14th USENIX Workshop on Offensive Technologies (WOOT'20)

Online
11 August 2020

ISBN: 978-1-7138-1533-4

Printed from e-media with permission by:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571

Some format issues inherent in the e-media version may also appear in this print version.

Usenix Association
2560 Ninth Street, Suite 215
Berkeley, California, 94710

https://www.usenix.org/

Additional copies of this publication are available from:

Curran Associates, Inc.
57 Morehouse Lane
Red Hook, NY 12571 USA
Phone: 845-758-0400
Fax: 845-758-2633
Email: curran@proceedings.com
Web: www.proceedings.com

TABLE OF CONTENTS

EXPLOITING USES OF UNINITIALIZED STACK VARIABLES IN LINUX KERNELS TO LEAK KERNEL POINTERS 1
Haehyun Cho, Jinbum Park, Joonwon Kang, Tiffany Bao, Ruoyu Wang, Yan Shoshitaishvili, Adam Doupé, Gail-Joon Ahn

AUTOMATIC GENERATION OF COMPACT PRINTABLE SHELLCODES FOR X86 12
Dhrumil Patel, Aditya Basu, Anish Mathuria

UNEARTHING THE TRUSTEDCORE: A CRITICAL REVIEW ON HUAWEI'S TRUSTED EXECUTION ENVIRONMENT 23
Marcel Busch, Johannes Westphal, Tilo Mueller

NFCGATE: OPENING THE DOOR FOR NFC SECURITY RESEARCH WITH A SMARTPHONE-BASED TOOLKIT 36
Steffen Klee, Alexandros Roussos, Max Maass, Matthias Hollick

ONE EXPLOIT TO RULE THEM ALL? ON THE SECURITY OF DROP-IN REPLACEMENT AND COUNTERFEIT MICROCONTROLLERS 49
Johannes Obermaier, Marc Schink, Kosma Moczek

TOOTHPICKER: APPLE PICKING IN THE IOS BLUETOOTH STACK 62
Dennis Heinze, Jiska Classen, Matthias Hollick

BLESA: SPOOFING ATTACKS AGAINST RECONNECTIONS IN BLUETOOTH LOW ENERGY 77
Jianliang Wu, Yuhong Nan, Vireshwar Kumar, Dave (Jing) Tian, Antonio Bianchi, Mathias Payer, Dongyan Xu

AFL++ : COMBINING INCREMENTAL STEPS OF FUZZING RESEARCH 89
Andrea Fioraldi, Dominik Maier, Heiko Eibfeldt, Marc Heuse

BANKRUPT COVERT CHANNEL: TURNING NETWORK PREDICTABILITY INTO VULNERABILITY 101
Dmitrii Ustiugov, Plamen Petrov, Siavash Katebzadeh, Boris Grot

OFFICE DOCUMENT SECURITY AND PRIVACY 114
Jens Müller, Fabian Ising, Christian Mainka, Vladislav Mladenov, Sebastian Schinzel, Jörg Schwenk

Author Index