Bug Finding I

How Double-Fetch Situations turn into Double-Fetch Vulnerabilities: A Study of Double Fetches in the Linux Kernel ...........................................1
Pengfei Wang, National University of Defense Technology; Jens Krinke, University College London; Kai Lu and Gen Li, National University of Defense Technology; Steve Dodier-Lazaro, University College London

Postmortem Program Analysis with Hardware-Enhanced Post-Crash Artifacts .................................................17
Jun Xu, The Pennsylvania State University; Dongliang Mu, Nanjing University; Xinyu Xing, Peng Liu, and Ping Chen, The Pennsylvania State University; Bing Mao, Nanjing University

Ninja: Towards Transparent Tracing and Debugging on ARM .................................................................33
Zhenyu Ning and Fengwei Zhang, Wayne State University

Side-Channel Attacks I

Prime+Abort: A Timer-Free High-Precision L3 Cache Attack using Intel TSX ..............................................51
Craig Disselkoen, David Kohlbrenner, Leo Porter, and Dean Tullsen, University of California, San Diego

On the effectiveness of mitigations against floating-point timing channels ..............................................69
David Kohlbrenner and Hovav Shacham, UC San Diego

Constant-Time Callees with Variable-Time Callers .................................................................83
Cesar Pereida García and Billy Bob Brumley, Tampere University of Technology

Systems Security I

Neural Nets Can Learn Function Type Signatures From Binaries ..........................................................99
Zheng Leong Chua, Shiqi Shen, Prateek Saxena, and Zhenkai Liang, National University of Singapore

CAAn’t Touch This: Software-only Mitigation against Rowhammer Attacks targeting Kernel Memory .............................................117
Ferdinand Brasser, Technische Universität Darmstadt; Lucas Davi, University of Duisburg-Essen; David Gens, Christopher Liebchen, and Ahmad-Reza Sadeghi, Technische Universität Darmstadt

Efficient Protection of Path-Sensitive Control Security .................................................................131
Ren Ding and Chenxiong Qian, Georgia Tech; Chengyu Song, UC Riverside; Bill Harris, Taesoo Kim, and Wenke Lee, Georgia Tech

Bug Finding II

Digtool: A Virtualization-Based Framework for Detecting Kernel Vulnerabilities ................................149
Jianfeng Pan, Guanglu Yan, and Xiaocao Fan, IceSword Lab, 360 Internet Security Center

kAFL: Hardware-Assisted Feedback Fuzzing for OS Kernels ........................................................167
Sergej Schumilo, Cornelius Aschermann, and Robert Gawlik, Ruhr-Universität Bochum; Sebastian Schinzel, Münster University of Applied Sciences; Thorsten Holz, Ruhr-Universität Bochum

Venerable Variadic Vulnerabilities Vanquished .................................................................183
Priyam Biswas, Purdue University; Alessandro Di Federico, Politecnico di Milano; Scott A. Carr, Purdue University; Prabhu Rajasekaran, Stijn Volckaert, Yeoul Na, and Michael Franz, University of California, Irvine; Mathias Payer, Purdue University

(continued on next page)
Side-Channel Countermeasures
Towards Practical Tools for Side Channel Aware Software Engineering: ‘Grey Box’ Modelling for Instruction Leakages .......................................................... 199
David McCann, Elisabeth Oswald, and Carolyn Whitnall, University of Bristol

Strong and Efficient Cache Side-Channel Protection using Hardware Transactional Memory .............. 217
Daniel Gruss, Graz University of Technology, Graz, Austria; Julian Lettner, University of California, Irvine, USA; Felix Schuster, Olya Ohrimenko, Istvan Haller, and Manuel Costa, Microsoft Research, Cambridge, UK

CacheD: Identifying Cache-Based Timing Channels in Production Software .................................. 235
Shuai Wang, Pei Wang, Xiao Liu, Danfeng Zhang, and Dinghao Wu, The Pennsylvania State University

Malware and Binary Analysis
BinSim: Trace-based Semantic Binary Diffing via System Call Sliced Segment Equivalence Checking .... 253
Jiang Ming, University of Texas at Arlington; Dongpeng Xu, Yufei Jiang, and Dinghao Wu, Pennsylvania State University

