



Dirk Westhoff

Mobile Security

Schwachstellen verstehen
und Angriffsszenarien nachvollziehen

EBOOK INSIDE

 Springer Vieweg



Mobile Security

Dirk Westhoff

Mobile Security

Schwachstellen verstehen und
Angriffsszenarien nachvollziehen

Dirk Westhoff
Offenburg, Baden-Württemberg, Deutschland

ISBN 978-3-662-60854-8 ISBN 978-3-662-60855-5 (eBook)
<https://doi.org/10.1007/978-3-662-60855-5>

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

© Springer-Verlag GmbH Deutschland, ein Teil von Springer Nature 2020

Das Werk einschließlich aller seiner Teile ist urheberrechtlich geschützt. Jede Verwertung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen Zustimmung des Verlags. Das gilt insbesondere für Vervielfältigungen, Bearbeitungen, Übersetzungen, Mikroverfilmungen und die Einspeicherung und Verarbeitung in elektronischen Systemen.

Die Wiedergabe von allgemein beschreibenden Bezeichnungen, Marken, Unternehmensnamen etc. in diesem Werk bedeutet nicht, dass diese frei durch jedermann benutzt werden dürfen. Die Berechtigung zur Benutzung unterliegt, auch ohne gesonderten Hinweis hierzu, den Regeln des Markenrechts. Die Rechte des jeweiligen Zeicheninhabers sind zu beachten.

Der Verlag, die Autoren und die Herausgeber gehen davon aus, dass die Angaben und Informationen in diesem Werk zum Zeitpunkt der Veröffentlichung vollständig und korrekt sind. Weder der Verlag, noch die Autoren oder die Herausgeber übernehmen, ausdrücklich oder implizit, Gewähr für den Inhalt des Werkes, etwaige Fehler oder Äußerungen. Der Verlag bleibt im Hinblick auf geografische Zuordnungen und Gebietsbezeichnungen in veröffentlichten Karten und Institutionsadressen neutral.

Planung/Lektorat: Martin Börger

Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.

Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Man sieht nur, was man weiß.
Johann Wolfgang von Goethe

Für Charlotte, Johanna und Jutta

Vorwort

Es sind schon eine ganze Reihe Bücher zum Thema mobile und drahtlose Sicherheit verfasst worden [1–5], sodass man sich mit Recht fragen kann, inwieweit ein weiteres Buch zu diesem Thema sinnvoll erscheint. Die Anregung hierzu liefert der Begriff „*Selected Areas of...*“. Bei der Erstellung der Mastervorlesung „Mobile Security“ im Studiengang Enterprise- and IT-Security (ENITS) an der Hochschule Offenburg hat sich gezeigt, dass dieses Feld (bis zum Jahre 2019) so mannigfaltig angewachsen ist, dass es sich in dem Format einer ‚Zwei-plus-zwei‘-Veranstaltung innerhalb eines Semesters nicht annähernd abdecken lässt. Allerdings sollte ein Fachbuch aus meiner Sicht auch nicht deutlich umfangreicher sein, um die Leserschaft nicht schon aufgrund der schierer Seitenzahl abzuschrecken. So möchte ich mich, auch wenn der Themenbereich Mobile Security sicherlich einige Anknüpfungspunkte an das Thema *Social-Engineering-Angriffe* bietet, darauf beschränken, hierzu auf [6] hinzuweisen. Ähnliches gilt für den technischen Datenschutz, oder *privacy-by-design*. Auch wenn dieses Thema zum Ende des Buches angeschnitten wird so möchte ich für ein tieferes Studium auf [7] verweisen.

Die rasante Entwicklung digitaler Technologien wird offenkundig, wenn man sich zwei inzwischen berühmte Zitate vergegenwärtigt: So behauptete Thomas John Watson, Vorstandsvorsitzender bei IBM, im Jahre 1943: „*Ich glaube, dass es wohl weltweit einen Markt für vielleicht fünf Computer gibt.*“. Ein wenig weitsichtiger formuliert hat es Mark Weiser, Chef-Entwickler bei Rank Xerox, Palo Alto Research Center, USA, mit seinem 1991 geäußerten Begriff des „*Ubiquitous Computing*“. Dieser ein halbes Jahrhundert nach Watson geformte Begriff des allgegenwärtigen Rechnens kumulierte eine ganze Reihe technologischer Entwicklungen. Er prognostizierte quasi implizit die Säulen der modernen IT: die Möglichkeit der Massenfertigung durch die Chipindustrie, massiv erweiterte Adressräume, deutlich kleinere Formfaktoren der Geräte, tragbare digitale sowie eingebettete digitale Geräte, die mehrheitlich drahtlos kommunizieren. Nun, die Prognose Mark Weisers hat sich in schon fast verstörender Weise bewahrheitet und die Zukunft dürfte aller Voraussicht nach wohl noch „*ubiquitärer*“ werden. Wer dabei einordnen möchte, welche Autonomieverschiebungen durch Informations- und Kommunikationstechnologie derartige Entwicklungen der Gesellschaft abverlangen, der sei beispielsweise auf [8] verwiesen.

Das Anliegen dieses Buches ist es nunmehr, durch eine gezielte Auswahl einzelner Schwerpunkte dem Leser einen soliden Einblick in Fragestellungen rund um die IT-Sicherheit mobiler drahtloser digitaler Consumer-Geräte zu geben und ihm die dahinterliegenden Architekturen respektive deren Angreifbarkeit zu vermitteln. Dabei sollen uns nicht nur Fragen der Verwundbarkeit einzelner Technikkomponenten interessieren, sondern oftmals auch Aspekte der Privatheit der Nutzer solcher Systeme.

