PRACTICAL IOT HACKING

The Definitive Guide to Attacking the Internet of Things

by Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, and Beau Woods

no starch press

San Francisco

ISBN-13: 978-1-7185-0090-7 (print)
ISBN-13: 978-1-7185-0091-4 (ebook)

FSC LOGO
FPO

Publisher: William Pollock
Executive Editor: Barbara Yien
Production Editor: Dapinder Dosanjh
Developmental Editor: Frances Saux
Cover Illustration: Rick Reese
Interior Design: Octopod Studios
Technical Reviewer: Aaron Guzman
Copyeditor: Anne Marie Walker
Compositor: Jeff Wilson, Happenstance Type-O-Rama
Proofreader: Elizabeth Littrell
Indexer: BIM Creatives, LLC

For information on book distributors or translations, please contact No Starch Press, Inc. directly:
No Starch Press, Inc.
245 8th Street, San Francisco, CA 94103
phone: 1-415-863-9900; info@nostarch.com
www.nostarch.com

Library of Congress Cataloging-in-Publication Data

Names: Chantzis, Fotios, author. | Stais, Ioannis, author. | Calderon, Paulino, author. | Deirmentzoglou, Evangelos, author. | Woods, Beau, author.
Title: Practical IoT hacking : the definitive guide to attacking the internet of things / Fotios Chantzis, Ioannis Stais, Paulino Calderon, Evangelos Deirmentzoglou, and Beau Woods.
Description: San Francisco : No Starch Press, Inc., 2020. | Includes index.
Identifiers: LCCN 2020029866 (print) | LCCN 2020029867 (ebook) | ISBN 9781718500907 | ISBN 9781718500914 (ebook)
Subjects: LCSH: Internet of things--Security measures. | Penetration testing (Computer security)
Classification: LCC TK5105.8857 .C533 2020 (print) | LCC TK5105.8857 (ebook) | DDC 005.8/7--dc23
LC record available at https://lccn.loc.gov/2020029866
LC ebook record available at https://lccn.loc.gov/2020029867

Dedicated to Klajdi and Miranta.

.....

About the Authors

Fotios (Fotis) Chantzis (@ithilgore) is laying the foundation for a safe and secure Artificial General Intelligence (AGI) at OpenAI. Previously, he worked as a principal information security engineer at Mayo Clinic, where he managed and conducted technical security assessments on medical devices, clinical support systems, and critical healthcare infrastructure. He has been a member of the core Nmap development team since 2009, when he wrote Ncrack under the mentorship of Gordon "Fyodor" Lyon, the original author of Nmap, during the Google Summer of Code. He later worked as a mentor for the Nmap project during the Google Summer of Code 2016 and 2017 and has authored a video course about Nmap. His research on network security includes exploiting the TCP Persist Timer (you can find his paper on the topic published in Phrack #66) and inventing a stealthy port scanning attack by abusing XMPP. Fotis has presented at notable security conferences, including DEF CON. Highlights of his work can be found at his site *https://sock-raw.org/*.

Ioannis Stais (@Einstais) is a senior IT security researcher and head of red teaming at CENSUS S.A., a company that offers specialized cybersecurity services to customers worldwide. Ioannis has participated in more than 100 security assessment projects, including the assessment of communication protocols, web and mobile banking services, NFC payment systems, ATMs and point-of-sale systems, critical medical appliances, and MDM solutions. He holds a master's degree in computer systems technology from the University of Athens. His research currently focuses on the development of machine learning algorithms for improving vulnerability research, the enhancement of fuzzing frameworks, and an exploration of the current threats in mobile and web applications. He has presented his research at security conferences such as Black Hat Europe, Troopers NGI, and Security BSides Athens.

About the Co-Authors

Paulino Calderon (@calderpwn) is a published author and international speaker with over 12 years of experience in network and application security. When he isn't traveling to security conferences or consulting for Fortune 500 companies with Websec, a company he co-founded in 2011, he spends peaceful days enjoying the beach in Cozumel, Mexico. He loves open source software and has contributed to many projects, including Nmap, Metasploit, OWASP Mobile Security Testing Guide (MSTG), OWASP Juice Shop, and OWASP IoT Goat.

Evangelos Deirmentzoglou (@edeirme) is an information security professional interested in solving security problems at scale. He led and structured the cybersecurity capability of the financial tech startup Revolut. A member of the open source community since 2015, he has made multiple contributions to Nmap and Ncrack. He is currently researching a cybersecurity PhD focusing on source code analysis, which he has previously applied for many major US technology vendors, Fortune 500 companies, and financial and medical institutions.

Beau Woods (@beauwoods) is a cyber safety innovation fellow with the Atlantic Council and a leader with the I Am The Cavalry grassroots initiative. He is also the founder and CEO of Stratigos Security and sits on the board of several nonprofits. In his work, which bridges the gap between the security research and public policy communities, he ensures that any connected technology able to impact human safety is worthy of our trust. He formerly served as an entrepreneur in residence with the US FDA and a managing principal consultant at Dell SecureWorks. He has spent the past several years consulting with the energy, healthcare, automotive, aviation, rail, and IoT industries, as well as with cybersecurity researchers, US and international policymakers, and the White House. Beau is a published author and frequent public speaker.

About the Technical Reviewer

Aaron Guzman is co-author of the IoT Penetration Testing Cookbook and a technical leader for Cisco Meraki's security team. As part of OWASP's IoT and Embedded Application Security projects, he leads open source initiatives that raise awareness of IoT security defensive strategies and lower the barrier for entry into IoT hacking. Aaron is co-chair of Cloud Security Alliance's IoT Working Group and a technical reviewer for several IoT security books. He has extensive public speaking experience, delivering conference presentations, trainings, and workshops globally. Follow Aaron's research on Twitter at @scriptingxss.

BRIEF CONTENTS

CONTENTS IN DETAIL