The IoT Hacker's Handbook

A Practical Guide to Hacking the Internet of Things

Aditya Gupta

Apress®

The IoT Hacker's Handbook: A Practical Guide to Hacking the Internet of Things

Aditya Gupta
Walnut, CA, USA

ISBN-13 (pbk): 978-1-4842-4299-5 ISBN-13 (electronic): 978-1-4842-4300-8
https://doi.org/10.1007/978-1-4842-4300-8

Trademarked names, logos, and images may appear in this book. Rather than use a trademark symbol with every occurrence of a trademarked name, logo, or image we use the names, logos, and images only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The use in this publication of trade names, trademarks, service marks, and similar terms, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Managing Director, Apress Media LLC: Welmoed Spahr
Acquisitions Editor: Natalie Pao
Development Editor: James Markham
Coordinating Editor: Jessica Vakili

Cover image designed by Freepik (www.freepik.com)

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springeronline.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a **Delaware** corporation.

For information on translations, please e-mail rights@apress.com, or visit http://www.apress.com/rights-permissions.

Apress titles may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Print and eBook Bulk Sales web page at http://www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this book is available to readers on GitHub via the book's product page, located at www.apress.com/978-1-4842-4299-5. For more detailed information, please visit http://www.apress.com/source-code.

Printed on acid-free paper

Table of Contents

About the Author

Aditya Gupta is the founder and CEO of Attify, Inc., a specialized security firm offering IoT penetration testing and security training on IoT exploitation. Over the past couple of years, Aditya has performed in-depth research on the security of these devices including smart homes, medical devices, ICS and SCADA systems. He has also spoken at numerous international security conferences, teaching people about the insecurity in these platforms and how they can be exploited. Aditya is also the co-author of the *IoT Pentesting Cookbook* and the author of *Learning Pentesting for Android Devices*.

About the Technical Reviewer

Adeel Javed is an intelligent automation consultant, an author, and a speaker. He helps organizations automate work using business process management (BPM), robotic process automation (RPA), business rules management (BRM), and integration platforms.

He loves exploring new technologies and writing about them. He published his first book, *Building Arduino Projects for the Internet of Things*, with Apress back in 2015. He shares his thoughts on various technology trends on his personal blog (adeeljaved.com).

Acknowledgments

This book could never have been finished without my amazing team at Attify, who poured in their day and night to make sure that we produced quality content as a team.

Introduction

The ten chapters of this book cover a number of topics, ranging from hardware and embedded exploitation, to firmware exploitation, to radio communication, including BLE and ZigBee exploitation.

For me, writing this book was an exciting and adventurous journey, sharing my experiences and the various things I have learned in my professional career and pouring everything into these ten chapters.

I hope you can make the most out of this book and I would highly encourage you to take all the skill sets learned in this book and apply them to real-world problems and help make the Internet of Things (IoT) ecosystem more secure. It is individual contributions that will help us create a safer and more secure world, and you reading this book can play a part in that.

No one is perfect, and this book is bound to have a minor error or two. If you encounter any of those mistakes, let me know and I would be happy to correct them in future editions of *The IoT Hacker's Handbook*.

I also teach three-day and five-day training classes on offensive IoT exploitation, which I would encourage you to attend to get hands-on experience with everything covered in the book. For more information about the online training and live classes, feel free to check out attify-store.com.

The last and the most important part is community! For you, the reader, I want you to be willing enough to share your knowledge with your peers or even with someone who is new to this field. This is how we, as a community, will grow.

That is all from my end. Again, thanks for reading *The IoT Hacker's Handbook* and I wish you all the best for your IoT exploitation endeavors.

Aditya Gupta (@adi1391)
Founder and Chief Hacker,
Attify