Network
PKI	Public-Key-Infrastruktur
PPP	Point-to-Point Protocol
QUIC	Quick UDP Internet Connections
RFC	Requests For Comment
SDN	Software-Defined Networking
SIM	Subscriber Identity Module
SMS	Short Message Service
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UMTS	Universal Mobile Telecommunication System
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VXLAN	Virtual eXtensible LAN
VPN	Virtual Private Network
WAN	Wide Area Network
WLAN	Wireless Local Area Network

Z301 Grundlagen der Netzsicherheit

Die Lehrveranstaltung „Grundlagen der Netzsicherheit“ gibt Ihnen einen Überblick über die eingesetzten Technologien von Rechnernetzen und zeigt die wichtigsten Merkmale und Eigenschaften von klassischen und modernen Datennetzen. Es werden die wichtigsten Sicherheitsprotokolle, die häufigsten Angriffe auf Netzwerke und die entsprechenden Verteidigungsmaßnahmen erläutert. Sie lernen die Funktionsweise und Sicherheitsarchitektur der drahtlosen Netzwerke WLAN, Bluetooth und Mobilfunk kennen. In Übungen im virtuellen Labor führen Sie selbst Angriffe durch, um im Anschluss Bedrohungsszenarien nachvollziehen und einordnen zu können.

Im ersten Studienbrief „Einführung“ werden Grundlagen in den Bereichen Rechnernetze, Kryptografie und IT-Sicherheit behandelt, um vorhandenes Wissen zu reaktivieren und einen gemeinsamen Ausgangspunkt für dieses Modul zu schaffen.

Im zweiten Studienbrief „Sicherheit von Rechnernetzen“ erlernen Sie generelle Sicherheitskonzepte für Netzwerke. Anhand von realitätsnahen Angriffsszenarien und relevanten Verteidigungsmaßnahmen werden Sicherheitseigenschaften von Netzwerktechnologien praxisorientiert vorgestellt.

Im dritten Studienbrief „Zugriffsmanagement“ wird ein Überblick über das Thema Zugriffssteuerung gegeben. Außerdem werden verschiedene Protokolle und Systeme behandelt, die einen wirksamen Schutz ermöglichen.

Im vierten Studienbrief „Klassische Netzwerke“ wird die Architektur der LAN/WAN-Netze anhand des Schichtenmodells vorgestellt. Darüber hinaus wird dargelegt, welche Angriffsarten auf welcher Ebene möglich sind. Zusätzlich werden die verbreitetsten Angriffsarten auf WLAN-Netzwerke behandelt und erläutert, welche Gegenmaßnahmen hier existieren. Anhand des Bluetooth Protokolls wird ein alternatives Funknetzwerk beschrieben. Außerdem gibt es einen Ausblick auf die verwendeten Sicherheitskonzepte der Mobilfunknetze und deren Weiterentwicklung.

Im letzten Studienbrief „Moderne Netzwerke“ wird ein Ausblick auf flexible und softwaregesteuerte Netzwerktechniken gegeben. Anhand von verschiedenen Konzepten und Protokollen werden die Grundlagen erklärt und der konkrete Einsatz mit Beispielen erläutert.

Nach erfolgreichem Abschluss des Moduls haben Sie Kenntnisse über die wichtigsten Merkmale und Eigenschaften von klassischen und modernen Netzwerken und können die verwendeten Sicherheitskonzepte einordnen. Des Weiteren können Sie die Funktionsweise und Sicherheitseigenschaften von klassischen und modernen Netzwerktechnologien exemplarisch anwenden.

Zertifikatsprogramm

Die Zertifikatsmodule auf wissenschaftlichem Niveau und mit hohem Praxisbezug bilden ein passgenaues Angebot an Qualifikation und Spezialisierung in der nebenberuflichen Weiterbildung. Damit können einzelne Module nebenberuflich studiert werden. Durch die Vergabe von ECTS-Punkten können sie auf ein Studium angerechnet werden.

<http://zertifikatsprogramm.de>