PlatPal: Detecting Malicious Documents with Platform Diversity ................................................. 271
Meng Xu and Taesoo Kim, Georgia Institute of Technology

Malton: Towards On-Device Non-Invasive Mobile Malware Analysis for ART ................................ 289
Lei Xue, The Hong Kong Polytechnic University; Yajin Zhou, unaffiliated; Ting Chen, University of Electronic Science and Technology of China; Xiapu Luo, The Hong Kong Polytechnic University; Guofei Gu, Texas A&M University

Censorship
Global Measurement of DNS Manipulation .......................................................... 307
Paul Pearce, UC Berkeley; Ben Jones, Princeton; Frank Li, UC Berkeley; Roya Ensafi and Nick Feamster, Princeton; Nick Weaver, ICSI; Vern Paxson, UC Berkeley

Characterizing the Nature and Dynamics of Tor Exit Blocking ............................................. 325
Rachee Singh, University of Massachusetts – Amherst; Rishab Nithyanand, Stony Brook University; Sadia Afroz, University of California, Berkeley and International Computer Science Institute; Paul Pearce, UC Berkeley; Michael Carl Tschantz, International Computer Science Institute; Phillipa Gill, University of Massachusetts – Amherst; Vern Paxson, University of California, Berkeley and International Computer Science Institute

DeTor: Provably Avoiding Geographic Regions in Tor ............................................................. 343
Zhihao Li, Stephen Herwig, and Dave Levin, University of Maryland

Embedded Systems
SmartAuth: User-Centered Authorization for the Internet of Things .......................................... 361
Yuan Tian, Carnegie Mellon University; Nan Zhang, Indiana University, Bloomington; Yueh-Hsun Lin, Samsung; Xiaofeng Wang, Indiana University, Bloomington; Blase Ur, University of Chicago; Xianzheng Guo and Patrick Tague, Carnegie Mellon University

AWARE: Preventing Abuse of Privacy-Sensitive Sensors via Operation Bindings .......................... 379

6thSense: A Context-aware Sensor-based Attack Detector for Smart Devices .............................. 397
Amit Kumar Sikder, Hidayet Aksu, and A. Selcuk Uluagac, Florida International University
Networking Security

Identifier Binding Attacks and Defenses in Software-Defined Networks .............................................................. 415
Samuel Jero, Purdue University; William Koch, Boston University; Richard Skowyra and Hamed Okhravi, MIT
Lincoln Laboratory; Cristina Nita-Rotaru, Northeastern University; David Bigelow, MIT Lincoln Laboratory

HELP: Helper-Enabled In-Band Device Pairing Resistant Against Signal Cancellation ................................. 433
Nirnimesh Ghose, Loukas Lazos, and Ming Li, Electrical and Computer Engineering, University of Arizona,
Tucson, AZ

Attacking the Brain: Races in the SDN Control Plane ......................................................................................... 451
Lei Xu, Jeff Huang, and Sungmin Hong, Texas A&M University; Jialong Zhang, IBM Research; Guofei Gu, Texas
A&M University

Targeted Attacks

Detecting Credential Spearphishing Attacks in Enterprise Settings ................................................................. 469
Grant Ho, UC Berkeley; Aashish Sharma, The Lawrence Berkeley National Laboratory; Mobin Javed, UC
Berkeley; Vern Paxson, UC Berkeley and ICSI; David Wagner, UC Berkeley

SLEUTH: Real-time Attack Scenario Reconstruction from COTS Audit Data ..................................................... 487
Md Nahid Hossain, Stony Brook University; Sadegh M. Milajerdi, University of Illinois at Chicago; Junao Wang,
Stony Brook University; Birhanu Estete and Rigel Gjomemo, University of Illinois at Chicago; R. Sekar and
Scott Stoller, Stony Brook University; V.N. Venkatakrishnan, University of Illinois at Chicago

When the Weakest Link is Strong: Secure Collaboration in the Case of the Panama Papers ..................... 505
Susan E. McGregor, Columbia Journalism School; Elizabeth Anne Watkins, Columbia University; Mahdi
Nasrullah Al-Ameen and Kelly Caine, Clemson University; Franziska Roesner, University of Washington

