Nicht hackbare Rechner und nicht brechbare Kryptographie

Wolfgang A. Halang · Robert Fitz

Nicht hackbare Rechner und nicht brechbare Kryptographie

2., wesentlich neu bearbeitete und erweiterte Auflage

Springer Vieweg

Wolfgang A. Halang
Qingdao Uni. of Science
and Technology
Qingdao
China

Robert Fitz
Hochschule f. Angewandte
Wiss. Hamburg
Hamburg
Deutschland

ISBN 978-3-662-58026-4 ISBN 978-3-662-58027-1 (eBook)
https://doi.org/10.1007/978-3-662-58027-1

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

Springer Vieweg

Ursprünglich erschienen im Datakontext-Verlag, 2002

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

Vorwort

Jedesmal, wenn in den Medien wieder über Fälle wie einen großen Datendiebstahl bei einem Internetkonzern, über das Eindringen von Hackern in das Netz des Deutschen Bundestages oder eine Abhöraffäre sowie die damit verbundenen Schäden berichtet und suggeriert wird, dass es letztendlich keinen wirklich effektiven Schutz dagegen gebe, halten sich die beiden Autoren dieses Buches die Bäuche vor Lachen. Genauso würde wahrscheinlich auch Konrad Zuse, der Erfinder programmgesteuerter Datenverarbeitungsmaschinen, über heutige IKT-Sicherheitsprobleme lachen. Wenn Sie das vorliegende Buch gelesen haben werden, werden auch Sie zu den Lachern gehören.

Der Tatsache, dass alle heute gegen Hacker- und Abhörangriffe eingesetzten Maßnahmen weder uneingeschränkt wirksam und schon gar nicht nachhaltig sind, stellt das vorliegende Buch seine Botschaft entgegen: Schadprogramme, also Viren, Würmer, Trojanische Pferde und ausführbare Internetinhalte, verursachen zwar große Verluste, stellen aber ein technisch sehr leicht lösbares Problem dar; denn – wie wir sehen werden – ist seit fast zwei Jahrhunderten das Konstruktionsprinzip bekannt, programmgesteuerte Digitalrechner mit physisch von ihren Datenspeichern getrennten sowie gerätetechnisch schreibgeschützten Programmspeichern auszustatten und derart unüberwindbar gegen alle heutigen und zukünftigen, auf Schadprogrammen basierenden Angriffsarten zu schützen. Weiterhin gibt es auch seit rund eineinhalb Jahrhunderten perfekt sichere Methoden zur Datenchiffrierung mit Einmalschlüsseln, die nicht nur systematisch nicht brechbar sind und es auch nie sein werden, sondern die auch einfach und leicht verständlich sind. Allein ihre Anwendung kann das Ausspähen abgehörter oder gespeicherter Daten nachhaltig verhindern.

Das vorliegende Buch richtet sich einerseits an alle technisch interessierten Anwender, die mehr über die wahren Gründe der Angreifbarkeit heutiger Systeme und Netze erfahren möchten, um kompetent mitreden und um sichere Systeme und Netze einfordern zu können. In der Komplexität heutiger Systeme wird der Leser ein Flickwerk aus wenig durchdachten und sich als ungeeignet erweisenden Lösungen erkennen, die jeglicher Innovation entgegenstehen. Andererseits werden in Form von Patenten bzw. Patentanmeldungen seit bereits etwa zwei Jahrzehnten den Stand der Technik definierende Architekturkonzepte zur Entwicklung sicherer Rechensysteme vorgestellt. Die entsprechenden

Maßnahmen sind auch zur Sicherung handlicher Kommunikations- und Datenverarbeitungsgeräte (Mobiltelefone, Smartphones, Tablet-PCs etc.) geeignet, die sich in den letzten Jahren rasant verbreitet haben, womit sie in den Fokus von Angreifern gerückt sind. Wegen ihrer Angreifbarkeit durch direkten physikalischen Zugriff bedarf diese Geräteklasse jedoch zusätzlichen Schutzes. Wie er sich technisch recht leicht realisieren lässt, wird hier gezeigt.

Zweifelsohne ist der Titel dieses Buches mit dem zweimal darin enthaltenen „nicht“ stilistisch nicht gelungen. Aber den Autoren ist nichts Besseres eingefallen, um absolut unmissverständlich auszudrücken, dass es einerseits um Digitalrechner geht, die schlicht und einfach nicht gehackt werden können, weil dies konstruktionsbedingt ausgeschlossen ist, und andererseits um kryptographische Verfahren, deren perfekte Sicherheit auf der mathematischen Unmöglichkeit beruht, eine Gleichung mit zwei Unbekannten zu lösen. Von gegen Schadprogramme gesicherten Rechnern und sicherer Kryptographie zu reden, wäre zu schwach gewesen, weil das auch andere tun, wenn sie über marktübliche Abwehrmaßnahmen gegen Hacking sowie gängige kryptographische Verfahren berichten, die aber nie absolut sicher sind. Außerdem ist der Begriff Sicherheit nach DIN/VDE 31 000 Teil 2 relativ: Er lässt immer noch ein Restrisiko jenseits eines gesellschaftlich als tragbar angesehenen Grenzrisikos zu. In den hier betrachteten Domänen besteht jedoch kein Restrisko: Digitalrechner lassen sich absolut hackingresistent bauen und Verschlüsselungen können perfekt sicher, d. h. unbrechbar sein.

