

## Contents – Part II

### Leakage Management and Obfuscation

Towards Efficient Evaluation of a Time-Driven Cache Attack on Modern Processors . . . . .	3
<i>Andreas Zankl, Katja Miller, Johann Heyszl, and Georg Sigl</i>	
More Practical and Secure History-Independent Hash Tables . . . . .	20
<i>Michael T. Goodrich, Evgenios M. Kornaropoulos, Michael Mitzenmacher, and Roberto Tamassia</i>	
On Manufacturing Resilient Opaque Constructs Against Static Analysis. . . . .	39
<i>Brendan Sheridan and Micah Sherr</i>	

### Secure Multiparty Computation

Robust Password-Protected Secret Sharing . . . . .	61
<i>Michel Abdalla, Mario Cornejo, Anca Nitulescu, and David Pointcheval</i>	
Compiling Low Depth Circuits for Practical Secure Computation . . . . .	80
<i>Niklas Buescher, Andreas Holzer, Alina Weber, and Stefan Katzenbeisser</i>	
Secure Computation of MIPS Machine Code . . . . .	99
<i>Xiao Wang, S. Dov Gordon, Allen McIntosh, and Jonathan Katz</i>	

### Secure Logging

Insynd: Improved Privacy-Preserving Transparency Logging . . . . .	121
<i>Roel Peeters and Tobias Pulls</i>	
Secure Logging Schemes and Certificate Transparency . . . . .	140
<i>Benjamin Dowling, Felix Günther, Udyani Herath, and Douglas Stebila</i>	

### Economics of Security

Banishing Misaligned Incentives for Validating Reports in Bug-Bounty Platforms . . . . .	161
<i>Aron Laszka, Mingyi Zhao, and Jens Grossklags</i>	
Efficient Numerical Frameworks for Multi-objective Cyber Security Planning . . . . .	179
<i>MHR. Khouzani, P. Malacaria, C. Hankin, A. Fielder, and F. Smeraldi</i>	

## E-voting and E-commerce

On Bitcoin Security in the Presence of Broken Cryptographic Primitives . . . .	201
<i>Ilias Giechaskiel, Cas Cremers, and Kasper B. Rasmussen</i>	
DRE-ip: A Verifiable E-Voting Scheme Without Tallying Authorities . . . . .	223
<i>Siamak F. Shahandashti and Feng Hao</i>	
When Are Three Voters Enough for Privacy Properties? . . . . .	241
<i>Myrto Arapinis, Véronique Cortier, and Steve Kremer</i>	
Efficient Zero-Knowledge Contingent Payments in Cryptocurrencies Without Scripts. . . . .	261
<i>Wacław Banasik, Stefan Dziembowski, and Daniel Malinowski</i>	

## Security of the Internet of Things

LeiA: A <u>L</u> ightweight <u>A</u> uthentication <u>P</u> rotocol for <u>C</u> AN . . . . .	283
<i>Andreea-Ina Radu and Flavio D. Garcia</i>	
Privacy, Discovery, and Authentication for the Internet of Things . . . . .	301
<i>David J. Wu, Ankur Taly, Asim Shankar, and Dan Boneh</i>	
Secure Code Updates for Mesh Networked Commodity Low-End Embedded Devices . . . . .	320
<i>Florian Kohnhäuser and Stefan Katzenbeisser</i>	
Authenticated Key Agreement Mediated by a Proxy Re-encryptor for the Internet of Things. . . . .	339
<i>Kim Thuat Nguyen, Nouha Oualha, and Maryline Laurent</i>	

## Data Privacy

Information Control by Policy-Based Relational Weakening Templates . . . . .	361
<i>Joachim Biskup and Marcel Preuß</i>	
Quantifying Location Privacy Leakage from Transaction Prices . . . . .	382
<i>Arthur Gervais, Hubert Ritzdorf, Mario Lucic, Vincent Lenders, and Srdjan Capkun</i>	
A Formal Treatment of Privacy in Video Data . . . . .	406
<i>Valerie Fetzer, Jörn Müller-Quade, and Tobias Nilges</i>	

## Security of Cyber-Physical Systems

On Attacker Models and Profiles for Cyber-Physical Systems. . . . .	427
<i>Marco Rocchetto and Nils Ole Tippenhauer</i>	

