

Contents – Part I

From Intrusion Detection to Software Design ............................................. 1
Sandro Etalle

Justifying Security Measures — a Position Paper ................................. 11
Cormac Herley

The Once and Future Onion ................................................................. 18
Paul Syverson

Tightly Secure Ring-LWE Based Key Encapsulation
with Short Ciphertexts ................................................................. 29
Martin R. Albrecht, Emmanuela Orsini, Kenneth G. Paterson,
Guy Peer, and Nigel P. Smart

Tree-Based Cryptographic Access Control ........................................... 47
James Alderman, Naomi Farley, and Jason Crampton

Source Code Authorship Attribution Using Long Short-Term Memory
Based Networks .................................................................................. 65
Bander Alsulami, Edwin Dauber, Richard Harang, Spiros Mancoridis,
and Rachel Greenstadt

Is My Attack Tree Correct? ................................................................. 83
Maxime Audinot, Sophie Pinchinat, and Barbara Kordy

Server-Aided Secure Computation with Off-line Parties .................... 103
Foteini Baldimtsi, Dimitrios Papadopoulos, Stavros Papadopoulos,
Alessandra Scafuro, and Nikos Triandopoulos

We Are Family: Relating Information-Flow Trackers .......................... 124
Musard Balliu, Daniel Schoepe, and Andrei Sabelfeld

Labeled Homomorphic Encryption: Scalable and Privacy-Preserving
Processing of Outsourced Data .......................................................... 146
Manuel Barbosa, Dario Catalano, and Dario Fiore

MTD CBITS: Moving Target Defense for Cloud-Based IT Systems ...... 167
Alexandru G. Bardas, Sathya Chandran Sundaramurthy,
Xinning Ou, and Scott A. DeLoach

Modular Verification of Protocol Equivalence in the Presence
of Randomness .................................................................................. 187
Matthew S. Bauer, Rohit Chadha, and Mahesh Viswanathan
Non-interactive Provably Secure Attestations for Arbitrary RSA Prime Generation Algorithms .......................................................... 206
   Fabrice Benhamouda, Houda Ferradi, Rémi Géraud, and David Naccache

Reusing Nonces in Schnorr Signatures: (and Keeping It Secure...) .......... 224
   Marc Beunardeau, Aisling Connolly, Houda Ferradi, Rémi Géraud, David Naccache, and Damien Vergnaud

WebPol: Fine-Grained Information Flow Policies for Web Browsers ............ 242
   Abhishek Bichhawat, Vineet Rajani, Jinank Jain, Deepak Garg, and Christian Hammer

Verifying Constant-Time Implementations by Abstract Interpretation .......... 260
   Sandrine Blazy, David Pichardie, and Alix Trieu

Mirage: Toward a Stealthier and Modular Malware Analysis Sandbox for Android .......................................................... 278
   Lorenzo Bordoni, Mauro Conti, and Riccardo Spolaor

Zero Round-Trip Time for the Extended Access Control Protocol .............. 297
   Jacqueline Brendel and Marc Fischlin

Server-Supported RSA Signatures for Mobile Devices .......................... 315
   Ahto Buldas, Aivo Kalu, Peeter Laud, and Mart Oruaas

Verifiable Document Redacting ...................................................... 334
   Hervé Chabanne, Rodolphe Hugel, and Julien Keuffer

Securing Data Analytics on SGX with Randomization .......................... 352
   Swarup Chandra, Vishal Karande, Zhiqiang Lin, Latifur Khan, Murat Kantarcioğlu, and Bhavani Thuraisingham

DeltaPhish: Detecting Phishing Webpages in Compromised Websites ........ 370
   Igino Corona, Battista Biggio, Matteo Contini, Luca Piras, Roberto Corda, Mauro Meru, Guido Mureddu, Davide Ariu, and Fabio Roli

Secure Authentication in the Grid: A Formal Analysis of DNP3: SAv5 ....... 389
   Cas Cremers, Martin Dehnel-Wild, and Kevin Milner

Per-Session Security: Password-Based Cryptography Revisited ............... 408
   Grégory Demay, Peter Gaži, Ueli Maurer, and Björn Tackmann

AVR Processors as a Platform for Language-Based Security ................... 427
   Florian Dewald, Heiko Mantel, and Alexandra Weber
A Better Composition Operator for Quantitative Information Flow Analyses ................................................................. 446

Kai Engelhardt

Analyzing the Capabilities of the CAN Attacker ................................. 464

Sibylle Fröschle and Alexander Stühring

Author Index ................................................................. 483
## Contents – Part II

Automated Analysis of Equivalence Properties for Security Protocols Using Else Branches ......................................................... 1  
*Ivan Gazeau and Steve Kremer*

Quantifying Web Adblocker Privacy .............................................. 21  
*Arthur Gervais, Alexandros Filios, Vincent Lenders, and Srdjan Capkun*

More Efficient Structure-Preserving Signatures - Or: Bypassing the Type-III Lower Bounds ...................................................... 43  
*Essam Ghadafi*

Adversarial Examples for Malware Detection ................................. 62  
*Kathrin Grosse, Nicolas Papernot, Praveen Manoharan, Michael Backes, and Patrick McDaniel*

PerfWeb: How to Violate Web Privacy with Hardware Performance Events ............................................................................... 80  
*Berk Gulmezoglu, Andreas Zankl, Thomas Eisenbarth, and Berk Sunar*

Acoustic Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard-Drive Noise (‘DiskFiltration’) ......................................................... 98  
*Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, and Yuval Elovici*