Offenburg, Deutschland
Dezember 2019

Prof. Dr. Dirk Westhoff

Literatur

1. Buttyan, L., Hubaux, J.P.: Security and Cooperation in Wireless Networks – Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing. Cambridge University Press, Cambridge (2007)
2. Chen, Y., Xu, W., Trappe, W., Zheng, Y.: Securing Emerging Wireless Systems – Lower-Layer Approaches. Springer, New York (2009)
3. Osterhage, W.: Sicher & Mobil: Sicherheit in der drahtlosen Kommunikation. Springer, Heidelberg (2010)
4. Spreitzenbarth, M.: Mobile Hacking. dpunkt, Heidelberg (2017)
5. Stajano, F.: Security for Ubiquitous Computing. Wiley, Chichester (2002)
6. Drechsler, D. (Hrsg.): Schutz vor Social Engineering – Angriffspunkte und Abwehrmöglichkeiten in digitalwirtschaftlichen Ökosystemen. Schmidt, Berlin (2019)
7. Petrlc, R., Sorge, C.: Datenschutz – Einführung in technischen Datenschutz, Datenschutzrecht und angewandte Kryptographie. Springer Vieweg, Wiesbaden (2017)
8. Westhoff, D.: Gedanken zu Autonomieverschiebungen durch Informations- und Kommunikationstechnologie. In: Breyer-Mayländer, T. (Hrsg.) Das Streben nach Autonomie – Reflexionen zum Digitalen Wandel, S. 67–79. Nomos, Baden-Baden (2018)

Inhaltsverzeichnis

1	Einführung	1
1.1	Was nicht Gegenstand dieses Buches ist	2
1.2	Was die Themen dieses Buches sind	4
1.3	Danksagung	6
1.4	Noch eine Bemerkung in eigener Sache	6
	Literatur	7
Teil I Grundlagen		
2	Wissenswertes zu Netzen, sowie mathematische und kryptografische Hintergründe	11
2.1	Anmerkungen zur Notation	11
2.2	Wissenswertes zu Netzen und Protokollen	13
2.2.1	Protokolle	13
2.2.2	Aus der Praxis	16
2.2.3	Zwei-Armeen-Problem	18
2.3	Ausgewählte zahlentheoretische Aspekte	19
2.3.1	Kongruenz	19
2.3.2	Ganzzahliger Ring	20
2.3.3	Chinesischer Restsatz	20
2.4	Elementare kryptografische Bausteine	21
2.4.1	XOR	21
2.4.2	Hashfunktionen	24
2.4.3	Message Authentication Codes	27
2.4.4	Digitale Signaturen	29
2.4.5	Verschlüsselung	32
2.4.6	Schlüsselübereinkunft	35

2.4.7	Zertifikate	37
2.4.8	Bloom-Filter	38
2.4.9	Zusammenfassung	39
	Literatur	40

Teil II Verwundbarkeiten drahtloser Kommunikationssysteme

3	Verwundbarkeiten in drahtlosen lokalen Netzen	43
3.1	Grundsätzliche Bemerkungen zur Funktionsweise der Sicherungsschicht	43
3.2	Verwundbarkeit von IEEE 802.15.4	45
3.3	Maßnahmen gegen einen Paket-in-Paket-Injizier-Angriff	50
3.3.1	Byte-Stuffing	50
3.3.2	Verwendung der in IEEE 802.15.4 vorgesehenen AES-Varianten	51
3.4	Anmerkungen zur Analyse proprietärer Protokolle	52
3.5	Verwundbarkeiten von WLAN	53
3.5.1	Designschwächen von WEP	53
3.5.2	WiFi Protected Access und IEEE 802.11i	59
3.5.3	Designschwächen von WPA und WPA2	66
3.5.4	WPA3	75
3.6	Zusammenfassung	78
	Literatur	80
4	Verwundbarkeiten in Personal Area Networks	81
4.1	Bluetooth	81
4.1.1	Pairing-Modi und Pairing-Phasen	82
4.2	LE Privacy	86
4.3	Blueborne	88
4.3.1	Entfernte Codeausführung	88
4.3.2	Ein einfacher Man-in-the-Middle-Angriff	91
4.4	Ungültige Kurvenpunkte und geänderte Punktkoordinaten	93
4.4.1	Einleitende Bemerkungen	93
4.4.2	Varianten der Diffie-Hellman-Schlüsselübereinkunft	94
4.4.3	Angriffe über ungültige Kurven	98
4.4.4	Anmerkungen zu Seitenkanalangriffen auf ECC und ECDH	107
4.5	Das „blutende“ Bit	110
4.6	Praktische Auswirkungen	113
4.7	Near Field Communication	114
4.7.1	Einleitende Bemerkungen	114
4.7.2	Authentifizierung zwischen Lesegerät und Tag	116
4.7.3	Ausgewählte Angriffe auf ältere Tags	117

4.7.4	Erhöhte Sicherheit mit neueren Tag-Modellen	126
4.7.5	Authentifizierung bei Mifare DESFire EV1	128
4.7.6	Aus der Praxis	128
4.8	Zusammenfassung	129
	Literatur	132
5	Verwundbarkeiten innerhalb der Mobiltelefonie	135
5.1	Verwundbarkeit von DECT	135
5.1.1	Einleitende Bemerkungen zur Verwundbarkeit von DECT	135
5.1.2	Das DECT-Protokoll und seine Übertragungstechnologie	137
5.1.3	DECT-Authentifizierung DSAA und Verschlüsselung DSC	138
5.1.4	Interaktive DECT-Entschlüsselung	140
5.1.5	War da nicht was?	142
5.1.6	DECT-Verschlüsselung mit AES	142
5.2	Verwundbarkeit über das Baseband-Modem	142
5.3	5G-Sicherheitsarchitektur	144
5.3.1	Einleitung und Anwendungsfelder	145
5.3.2	Netzwerk-Virtualisierung und Netzwerk-Slicing	146
5.3.3	Konzepte zur Erhöhung der Sicherheit	146
5.3.4	Authentifizierung und Schlüsselübereinkunft	148
5.3.5	Verschlüsselung und Integritätsprüfung	150
5.3.6	Beispielhafte konkrete Angriffsszenarien	151
5.4	Zusammenfassung	154
	Literatur	155
6	Klassifizierung und Risikoabschätzung	157
6.1	Was haben wir gelernt?	157
6.2	Risikoabschätzung	159
 Teil III Softwarekomponenten mobiler digitaler Geräte		
7	Das Betriebssystem Android	167
7.1	Die Android-Systemarchitektur	167
7.1.1	Grundlagen zur Systemarchitektur	167
7.1.2	Der Bootvorgang, ART und Zygote	169
7.1.3	Abgesichertes Hochfahren	171
7.2	Aufbau einer Android-App	171
7.2.1	Aufbau und Komponenten	171
7.2.2	Mögliche Kommunikationswege zwischen Android-Applikationen	173

