

18th USENIX WOOT Conference on Offensive Technologies (WOOT '24)

August 12–13, 2024
Philadelphia, PA, USA

Monday, August 12

Practitioners at Work

Achilles Heel in Secure Boot: Breaking RSA Authentication and Bitstream Recovery from Zynq-7000 SoC 1
Prasanna Ravi and Arpan Jati, *Temasek Laboratories, Nanyang Technological University, Singapore*; Shivam Bhasin, *National Integrated Centre for Evaluation (NiCE), Nanyang Technological University, Singapore*

WhatsApp with privacy? Privacy issues with IM E2EE in the Multi-device setting 11
Tal A. Be'ery, *Zengo*

Introduction to Procedural Debugging through Binary Libification 17
Jonathan Brossard, *Conservatoire National des Arts et Métiers, Paris*

Security Can Be Tricky

The Power of Words: Generating PowerShell Attacks from Natural Language 27
Pietro Liguori, Christian Marescalco, Roberto Natella, Vittorio Orbinato, and Luciano Pianese, *DIETI, Università degli Studi di Napoli Federico II*

Attacking with Something That Does Not Exist: ‘Proof of Non-Existence’ Can Exhaust DNS Resolver CPU 45
Olivia Gruza, Elias Heftrig, Oliver Jacobsen, Haya Schulmann, and Niklas Vogel, *National Research Center for Applied Cybersecurity ATHENE, Goethe-Universität Frankfurt*; Michael Waidner, *National Research Center for Applied Cybersecurity ATHENE, Technische Universität Darmstadt, Fraunhofer Institute for Secure Information Technology SIT*

Amplifying Threats: The Role of Multi-Sender Coordination in SMS-Timing-Based Location Inference Attacks . . 59
Evangelos Bitsikas, *Northeastern University*; Theodor Schnitzler, *Research Center Trustworthy Data Science and Security and Maastricht University*; Christina Pöpper, *New York University Abu Dhabi*; Aanjhan Ranganathan, *Northeastern University*

Embedded Security

MakeShift: Security Analysis of Shimano Di2 Wireless Gear Shifting in Bicycles 75
Maryam Motallebigohmi, *Northeastern University*; Earlence Fernandes, *UC San Diego*; Aanjhan Ranganathan, *Northeastern University*

Engineering a backdoored bitcoin wallet 89
Adam Scott and Sean Andersen, *Block, Inc.*

Oh No, My RAN! Breaking Into an O-RAN 5G Indoor Base Station 101
Leon Janzen, Lucas Becker, Colin Wiesenäcker, and Matthias Hollick, *Technical University of Darmstadt (TUDa)*

Tuesday, August 13

Hardware Security

RIPencapsulation: Defeating IP Encapsulation on TI MSP Devices 117
Prakhar Sah and Matthew Hicks, *Virginia Tech*

Reverse Engineering the Eufy Ecosystem: A Deep Dive into Security Vulnerabilities and Proprietary Protocols . . 133
Victor Goeman, Dairo de Ruck, Tom Cordemans, Jorn Lapon, and Vincent Naessens, *DistriNet-KU Leuven*

SoK: Where’s the “up”?! A Comprehensive (bottom-up) Study on the Security of Arm Cortex-M Systems 149
Xi Tan and Zheyuan Ma, *CactiLab, University at Buffalo*; Sandro Pinto, *Universidade do Minho*; Le Guan, *University of Georgia*; Ning Zhang, *Washington University in St. Louis*; Jun Xu, *The University of Utah*; Zhiqiang Lin, *Ohio State University*; Hongxin Hu, *University at Buffalo*; Ziming Zhao, *CactiLab, University at Buffalo*

Memory Corruption Is a Solved Problem

Not Quite Write: On the Effectiveness of Store-Only Bounds Checking171

Adriaan Jacobs and Stijn Volckaert, *DistriNet, KU Leuven*

SoK: On the Effectiveness of Control-Flow Integrity in Practice 189

Lucas Becker and Matthias Hollick, *Technical University of Darmstadt*; Jiska Classen, *Hasso Plattner Institute, University of Potsdam*

Exploiting Android’s Hardened Memory Allocator 211

Philipp Mao, Elias Valentin Boschung, Marcel Busch, and Mathias Payer, *EPFL*

Physical Attacks

Breaking Espressif’s ESP32 V3: Program Counter Control with Computed Values using Fault Injection 229

Jeroen Delvaux, *Technology Innovation Institute*; Cristofaro Mune, *Raelize*; Mario Romero, *Technology Innovation Institute*; Niek Timmers, *Raelize*

Basilisk: Remote Code Execution by Laser Excitation of P–N Junctions Without Insider Assistance 245

Joe Loughry, *Netoir.com*; Kasper Rasmussen, *University of Oxford*

SOK: 3D Printer Firmware Attacks on Fused Filament Fabrication 263

Muhammad Haris Rais, *Virginia State University*; Muhammad Ahsan and Irfan Ahmed, *Virginia Commonwealth University*