PREVENTING BLUETOOTH AND WIRELESS ATTACKS IN IoMT HEALTHCARE SYSTEMS

JOHN CHIRILLO

WILEY

Preventing Bluetooth and Wireless Attacks in IoMT Healthcare Systems is a comprehensive companion for anyone in healthcare. The insights you gain here will enhance your understanding and help drive the mission to create a safer, more secure healthcare environment for everyone.

—Tom Brays
Cybersecurity Analyst and Technical Editor

Preventing Bluetooth and Wireless Attacks in IoMT Healthcare Systems is a masterful guide for navigating the challenges of securing healthcare environments, from physical spaces to digital systems. It empowers leaders to protect what matters most. Worth a read for anyone committed to advancing the safety and integrity of our healthcare institutions.

—Robert Blake
President, E1

I've worked in healthcare for over 30 years and *Preventing Bluetooth and Wireless Attacks in IoMT Healthcare Systems* is necessary reading.

—Jean Dwyer
RN and Clinical Educator in Labor & Delivery

Preventing Bluetooth and Wireless Attacks in IoMT Healthcare Systems is vital for anyone navigating the intersection of healthcare and cybersecurity. With real-world insight and practical strategies, I can confidently say it belongs on every security leader's shelf.

—T. Mills
Chief Information Security Officer and Author

I highly recommend reading as it illustrates the importance of cybersecurity in healthcare, ethical concerns, and how devastating life can be without it.

—Deb Martin
Privacy and Security Advisor

Preventing Bluetooth and Wireless Attacks in IoMT Healthcare Systems unpacks the complexities of technologies in healthcare with a playbook of security strategies.

—Renee Vogley
Director, Business Operations at Cardinal Health

Preventing Bluetooth and Wireless Attacks in IoMT Healthcare Systems tackles Bluetooth and wireless communication vulnerabilities within connected medical device infrastructures. Moreover, it offers practical mitigation strategies such as encryption, secure device pairing, continuous network monitoring, and multifactor authentication—solutions that align with modern cybersecurity best practices. Its clear structure makes it accessible to both technical professionals and nontechnical audiences.

—Pam Kennedy
Security Compliance Auditor and Technical Editor

Whether you're fortifying infrastructure or ensuring compliance in 2025's stricter regulatory requirements, *Preventing Bluetooth and Wireless Attacks in IoMT Healthcare Systems* is an indispensable tool.

—Kevin Knapp
Sr. Cybersecurity Engineer

John has done a phenomenal job creating a comprehensive treatise on IoMT threat management. This is worth a read for anyone dealing with the deployment and operational use of technology in healthcare. He adeptly covers the technical security challenges but does not stop there. Healthcare administrators, clinical staff, support, and even patients will find this book invaluable. Join John on the journey as he digs into the overall threat landscape, enumerating indicators of threat and attack while offering crucial guidance on best practices, security testing, policy, and response.

—Steve Nardone
Division Chief and Head of the Trusted Product
Evaluation Program at the NSA
Sr. Dir. Security and Compliance, Ret.

Preventing Bluetooth and Wireless Attacks in IoMT Healthcare Systems

Preventing Bluetooth and Wireless Attacks in IoMT Healthcare Systems

John Chirillo

WILEY

Copyright © 2025 by John Wiley & Sons, Inc. All rights reserved, including rights for text and data mining and training of artificial intelligence technologies or similar technologies.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

Published simultaneously in Canada and the United Kingdom.

ISBNs: 9781394349418 (Paperback), 9781394349432 (ePDF), 9781394349425 (ePub)

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at `www.copyright.com`. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at `http://www.wiley.com/go/permission`.

The manufacturer's authorized representative according to the EU General Product Safety Regulation is Wiley-VCH GmbH, Boschstr. 12, 69469 Weinheim, Germany, e-mail: `Product_Safety@wiley.com`.

Trademarks: Wiley and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries and may not be used without written permission. Bluetooth is registered trademark of Bluetooth Sig, Inc. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002. For product technical support, you can find answers to frequently asked questions or reach us via live chat at `https://support.wiley.com`.

If you believe you've found a mistake in this book, please bring it to our attention by emailing our reader support team at `wileysupport@wiley.com` with the subject line "Possible Book Errata Submission."

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at `www.wiley.com`.

Library of Congress Control Number: 2025934397

Cover image: © sudok1/Getty Images
Cover design: Wiley

About the Author

John Chirillo, an accomplished and published programmer and author, has written numerous influential books on cybersecurity, ethical hacking, and IT compliance. His writings are celebrated for their ability to demystify intricate technical concepts, making them accessible to professionals and enthusiasts alike. With decades of hands-on experience, John has built a career that seamlessly integrates the art of ethical hacking with the science of IT governance. His work ensures that businesses stay ahead in an ever-evolving threat landscape.

About the Technical Editors

Stephen Nardone has been involved in almost every aspect of information security for over 40 years. This includes systems security, operations security, telecommunications security, testing, evaluation, and program security. He began his career at the National Security Agency, where he spent 15 years supporting the NSA's mission in various challenging roles. He was division chief and head of the Trusted Product Evaluation Program at the NSA, responsible for executing security evaluations against DoD Standard 5200.28 and the "Rainbow" series of documents (Orange, Red, and Lavender Books). The Orange Book, *DOD 5200.28-STD, The Department of Defense Trusted Computer System Evaluation Criteria*, published in December 1985, set the standard for computer systems security evaluations.