7.3	Signaturen und Zertifikate unter Android	175
7.3.1	Digitales Signieren von Android-Apps	175
7.3.2	Zertifikate unter Android	176
7.4	Das Rechemodell von Android	177
7.4.1	Zusammenwirken von Android mit SELinux	179
7.4.2	Android Keystore	181
7.5	Rechteausweitung unter Android	182
7.5.1	Ansätze zur Abschwächung horizontaler Rechteausweitung	183
7.6	Android und NFC	187
7.7	Zusammenfassung	188
	Literatur	190
8	Umsetzung sicherheitskritischer Anwendungen	191
8.1	Mobile Banking-Verfahren mittels App	191
8.1.1	Richtlinie über Zahlungsdienstleistungen	191
8.1.2	SMS-TAN und push-TAN	192
8.1.3	Sicherheitsvorgaben für TAN-Apps	194
8.2	Zusammenfassung	201
	Literatur	202
9	Techniken des Zertifikats-Pinning	203
9.1	Techniken des Zertifikats-Pinning und deren Umgehung	203
9.1.1	Varianten der Implementierung von Zertifikats-Pinning	203
9.1.2	Zertifikatsarten	204
9.1.3	Aufbrechen von Zertifikats-Pinning ohne Obfuskierung	205
9.1.4	Aufbrechen von Zertifikats-Pinning mit Obfuskierung	206
9.1.5	Maßnahmen gegen das Aufbrechen von Zertifikats-Pinning	207
9.2	Zusammenfassung	208
	Literatur	210
10	Obfuskierung und Deobfuskierung	211
10.1	Techniken zur Obfuskierung und Deobfuskierung von Apps	211
10.1.1	Techniken zur Deobfuskierung	212
10.1.2	Einfache Techniken der Bytecode-Obfuskierung	216
10.2	Zusammenfassung	219
	Literatur	221

11 QR-Codes, Web-Apps und der Air-Gap	223
11.1 QR-Codes und Web-Apps	223
11.2 Überwinden des Air-Gap	225
11.3 Zusammenfassung	228
Literatur.	229
12 Positionsbestimmung und Standortverfolgung	231
12.1 Verfahren zur Positionsbestimmung und Standortverfolgung	232
12.1.1 Positionsbestimmung und Standortverfolgung mittels aktiven WLAN-Scanning	232
12.1.2 Positionsbestimmung und Standortverfolgung mittels Swarm-Mapping.	234
12.1.3 Positionsbestimmung und Standortverfolgung durch Swarm-Mapping+	237
12.1.4 Auswirkungen von Swarm-Mapping+	241
12.1.5 Gegenüberstellung der Verfahren zur Positionsbestimmung	242
12.1.6 Auskunftsansprüche und datenschutzrechtliche Erwägungen	243
12.1.7 Auskunftsansprüche mit technischem Datenschutz	245
12.2 Zusammenfassung	249
Literatur.	251
 Teil IV Fazit und Ausblick	
13 Nicht technische Ursachenforschung	255
14 Ausblick mit Blick auf den Leser	261

Abkürzungsverzeichnis

ACK	Acknowledgment
ACM	Association for Computing Machinery
AES	Advanced Encryption Standard
AMI	Advanced Metering Infrastructure
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSSID	Basic Service Set Identifier
CBC	Cipher block chaining
CCM	Counter with CBC-MAC
CCMP	Counter-Mode/CBC-MAC Protocol
CPS	Cipher-physisches System
CRC	Cyclic Redundancy Check
CRL	Certificate Revocation List
CSS	Cascading Style Sheets
CTR	Counter mode
DAC	Discretionary Access Control
DES	Data Encryption Standard
DLP	Discrete Logarithm Problem
DoS	Denial of Service
DSGVO	Datenschutz-Grundverordnung
EAPOL	Extensible Authentication Protocol over Local Area Network
ENITS	Enterprise and IT-Security
ETSI	Europäisches Institut für Telekommunikationsnorme
FFT	Fast Fourier-Transformation
GCHQ	Government Communications Headquarters
GCMP	Galois/Counter Mode
GPS	Global positioning system

HKPK	HTTP Public Key Pinning
HTML	Hypertext Markup Language
HTTPS	Hypertext Transfer Protocol Secure
ICV	Integrity Check Value
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IPC	Inter Process Communication
IV	Initialisierungsvektor
LBS	Location based service
LFSR	linear feedback shift register
MAC	Mandatory Access Control
MAC	medium access control
MIC	message integrity code
MitM	Man in the middle
NFC	near field communication
NIC	network Interface card
NIDS	network intrusion detection system
NIPS	network intrusion prevention
NIST	National Institute of Standards and Technologies
Nonce	number used only once
OMA	Open mobile alliance
OWASP	Open Web Application Security Project
PAN	Personal Area Network
PHY	Physical Layer
PIN	Persönliche Identifikationsnummer
PKI	Public Key Infrastructure
PMK	Pairwise Master Key
PRNG	Pseudorandom Number Generator
RFC	Request for Comments
RPC	Remote Procedure Call
RSSI	Received Signal Strength Indication
SCADA	Supervisory Control and Data Acquisition
SE	Secure Element
SSID	Service Set Identifier
TEE	Trusted Execution Environment
TKG	Telekommunikationsgesetz
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
ToFU	Trust-on-first-use
TRNG	True Random Number Generator

WLAN	Wireless Local Area Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
USB	Universal Serial Bus

Abbildungsverzeichnis

Abb. 2.1	Notation einer Kommunikation mit passivem Angreifer (E)ve.	12
Abb. 2.2	Notation einer Kommunikation mit aktivem Angreifer (M)allory	12
Abb. 2.3	Notation einer Kommunikation mit aktivem Angreifer sowie dem zu korrumpierenden Opfergerät	12
Abb. 2.4	Notation einer Kommunikation mit passivem (P)roxy.	13
Abb. 2.5	Einfaches, fiktives Handshake-Protokoll zwischen Client und Server	15
Abb. 2.6	Übertragungsfehler beim Versenden der eigentlichen Nachricht m	18
Abb. 2.7	Übertragungsfehler beim Versenden der Bestätigung $ACK(m)$ zum Erhalt der Nachricht m	18
Abb. 2.8	Beispielhaftes Verschlüsseln und Entschlüsseln mittels XOR (\oplus)	22
Abb. 2.9	Wahrheitstabelle für Modulo-2-Addition und für XOR (\oplus)	23
Abb. 2.10	Charakter einer Einwegfunktion $f : X \rightarrow Y$	25
Abb. 2.11	Aufbau einer Hashfunktion nach Merkle-Damgard-Konstruktion.	27
Abb. 2.12	Verwendung eines MAC zur Überprüfung der Integrität und Authentizität einer Nachricht.	27
Abb. 2.13	Verwendung eines HMAC zur Überprüfung der Integrität und Authentizität einer Nachricht.	28
Abb. 2.14	Verwundbarkeit eines naiven MAC-Konstruktes mit MitM-Mallory	29
Abb. 2.15	Signaturbildung unter Verwendung einer Hashfunktion durch Alice und deren Prüfung durch Bob.	30

