Zertifikatsprogramm - Z301

Grundlagen der Netzsicherheit

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

Tobias Scheible, M.Eng.

Open C³S
Open Competence Center for Cyber Security

Hochschule
Albstadt-Sigmaringen
Albstadt-Sigmaringen University

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

Hochschule Albstadt-Sigmaringen
Zertifikatsprogramm
Poststraße 6
72458 Albstadt

Version 1.0.0

1. Auflage (2021-04-14)

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

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*

Profil | Blog | Twitter | Linkedin | Xing

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

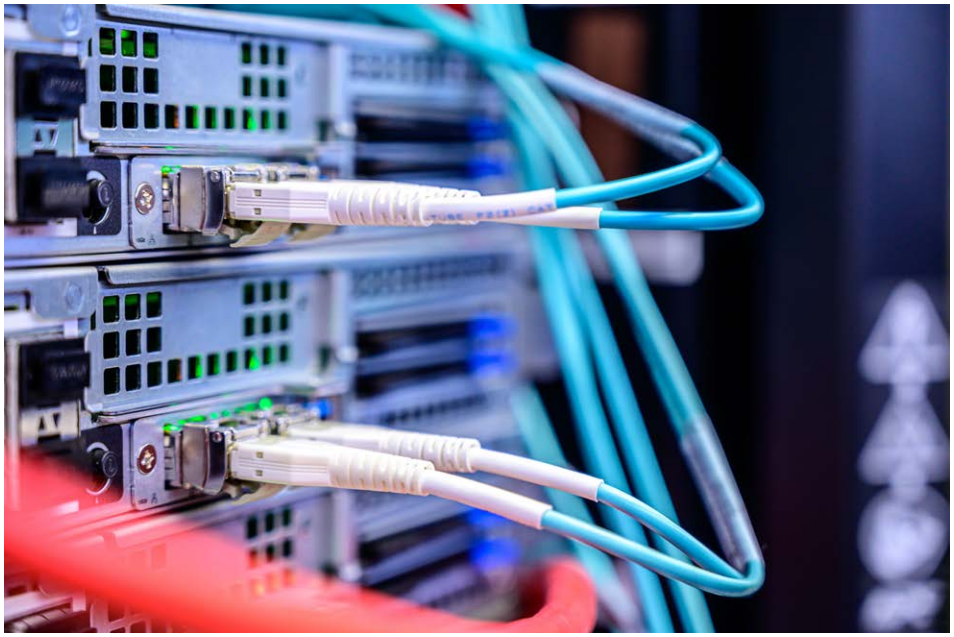
Zusätzlich kann noch die folgende Online-Quelle zur Unterstützung genutzt werden:

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

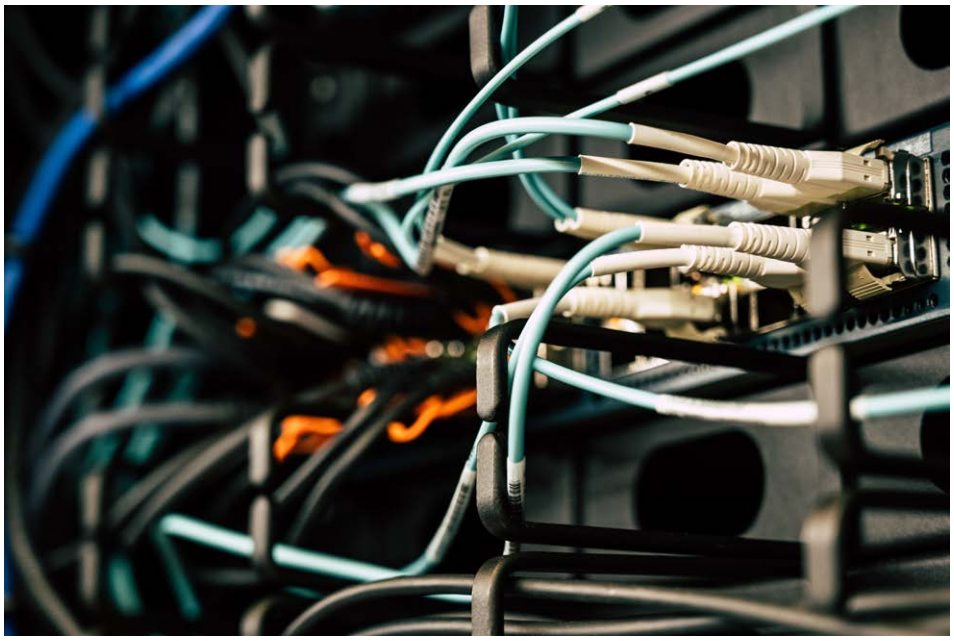
4.1 Lernergebnisse

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

II. Beispiele

III. Definitionen

IV. Exkurse

V. Kontrollaufgaben

VI. Tabellen

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-Grundschutz-Bausteine. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/IT-Grundschutz-Bausteine/Bausteine_Download_Edition_node.html. Letzter Zugriff: 16.02.2021.

[12] Bundesamt für Sicherheit in der Informationstechnik (BSI). BSI-Standard 100-2 - IT-Grundschutz-Vorgehensweise. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/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.mindux.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-O2-10935096.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-Verschluesselung-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.funkschau.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 WiFi2.4G 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-interoper 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

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 vorhandenesWissen 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