

THE HARDWARE HACKING HANDBOOK. Copyright © 2022 by Jasper van Woudenberg and Colin O'Flynn.

All rights reserved. No part of this work may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage or retrieval system, without the prior written permission of the copyright owner and the publisher.

Printed in the United States of America

First printing

25 24 23 22 21 1 2 3 4 5 6 7 8 9

ISBN-13: 978-1-59327-874-8 (print)

ISBN-13: 978-1-59327-875-5 (ebook)

Publisher: William Pollock

Production Manager and Editor: Rachel Monaghan

Developmental Editors: William Pollock, Neville Young, and Jill Franklin

Cover Illustrator: Garry Booth

Cover and Interior Design: Octopod Studios

Technical Reviewer: Patrick Schaumont

Copyeditor: Barton Reed

Compositor: Jeff Wilson, Happenstance Type-O-Rama

Proofreader: Rebecca Rider

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: Woudenberg, Jasper van, author. | O'Flynn, Colin, author.

Title: The hardware hacking handbook : breaking embedded security with hardware attacks / by Jasper van Woudenberg and Colin O'Flynn.

Description: San Francisco, CA : No Starch Press, 2022. | Includes bibliographical references and index. | Summary: "A deep dive into hardware attacks on embedded systems explained by experts in the field through real-life examples and hands-on labs. Topics include the embedded system threat model, hardware interfaces, various side-channel and fault injection attacks, and voltage and clock glitching"--Provided by publisher.

Identifiers: LCCN 2021027424 (print) | LCCN 2021027425 (ebook) | ISBN 9781593278748 (print) | ISBN 9781593278755 (ebook)

Subjects: LCSH: Embedded computer systems--Security measures. | Electronic apparatus and appliances--Security measures. | Penetration testing (Computer security)

Classification: LCC TK7895.E42 W68 2022 (print) | LCC TK7895.E42 (ebook) | DDC 006.2/2--dc23

LC record available at <https://lcn.loc.gov/2021027424>

LC ebook record available at <https://lcn.loc.gov/2021027425>

No Starch Press and the No Starch Press logo are registered trademarks of No Starch Press, Inc. Other product and company names mentioned herein may be the trademarks of their respective owners. Rather than use a trademark symbol with every occurrence of a trademarked name, we are using the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

The information in this book is distributed on an "As Is" basis, without warranty. While every precaution has been taken in the preparation of this work, neither the authors nor No Starch Press, Inc. shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the information contained in it.