Abb. 2.16	Darstellung einer verschlüsselten Kommunikation mittels <i>symmetrischer</i> Verschlüsselung in Gegenwart eines passiven Angreifers (E)ve	33
Abb. 2.17	Darstellung einer verschlüsselten Kommunikation mittels <i>asymmetrischer</i> Verschlüsselung in Gegenwart eines passiven Angreifers (E)ve	34
Abb. 2.18	Abfolge der Diffie-Hellman-Schlüsselübereinkunft	36
Abb. 2.19	Abfolge der Diffie-Hellman-Schlüsselübereinkunft mit MitM-Mallory	36
Abb. II.1	Klassifikation drahtloser Kommunikationssysteme	42
Abb. 3.1	PiP mit Mallory und Opfer	46
Abb. 3.2	Schematische Darstellung der Datenformate der PHY- und der MAC-Schicht für IEEE 802.15.4	47
Abb. 3.3	Beispielhafter IEEE-802.15.4-Rahmen	48
Abb. 3.4	Beispielhafter IEEE-802.15.4-Rahmen mit eingefügten inneren Rahmen	48
Abb. 3.5	32-Bit-Chipfolge des Hex-Wertes 0 laut IEEE 802.15.4	48
Abb. 3.6	2 × 32-Bit-Chipfolgen des a7-Sync-Bereiches eines IEEE-802.15.4-Rahmens	49
Abb. 3.7	PiP-Angriff mit Mallory und Opfer unter Ausnutzung der Fehlerbehebung	50
Abb. 3.8	Schematische Darstellung der WEP-Verschlüsselung und der WEP-Entschlüsselung bei Mitsamt Prüfsummenbildung	54
Abb. 3.9	Sniffen eines Klartext-Krypto-Paares (M_1, C_1) während der Challenge-Response-basierten Authentifizierung des Clients gegenüber dem Access-Point. Das Paar (M_1, C_1) dient der Vorbereitung des Einschleusens gefälschter Nachrichten M_2 an den Client	58
Abb. 3.10	WLAN-ARP-Spoofing eines bereits angemeldeten ‚Insider Mallory‘, um unerkannt Proxy im WLAN-Netzwerk zu werden	61
Abb. 3.11	Vereinfachte Darstellung der Verwendung von AES innerhalb von WPA2 zur gleichzeitigen Verschlüsselung und Authentifizierung	65
Abb. 3.12	Erfolgreiche Abfolge des Vier-Wege-Handshakes zwischen WLAN-Access-Point und Client	68
Abb. 3.13	Zustände und Zustandsübergänge am WLAN-Client in Anlehnung an IEEE 802.11.r	70

Abb. 3.14	Abfolge des KRACK-Angriffs durch Abfangen der vierten Nachricht und clientseitiges unverschlüsseltes Senden der vierten Nachricht; Darstellung hier nur für <i>PTK</i> (und nicht auch für <i>GTK</i>)	74
Abb. 3.15	Darstellung des KRACK-Angriffs mittels Wireshark unter Verwendung der PoC-Implementierung von Mathy Vanhoef für den Fall des unverschlüsselten wiederholten Sendens	75
Abb. 4.1	Bluetooth-Authentifizierung unter Verwendung des Pairing-Modus <i>Numeric Comparison</i>	84
Abb. 4.2	Bluetooth-Authentifizierung unter Verwendung des Pairing-Modus <i>Passkey Entry</i>	84
Abb. 4.3	Verwundbarkeit durch fehlerhafte Verwendung von <code>memcpy()</code>	89
Abb. 4.4	BNEP-Paket, das den Pufferüberlauf beim Empfänger auslöst	89
Abb. 4.5	Allotierter Speicher und tatsächlich benötigter Speicher	90
Abb. 4.6	Just-Works-Implementierung unter Android	92
Abb. 4.7	Grafische Darstellung einer Punktaddition der Punkte P und Q zu $R=P+Q$	96
Abb. 4.8	Grafische Darstellung einer Punktdopplung des Punktes P zu $R=P+P$	96
Abb. 4.9	Abfolge der ECDH-Schlüsselübereinkunft	97
Abb. 4.10	Protokollnachrichten der ECDH-Schlüsselübereinkunft bei Angriff mit ungültigen Kurvenpunkten $Q_i \in E_i$ und $E_i \neq E$	100
Abb. 4.11	Grafische Darstellung eines Punktes $A' = (x_A, 0)$ auf E mit $b' \equiv -x_A^3 - ax_A \pmod{q}$	103
Abb. 4.12	Erfolgsaussichten des Angriffs auf ECDH über geänderte y -Koordinaten in Abhängigkeit von der Beschaffenheit der geheimen Skalare α und β	104
Abb. 4.13	Protokollabfolge der semipassiven-Variante des Angriffs über ‚ungültige Kurven‘. In dem dargestellten Fall ist der Angriff erfolgreich da sowohl das Opfer Alice als auch das Opfer Bob gerade Skalare α_g und β_g verwenden	105
Abb. 4.14	Schlüsselverteilung nach erfolgreichem herkömmlichem MitM- und ‚Ungültige Kurve‘-MitM-Angriff	105
Abb. 4.15	Übertragung der Punktkoordinaten in Bluetooth-Paketen bei ECDH in Abhängigkeit von der zugrundeliegenden Schlüssellänge: links für Schlüssellängen <256 Bit, rechts für Schlüssellängen ≥ 256 Bit	107

