

Contents – Part I

From Intrusion Detection to Software Design	1
<i>Sandro Etalle</i>	
Justifying Security Measures — a Position Paper	11
<i>Cormac Herley</i>	
The Once and Future Onion	18
<i>Paul Syverson</i>	
Tightly Secure Ring-LWE Based Key Encapsulation with Short Ciphertexts	29
<i>Martin R. Albrecht, Emmanuela Orsini, Kenneth G. Paterson, Guy Peer, and Nigel P. Smart</i>	
Tree-Based Cryptographic Access Control	47
<i>James Alderman, Naomi Farley, and Jason Crampton</i>	
Source Code Authorship Attribution Using Long Short-Term Memory Based Networks	65
<i>Bander Alsulami, Edwin Dauber, Richard Harang, Spiros Mancoridis, and Rachel Greenstadt</i>	
Is My Attack Tree Correct?	83
<i>Maxime Audinot, Sophie Pinchinat, and Barbara Kordy</i>	
Server-Aided Secure Computation with Off-line Parties	103
<i>Foteini Baldimtsi, Dimitrios Papadopoulos, Stavros Papadopoulos, Alessandra Scafuro, and Nikos Triandopoulos</i>	
We Are Family: Relating Information-Flow Trackers	124
<i>Musard Balliu, Daniel Schoepe, and Andrei Sabelfeld</i>	
Labeled Homomorphic Encryption: Scalable and Privacy-Preserving Processing of Outsourced Data	146
<i>Manuel Barbosa, Dario Catalano, and Dario Fiore</i>	
MTD CBITS: Moving Target Defense for Cloud-Based IT Systems	167
<i>Alexandru G. Bardas, Sathya Chandran Sundaramurthy, Xinming Ou, and Scott A. DeLoach</i>	
Modular Verification of Protocol Equivalence in the Presence of Randomness	187
<i>Matthew S. Bauer, Rohit Chadha, and Mahesh Viswanathan</i>	

Non-interactive Provably Secure Attestations for Arbitrary RSA Prime Generation Algorithms	206
<i>Fabrice Benhamouda, Houda Ferradi, Rémi Géraud, and David Naccache</i>	
Reusing Nonces in Schnorr Signatures: (and Keeping It Secure...)	224
<i>Marc Beunardeau, Aisling Connolly, Houda Ferradi, Rémi Géraud, David Naccache, and Damien Vergnaud</i>	
WebPol: Fine-Grained Information Flow Policies for Web Browsers	242
<i>Abhishek Bichhawat, Vineet Rajani, Jinank Jain, Deepak Garg, and Christian Hammer</i>	
Verifying Constant-Time Implementations by Abstract Interpretation	260
<i>Sandrine Blazy, David Pichardie, and Alix Trieu</i>	
Mirage: Toward a Stealthier and Modular Malware Analysis Sandbox for Android	278
<i>Lorenzo Bordonì, Mauro Conti, and Riccardo Spolaor</i>	
Zero Round-Trip Time for the Extended Access Control Protocol	297
<i>Jacqueline Brendel and Marc Fischlin</i>	
Server-Supported RSA Signatures for Mobile Devices	315
<i>Ahto Buldas, Aivo Kalu, Peeter Laud, and Mart Oruaas</i>	
Verifiable Document Redacting.	334
<i>Hervé Chabanne, Rodolphe Hugel, and Julien Keuffer</i>	
Securing Data Analytics on SGX with Randomization	352
<i>Swarup Chandra, Vishal Karande, Zhiqiang Lin, Latifur Khan, Murat Kantarcioglu, and Bhavani Thuraisingham</i>	
DeltaPhish: Detecting Phishing Webpages in Compromised Websites	370
<i>Igino Corona, Battista Biggio, Matteo Contini, Luca Piras, Roberto Corda, Mauro Mereu, Guido Mureddu, Davide Ariu, and Fabio Roli</i>	
Secure Authentication in the Grid: A Formal Analysis of DNP3: SAV5	389
<i>Cas Cremers, Martin Dehnel-Wild, and Kevin Milner</i>	
Per-Session Security: Password-Based Cryptography Revisited	408
<i>Grégory Demay, Peter Gazi, Ueli Maurer, and Björn Tackmann</i>	
AVR Processors as a Platform for Language-Based Security	427
<i>Florian Dewald, Heiko Mantel, and Alexandra Weber</i>	

A Better Composition Operator for Quantitative Information Flow Analyses	446
<i>Kai Engelhardt</i>	
Analyzing the Capabilities of the CAN Attacker	464
<i>Sibylle Fröschle and Alexander Stühling</i>	
Author Index	483

