Dirk Westhoff

Mobile Security

Schwachstellen verstehen und Angriffsszenarien nachvollziehen

EBOOK INSIDE

Springer Vieweg

Mobile Security

Dirk Westhoff

Mobile Security

Schwachstellen verstehen und Angriffsszenarien nachvollziehen

Springer Vieweg

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.

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 schieren 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 Prof. Dr. Dirk Westhoff
Dezember 2019

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. Petrlic, 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

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 an 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 Infratructure
PMK	Pairwise Master Key
PRNG	Pseudorandom Number Generator
RFC	Request for Comments
RPC	Remote Procedure Call
RSSI	Received Singal 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

Einführung

1

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

D. Westhoff, *Mobile Security,* https://doi.org/10.1007/978-3-662-60855-5_1

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 gewahr. 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-Techologie (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 Alamierungs- 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 findig 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 Sicherungsseil 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&Sens[1] (Technischer Projektleiter), EU FP7-IST SENSEI[2] sowie EU FP7-IST STREP WSAN4CIP[3], bei denen ein Schwerpunkt auf der Erarbeitung von Sicherheitslösungen für drahtlose Sensornetze lag. Projekte aus Hamburger Zeiten sind SKIMS[4] (BMBF) und Smart Power Hamburg[5] (BMWI). In Furtwangen und Offenburg erfolgten Arbeiten auf den BMBF-Projekten UNIKOPS[6] und ProSeCCo[7] sowie dem Projekt PAL-SAaaS[8], wobei UNIKOPS sich der Erarbeitung universell konfigurierbarer Sicherheitslösungen für Cyber-physische Systeme widmete. Dr. Westhoff ist Mitbegründer der Springer-Serie LNCS ESAS[9] 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. Chekoway, 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)

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

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

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

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

[5]SmartPower Hamburg – Security for smart grid IT architectures.

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

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

[8]PAL-SAaaS – Building Triangular Trust for Secure Cloud Auditing.

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