

13th USENIX Workshop on Offensive Technologies (WOOT'19)

Santa Clara, California, USA
12 – 13 August 2019

ISBN: 978-1-7138-0452-9

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.

Copyright© (2019) by Usenix Association
All rights reserved.

Printed with permission by Curran Associates, Inc. (2020)

For permission requests, please contact Usenix Association
at the address below.

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

GOING SIDEWAYS

| | |
|---|----|
| TAKING A LOOK INTO EXECUTE-ONLY MEMORY | 1 |
| <i>M. Schink, J. Obermaier</i> | |
| CROSS-ROUTER COVERT CHANNELS | 14 |
| <i>A. Ovadya, R. Ogen, Y. Mallah, N. Gilboa, Y. Oren</i> | |
| TWO METHODS FOR EXPLOITING SPECULATIVE CONTROL FLOW HIJACKS | 26 |
| <i>A. Mambretti, A. Sandulescu, M. Neugschwandtner, A. Sorniotti, A. Kurmus</i> | |
| HOW SHARP IS SHARP ? | 34 |
| <i>D. Kumar, B. Panda, C. Yashavant, V. Gupta</i> | |

BREAKING AND ENTERING

| | |
|--|----|
| DEFEATING CISCO TRUST ANCHOR: A CASE-STUDY OF RECENT ADVANCEMENTS IN DIRECT FPGA BITSTREAM MANIPULATION | 45 |
| <i>J. Kataria, R. Housley, J. Pantoga, A. Cui</i> | |
| RISC-V: #ALPHANUMERICSHHELLCODING | 58 |
| <i>H. Barral, R. Geraud-Stewart, G. Jaloyan, D. Naccache</i> | |
| VACUUMS IN THE CLOUD: ANALYZING SECURITY IN A HARDENED IOT ECOSYSTEM..... | 69 |
| <i>F. Ullrich, J. Classen, J. Eger, M. Hollick</i> | |
| UNICOREFUZZ: ON THE VIABILITY OF EMULATION FOR KERNELSPACE FUZZING | 80 |
| <i>D. Maier, B. Radtke, B. Harren</i> | |

TOWN CALLED MALICE

| | |
|---|-----|
| A BETTER ZIP BOMB | 91 |
| <i>D. Fifield</i> | |
| D-TIME: DISTRIBUTED THREADLESS INDEPENDENT MALWARE EXECUTION FOR RUNTIME OBFUSCATION | 102 |
| <i>J. Pavithran, M. Patnaik, C. Rebeiro</i> | |
| BREAKING TURTLES ALL THE WAY DOWN: AN EXPLOITATION CHAIN TO BREAK OUT OF VMWARE ESXI..... | 116 |
| <i>H. Zhao, Y. Zhang, K. Yang, T. Kim</i> | |
| ALTERNATIVE (AB)USES FOR HTTP ALTERNATIVE SERVICES | 125 |
| <i>T. Tiwari, A. Trachtenberg</i> | |

CRYPTO MEANS...

| | |
|---|-----|
| WHO SPENT MY EOS? ON THE (IN)SECURITY OF RESOURCE MANAGEMENT OF EOS.IO | 137 |
| <i>S. Lee, D. Kim, D. Kim, S. Son, Y. Kim</i> | |

DISTRIBUTED PASSWORD HASH COMPUTATION ON COMMODITY HETEROGENEOUS
PROGRAMMABLE PLATFORMS 148
B. Pervan, J. Knezovic, K. Pericin

LET'S GET PHYSICAL

MINIMUM FAILURE: EMFI ATTACKS AGAINST USB STACKS 156
C. O'Flynn

AUTOMATIC WIRELESS PROTOCOL REVERSE ENGINEERING 166
J. Pohl, A. Noack

Author Index