Towards the Automated Verification of Cyber-Physical Security Protocols: Bounding the Number of Timed Intruders . . . . .	450
<i>Vivek Nigam, Carolyn Talcott, and Abraão Aires Urquiza</i>	

Safeguarding Structural Controllability in Cyber-Physical Control Systems. . .	471
<i>Cristina Alcaraz and Javier Lopez</i>	

## Attacks

The Beauty or The Beast? Attacking Rate Limits of the Xen Hypervisor . . . .	493
<i>Johanna Ullrich and Edgar Weippl</i>	

Autocomplete Injection Attack . . . . .	512
<i>Nethanel Gelernter and Amir Herzberg</i>	

Breaking into the KeyStore: A Practical Forgery Attack Against Android KeyStore . . . . .	531
<i>Mohamed Sabt and Jacques Traorè</i>	

## Attribute-Based Cryptography

Traceable CP-ABE with Short Ciphertexts: How to Catch People Selling Decryption Devices on eBay Efficiently. . . . .	551
<i>Jianting Ning, Zhenfu Cao, Xiaolei Dong, Junqing Gong, and Jie Chen</i>	

Server-Aided Revocable Attribute-Based Encryption . . . . .	570
<i>Hui Cui, Robert H. Deng, Yingjiu Li, and Baodong Qin</i>	

Online/Offline Public-Index Predicate Encryption for Fine-Grained Mobile Access Control . . . . .	588
<i>Weiran Liu, Jianwei Liu, Qianhong Wu, Bo Qin, and Kaitai Liang</i>	

<b>Author Index</b> . . . . .	607
-------------------------------	-----

# Contents – Part I

## Network and Web Security

Understanding Cross-Channel Abuse with SMS-Spam Support Infrastructure Attribution . . . . .	3
<i>Bharat Srinivasan, Payas Gupta, Manos Antonakakis, and Mustaque Ahamad</i>	
Toward an Efficient Website Fingerprinting Defense . . . . .	27
<i>Marc Juarez, Mohsen Imani, Mike Perry, Claudia Diaz, and Matthew Wright</i>	
Proactive Verification of Security Compliance for Clouds Through Pre-computation: Application to OpenStack . . . . .	47
<i>Suryadipta Majumdar, Yosr Jarraya, Taous Madi, Amir Alimohammadifar, Makan Pourzandi, Lingyu Wang, and Mourad Debbabi</i>	

## Authentication

Comparing Password Ranking Algorithms on Real-World Password Datasets . . . . .	69
<i>Weining Yang, Ninghui Li, Ian M. Molloy, Youngja Park, and Suresh N. Chari</i>	
Scalable Two-Factor Authentication Using Historical Data . . . . .	91
<i>Aldar C.-F. Chan, Jun Wen Wong, Jianying Zhou, and Joseph Teo</i>	
On the Implications of Zipf’s Law in Passwords . . . . .	111
<i>Ding Wang and Ping Wang</i>	

## Encrypted Search

PPOPM: More Efficient Privacy Preserving Outsourced Pattern Matching . . .	135
<i>Jun Zhou, Zhenfu Cao, and Xiaolei Dong</i>	
An Efficient Non-interactive Multi-client Searchable Encryption with Support for Boolean Queries . . . . .	154
<i>Shi-Feng Sun, Joseph K. Liu, Amin Sakzad, Ron Steinfeld, and Tsz Hon Yuen</i>	
Efficient Encrypted Keyword Search for Multi-user Data Sharing . . . . .	173
<i>Aggelos Kiayias, Ozgur Oksuz, Alexander Russell, Qiang Tang, and Bing Wang</i>	

## Detection and Monitoring

Membrane: A Posteriori Detection of Malicious Code Loading by Memory Paging Analysis . . . . .	199
<i>Gábor Pék, Zsombor Lázár, Zoltán Várnagy, Márk Félegyházi, and Levente Buttyán</i>	
Mobile Application Impersonation Detection Using Dynamic User Interface Extraction . . . . .	217
<i>Luka Malisa, Kari Kostinen, Michael Och, and Srdjan Capkun</i>	
A Machine Learning Approach for Detecting Third-Party Trackers on the Web . . . . .	238
<i>Qianru Wu, Qixu Liu, Yuqing Zhang, Peng Liu, and Guanxing Wen</i>	

