

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zurich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology Madras, Chennai, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7410>

Michael Bailey · Thorsten Holz
Manolis Stamatogiannakis · Sotiris Ioannidis (Eds.)

Research in Attacks, Intrusions, and Defenses

21st International Symposium, RAID 2018
Heraklion, Crete, Greece, September 10–12, 2018
Proceedings

Preface

Welcome to the 21st International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2018)!

This year, RAID 2018 received *145 submissions* of which 32 were accepted (*21% acceptance rate*). As in previous years, a double-blind reviewing process was used to ensure that the reviewers remained unaware of the authors, names or affiliations during the discussion. Each paper received at least three reviews and the final decision for each paper was made during a face-to-face Program Committee (PC) meeting following the IEEE Symposium on Security and Privacy in San Jose (CA) in May 2018.

The quality and commitment of the PC is paramount to the success of any conference. This year, roughly 75% of the PC members were from academia and the remaining quarter from government, industry, or a mix. Roughly 20% of the PC was from outside the USA. This year's PC included ten new PC members who have never served on the RAID PC and 23 who have served before, including three members, each serving for their eighth time.

While RAID has previously awarded an "*influential paper*" award every five years for papers appearing at RAID that have been important in the community, this year's RAID saw the permanent addition of a yearly *best paper award*. A subset of five PC members was selected by the chairs and served as the award committee. A two-phase process was used in which papers were nominated and discussed amongst the awards committee and then a vote amongst the committee decided the award winner. This year we were also pleased to offer a "*community service*" award to recognize an outstanding contribution to the security community and to RAID in particular. This award, given to Marc Dacier, recognizes the pivotal role he played in creating and shaping the RAID conference we enjoy today.

RAID only exists because of the community that supports it. Indeed, RAID is completely self-funded. Every organizer independently shoulders the financial risks associated with its organization. The sponsors, therefore, play a very important role and ensure that the registration fees remain very reasonable. Therefore, we want to take this opportunity to thank Niometrics and Comcast for their generous sponsorships to RAID 2018. We, of course, are very grateful to the general chair, Sotiris Ioannidis, from FORTH-ICS, and his assembled team for ensuring that the conference ran smoothly. Special thanks go to the local arrangement and sponsor chair, Ioannis Askoxylakis, also from FORTH-ICS; to the publication chair, Manolis Stamatogiannakis, from Vrije Universiteit Amsterdam; and to the publicity chair, Michalis Polychronakis, from Stony Brook University.

We hope you enjoyed the conference!

August 2018

Michael Bailey
Thorsten Holz

Organization

Organizing Committee

General Chair

Sotiris Ioannidis Foundation for Research and Technology – Hellas, Greece

Program Committee Chair

Michael Bailey University of Illinois at Urbana-Champaign, USA

Program Committee Co-chair

Thorsten Holz Ruhr-Universität Bochum, Germany

Publication Chair

Manolis
Stamatogiannakis Vrije Universiteit Amsterdam, The Netherlands

Publicity Chair

Michalis
Polychronakis Stony Brook University, USA

Local Arrangements and Sponsor Chair

Ioannis Askoxylakis Foundation for Research and Technology – Hellas, Greece

Program Committee

Sadia Afroz ICSI, UC Berkeley, USA
Magnus Almgren Chalmers University of Technology, Sweden
Johanna Amann ICSI, UC Berkeley, USA
Leyla Bilge Symantec Research Labs, France
Srdjan Capkun ETH Zurich, Switzerland
Lorenzo Cavallaro Royal Holloway University of London, UK
Lucas Davi University of Duisburg-Essen, Germany
Tudor Dumitras The University of Maryland, USA
Zakir Durumeric Stanford University, USA
Manuel Egele Boston University, USA
Roya Ensafi University of Michigan, USA
Giulia Fanti Carnegie Mellon University, USA
Carrie Gates Securelytix, USA
Jon Giffin Google, USA
Guofei Gu Texas A&M University, USA

