

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
<i>Tom Chothia, Flavio D. Garcia, Joeri de Ruiter, Jordi van den Breekel, and Matthew Thompson</i>	
Private and Secure Public-Key Distance Bounding: Application to NFC Payment	207
<i>Serge Vaudenay</i>	
Purchase Details Leaked to PayPal	217
<i>Sören Preibusch, Thomas Peetz, Gunes Acar, and Bettina Berendt</i>	
How the Estonian Tax and Customs Board Evaluated a Tax Fraud Detection System Based on Secure Multi-party Computation	227
<i>Dan Bogdanov, Marko Jõemets, Sander Siim, and Meril Vaht</i>	

Authentication and Access Control

Tactile One-Time Pad: Leakage-Resilient Authentication for Smartphones . . .	237
<i>Sebastian Uellenbeck, Thomas Hupperich, Christopher Wolf, and Thorsten Holz</i>	
User Authentication Using Human Cognitive Abilities	254
<i>Asadullah Al Galib and Reihaneh Safavi-Naini</i>	
Smart and Secure Cross-Device Apps for the Internet of Advanced Things . . .	272
<i>Christoph Busold, Stephan Heuser, Jon Rios, Ahmad-Reza Sadeghi, and N. Asokan</i>	

Cryptographic Primitives

Signatures and Efficient Proofs on Committed Graphs and NP-Statements . . .	293
<i>Thomas Groß</i>	
Efficient Statically-Secure Large-Universe Multi-Authority Attribute-Based Encryption	315
<i>Yannis Rouselakis and Brent Waters</i>	
Augmented Learning with Errors: The Untapped Potential of the Error Term	333
<i>Rachid El Bansarkhani, Özgür Dagdelen, and Johannes Buchmann</i>	

Mobile Security

BabelCrypt: The Universal Encryption Layer for Mobile Messaging Applications	355
<i>Ahmet Talha Ozcan, Can Gemiciloglu, Kaan Onarlioglu, Michael Weissbacher, Collin Mulliner, William Robertson, and Engin Kirda</i>	

METDS - A Self-contained, Context-Based Detection System for Evil Twin Access Points	370
<i>Christian Szongott, Michael Brenner, and Matthew Smith</i>	
Market-Driven Code Provisioning to Mobile Secure Hardware	387
<i>Alexandra Dmitrienko, Stephan Heuser, Thien Duc Nguyen, Marcos da Silva Ramos, Andre Rein, and Ahmad-Reza Sadeghi</i>	
Privacy and Incentives	
On Non-cooperative Genomic Privacy	407
<i>Mathias Humbert, Erman Ayday, Jean-Pierre Hubaux, and Amalio Telenti</i>	
A Short Paper on the Incentives to Share Private Information for Population Estimates	427
<i>Michela Chessa, Jens Grossklags, and Patrick Loiseau</i>	
Paying the Guard: An Entry-Guard-Based Payment System for Tor.	437
<i>Paolo Palmieri and Johan Pouwelse</i>	
Proof-of-Work as Anonymous Micropayment: Rewarding a Tor Relay	445
<i>Alex Biryukov and Ivan Pustogarov</i>	
Applications and Attacks	
Privacy Preserving Collaborative Filtering from Asymmetric Randomized Encoding	459
<i>Yongjun Zhao and Sherman S.M. Chow</i>	
Anonymous and Publicly Linkable Reputation Systems	478
<i>Johannes Blömer, Jakob Juhnke, and Christina Kolb</i>	
Hard Drive Side-Channel Attacks Using Smartphone Magnetic Field Sensors	489
<i>Sebastian Biedermann, Stefan Katzenbeisser, and Jakub Szefer</i>	
Hierarchical Deterministic Bitcoin Wallets that Tolerate Key Leakage	497
<i>Gus Gutoski and Douglas Stebila</i>	
Authenticated Data Structures	
Secure High-Rate Transaction Processing in Bitcoin	507
<i>Yonatan Sompolsky and Aviv Zohar</i>	
Inclusive Block Chain Protocols	528
<i>Yoad Lewenberg, Yonatan Sompolsky, and Aviv Zohar</i>	

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 Norta

OpenCard (Poster Abstract) 571
Pascal Paillier and Tancrede Lepoint

Author Index 573

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