Trusted Hardware

Hacking in Darkness: Return-oriented Programming against Secure Enclaves .............................................. 523
Jaehyuk Lee and Jinsoo Jang, KAIST; Yeongjin Jang, Georgia Institute of Technology; Nohyun Kwak, Yeseul
Choi, and Changho Choi, KAIST; Tae soo Kim, Georgia Institute of Technology; Marcus Peinado, Microsoft
Research; Brent Byunghoon Kang, KAIST

vTZ: Virtualizing ARM TrustZone ...................................................... 541
Zhichao Hua, Jinyu Gu, Yubin Xia, and Haibo Chen, Institute of Parallel and Distributed Systems, Shanghai
Jiao Tong University; Shanghai Key Laboratory of Scalable Computing and Systems, Shanghai Jiao Tong
University; Binyu Zhang, Institute of Parallel and Distributed Systems, Shanghai Jiao Tong University; Haibing
Guan, Shanghai Key Laboratory of Scalable Computing and Systems, Shanghai Jiao Tong University

Inferring Fine-grained Control Flow Inside SGX Enclaves with Branch Shadowing ................................... 557
Sangho Lee, Ming-Wei Shih, Prasun Gera, Taesoo Kim, and Hyesoon Kim, Georgia Institute of Technology; Marcus Peinado, Microsoft Research

Authentication

AuthentiCall: Efficient Identity and Content Authentication for Phone Calls .............................................. 575
Bradley Reaves, North Carolina State University; Logan Blue, Hadi Abdullah, Luis Vargas, Patrick Traynor, and
Thomas Shrimpton, University of Florida

Picking Up My Tab: Understanding and Mitigating Synchronized Token Lifting and Spending
in Mobile Payment .................................................................................................................. 593
Xiaolong Bai, Tsinghua University; Zhe Zhou, The Chinese University of Hong Kong; Xiaofeng Wang,
Indiana University Bloomington; Zhou Li, IEEE Member; Xianghang Mi and Nan Zhang, Indiana University
Bloomington; Tongxin Li, Peking University; Shi-Min Hu, Tsinghua University; Kehuan Zhang, The Chinese
University of Hong Kong

(continued on next page)
TrustBase: An Architecture to Repair and Strengthen Certificate-based Authentication .......................... 609
Mark O’Neill, Scott Heidbrink, Scott Ruoti, Jordan Whitehead, Dan Bunker, Luke Dickinson, Travis Hendershot,
Joshua Reynolds, Kent Seamons, and Daniel Zappala, Brigham Young University

Malware and Obfuscation

Transcend: Detecting Concept Drift in Malware Classification Models ................................. 625
Roberto Jordaney, Royal Holloway, University of London; Kumar Sharad, NEC Laboratories Europe; Santanu
K. Dash, University College London; Zhi Wang, Nankai University; Davide Papini, Elettronica S.p.A.; Ilia
Nouretdinov and Lorenzo Cavallaro, Royal Holloway, University of London

Syntia: Synthesizing the Semantics of Obfuscated Code .......................................................... 643
Tim Blazytko, Moritz Contag, Cornelius Aschermann, and Thorsten Holz, Ruhr-Universität Bochum

Predicting the Resilience of Obfuscated Code Against Symbolic Execution Attacks via
Machine Learning ......................................................................................................................... 661
Sebastian Banescu, Technische Universität München; Christian Collberg, University of Arizona; Alexander
Pretschner, Technische Universität München

Web Security I

Extension Breakdown: Security Analysis of Browsers Extension Resources Control Policies .............. 679
Iskander Sanchez-Rola and Igor Santos, DeustoTech, University of Deusto; Davide Balzarotti, Eurecom

CCSP: Controlled Relaxation of Content Security Policies by Runtime Policy Composition ................ 695
Stefano Calzavara, Alvise Rabitti, and Michele Bugliesi, Università Ca’ Foscari Venezia

Same-Origin Policy: Evaluation in Modern Browsers ....................................................................... 713
Jörg Schwenk, Marcus Niemietz, and Christian Mainka, Horst Görtz Institute for IT Security, Chair for Network
and Data Security, Ruhr-University Bochum

Privacy

Locally Differentially Private Protocols for Frequency Estimation .................................................. 729
Tianhao Wang, Jeremiah Blocki, and Ninghui Li, Purdue University; Somesh Jha, University of Wisconsin
Madison