Contents – Part II

Automated Analysis of Equivalence Properties for Security Protocols Using Else Branches	1
<i>Ivan Gazeau and Steve Kremer</i>	
Quantifying Web Adblocker Privacy	21
<i>Arthur Gervais, Alexandros Filios, Vincent Lenders, and Srdjan Capkun</i>	
More Efficient Structure-Preserving Signatures - Or: Bypassing the Type-III Lower Bounds	43
<i>Essam Ghadafi</i>	
Adversarial Examples for Malware Detection	62
<i>Kathrin Grosse, Nicolas Papernot, Praveen Manoharan, Michael Backes, and Patrick McDaniel</i>	
PerfWeb: How to Violate Web Privacy with Hardware Performance Events.	80
<i>Berk Gulmezoglu, Andreas Zankl, Thomas Eisenbarth, and Berk Sunar</i>	
Acoustic Data Exfiltration from Speakerless Air-Gapped Computers via Covert Hard-Drive Noise (‘DiskFiltration’)	98
<i>Mordechai Guri, Yosef Solewicz, Andrey Daidakulov, and Yuval Elovici</i>	
DOMPurify: Client-Side Protection Against XSS and Markup Injection	116
<i>Mario Heiderich, Christopher Späth, and Jörg Schwenk</i>	
Preventing DNS Amplification Attacks Using the History of DNS Queries with SDN.	135
<i>Soyoung Kim, Sora Lee, Geumhwan Cho, Muhammad Ejaz Ahmed, Jaehoon (Paul) Jeong, and Hyoungshick Kim</i>	
A Traceability Analysis of Monero’s Blockchain.	153
<i>Amrit Kumar, Clément Fischer, Shruti Tople, and Prateek Saxena</i>	
Multi-rate Threshold FlipThem	174
<i>David Leslie, Chris Sherfield, and Nigel P. Smart</i>	
Practical Keystroke Timing Attacks in Sandboxed JavaScript	191
<i>Moritz Lipp, Daniel Gruss, Michael Schwarz, David Bidner, Clémentine Maurice, and Stefan Mangard</i>	
On-Demand Time Blurring to Support Side-Channel Defense	210
<i>Weijie Liu, Debin Gao, and Michael K. Reiter</i>	

VuRLE: Automatic Vulnerability Detection and Repair by Learning from Examples	229
<i>Siqi Ma, Ferdian Thung, David Lo, Cong Sun, and Robert H. Deng</i>	
Link-Layer Device Type Classification on Encrypted Wireless Traffic with COTS Radios	247
<i>Rajib Ranjan Maiti, Sandra Siby, Ragav Sridharan, and Nils Ole Tippenhauer</i>	
LeaPS: Learning-Based Proactive Security Auditing for Clouds	265
<i>Suryadipta Majumdar, Yosr Jarraya, Momen Oqaily, Amir Alimohammadifar, Makan Pourzandi, Lingyu Wang, and Mourad Debbabi</i>	
Identifying Multiple Authors in a Binary Program.	286
<i>Xiaozhu Meng, Barton P. Miller, and Kwang-Sung Jun</i>	
Secure IDS Offloading with Nested Virtualization and Deep VM Introspection	305
<i>Shohei Miyama and Kenichi Kourai</i>	
Privacy Implications of Room Climate Data	324
<i>Philipp Morgner, Christian Müller, Matthias Ring, Björn Eskofier, Christian Riess, Frederik Armknecht, and Zinaida Benenson</i>	
Network Intrusion Detection Based on Semi-supervised Variational Auto-Encoder.	344
<i>Genki Osada, Kazumasa Omote, and Takashi Nishide</i>	
No Sugar but All the Taste! Memory Encryption Without Architectural Support	362
<i>Panagiotis Papadopoulos, Giorgos Vasiliadis, Giorgos Christou, Evangelos Markatos, and Sotiris Ioannidis</i>	
Inference-Proof Updating of a Weakened View Under the Modification of Input Parameters	381
<i>Joachim Biskup and Marcel Preuß</i>	
Preventing Advanced Persistent Threats in Complex Control Networks	402
<i>Juan E. Rubio, Cristina Alcaraz, and Javier Lopez</i>	
Shortfall-Based Optimal Placement of Security Resources for Mobile IoT Scenarios	419
<i>Antonino Rullo, Edoardo Serra, Elisa Bertino, and Jorge Lobo</i>	

Boot Attestation: Secure Remote Reporting with Off-The-Shelf IoT Sensors	437
<i>Steffen Schulz, André Schaller, Florian Kohnhäuser, and Stefan Katzenbeisser</i>	
RingCT 2.0: A Compact Accumulator-Based (Linkable Ring Signature) Protocol for Blockchain Cryptocurrency Monero.	456
<i>Shi-Feng Sun, Man Ho Au, Joseph K. Liu, and Tsz Hon Yuen</i>	
SePCAR: A Secure and Privacy-Enhancing Protocol for Car Access Provision	475
<i>Iraklis Symeonidis, Abdelrahman Aly, Mustafa Asan Mustafa, Bart Mennink, Siemen Dhooghe, and Bart Preneel</i>	
Privacy-Preserving Decision Trees Evaluation via Linear Functions.	494
<i>Raymond K.H. Tai, Jack P.K. Ma, Yongjun Zhao, and Sherman S.M. Chow</i>	
Stringer: Measuring the Importance of Static Data Comparisons to Detect Backdoors and Undocumented Functionality.	513
<i>Sam L. Thomas, Tom Chothia, and Flavio D. Garcia</i>	
Generic Constructions for Fully Secure Revocable Attribute-Based Encryption.	532
<i>Kotoko Yamada, Nuttapong Attrapadung, Keita Emura, Goichiro Hanaoka, and Keisuke Tanaka</i>	
Enforcing Input Correctness via Certification in Garbled Circuit Evaluation	552
<i>Yihua Zhang, Marina Blanton, and Fattaneh Bayatbabolghani</i>	
Author Index	571

Computer Security – ESORICS 2017

22nd European Symposium on Research in Computer
Security, Oslo, Norway, September 11-15, 2017,
Proceedings, Part I

Foley, S.N.; Gollmann, D.; Snekkenes, E. (Eds.)

2017, XXI, 485 p. 106 illus., Softcover

ISBN: 978-3-319-66401-9