20th USENIX WOOT Conference on Offensive Technologies (WOOT '26)

August 10–11, 2026
Baltimore, MD, USA

Monday, August 10

Embedded, Automotive, and Platform Security

HotWire: Real-World Impersonation and Discharge Attacks on Electric Vehicle Charging Systems 1
Kuan Yu Chen, *National Taiwan University of Science and Technology;* Md Hasan Shahriar, *Virginia Tech;* Wen Wei Li and Shi Cho Cha, *National Taiwan University of Science and Technology;* Wenjing Lou, *Virginia Tech*

Real-Time Compromise: Investigating RTC Security in Consumer IoT 17
Victor Goeman, Tom Cordemans, Christoph Sanders, Jorn Lapon, and Vincent Naessens, *DistriNet, KU Leuven*

DisARMed: Attacking ARM TrustZone from Userspace with Memory Aliasing 31
Jacqueline Henes, Matthew Bowden, and Mihai Ordean, *University of Birmingham;* David Oswald, *Durham University*

Security Analysis of LTE Connectivity in Connected Cars: A Case Study of Tesla 49
Evangelos Bitsikas, Jason Veara, and Aanjhan Ranganathan, *Northeastern University*

SoK: 20 Years of Power, Privilege, and Peril in x86 System Management Mode. 73
Antonis Louka and Jo Van Bulck, *DistriNet, KU Leuven*

Program Analysis and Fuzzing

SemSan: a Configurable Sanitizer for Detecting System-Level Semantic Bugs 95
Moritz Sanft and Flavio Toffalini, *Ruhr-Universität Bochum*

FuzzBT: Holistic-State-Guided Fuzzing for Bluetooth Host Stack in Kernels. 113
Sungwoo Kim, *Purdue University;* Hui Peng, *Google, Inc.;* Imtiaz Karim, *The University of Texas at Dallas;* Ruoyu Wu, *Purdue University;* Jianliang Wu, *Simon Fraser University;* Elisa Bertino, *Purdue University;* Mathias Payer, *EPFL;* Dave (Jing) Tian, *Purdue University*

Squeezing Juicy Variant Bugs Out of Modern Browsers 131
Han Zheng, *EPFL;* Flavio Toffalini, *Ruhr-Universität Bochum;* Qiang Liu and Mathias Payer, *EPFL*

SoK: Multi-Layer Indirect Call Analysis in the Real World 153
Yufei Du, *Georgia Institute of Technology;* Vasileios P. Kemerlis, *Brown University;* Michalis Polychronakis, *Stony Brook University;* Fabian Monrose, *Georgia Institute of Technology*

Hardware Security

Swarm in EM Hay: Particle Swarm-guided Probe Placement for EM SCA 171
Dev Mehta, Seyedmohammad Nouraniboosjin, Maryam S. Safa, Shahin Tajik, and Fatemeh Ganji, *Worcester Polytechnic Institute*

Breaking Infrared Recapture Detection: Optical-Synthesis Attacks and Depth-Aware In-Sensor Countermeasures 189
Tetsu Ishizue, *The University of Electro-Communications;* Sara Rampazzi, *University of Florida;* Takeshi Sugawara, *University of Electro-Communications*

PowerHooK: Enabling Software-Based Power Side Channels Against AMD SEV Technologies via Transient-Execution Replay. 211
Mathias Oberhuber, Martin Unterguggenberger, and Martin Wistauder, *Graz University of Technology;* Andreas Kogler, *Graz University of Technology Alumni;* Rishub Nagpal and Stefan Mangard, *Graz University of Technology*

Flash [Re]Loaded: Body Bias Injection on Flash Memory. 229
Valentin Huber and Marc Schink, *Fraunhofer AISEC, Technical University of Munich (TUM)*

Tuesday, August 11

Machine Learning, Large Language Models, and Cyber Reasoning Systems

You Have Been LaTeXpOsEd: A Large-Scale Systematic Analysis of Information Leakage in Preprint Archives Using Large Language Models 247
Richard A. Dubniczky and Bertalan Borsos, *Eötvös Loránd University;* Tamas Bisztray, *HUN-REN Sztaki;* Norbert Tihanyi, *Technology Innovation Institute*

Are Neuro-Inspired Multi-Modal Vision-Language Models Resilient to Membership Inference Privacy Leakage? 263
David Amebley and Sayanton Dibbo, *The University of Alabama*

LIMA: Defining, Benchmarking and Detecting Cross-Layer Vulnerabilities in LLM Inference Frameworks 287
Sanjib Kumar Sen, Hannah Longoria, and Bozhen Liu, *Texas A&M University - Corpus Christi*

OSS-CRS: Liberating AIxCC Cyber Reasoning Systems for Real-World Open-Source Security 305
Andrew Chin, *Georgia Institute of Technology;* Dongkwan Kim, *Microsoft;* Yu-Fu Fu, Fabian Fleischer, and Youngjoon Kim, *Georgia Institute of Technology;* HyungSeok Han and Cen Zhang, *Microsoft;* Brian Junekyu Lee and Hanqing Zhao, *Georgia Institute of Technology;* Taesoo Kim, *Georgia Institute of Technology and Microsoft*

Software Security and Malware Analysis

Defective by Design: Universal Recovery of All Widevine-Protected Content on Desktop Environments 321
Florian Roudot and Mohamed Sabt, *Univ Rennes, CNRS, IRISA*

Evading and crashing anti-malware solutions via data collection overloading during analysis serialization. 337
Evgenios Gkritsis, *Athens University of Economics and Business;* Constantinos Patsakis, *University of Piraeus and Information Management Systems Institute of Athena Research Centre;* George Stergiopoulos, *Athens University of Economics and Business*

Onelogon: Taking over Active Directory Accounts via Netlogon 355
Alexander Neff, Tobias Holl, and Kevin Borgolte, *Ruhr University Bochum*

SoK: The Constant Time Model 369
Billy Bob Brumley, *Rochester Institute of Technology*

Mobile, Wireless, and Cellular Protocol Security

Protocol Prying: Systematic Vulnerability Research in the Apple AirDrop and Android Quick Share Proximity Transfer Protocols 385
Arash Ale Ebrahim and Nils Ole Tippenhauer, *CISPA Helmholtz Center for Information Security*

Exploiting Android Apps with Counterfeit Art 399
Rokhaya-Diamil Fall and Philipp Mao, *EPFL;* Martin Wagner, *Asymmetric Research;* Mathias Payer, *EPFL*

Practical Attacks on a Decentralized Secure Messenger Session 413
Kota Urushigaki, *The University of Osaka;* Hayato Kimura, *NICT and The University of Osaka;* Atsushi Tanaka and Takanori Isobe, *The University of Osaka*

CATana: On the Dangers of SIM-Originating AT Commands 429
Tomasz Lisowski, *University of Birmingham;* Kristian Covic, *Fuzzware;* Marius Muench, *University of Birmingham*

SoK: Insecurity of Cellular Basebands. 445
Henri Carnot, *Avantix and EURECOM;* Aurélien Francillon, *EURECOM*