Dieses Buch zeigt auf, was entweder in Vergessenheit geraten ist oder permanent aus welchen Gründen auch immer von Fachwelt und Öffentlichkeit ignoriert wird. Es legt dar, dass abschließende Lösungen für allgemein als gesellschaftliche Probleme betrachtete und durch den Einsatz ungeeigneter Methoden und minderwertiger technischer Artefakte verursachte Schwierigkeiten seit Jahrzehnten bzw. fast zwei Jahrhunderten bekannt sind – mithin schon zu Zeiten, als es weder Digitalrechner noch Rechnernetze gab und die Probleme noch gar nicht entstanden waren. Warum diese Lösungen nicht auf dem Markt erhältlich sind und warum sie in der Praxis nicht eingesetzt werden, möchten die Autoren hier nicht diskutieren. Sie überlassen es Ihnen, sich zu dieser höchst interessanten Fragestellung eine eigene Meinung zu bilden.

Im Sommer 2018

Prof. Dr. Dr. Wolfgang A. Halang
Prof. Dr.-Ing. Robert Fitz

Inhaltsverzeichnis

Abkürzungen und Akronyme

AES	Advanced Encryption Standard
API	Application Programming Interface
App	Applikation
ASCII	American Standard Code for Information Interchange
BASIC	Beginner's All-Purpose Symbolic Instruction Code
BAT	Batch
BGB	Bürgerliches Gesetzbuch
BIOS	Basic Input Output System
BK	Bundeskriminalamt (in Österreich)
BKA	Bundeskriminalamt
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BMWi	Bundesministerium für Wirtschaft und Technologie
Bot	Roboter
BSI	Bundesamt für Sicherheit in der Informationstechnik
CAD	Computer Added Design
CD	Compact Disk
CD-ROM	Compact Disk-Read Only Memory
CD-RW	Compact Disk-Read Write
CERT	Computer Emergency Response Team
CERT/CC	Computer Emergency Response Team / Coordination Center
CMOS	Complementary Metal Oxid Semiconductor
COM	Command
CPU	Central Processing Unit
CSI	Computer Security Institute

DCC	Direct Client Connection
DD	Double Density
DES	Data Encryption Standard
DFN	Deutsches Forschungsnetz
DIN	Deutsches Institut für Normung e.V.
DLL	Dynamic Link Library
DMV	Demonstrationsmakrovirus
DNS	Domain Name Service
DOC	Document
DOS	Disk Operating System
DOS/VS	Disk Operating System/Virtual Storage
DOT	Document Template
DVD	Digital Versatile Disk
EDV	Elektronische Datenverarbeitung
EEPROM	Electrical Erasable Programmable Read Only Memory
EIDE	Enanced Integrated Drive Electronics
EPROM	Erasable Programmable Read Only Memory
Europol	Europäisches Polizeiamt
EXE	Executable
E-Business	Electronic Business
E-Commerce	Electronic Commerce
E-Mail	Electronic Mail
FAT	File Allocation Table
FBI	Federal Bureau of Investigation
FIRST	Forum of Incident Response and Security Teams
FPGA	Field Programmable Gate Array
FTP	File Transfer Protocol
GPS	Global Positioning System
GPT	GUID Partition Table
GSM	Global System for Mobile Communication
GUID	Globally Unique Identifier
HD	High Density
HTML	Hyper Text Markup Language
IBAN	International Bank Account Number
ICSA	International Computer Security Association
IDE	Integrated Drive Electronics
IDPS	Intrusion Detection and Prevention Systems
IDS	Intrusion Detection Systems

IKT	Informations- und Kommunikationstechnik
IP	Internet Protocol
IPS	Intrusion Prevention Systems
IRC	Internet Relay Chat
IrDA	Infrared Data Association
IRS	Intrusion Reaction Systems
ISDN	Integrated Services Digital Network
IT	Informationstechnologie
iTAN	indizierte Transaktionsnummer
ITW	In The Wild
JCL	Job Control Language
LAN	Local Area Network
LBA	Linear Block Address
MAPI	Messaging Application Programming Interface
MBR	Master Boot Record
Me	Millennium edition
MS	Microsoft
NATO	North Atlantic Treaty Organization
NCSA	National Computer Security Association
NT	New Technology
NTFS	New Technology File System
OSI	Open System Interconnection
OS/2	Operating System/2
OVL	Overlay
PC	Personal Computer
PDA	Personal Digital Assistent
PGP	Pretty Good Privacy
PIN	Personal Identification Number
POST	Power On Self Test
PROM	Programmable Read Only Memory
RAM	Random Access Memory
RISC	Reduced Instruction Set Computer
ROM	Read Only Memory
SCR	Script
SD	Secure Digital
SoC	System on Chip
SPS	Speicherprogrammierbare Steuerung
SSD	Solid State Disk

StGB	Strafgesetzbuch
SYS	System
S/MIME	Secure / Multipurpose Internet Mail Extensions
TCP	Transmission Control Protocol
TSR	Terminate Stay Resident
UEFI	Unified Extensible Firmware Interface
URL	Uniform Resource Locator
USA	United States of America
USB	Universal Serial Bus
VBA	Visual Basic for Applications
VBS	Visual Basic Script
VDE	Verband der Elektrotechnik Elektronik Informationstechnik e.V.
WAB	Windows Address Book
WAN	Wide Area Network
WAP	Wireless Application Protocol
WinCC	Windows Control Center
WLAN	Wireless Local Area Network
WSH	Windows Scripting Host
WWW	World Wide Web