

Contents

Invited Talk

What Satoshi Did Not Know	3
<i>Gavin Andresen</i>	

Cybercrime

Are You at Risk? Profiling Organizations and Individuals Subject to Targeted Attacks	13
<i>Olivier Thonnard, Leyla Bilge, Anand Kashyap, and Martin Lee</i>	
Computer-Supported Cooperative Crime	32
<i>Vaibhav Garg, Sadia Afroz, Rebekah Overdorf, and Rachel Greenstadt</i>	
There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Currency Scams	44
<i>Marie Vasek and Tyler Moore</i>	

Sidechannels

Multi-class Traffic Morphing for Encrypted VoIP Communication	65
<i>W. Brad Moore, Henry Tan, Micah Sherr, and Marcus A. Maloof</i>	
Protecting Encrypted Cookies from Compression Side-Channel Attacks	86
<i>Janaka Alawatugoda, Douglas Stebila, and Colin Boyd</i>	
Fingerprinting Web Users Through Font Metrics	107
<i>David Fifield and Serge Egelman</i>	

Cryptography in the Cloud

Sorting and Searching Behind the Curtain	127
<i>Foteini Baldimtsi and Olga Ohrimenko</i>	
Resizable Tree-Based Oblivious RAM	147
<i>Tarik Moataz, Travis Mayberry, Erik-Oliver Blass, and Agnes Hui Chan</i>	
Sublinear Scaling for Multi-Client Private Information Retrieval	168
<i>Wouter Lueks and Ian Goldberg</i>	

Payment and Fraud Detection

Relay Cost Bounding for Contactless EMV Payments 189
*Tom Chothia, Flavio D. Garcia, Joeri de Ruiter, Jordi van den Brekel,
and Matthew Thompson*

Private and Secure Public-Key Distance Bounding: Application
to NFC Payment 207
Serge Vaudenay

Purchase Details Leaked to PayPal 217
Sören Preibusch, Thomas Peetz, Gunes Acar, and Bettina Berendt

How the Estonian Tax and Customs Board Evaluated a Tax Fraud
Detection System Based on Secure Multi-party Computation 227
Dan Bogdanov, Marko Jõemets, Sander Siim, and Meril Vaht

Authentication and Access Control

Tactile One-Time Pad: Leakage-Resilient Authentication for Smartphones . . . 237
*Sebastian Uellenbeck, Thomas Hupperich, Christopher Wolf,
and Thorsten Holz*

User Authentication Using Human Cognitive Abilities 254
Asadullah Al Galib and Reihaneh Safavi-Naini

Smart and Secure Cross-Device Apps for the Internet of Advanced Things . . . 272
*Christoph Busold, Stephan Heuser, Jon Rios, Ahmad-Reza Sadeghi,
and N. Asokan*

Cryptographic Primitives

Signatures and Efficient Proofs on Committed Graphs and NP-Statements . . . 293
Thomas Groß

Efficient Statically-Secure Large-Universe Multi-Authority
Attribute-Based Encryption 315
Yannis Rouselakis and Brent Waters

Augmented Learning with Errors: The Untapped Potential
of the Error Term 333
Rachid El Bansarkhani, Özgür Dagdelen, and Johannes Buchmann

Mobile Security

BabelCrypt: The Universal Encryption Layer for Mobile
Messaging Applications 355
*Ahmet Talha Ozcan, Can Gemicioglu, Kaan Onarlioglu,
Michael Weissbacher, Collin Mulliner, William Robertson,
and Engin Kirda*

METDS - A Self-contained, Context-Based Detection System for Evil
Twin Access Points 370
Christian Szongott, Michael Brenner, and Matthew Smith

Market-Driven Code Provisioning to Mobile Secure Hardware 387
*Alexandra Dmitrienko, Stephan Heuser, Thien Duc Nguyen,
Marcos da Silva Ramos, Andre Rein, and Ahmad-Reza Sadeghi*

Privacy and Incentives

On Non-cooperative Genomic Privacy 407
*Mathias Humbert, Erman Ayday, Jean-Pierre Hubaux,
and Amalio Telenti*

A Short Paper on the Incentives to Share Private Information
for Population Estimates 427
Michela Chessa, Jens Grossklags, and Patrick Loiseau

Paying the Guard: An Entry-Guard-Based Payment System for Tor. 437
Paolo Palmieri and Johan Pouwelse

Proof-of-Work as Anonymous Micropayment: Rewarding a Tor Relay 445
Alex Biryukov and Ivan Pustogarov

Applications and Attacks

Privacy Preserving Collaborative Filtering from Asymmetric
Randomized Encoding 459
Yongjun Zhao and Sherman S.M. Chow

Anonymous and Publicly Linkable Reputation Systems 478
Johannes Blömer, Jakob Juhnke, and Christina Kolb

Hard Drive Side-Channel Attacks Using Smartphone Magnetic
Field Sensors 489
Sebastian Biedermann, Stefan Katzenbeisser, and Jakub Szefer

Hierarchical Deterministic Bitcoin Wallets that Tolerate Key Leakage 497
Gus Gutoski and Douglas Stebila

Authenticated Data Structures

Secure High-Rate Transaction Processing in Bitcoin 507
Yonatan Sompolinsky and Aviv Zohar

Inclusive Block Chain Protocols 528
Yoad Lewenberg, Yonatan Sompolinsky, and Aviv Zohar

VeriStream – A Framework for Verifiable Data Streaming 548
Dominique Schöder and Mark Simkin

Poster Abstracts

Cryptanalysis of a Protocol from FC'10 (Poster Abstract) 569
Mohsen Toorani

Web Application Security with Contactless Identity Cards
Using Near Field Communication (Poster Abstract) 570
Arvo Sulakatko and Alex Norton

OpenCard (Poster Abstract) 571
Pascal Paillier and Tancreède Lepoint

Author Index 573



<http://www.springer.com/978-3-662-47853-0>

Financial Cryptography and Data Security
19th International Conference, FC 2015, San Juan,
Puerto Rico, January 26-30, 2015, Revised Selected
Papers

Böhme, R.; Okamoto, T. (Eds.)

2015, XIV, 574 p. 119 illus., Softcover

ISBN: 978-3-662-47853-0