Abb. 4.16	Pseudocode zur Berechnung von dP in einer Variante des <i>Double-and-Add</i> -Algorithmus	108
Abb. 4.17	Versuchsaufbau für einen Seitenkanalangriff auf eine Implementierung des <i>Double-and-Add</i> -Algorithmus am IHP in Frankfurt-/Oder in der Arbeitsgruppe von Peter Langendörfer	109
Abb. 4.18	Teilschritte zur Verwundbarkeit mittels eines ‚blutendes‘ Bits auf ein Gerät mit BLE-Chip	113
Abb. 4.19	NFC-A-konforme beidseitige Authentifizierung zwischen NFC-Lesegerät und Tag	116
Abb. 4.20	Known-Plaintext-Angriff unter Ausnutzung des Verhaltens am Tag bei Prüfung der Paritätsbits	119
Abb. 4.21	Beidseitige Authentifizierung zwischen NFC-Lesegerät und Tag unter Einbeziehung eines Proximity-Checks	127
Abb. 4.22	Authentifizierung mit AES beim Tag-Modell Mifare DESFire EV1	129
Abb. 5.1	Authentifizierung des DECT Portable Part (PP) gegenüber dem DECT Fixed Part (FP)	139
Abb. 7.1	Übersicht der Architektur des Android-Betriebssystems	168
Abb. 7.2	Boot-Reihenfolge von Android beim Hochfahren eines mobilen Gerätes	169
Abb. 7.3	Android-Kommunikationswege nach Komponenten	174
Abb. 7.4	Signieren von APK-Archiven unter Verwendung eines selbstsignierten Zertifikates $Cert(ID_{Ent}, k_{pub})$ des Entwicklers	175
Abb. 7.5	Horizontale Rechteausweitung aufgrund von IPC-Nutzung zwischen den Apps SMS-Formatter und Task-Scheduler	184
Abb. 7.6	Varianten der horizontalen Rechteausweitung durch IPC-Nutzung: IPC zwischen bössartiger App und gutartiger App oder konspirative IPC zwischen zwei bössartigen Apps	184
Abb. 7.7	Das Versagen Taint-basierter Ansätze zur Erkennung horizontaler Rechteausweitung bei zeitversetzter asynchroner Kommunikation und Ablage in einer Datenbank	186
Abb. 8.1	Klassisches SMS-TAN-Verfahren	193
Abb. 8.2	pushTAN-Variante 1 mit separaten Apps für TAN-Empfang (TAN-App) und Banking (\$-App) und Variante 2 mit einer einzigen App für TAN-Empfang und Banking (TAN-\$-App)	194
Abb. 8.3	Zertifikats-Pinning für mobile Banking-Verfahren unter <i>Trust-on-First-Use</i> -Annahme	199
Abb. 10.1	Schematische Darstellung einer Java-Quelltext-Obfuskierung mithilfe von Werkzeugen wie ProGuard	218

Abb. 11.1	Überwindung des Air-Gap mittels Malware und Spionage-App DiskFiltration	228
Abb. 12.1	WLAN-Scanning im <i>passiven</i> Modus	233
Abb. 12.2	WLAN-Scanning im <i>aktiven</i> Modus	233
Abb. 12.3	Grafische Darstellung des Ausdrucks $d(RSSI) \approx \sqrt{ x_{SP} - x_{BS} ^2 + y_{SP} - y_{BS} ^2}$ aus dem Satz von Pythagoras	237
Abb. 12.4	Beispielhafte <i>RSSI</i> -Werte zweier Smartphones zu verschiedenen Zeitpunkten t	239
Abb. 12.5	Ergebnis der ersten Korrelationsstufe: SP_1 erhält zwei Optionen für eine mögliche Position der Basisstation	240
Abb. 12.6	Ergebnis der ersten Korrelationsstufe: Auch SP_2 erhält zwei Optionen für eine mögliche Position der Basisstation.	240
Abb. 12.7	Ergebnis der zweiten Korrelationsstufe: Durch Zusammenlegen der Korrelationen von SP_1 und SP_2 ergibt sich für Google/Apple eine eindeutige Position für die Basisstation.	241
Abb. 12.8	Mögliche nicht interaktive Protokollabfolge zum behördlichen Auskunftsanspruch bei Strafverfolgung mit technischem Datenschutz, basierend auf Bloom-Filtern	248

Es ist wohlbekannt, dass mobile eingebettete Geräte schon jetzt in ihrer Anzahl einen signifikanten und in ihrer wirtschaftlichen Bedeutung höchst relevanten Anteil an der heutigen Netzlandschaft darstellen. Beispielsweise spielen CPUs für Laptops und PCs im Mikroprozessormarkt zahlenmäßig mit etwa 1 % nur eine geringe Rolle, während der Anteil eingebetteter Prozessoren bei weit über 90 % liegt. Dies gilt insbesondere für Deutschland, da hier neben der stark anwachsenden Anzahl mobiler digitaler Geräte für den Consumer-Bereich (Smartphone, Tablet, Smartwatch) einer vergleichsweise schwach ausgeprägten PC-Industrie auch Schlüsselindustrien wie Maschinenbau, Automobil oder Medizintechnik gegenüberstehen, bei denen eingebettete Geräte von zentraler Bedeutung sind. Während der letzten Dekade wurden diese Geräte immer mehr vernetzt, wobei funkbasierte Anbindungen zunehmend dominieren. Drahtlose mobile Endgeräte sind allerdings aufgrund ihrer Ressourcenbeschränktheit und dem per se offenen Übertragungsmedium Luft prominente Angriffsziele. Fälle aus der jüngeren Vergangenheit wie der Stuxnet-Virus [1] oder Angriffe gegen Fahrzeuge über die GSM-Schnittstelle [2] haben zudem das erhebliche und im Fall Stuxnet nicht nur hypothetische Schadenspotenzial von Angriffen auf eingebettete Geräte aufgezeigt. In der Zukunft werden eingebettete und oftmals mobile Geräte und Systeme, die besonders eng mit der physikalischen Umgebung verbunden sind, eine sehr wichtige Rolle spielen. Unter diese sogenannten Cyber-physische Systeme (CPS) fallen viele gerade für die deutsche Wirtschaft wichtige Industrien, z. B. Sensornetze in der Automatisierung, Überwachung und Steuerung von Stromnetzen mittels ‚Supervisory Control and Data Acquisition‘ (SCADA)-Systemen, Smart Metering, Sensoren in der Medizintechnik und zahlreiche weitere als „Internet of Things (IoT)“ bzw. Industrie 4.0 bezeichnete Anwendungen.

Neben der Sicherheit werden in zunehmendem Maße Lösungen zu entwickeln sein, unter anderem aufgrund von einer steigenden Zahl mobiler Geräte beispielsweise durch fahrerlose Transportsysteme, aber auch durch Einbindung von Smartphone und Tablet

in diverse digitale Geschäftsprozesse. Drahtlose Nachrichtenübertragungssysteme stellen hierfür geeignete Technologien der Nachrichtenübertragung dar. Die Verwendung eines gemeinsam genutzten Übertragungsmediums macht drahtlose Nachrichtenübertragungssysteme allerdings verwundbar, sowohl im Hinblick auf die Zuverlässigkeit und Verfügbarkeit der Nachrichtenverbindung, z. B. bei Interferenz, als auch wegen ihrer Verwundbarkeit gegenüber Angriffen auf dem gemeinsam genutzten Übertragungsmedium. Die Systeme bedürfen daher einer verlässlichen Nachrichtenverbindung – sowohl im Sinne der Verfügbarkeit als auch im Sinne der Echtheit, Vertraulichkeit und Einmaligkeit der Daten – über die eingesetzten Kommunikationssysteme. Insbesondere aufgrund langer Innovationszyklen in Industrieanlagen ist die Bereitstellung von verlässlichen Nachrichtenverbindungen auf Grundlage verfügbarer Technologien der drahtlosen Kommunikation daher von großer Bedeutung. Eine zusätzliche Angriffsfläche ist der Tatsache geschuldet, dass die mobilen Betriebssysteme und die auf ihnen laufenden Anwendungen heutiger mobiler Consumer-Geräte eine Reihe Einfallstore bereitstellen. Gleichzeitig offenbart sich, dass das Ausspähen sensibler Daten zur Wirtschaftsspionage deutlich auf dem Vormarsch ist [3].