DOMPurify: Client-Side Protection Against XSS and Markup Injection ................................................................. 116  
*Mario Heiderich, Christopher Späth, and Jörg Schwenk*

Preventing DNS Amplification Attacks Using the History of DNS Queries with SDN ................................................................. 135  
*Soyoung Kim, Sora Lee, Geumhwan Cho, Muhammad Ejaz Ahmed, Jaehoon (Paul) Jeong, and Hyoungshick Kim*

A Traceability Analysis of Monero’s Blockchain ................................. 153  
*Amrit Kumar, Clément Fischer, Shruti Tople, and Prateek Saxena*

Multi-rate Threshold FlipThem ...................................................... 174  
*David Leslie, Chris Sherfield, and Nigel P. Smart*

Practical Keystroke Timing Attacks in Sandboxed JavaScript ........................................................................... 191  
*Moritz Lipp, Daniel Gruss, Michael Schwarz, David Bidner, Clémentine Maurice, and Stefan Mangard*

On-Demand Time Blurring to Support Side-Channel Defense ................ 210  
*Weijie Liu, Debin Gao, and Michael K. Reiter*
VuRLE: Automatic Vulnerability Detection and Repair by Learning from Examples ................................................................. 229
   Siqi Ma, Ferdian Thung, David Lo, Cong Sun, and Robert H. Deng

Link-Layer Device Type Classification on Encrypted Wireless Traffic with COTS Radios ....................................................... 247
   Rajib Ranjan Maiti, Sandra Siby, Ragav Sridharan, and Nils Ole Tippenhauer

LeaPS: Learning-Based Proactive Security Auditing for Clouds ............... 265
   Suryadipta Majumdar, Yosr Jarraya, Momen Oqaily, Amir Alimohammadiifar, Makan Pourzandi, Lingyu Wang, and Mourad Debbabi

Identifying Multiple Authors in a Binary Program .................................. 286
   Xiaozhu Meng, Barton P. Miller, and Kwang-Sung Jun

Secure IDS Offloading with Nested Virtualization and Deep VM Introspection ................................................................. 305
   Shohei Miyama and Kenichi Kourai

Privacy Implications of Room Climate Data ........................................ 324
   Philipp Morgner, Christian Müller, Matthias Ring, Björn Eskofier, Christian Riess, Frederik Armknecht, and Zinaida Benenson

Network Intrusion Detection Based on Semi-supervised Variational Auto-Encoder ..................................................... 344
   Genki Osada, Kazumasa Omote, and Takashi Nishide

No Sugar but All the Taste! Memory Encryption Without Architectural Support .................................................. 362
   Panagiotis Papadopoulos, Giorgos Vasiliadis, Giorgos Christou, Evangelos Markatos, and Sotiris Ioannidis

Inference-Proof Updating of a Weakened View Under the Modification of Input Parameters ........................................ 381
   Joachim Biskup and Marcel Preuß

Preventing Advanced Persistent Threats in Complex Control Networks ....... 402
   Juan E. Rubio, Cristina Alcaraz, and Javier Lopez

Shortfall-Based Optimal Placement of Security Resources for Mobile IoT Scenarios ..................................................... 419
   Antonino Rullo, Edoardo Serra, Elisa Bertino, and Jorge Lobo
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boot Attestation: Secure Remote Reporting with Off-The-Shelf IoT Sensors</td>
<td>437</td>
</tr>
<tr>
<td>Steffen Schulz, Andrè Schaller, Florian Kohnhäuser, and Stefan Katzenbeisser</td>
<td></td>
</tr>
<tr>
<td>RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero</td>
<td>456</td>
</tr>
<tr>
<td>Shi-Feng Sun, Man Ho Au, Joseph K. Liu, and Tsz Hon Yuen</td>
<td></td>
</tr>
<tr>
<td>SePCAR: A Secure and Privacy-Enhancing Protocol for Car Access Provision</td>
<td>475</td>
</tr>
<tr>
<td>Iraklis Symeonidis, Abdelrahman Aly, Mustafa Asan Mustafa, Bart Mennink, Siemen Dhooghe, and Bart Preneel</td>
<td></td>
</tr>
<tr>
<td>Privacy-Preserving Decision Trees Evaluation via Linear Functions</td>
<td>494</td>
</tr>
<tr>
<td>Raymond K.H. Tai, Jack P.K. Ma, Yongjun Zhao, and Sherman S.M. Chow</td>
<td></td>
</tr>
<tr>
<td>Stringer: Measuring the Importance of Static Data Comparisons to Detect Backdoors and Undocumented Functionality</td>
<td>513</td>
</tr>
<tr>
<td>Sam L. Thomas, Tom Chothia, and Flavio D. Garcia</td>
<td></td>
</tr>
<tr>
<td>Generic Constructions for Fully Secure Revocable Attribute-Based Encryption</td>
<td>532</td>
</tr>
<tr>
<td>Kotoko Yamada, Nuttapong Attrapadung, Keita Emura, Goichiro Hanaoka, and Keisuke Tanaka</td>
<td></td>
</tr>
<tr>
<td>Enforcing Input Correctness via Certification in Garbled Circuit Evaluation</td>
<td>552</td>
</tr>
<tr>
<td>Yihua Zhang, Marina Blanton, and Fattaneh Bayatbabolghani</td>
<td></td>
</tr>
<tr>
<td>Author Index</td>
<td>571</td>
</tr>
</tbody>
</table>
Computer Security – ESORICS 2017
Foley, S.N.; Gollmann, D.; Snekkenes, E. (Eds.)
2017, XXI, 485 p. 106 illus., Softcover
ISBN: 978-3-319-66401-9