Stephen became the chief technology and security officer for the Commonwealth of Massachusetts, eventually leading to his role as senior director of the Security Center of Excellence at Connection. He is now enjoying retirement while staying engaged in the evolving world of cybersecurity.

Pamela Kennedy has over 20 years of experience in IT service management (ITSM), cybersecurity, compliance, and IT audit. She has developed deep expertise in government, healthcare, and financial services. Pamela specializes in cybersecurity, auditing, and regulatory compliance, providing assurance and advisory services to organizations looking to strengthen or expand their internal controls to meet regulatory requirements. Her experience spans cyber policy and risk analysis, including information security, protection of critical national infrastructure, IT operations, government regulatory assessments, control design, IT compliance, governance, and incident response. She has led initiatives to help organizations align their IT policies, security protocols, and operational strategies with industry best practices and regulatory mandates.

Acknowledgments

First and foremost, I want to express my heartfelt thanks to my family and friends for their unwavering support and patience throughout the writing process. This is especially true for my wife, Kristi, and son, Conner. Your understanding during long nights and busy weekends has been invaluable.

I am profoundly grateful to my cybersecurity and healthcare IT colleagues, who have shared their knowledge and experiences.

I want to acknowledge the contributions of the ethical hacking community, whose responsible disclosure of vulnerabilities has been crucial in advancing IoMT security. Your work continues to be a driving force in improving the safety of medical devices.

My gratitude extends to the legal and ethics experts who provided invaluable insights into the complex regulatory landscape of healthcare technology. Your guidance has been essential in addressing this field's critical legal and ethical considerations.

I am grateful to my publisher, Wiley, for believing in the importance of this project and providing the platform to share this critical information with the broader community. A special note of thanks goes to the managing editor, Navin Vijayakumar; acquisitions editor, James Minatel; editorial assistant, Annie Melnick; and project manager, Brad Jones, whose keen eyes and insightful suggestions have greatly improved the clarity and structure of this book. Also, to my technical editors and reviewers, Stephen Nardone and Pamela Kennedy, your expertise has been instrumental in making complex topics accessible to a diverse readership.

Lastly, I want to thank my readers—the cybersecurity professionals, healthcare leadership, IT specialists, and experts who protect our medical systems. Your dedication to securing the Internet of Medical Things inspired me to write this book. I hope the knowledge shared here will support your crucial work.

I sincerely thank everyone who has contributed, directly or indirectly, to the realization of this book. This work is a testament to the collaborative spirit of the cybersecurity and healthcare communities, which are united to create a safer digital healthcare environment for all.

Contents at a Glance

Contents

Preface

In today's world, healthcare and technology are deeply intertwined, transforming how we diagnose, treat, and care for patients. At the center of this transformation are connected medical devices—smart tools that collect, share, and analyze health data in real time. These devices improve daily lives, from wearable heart monitors to robotic surgical systems. But with this progress comes a growing challenge: ensuring the security of the technology we increasingly rely on. The Internet of Medical Things (IoMT) has introduced new risks as cyber threats targeting healthcare systems become more sophisticated. This book was born from the need to understand these evolving risks and offer practical solutions to protect the devices that keep us healthy. I hope to shed light on cybersecurity's critical role in our connected health systems through this book's use cases and case studies and make complex topics accessible.

Part I explores the rapid rise of connected medical devices and the technologies behind them. It explains why securing these devices is essential—not just for technical reasons but also for the safety and well-being of patients and healthcare providers.

Part II examines the attack vectors that threaten IoMT systems. I analyze how malicious actors exploit vulnerabilities in Bluetooth and other wireless protocols standard in healthcare, equipping defenders with a deeper understanding of these threats.

Part III brings theory to life with case studies that show how security breaches have impacted healthcare institutions and patients. These examples underscore why cybersecurity must be a top priority.

Part IV focuses on solutions and best practices for securing IoMT devices and preventing attacks. I highlight the latest advancements in safeguarding healthcare technology, from artificial intelligence to advanced encryption methods.

Part V looks ahead to emerging trends in IoMT security, including 5G/6G and quantum computing. These technologies offer new opportunities for innovation—but

also create new risks. I discuss what they mean for the future of secure healthcare systems.

To end, Part VI addresses the legal, ethical, and regulatory landscape of IoMT security. I explore the responsibilities of healthcare providers and manufacturers and how policies and privacy laws are evolving to protect patient data.

Securing medical devices is not just a technical challenge; it's a matter of patient safety and public health. I hope this book sparks greater awareness, better security practices, and continued innovation in protecting healthcare environments. As healthcare technology evolves, so too will the threats it faces. This book is just the beginning of an ongoing conversation. I encourage you to keep exploring, asking questions, and staying informed. Together, we can build a future where connected healthcare delivers its full potential—securely and safely.

Finally, I transformed several attack vectors into a story to help readers visualize the impact. Suppose you're interested in a fast-paced fictional depiction of the latest in healthcare attack vectors. In that case, you can find my novel, *Silent Intrusions*, in various marketplaces online or scan the following QR code:

John Chirillo

Who Should Read This Book

This book is for anyone interested in the intersection of the Internet of Things (IoT), healthcare, and security threats. It is especially relevant to cybersecurity professionals, healthcare leadership, IT specialists, and experts protecting our medical systems, as it suggests exploring attack techniques, their impact, and mitigation strategies.