1.1 Was nicht Gegenstand dieses Buches ist

Wenn man eine Themenauswahl trifft, dann bedeutet es immer auch, dass einige Themen zwangsläufig nicht aufgenommen werden können. Daher skizzieren wir nun einzelne Themen, die wir im Rahmen dieses Buches nicht weiterverfolgen, an denen sich der Leser jedoch die Weitläufigkeit des Feldes bewusst machen kann:

Funktionale Sicherheit Bevor man sich an die Absicherung von Systemen zum Schutze gegen verschiedenste Arten von Angreifern macht, ist es unerlässlich, die funktionale Sicherheit eines Systems, also die Sicherstellung seiner korrekten Funktion, zu gewährleisten. So sind uns allen die Meldungen zu explodierten Akkus im Smartphone-Modell Samsung Galaxy 7 noch gut in Erinnerung. Sie verdeutlichen, auf welch vielfältige Aspekte Ingenieure und Produktentwickler eingehen müssen, um ein System ganzheitlich funktionsfähig, ausfallsicher, verfügbar, robust bzw. fehlertolerant zu gestalten. So behandelt beispielsweise die Norm EN/IEC 61508 die funktionale Sicherheit sicherheitsbezogener elektrischer, elektronischer und/oder programmierbarer Systeme.

Biometrische Authentifizierungsverfahren Die Nutzerauthentifizierung auf einem Smartphone mittels biometrischen Finger-Scanning ist noch viel zu einfach zu umgehen. Es reicht schon das Foto eines Fingers mit einer hochauflösenden digitalen Kamera, das dem Smartphone vorgehalten wird. Dies gilt auch für aktuelle Smartphones wie das im März 2019 erschienene Samsung Galaxy S10 mit Ultraschall-Sensoren, welche im Display verbaut sind. Vielleicht ist das ja ein Grund für die konsequente Raute-Stellung der Hände unserer Kanzlerin. Hat man es mit einem Smartphone-Nutzer zu tun, der derart

bedacht auf seine Handstellung ist und seinen Zeigefinger auf gar keinen Fall ablichten lassen möchte, so kann dessen biometrische Authentifizierung dennoch mittels Fingerabdrücken an Gegenständen wie beispielsweise Gläsern unterlaufen werden. Ähnliches gilt für biometrische Authentifizierungsverfahren mittels Gesichtserkennung: Auch hier ist es noch viel zu einfach, die Gesichtserkennungs-Software auszutricksen, indem man dem Smartphone mit der Gesichtserkennungs-Software einfach ein weiteres Smartphone mit dem Gesicht der Person auf dem Display gegenhält. Und schließlich: Biometrische Authentifizierungskennungen, die einmal genutzt als digitaler Repräsentant in die Hände von Betrügern fallen, können nicht wie das gute alte Passwort nach einiger Zeit geändert werden, sondern können von nun an fortwährend zum Identitätsdiebstahl verwendet werden.

Verwendung von USB-Kabeln Die Verwendung eines Universal-Serial-Bus-(USB-)Kabels ermöglicht immer eine zweiseitige Kommunikation. Die Sicherheitsproblematik ist damit inhärent. Wenn Sie also wieder einmal im Drogeriemarkt Ihre Urlaubsbilder ausdrucken, dann sollte Ihnen bewusst sein, dass hierbei auch Malware auf Ihr Smartphone aufgespielt werden könnte.

Stauvorhersage Seit einiger Zeit profitieren wir von den Stauvorhersagen durch Google Maps. Dabei tragen wir Smartphone-Nutzer aktiv zu diesem Location Based Service (LBS) bei, indem das Unternehmen Google Nutzer-Tracking durchführt. Bei iPhones betrifft dies all diejenigen Geräte, die Google Maps aktiviert haben, und bei Android-Geräten diejenigen, deren Lokationsdienste aktiviert sind. Diese Geräte senden ‚anonymisierte‘ Daten an Google. Auf Basis dieser Daten kann das Unternehmen Google nun auf die Gesamtzahl der Fahrzeuge auf einem Streckenabschnitt schließen und ermitteln, wie schnell diese sich fortbewegen, und zwar auf jeder Straße und zu jeder Zeit.

IMSI-Catcher und stille SMS Mit OpenBTS, OsmonconBB oder OpenLTE stehen neben Produkten wie IMSI-Catcher PKI 1640 eine Reihe von Lösungen für einen IMSI-Catcher-Angriff bereit. Somit kann die International Mobile Subscriber Identity (IMSI) des Mobiltelefons sowie dessen gegenwärtiger Standort in Erfahrung gebracht werden. Ebenso dient das Absetzen von stiller SMS der Erzeugung eines Ortungsimpulses für mobile Geräte. Dabei ist der Einsatz von stiller SMS als Ermittlungswerkzeug für Behörden insbesondere hinsichtlich der Tatsache zu diskutieren, dass hierbei die aktive Erzeugung eines Ortungsimpulses erforderlich ist. Dies ist mit dem klassischen Einsatz eines IMSI-Catchers nicht der Fall. Denn letztere Technologie agiert rein passiv. Das Eingehen einer stillen SMS zum Erhalt von Verbindungsinformationen durch den Mobilfunkanbieter wird der Nutzer des mobilen Gerätes nicht gewahrt. Mit HushSMS war lange Zeit eine App im Google Store verfügbar mit der ebenfalls SMS-Class-0-Ortungsimpulse versendet werden konnten.