Amin Kharraz	University of Illinois at Urbana-Champaign, USA
Tim Leek	MIT Lincoln Laboratory, USA
Corrado Leita	Lastline, UK
Bo Li	University of Illinois at Urbana-Champaign, USA
Zane Ma	University of Illinois at Urbana-Champaign, USA
Fabian Monrose	University of North Carolina at Chapel Hill, USA
Benjamin Morin	French Network and Information Security Agency (ANSSI), France
Alina Oprea	Northeastern University, USA
Christina Pöpper	New York University Abu Dhabi, UAE
Jason Polakis	University of Illinois at Chicago, USA
Vaibhav Rastogi	University of Wisconsin, USA
Joshua Reynolds	University of Illinois at Urbana-Champaign, USA
William Robertson	Northeastern University, USA
Brendan Saltaformaggio	Georgia Institute of Technology, USA
Angelos Stavrou	George Mason University, USA
Kurt Thomas	Google, USA
Eric Wustrow	University of Colorado Boulder, USA
Dongyan Xu	Purdue University, USA

External Reviewers

Christopher Wardlaw Fletcher	University of Illinois at Urbana-Champaign, USA
Jan Werner	University of North Carolina at Chapel Hill, USA
Joshua Mason	University of Illinois at Urbana-Champaign, USA
Roberto Perdisci	University of Georgia, USA

Steering Committee

Johanna Amann	International Computer Science Institute, USA
Davide Balzarotti	Eurecom Graduate School and Research Center, France
Marc Dacier	Eurecom Graduate School and Research Center, France
Zhiqiang Lin	University of Texas at Dallas, USA
Mathias Payer	Purdue University, USA
Michalis Polychronakis	Stony Brook University, USA
Salvatore Stolfo	Columbia University, USA
Angelos Stavrou	George Mason University, USA

Sponsors

Gold Sponsor

Niometrics – <https://www.niometrics.com/>

N I O M E T R I C S

Bronze Sponsor

Comcast – <https://corporate.comcast.com/>



Contents

Attacks

PROTEUS: Detecting Android Emulators from Instruction-Level Profiles	3
<i>Onur Sahin, Ayse K. Coskun, and Manuel Egele</i>	
BabelView: Evaluating the Impact of Code Injection Attacks in Mobile Webviews	25
<i>Claudio Rizzo, Lorenzo Cavallaro, and Johannes Kinder</i>	
Defeating Software Mitigations Against Rowhammer: A Surgical Precision Hammer	47
<i>Andrei Tatar, Cristiano Giuffrida, Herbert Bos, and Kaveh Razavi</i>	

Intrusion Detection and Prevention

Reading Between the Lines: Content-Agnostic Detection of Spear-Phishing Emails	69
<i>Hugo Gascon, Steffen Ullrich, Benjamin Stritter, and Konrad Rieck</i>	
Backdoors: Definition, Deniability and Detection	92
<i>Sam L. Thomas and Aurélien Francillon</i>	
RWGuard: A Real-Time Detection System Against Cryptographic Ransomware	114
<i>Shagufa Mehnaz, Anand Mudgerikar, and Elisa Bertino</i>	

DDoS Attacks

DNS Unchained: Amplified Application-Layer DoS Attacks Against DNS Authoritatives	139
<i>Jonas Bushart and Christian Rossow</i>	
Control Plane Reflection Attacks in SDNs: New Attacks and Countermeasures	161
<i>Menghao Zhang, Guanyu Li, Lei Xu, Jun Bi, Guofei Gu, and Jiasong Bai</i>	
Proof-of-Blackouts? How Proof-of-Work Cryptocurrencies Could Affect Power Grids	184
<i>Johanna Ullrich, Nicholas Stifter, Aljosha Judmayer, Adrian Dabrowski, and Edgar Weippl</i>	

Passwords, Accounts, and Users

Characterizing Eve: Analysing Cybercrime Actors in a Large Underground Forum 207
Sergio Pastrana, Alice Hutchings, Andrew Caines, and Paula Buttery

SybilBlind: Detecting Fake Users in Online Social Networks Without Manual Labels 228
Binghui Wang, Le Zhang, and Neil Zhenqiang Gong

GuidedPass: Helping Users to Create Strong and Memorable Passwords 250
Simon S. Woo and Jelena Mirkovic