## Cryptography for Cloud Computing

Privately Outsourcing Exponentiation to a Single Server: Cryptanalysis and Optimal Constructions . . . . .	261
<i>Céline Chevalier, Fabien Laguillaumie, and Damien Vergnaud</i>	
Attribute-Based Signatures for Supporting Anonymous Certification . . . . .	279
<i>Nesrine Kaaniche and Maryline Laurent</i>	
Privacy Preserving Computation in Cloud Using Noise-Free Fully Homomorphic Encryption (FHE) Schemes . . . . .	301
<i>Yongge Wang and Qutaibah M. Malluhi</i>	
Lightweight Delegatable Proofs of Storage . . . . .	324
<i>Jia Xu, Anjia Yang, Jianying Zhou, and Duncan S. Wong</i>	
Anonymous RAM. . . . .	344
<i>Michael Backes, Amir Herzberg, Aniket Kate, and Ivan Piryvalov</i>	
Efficient Sanitizable Signatures Without Random Oracles. . . . .	363
<i>Russell W.F. Lai, Tao Zhang, Sherman S.M. Chow, and Dominique Schröder</i>	

## Operating Systems Security

Intentio Ex Machina: Android Intent Access Control via an Extensible Application Hook . . . . .	383
<i>Carter Yagemann and Wenliang Du</i>	
Hey, You, Get Off of My Image: Detecting Data Residue in Android Images . . . . .	401
<i>Xiao Zhang, Yousra Aafer, Kailiang Ying, and Wenliang Du</i>	

NaCIDroid: Native Code Isolation for Android Applications. . . . .	422
<i>Elias Athanasopoulos, Vasileios P. Kemerlis, Georgios Portokalidis, and Angelos D. Keromytis</i>	
AsyncShock: Exploiting Synchronisation Bugs in Intel SGX Enclaves. . . . .	440
<i>Nico Weichbrodt, Anil Kurmus, Peter Pietzuch, and Rüdiger Kapitza</i>	
Stay in Your Cage! A Sound Sandbox for Third-Party Libraries on Android. . . . .	458
<i>Fabo Wang, Yuqing Zhang, Kai Wang, Peng Liu, and Wenjie Wang</i>	
Android Permission Recommendation Using Transitive Bayesian Inference Model . . . . .	477
<i>Bahman Rashidi, Carol Fung, Anh Nguyen, and Tam Vu</i>	
<b>Information Flow</b>	
Spot the Difference: Secure Multi-execution and Multiple Facets . . . . .	501
<i>Nataliia Bielova and Tamara Rezk</i>	
On Reductions from Multi-Domain Noninterference to the Two-Level Case . . .	520
<i>Oliver Woizekowski and Ron van der Meyden</i>	
Flexible Manipulation of Labeled Values for Information-Flow Control Libraries. . . . .	538
<i>Marco Vassena, Pablo Buiras, Lucas Waye, and Alejandro Russo</i>	
<b>Software Security</b>	
Let’s Face It: Faceted Values for Taint Tracking. . . . .	561
<i>Daniel Schoepe, Musard Balliu, Frank Piessens, and Andrei Sabelfeld</i>	
IFuzzer: An Evolutionary Interpreter Fuzzer Using Genetic Programming . . .	581
<i>Spandan Veggalam, Sanjay Rawat, Istvan Haller, and Herbert Bos</i>	
Automated Multi-architectural Discovery of CFI-Resistant Code Gadgets. . . .	602
<i>Patrick Wollgast, Robert Gawlik, Behrad Garmany, Benjamin Kollenda, and Thorsten Holz</i>	
<b>Author Index</b> . . . . .	621

Computer Security – ESORICS 2016

21st European Symposium on Research in Computer  
Security, Heraklion, Greece, September 26-30, 2016,  
Proceedings, Part II

Askoxylakis, I.; Ioannidis, S.; Katsikas, S.K.; Meadows, C.  
(Eds.)

2016, XIX, 609 p. 117 illus., Softcover

ISBN: 978-3-319-45740-6