Pager In Deutschland und Frankreich werden dedizierte Infrastrukturen auf Basis von NP2M-Technologie (Narrowband Point-to-Multipoint) betrieben, um im Falle von Katastrophen unabhängig von bekannten Netzbetreibern zu sein. Es wird eine Schmalbandtechnologie verwendet mit dem vorrangigen Ziel, versorgungssicher zu sein. Dabei geht es darum, eine große Anzahl von Empfängern in kürzester Zeit zu erreichen. Durch eine Standardisierung des ETSI (das Europäische Institut für Telekommunikationsnormen) aus dem Jahre 2013 ist es ideal für einen landes- und europaweiten Alarmierungs- und Informationsdienst. Allerdings hat sich herausgestellt, dass Pager wie e*message auch sehr leicht manipulierbar sind. Dies ist gerade als Kommunikationswahl in Katastrophenfällen nicht hinnehmbar.

Prozessoren Mit Spectre1, Spectre2, Meltdown und Spectre Next Generation sind seit 2017 eine Reihe von sehr ernstzunehmenden Seitenkanalangriffen auf Chiparchitekturen bekannt geworden, die auch in mobilen Geräten verbaut sind. Dabei kann man sich einen Seitenkanal als eine geteilte Ressource vorstellen, die ursprünglich nicht zum Austausch von Informationen konzipiert worden ist, jedoch finidig hinsichtlich dieser Eigenschaft zweckentfremdet wurde. Damit ist jedes digitale Gerät, welches solche Chips (Intel, Cortex-A75) hardwareseitig verbaut hat, anfällig gegenüber derartigen Angriffen. Solche Seitenkanalangriffe die im konkreten Fall auf Sprungvorhersage und auf einer Ausführung von Instruktionsabfolgen in einer anderen Reihenfolge als vorgesehen (*out-of-order execution*) basieren, ermöglichen einen unautorisierten Zugriff auf die Speicherbereiche fremder Prozesse. Und dies auch dann, wenn dem aufrufenden Prozess für diesen Prozess keine Zugriffsrechte vorliegen. Da die anfälligen Prozessoren auch in Smartphones und Tablets verwendet werden, sind diese Schwachstellen auch für mobile IT-Systeme von sehr großer Relevanz.

1.2 Was die Themen dieses Buches sind

Nachdem wir nun einen Eindruck gewinnen konnten, was dieses Buch inhaltlich nicht bietet, stellt sich die Frage nach dessen Beitrag. Wenn man eine grobe Einordnung treffen möchte, so werden Sicherheitskonzepte sowie bekannte Schwachstellen der folgenden beiden Säulen bedient:

- I. Drahtlose Übertragungstechnologien
- II. Softwarekomponenten mobiler digitaler Geräte

Es wird sich aber sehr schnell zeigen, dass solch eine strikte Klassifizierung oftmals nicht durchhaltbar ist. Beim Verfassen dieses Buches stellte sich zudem heraus, dass es häufig einfacher ist, die Verwundbarkeit einzelner Komponenten zu beschreiben, als über deren gelungene und im Idealfall beweisbar sichere Sicherheitsarchitektur zu berichten. Im Vordergrund steht daher vor allem die Vermittlung eines umfassenden Problembewusstseins

und die Erörterung der Fragestellung, warum es eben nicht so einfach oder nahezu unmöglich ist, komplexe IT-Systeme abzusichern. Hierzu muss man sich eigentlich nur anschauen, aus wie vielen Seiten Spezifikation einzelne Standarddokumente der Internet Engineering Task Force (IETF) bzw. des 3rd Generation Partnership Project (3GPP) oder des Europäischen Instituts für Telekommunikationsnormen (ETSI) bestehen. Oder aus wie vielen Lines-of-Code Bluetooth, WLAN und andere drahtlose Kommunikationsprotokolle bestehen bzw. wie ‚geschwätzig‘ heutige Betriebssysteme sind, was den ungefragten Aufbau von Verbindungen zu IP-Adressen in alle Welt angeht. Denn dann erhält man einen Eindruck von der allumfassenden Problematik, mit der sich nicht nur der IT-Sicherheitsbeauftragte und die IT-Abteilung eines Unternehmens auseinanderzusetzen haben. Nicht zu vergessen sind die vielfältigsten Aspekte und gegenseitigen Abhängigkeiten, die sich zum Teil aus der, in Standards vorgeschriebenen Abwärtskompatibilität einzelner kryptografischer Verfahren für Protokollklassen zur Drahtlos-Kommunikation ergeben oder ganz einfach durch offen formulierte respektive via *hidden agenda* ausgetragene Zielkonflikte einzelner Interessengruppen innerhalb derartiger Standardisierungsgremien.

Die Sorglosigkeit, mit der wir alles miteinander vernetzen, sei es in den Bereichen Industrie 4.0, Smart Home, Advanced Metering Infrastructure (AMI), oder im Bereich des autonomen Fahrens und der Fahrzeug-zu-Fahrzeug-Kommunikation macht zumindest mich schier fassungslos. Wie können wir annehmen, dass aus einer Reihe von nachweisbar unsicheren Komponenten ein sicheres und gegenüber verschiedensten Arten von Angreiferkategorien gehärtetes Gesamtsystem entsteht? Zauberformeln wie ‚*Predictive Maintenance*‘ oder ‚*Mensch, Maschine, Werkstück., alles digital vernetzt*‘ sollen gerade auch den deutschen Mittelstand bewegen, seine Produktionsstätten zu vernetzen, oftmals animiert durch weltweit agierende internationale Konzerne, deren Zulieferer sie sind.

So kann es bei aller Euphorie um die digital Vernetzung nicht schaden, einen Schritt zurückzugehen und sich die Diskussionen in ‚artfremden‘ Disziplinen vor Augen zu führen, in denen das Thema Sicherheit eine deutlich längere Tradition hat: Im Beitrag ‚*Sicherheitsforschung – Sichern auf Hochtour*‘ [4] wird für das alpine Gehen neben verschiedenen Seilsicherungsformen mit Seil auch das *seilfreie Gehen* als Option erörtert. Hierzu heißt es: „*Dem bewussten Verzicht auf ein Sicherheitsseil liegt eine nüchterne Risikoabwägung zugrunde: Das Schadensausmaß ist reduziert, wenn nur eine Person ins Rutschen kommt. ... Wenn dagegen eine angeseilte Seilschaft mal Fahrt aufgenommen hat, verheddern sich die Mitglieder im Seil und ziehen sich gegenseitig nach unten.*“ Und weiter: „*Die Abwägung, wann seilfreies Gehen noch für alle im Team passt, ist nicht einfach. Sie erfordert realistische Selbsteinschätzung, Einfühlungsvermögen und offene, klare Kommunikation. Wie generell jede Entscheidung über angemessene Sicherungsmaßnahmen.*“

Es ist nicht zuletzt diese Forderung einer klaren und ungeschönten Kommunikation über angemessene Sicherungsmaßnahmen, die die IT-Welt beherzigen und verinnerlichen sollte. Dies betrifft insbesondere die Unternehmensführung, die meist nicht mit ‚*Bits and Pieces*‘ behelligt werden möchte. Wer nun der Meinung ist, dass der obige Vergleich doch arg hinkt, der möge sich insbesondere mit den Themen dieses Buches auseinandersetzen. Übrigens: In der IT-Welt wären mit ‚*seilfreiem Gehen*‘ die ‚*air-gapped systems*‘ gemeint, also solche, die keinerlei Kommunikationsschnittstelle miteinander teilen.