Machine Learning for Computer Security

Fine-Pruning: Defending Against Backdooring Attacks on Deep Neural Networks 273
Kang Liu, Brendan Dolan-Gavitt, and Siddharth Garg

Dictionary Extraction and Detection of Algorithmically Generated Domain Names in Passive DNS Traffic 295
Mayana Pereira, Shaun Coleman, Bin Yu, Martine DeCock, and Anderson Nascimento

OTter: A Scalable High-Resolution Encrypted Traffic Identification Engine 315
Eva Papadogiannaki, Constantinos Halevidis, Periklis Akritidis, and Lazaros Koromilas

Hardware-Assisted Security

Hardware Assisted Randomization of Data 337
Brian Belleville, Hyungon Moon, Jangseop Shin, Dongil Hwang, Joseph M. Nash, Seonhwa Jung, Yeoul Na, Stijn Volckaert, Per Larsen, Yunheung Paek, and Michael Franz

MicroStache: A Lightweight Execution Context for In-Process Safe Region Isolation 359
Lucian Mogosanu, Ashay Rane, and Nathan Dautenhahn

CryptMe: Data Leakage Prevention for Unmodified Programs on ARM Devices 380
Chen Cao, Le Guan, Ning Zhang, Neng Gao, Jingqiang Lin, Bo Luo, Peng Liu, Ji Xiang, and Wenjing Lou

Software Security

PartiSan: Fast and Flexible Sanitization via Run-Time Partitioning 403
*Julian Lettner, Dokyung Song, Taemin Park, Per Larsen,
 Stijn Volckaert, and Michael Franz*

τ CFI: Type-Assisted Control Flow Integrity for x86-64 Binaries 423
*Paul Muntean, Matthias Fischer, Gang Tan, Zhiqiang Lin,
 Jens Grossklags, and Claudia Eckert*

Trusted Execution Path for Protecting Java Applications Against
 Deserialization of Untrusted Data 445
*Stefano Cristalli, Edoardo Vignati, Danilo Bruschi,
 and Andrea Lanzi*

Malware

Error-Sensor: Mining Information from HTTP Error Traffic
 for Malware Intelligence 467
*Jialong Zhang, Jiyong Jang, Guofei Gu, Marc Ph. Stoecklin,
 and Xin Hu*

Generic Black-Box End-to-End Attack Against State of the Art
 API Call Based Malware Classifiers 490
Ishai Rosenberg, Asaf Shabtai, Lior Rokach, and Yuval Elovici

Next Generation P2P Botnets: Monitoring Under Adverse Conditions 511
*Leon Böck, Emmanouil Vasilomanolakis, Max Mühlhäuser,
 and Shankar Karuppayah*

IoT/CPS Security

Malicious IoT Implants: Tampering with Serial Communication
 over the Internet 535
Philipp Morgner, Stefan Pfennig, Dennis Salzner, and Zinaida Benenson

Before Toasters Rise Up: A View into the Emerging IoT
 Threat Landscape 556
Pierre-Antoine Vervier and Yun Shen

Statistical Similarity of Critical Infrastructure Network Traffic Based
 on Nearest Neighbor Distances 577
*Jeong-Han Yun, Yoonho Hwang, Woomyo Lee, Hee-Kap Ahn,
 and Sin-Kyu Kim*

Security Measurements

PostScript Undead: Pwning the Web with a 35 Years Old Language 603
Jens Müller, Vladislav Mladenov, Dennis Felsch, and Jörg Schwenk

Identifying Key Leakage of Bitcoin Users 623
Michael Brengel and Christian Rossow

Defenses

Furnace: Self-service Tenant VMI for the Cloud 647
Micah Bushouse and Douglas Reeves

ShadowMonitor: An Effective In-VM Monitoring Framework with
Hardware-Enforced Isolation. 670
Bin Shi, Lei Cui, Bo Li, Xudong Liu, Zhiyu Hao, and Haiying Shen

KASR: A Reliable and Practical Approach to Attack Surface Reduction
of Commodity OS Kernels 691
*Zhi Zhang, Yueqiang Cheng, Surya Nepal, Dongxi Liu, Qingni Shen,
and Fethi Rabhi*

Author Index 711