BLENDER: Enabling Local Search with a Hybrid Differential Privacy Model .................................... 747
Brendan Avent and Aleksandra Korolova, University of Southern California; David Zeber and Torgeir Hovden,
Mozilla; Benjamin Livshits, Imperial College London

Computer Security, Privacy, and DNA Sequencing: Compromising Computers with Synthesized DNA,
Privacy Leaks, and More .............................................................................................................. 765
Peter Ney, Karl Koscher, Lee Organick, Luis Ceze, and Tadayoshi Kohno, University of Washington

Systems Security II

BootStomp: On the Security of Bootloaders in Mobile Devices ...................................................... 781
Nilo Redini, Aravind Machiry, Dipanjan Das, Yanick Fratantonio, Antonio Bianchi, Eric Gustafson, Yan
Shoshtaiashvili, Christopher Kruegel, and Giovanni Vigna, UC Santa Barbara

Seeing Through The Same Lens: Introspecting Guest Address Space At Native Speed .................... 799
Siqi Zhao and Xuhua Ding, Singapore Management University; Wen Xu, Georgia Institute of Technology;
Dawu Gu, Shanghai JiaoTong University

Oscar: A Practical Page-Permissions-Based Scheme for Thwarting Dangling Pointers ....................... 815
Thurston H.Y. Dang, University of California, Berkeley; Petros Maniatis, Google Brain; David Wagner,
University of California, Berkeley
### Web Security II

**PDF Mirage: Content Masking Attack Against Information-Based Online Services** .......................... 833  
Ian Markwood, Dakun Shen, Yao Liu, and Zhuo Lu, *University of South Florida*

**Loophole: Timing Attacks on Shared Event Loops in Chrome** .......................... 849  
Pepe Vila, *IMDEA Software Institute & Technical University of Madrid (UPM)*; Boris Köpf, *IMDEA Software Institute*

**Game of Registrars: An Empirical Analysis of Post-Expiration Domain Name Takeovers** .......................... 865  
Tobias Lauinger, *Northeastern University*; Abdelberi Chaabane, *Nokia Bell Labs*; Ahmet Salih Buyukkayhan, *Northeastern University*; Kaan Onarlioglu, [website](http://www.onarlioglu.com); William Robertson, *Northeastern University*

### Applied Cryptography

**Speeding up detection of SHA-1 collision attacks using unavoidable attack conditions** .......................... 881  
Marc Stevens, CWI; Daniel Shumow, *Microsoft Research*

**Phoenix: Rebirth of a Cryptographic Password-Hardening Service** .......................... 899  

**Vale: Verifying High-Performance Cryptographic Assembly Code** .......................... 917  

### Web Security III

**Exploring User Perceptions of Discrimination in Online Targeted Advertising** .......................... 935  
Angelisa C. Plane, Elissa M. Redmiles, and Michelle L. Mazurek, *University of Maryland*; Michael Carl Tschantz, *International Computer Science Institute*

**Measuring the Insecurity of Mobile Deep Links of Android** .......................... 953  
Fang Liu, Chun Wang, Andres Pico, Danfeng Yao, and Gang Wang, *Virginia Tech*

**How the Web Tangled Itself: Uncovering the History of Client-Side Web (In)Security** .......................... 971  
Ben Stock, *CISPA, Saarland University*; Martin Johns, *SAP SE*; Marius Steffens and Michael Backes, *CISPA, Saarland University*

### Software Security

**Towards Efficient Heap Overflow Discovery** .......................... 989  
Xiangkun Jia, *TCA/SKLCS, Institute of Software, Chinese Academy of Sciences*; Chao Zhang, *Institute for Network Science and Cyberspace, Tsinghua University*; Purui Su, Yi Yang, Huafeng Huang, and Dengguo Feng, *TCA/SKLCS, Institute of Software, Chinese Academy of Sciences*

**DR. CHECKER: A Soundy Analysis for Linux Kernel Drivers** .......................... 1007  
Aravind Machiry, Chad Spensky, Jake Corina, Nick Stephens, Christopher Kruegel, and Giovanni Vigna, *UC Santa Barbara*