1.3 Danksagung

Das vorliegende Buch wäre in seiner jetzigen Form nicht denkbar gewesen ohne die tatkräftige praktische Unterstützung einer ganzen Reihe von engagierten UNITS- und ENITS-Studierenden der Hochschule Offenburg. So haben insbesondere Max Bauert, Alexander Eger, Jan Breig und Moritz Kaumanns, aber auch andere Studierende verschiedenste Praxistests in der Laborumgebung durchgeführt. Darüber hinaus hat Frau Dr. Gisela Hillenbrand wertvolle Anregungen zur Verbesserung der Lesbarkeit zum Abschnitt Angriffe über ‚ungültige Kurven‘ beigetragen. Ohne die Arbeiten des Doktoranden Louis Tajan zur Anwendung von Bloom-Filtern wäre der Abschnitt zum Thema Auskunftsansprüche mit technischem Datenschutz in seiner jetzigen Form nicht entstanden. Ihnen allen gilt mein besonderer Dank!

1.4 Noch eine Bemerkung in eigener Sache

Bevor es los geht, noch eine Bemerkung in eigener Sache:

Wir wollen Schwachstellen verstehen und Angriffsszenarien nachvollziehen!

Wichtig dabei ist:

- Der Inhalt des Buches soll nicht als „Hacker-Anleitung“ dienen.
- Der Inhalt des Buches soll insbesondere nicht dazu beitragen, sich auf illegalem Wege Daten zu beschaffen

Vorsicht

Die Anwendung der gezeigten Techniken und Methoden kann gegen geltendes Recht verstoßen!

Im Einzelnen sind dies:

- StGB § 202a: Ausspähen von Daten
- StGB § 202b: Abfangen von Daten
- StGB § 202c: „**Der Hackerparagraph**“
- StGB § 303a: Datenveränderung
- StGB § 303b: Computersabotage

Prof. Dr. habil. Dirk Westhoff vertritt an der Hochschule Offenburg das Themengebiet Sicherheit und Verlässlichkeit in Informationssystemen. Er ist Gründungsmitglied des Institutes für verlässliche Embedded und Kommunikationselektronik (ivESK) und Studiendekan des Master-Studienganges ENITS (Enterprise- and IT-Security). Vorherige Stationen an Hochschulen für Angewandte Wissenschaften waren Hamburg und

Furtwangen. Dr. Westhoff habilitierte 2007 zum Thema Sicherheit und Verlässlichkeit drahtloser Zugangsnetze an der FernUniversität Hagen. Im Unternehmen NEC R&D am Standort Heidelberg war er zuständig für die Einwerbung und Durchführung von EU-Projekten wie EU FP6-IST STREP UbiSec&Sens¹ (Technischer Projektleiter), EU FP7-IST SENSEI² sowie EU FP7-IST STREP WSAN4CIP³, bei denen ein Schwerpunkt auf der Erarbeitung von Sicherheitslösungen für drahtlose Sensornetze lag. Projekte aus Hamburger Zeiten sind SKIMS⁴ (BMBF) und Smart Power Hamburg⁵ (BMW). In Furtwangen und Offenburg erfolgten Arbeiten auf den BMBF-Projekten UNIKOPS⁶ und ProSeCCo⁷ sowie dem Projekt PAL-SAAA⁸, wobei UNIKOPS sich der Erarbeitung universell konfigurierbarer Sicherheitslösungen für Cyber-physische Systeme widmete. Dr. Westhoff ist Mitbegründer der Springer-Serie LNCS ESAS⁹ und Co-Autor von ca. 90 Veröffentlichungen. Dr. Westhoff hält acht Patente zu Sicherheit in drahtlosen Sensornetzen sowie in verteilten Systemen.

Literatur

1. Brunner, M., Hofinger, H., Krauß, C., Roblee, C., Schoo, P., Todt, S.: Infiltrating critical infrastructures with next-generation attacks: W32.Stuxnet as a showcase threat. Fraunhofer SIT, Darmstadt. <https://www.sec.in.tum.de/i20/publications/infiltrating-critical-infrastructures-with-next-generation-attacks-w32-stuxnet-as-a-showcase-threat> (2010). Zugegriffen: 26. Apr. 2019
2. Chekoyaw, S., McCoy, D., Kantor, B., Anderson, D., Shacham, H., Savage, S., Koscher, K., Czekis, A., Roesner, F., Kohno, T.: Comprehensive experimental analyses of automotive attack surfaces. In: Proceedings of the 20th USENIX Conference on Security, SEC'11, San Francisco (2011)
3. Data Breach Investigations Report: www.verizonenterprise.com/de/DBIR/2015/ (2015). Zugegriffen: 1. Dez. 2015
4. Hellberg, F.: Sicherheitsforschung – Gletscher: Seil oder nicht Seil? DAV Panor. 3, 68–71 (2018)

¹UbiSec&Sens – Ubiquitous Sensing and Security in the European Homeland.

²SENSEI – Integrating the Physical with the Digital World of the Network of the Future.

³WSAN4CIP – Wireless Sensor and Actuator Networks for Critical Infrastructure Protection.

⁴SKIMS – Schichtenübergreifendes kooperatives Immunsystem für mobile, mehrseitige Sicherheit.

⁵SmartPower Hamburg – Security for smart grid IT architectures.

⁶UNIKOPS – Universell konfigurierbare Sicherheitslösung für Cyber-physische heterogene Systeme.

⁷ProSeCCo – Promotionsvorhaben zur Erarbeitung von Sicherheitserweiterungen für das Cloud Computing.

⁸PAL-SAAA – Building Triangular Trust for Secure Cloud Auditing.

⁹ESAS – European Workshop on Security in Ad Hoc & Sensor Networks.