

SpringerBriefs in Computer Science

Series editors

Stan Zdonik, Brown University, Providence, Rhode Island, USA

Shashi Shekhar, University of Minnesota, Minneapolis, Minnesota, USA

Jonathan Katz, University of Maryland, College Park, Maryland, USA

Xindong Wu, University of Vermont, Burlington, Vermont, USA

Lakhmi C. Jain, University of South Australia, Adelaide, South Australia, Australia

David Padua, University of Illinois Urbana-Champaign, Urbana, Illinois, USA

Xuemin (Sherman) Shen, University of Waterloo, Waterloo, Ontario, Canada

Borko Furht, Florida Atlantic University, Boca Raton, Florida, USA

V.S. Subrahmanian, University of Maryland, College Park, Maryland, USA

Martial Hebert, Carnegie Mellon University, Pittsburgh, Pennsylvania, USA

Katsushi Ikeuchi, University of Tokyo, Tokyo, Japan

Bruno Siciliano, Università di Napoli Federico II, Napoli, Italy

Sushil Jajodia, George Mason University, Fairfax, Virginia, USA

Newton Lee, Newton Lee Laboratories, LLC, Tujunga, California, USA

More information about this series at <http://www.springer.com/series/10028>

Maurizio Martellini · Stanislav Abaimov
Sandro Gaycken · Clay Wilson

Information Security of Highly Critical Wireless Networks

Maurizio Martellini
Landau Network Fondazione Volta
Milan
Italy

Stanislav Abaimov
University of Rome Tor Vergata
Rome
Italy

Sandro Gaycken
Digital Society Institute
European School of Management and
Technology (ESMT)
Berlin
Germany

Clay Wilson
Cybersecurity Studies Graduate Program
University of Maryland University College
Largo, MD
USA

ISSN 2191-5768 ISSN 2191-5776 (electronic)
SpringerBriefs in Computer Science
ISBN 978-3-319-52904-2 ISBN 978-3-319-52905-9 (eBook)
DOI 10.1007/978-3-319-52905-9

Library of Congress Control Number: 2017930284

© The Author(s) 2017

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Contents

1	Introduction	1
2	What Is Highly Critical Wireless Networking (HCWN)	3
2.1	ZigBee	3
2.2	Z-Wave	4
2.3	Cellular Network Communication	4
2.4	Wireless Mesh Networks	4
	References	5
3	Applications for HCWN	7
3.1	Terrestrial Trunked Radio	7
3.2	Medical Devices	8
3.3	SCADA Systems	8
3.4	Smart Grid	9
	References	9
4	Vulnerabilities and Security Issues	11
4.1	Wireless Vulnerabilities	12
4.1.1	Wireless Eavesdropping	12
4.1.2	WEP and WPA Encryption	12
4.1.3	Jamming	13
4.1.4	Rogue Access Points	13
4.1.5	Injection Attacks	13
4.2	Medical Device Vulnerabilities	13
4.3	Smart Grid, Mesh Network Vulnerabilities	14
	References	15
5	Modeling Threats and Risks	17
5.1	Passive Attacks	17
5.2	Active Attacks	17
	References	18

6	Modeling Vulnerabilities	19
	References.	20
7	Governance and Management Frameworks	21
7.1	FCC Rules	21
7.2	Spectrum Sharing	21
7.3	FDA	22
	References.	22
8	Security Technologies for Networked Devices	25
8.1	Basic Security Controls for All Wireless Networks	25
8.2	Encryption	26
8.3	Directional Transmission and Low Power Signals	26
	References.	26
9	Known Weaknesses with Security Controls	27
	References.	28
10	Competent Reliable Operation of HCWN	29
	Reference	30
11	Assessing the Effectiveness and Efficiency of Security Approaches	31
11.1	WEP Legacy Issues	31
11.2	Use of a DMZ for SCADA	31
	References.	32
12	Examples in Brief	33
12.1	SCADA Software from China	33
12.2	Angen 9-1-1	33
12.3	General Dynamics Smartphones	34
12.4	Medical Devices at VA.	34
12.5	Drug Infusion Pump	34
	References.	35
13	Testing the Resilience of HCWN	37
13.1	Introduction	37
13.2	Definitions	38
13.3	Goals of Cyber Security Testing.	39
13.4	Types of Cyber Security Testing	39
13.5	Network Communication Standards	40
13.6	Wireless Networks by Geographical Range	40
13.7	Wireless Operating Modes	43
13.7.1	Infrastructure Network Mode.	43
13.7.2	Ad Hoc Network Mode.	43
13.7.3	Wireless Distribution Mode.	44
13.7.4	Monitor Mode	44

13.8	Cyber Security Assessment Methodologies	44
13.9	Security Testing Practical Applications	46
13.9.1	Preparatory Stage	46
13.9.2	Scanning and Enumeration Techniques	50
13.9.3	Passive Traffic Capture and Identification	50
13.9.4	Simulated Attacks	50
13.9.5	Post-Exploitation	55
13.9.6	Reporting	55
13.10	Vulnerability Management	56
13.10.1	Incident Response	56
13.10.2	Operational Security	57
13.10.3	Vulnerability Classification	57
	References	57
14	Future Attack Patterns	59
14.1	Cyberattacks	59
14.2	Hybrid Attacks	59
14.2.1	Against Facilities	60
14.2.2	Against Consumer Products	60
14.2.3	Against AWS	61
14.2.4	Against Unmanned Vehicles	61
14.2.5	Against Satellites, Weaponization of the Outer-Space and Interplanetary Internet	61
14.2.6	Against Medical Equipment	62
15	Assessing Cyberattacks Against Wireless Networks of the Next Global Internet of Things Revolution: Industry 4.0	63
15.1	Introduction	63
15.2	Selected Security Threats of the Industry 4.0	66
15.3	Advanced Persistent Threats and Cyber-Espionage	66
15.4	Cyber-Terrorism	66
15.5	Supply Chain and the Extended Eco-System	67
15.6	Challenges of the Internet of Things	67
15.7	Autonomous Weapon Systems and Robots	68
	References	69
16	Conclusion	71