**Dead Store Elimination (Still) Considered Harmful** .......................... 1025  

### Side-Channel Attacks II

**Telling Your Secrets Without Page Faults: Stealthy Page Table-Based Attacks on Enclaved Execution** .......................... 1041  

(continued on next page)
Software Integrity

**Adaptive Android Kernel Live Patching** ......................................................... 1253
Yue Chen, *Florida State University*; Yulong Zhang, *Baidu* X-Lab; Zhi Wang, *Florida State University*
Liangzhao Xia, Chenfu Bao, and Tao Wei, *Baidu* X-Lab

**CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds** ................................................................. 1271
Kirill Nikitin, Eleftherios Kokoris-Kogias, Philipp Jovanovic, Nicolas Gailly, and Linus Gasser, *École polytechnique fédérale de Lausanne* (EPFL);
Ismail Khoffi, *University of Bonn*;
Justin Cappos, *New York University*;
Bryan Ford, *École polytechnique fédérale de Lausanne* (EPFL)

**ROTE: Rollback Protection for Trusted Execution** .............................................. 1289
Sinisa Matetic, Mansoor Ahmed, Kari Kostiainen, Aritra Dhar, David Sommer, and Arthur Gervais, *ETH Zurich*
Ari Juels, *Cornell Tech*; Srdjan Capkun, *ETH Zurich*

Crypto Deployment

**A Longitudinal, End-to-End View of the DNSSEC Ecosystem** ................................. 1307
Taejoong Chung, *Northeastern University*; Roland van Rijswijk-Deij, *University of Twente* and SURFnet bv;
Balakrishnan Chandrasekaran, *TU Berlin*; David Choffnes, *Northeastern University*;
Dave Levin, *University of Maryland*; Bruce M. Maggs, *Duke University* and *Akamai Technologies*;
Alan Mislove and Christo Wilson, *Northeastern University*

**Measuring HTTPS Adoption on the Web** ........................................................... 1323
Adrienne Porter Felt, *Google*; Richard Barnes, *Cisco*; April King, *Mozilla*;
Chris Palmer, Chris Bentzel, and Parisa Tabriz, *Google*

**“I Have No Idea What I’m Doing” - On the Usability of Deploying HTTPS** .............. 1339
Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, and Edgar Weippl, *SBA Research*

Privacy Attacks & Defense

**Beauty and the Burst: Remote Identification of Encrypted Video Streams** ............... 1357
Roei Schuster, *Tel Aviv University*; Vitaly Shmatikov, *Cornell Tech*; Eran Tromer, *Tel Aviv University*, *Columbia University*

**Walkie-Talkie: An Efficient Defense Against Passive Website Fingerprinting Attacks** 1375
Tao Wang, *Hong Kong University of Science and Technology*; Ian Goldberg, *University of Waterloo*

**A Privacy Analysis of Cross-device Tracking** .................................................... 1391
Sebastian Zimmeck, *Carnegie Mellon University*; Jie S. Li and Hyungtae Kim, *unaffiliated*;
Steven M. Bellovin and Tony Jebara, *Columbia University*

Blockchains

**SmartPool: Practical Decentralized Pooled Mining** .............................................. 1409
Loi Luu, *National University of Singapore*; Yaron Velner, *The Hebrew University of Jerusalem*;
Jason Teutsch, *TrueBit Foundation*; Prateek Saxena, *National University of Singapore*

**REM: Resource-Efficient Mining for Blockchains** .............................................. 1427
Fan Zhang, Ittay Eyal, and Robert Escriva, *Cornell University*; Ari Juels, *Cornell Tech*;
Robbert van Renesse, *Cornell University*

Databases

**Ensuring Authorized Updates in Multi-user Database-Backed Applications** ............... 1445
Kevin Eykholt, Atul Prakash, and Barzan Mozafari, *University of Michigan Ann Arbor*

**Qapla: Policy compliance for database-backed systems** ....................................... 1463
Aastha Mehta and Eslam Elnikety, *Max Planck Institute for Software Systems* (MPI-SWS);
Katura Harvey, *University of Maryland, College Park* and *Max Planck Institute for Software Systems* (MPI-SWS);
Deepak Garg and Peter Druschel, *Max Planck Institute for Software Systems* (MPI-SWS)