Contents

Payment Systems

Digital Check Forgery Attacks on Client Check Truncation Systems ........ 3
Rigel Gjomemo, Hafiz Malik, Nilesh Sumb, V.N. Venkatakrishnan,
and Rashid Ansari

Security Protocols and Evidence: Where Many Payment Systems Fail .... 21
Steven J. Murdoch and Ross Anderson

The Ghosts of Banking Past: Empirical Analysis of Closed Bank Websites . . . 33
Tyler Moore and Richard Clayton

Case Studies

Hawk and Aucitas: e-Auction Schemes from the Helios and Civitas
e-Voting Schemes ................................................................. 51
Adam McCarthy, Ben Smyth, and Elizabeth A. Quaglia

Sex, Lies, or Kittens? Investigating the Use of Snapchat’s
Self-Destructing Messages ................................................... 64
Franziska Roesner, Brian T. Gill, and Tadayoshi Kohno

On the Awareness, Control and Privacy of Shared Photo Metadata ........ 77
Benjamin Henne, Maximilian Koch, and Matthew Smith

Outsmarting Proctors with Smartwatches: A Case Study on Wearable
Computing Security ............................................................ 89
Alex Migicovsky, Zakir Durumeric, Jeff Ringenberg, and J. Alex Halderman

Cloud and Virtualization

A Secure Data Deduplication Scheme for Cloud Storage ..................... 99
Jan Stanek, Alessandro Sorniotti, Elli Androulaki, and Lukas Kencl

Confidentiality Issues on a GPU in a Virtualized Environment .......... 119
Clémentine Maurice, Christoph Neumann, Olivier Heen,
and Aurélien Francillon
Elliptic Curve Cryptography

Elligator Squared: Uniform Points on Elliptic Curves of Prime Order as Uniform Random Strings ......................................... 139
  *Mehdi Tibouchi*

Elliptic Curve Cryptography in Practice .......................................................... 157
  *Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow*

Privacy-Preserving Systems

Practical Secure Decision Tree Learning in a Teletreatment Application .......... 179
  *Sebastiaan de Hoogh, Berry Schoenmakers, Ping Chen, and Harm op den Akker*

Scaling Private Set Intersection to Billion-Element Sets .............................. 195
  *Seny Kamara, Payman Mohassel, Mariana Raykova, and Saeed Sadeghian*

Efficient Non-Interactive Zero Knowledge Arguments for Set Operations .......... 216
  *Prastudy Fauzi, Helger Lipmaa, and Bingsheng Zhang*

Garbled Searchable Symmetric Encryption ..................................................... 234
  *Kaoru Kurosawa*

Authentication and Visual Encryption

Efficient and Strongly Secure Dynamic Domain-Specific Pseudonymous Signatures for ID Documents ................................................. 255
  *Julien Bringer, Hervé Chabanne, Roch Lescuyer, and Alain Patey*

A Short Paper on How to Improve U-Prove Using Self-Blindable Certificates .... 273
  *Lucjan Hanzlik and Kamil Klucznik*

Attack on U-Prove Revocation Scheme from FC'13 - Passing Verification by Revoked Users ................................................................. 283
  *Lucjan Hanzlik, Kamil Klucznik, and Miroslaw Kutylowski*

Sample or Random Security – A Security Model for Segment-Based Visual Cryptography ................................................................. 291
  *Sebastian Pape*

Network Security

You Won’t Be Needing These Any More: On Removing Unused Certificates from Trust Stores ......................................................... 307
  *Henning Perl, Sascha Fahl, and Matthew Smith*
Challenges in Protecting Tor Hidden Services from Botnet Abuse. .... 316
Nicholas Hopper

Identifying Risk Factors for Webserver Compromise. .................... 326
Marie Vasek and Tyler Moore

Mobile System Security

Drone to the Rescue: Relay-Resilient Authentication using Ambient Multi-sensing. ......................................................... 349
Babins Shrestha, Nitesh Saxena, Hien Thi Thu Truong, and N. Asokan

On the (In)Security of Mobile Two-Factor Authentication .................. 365
Alexandra Dmitrienko, Christopher Liebchen, Christian Rossow, and Ahmad-Reza Sadeghi

MoP-2-MoP – Mobile Private Microblogging. ................................ 384
Marius Senftleben, Mihai Bucicoiu, Erik Tews, Frederik Armknecht, Stefan Katzenbeisser, and Ahmad-Reza Sadeghi

Incentives, Game Theory and Risk

Privacy Preserving Tâtonnement: A Cryptographic Construction of an Incentive Compatible Market. ........................................... 399
John Ross Wallrabenstein and Chris Clifton

Estimating Systematic Risk in Real-World Networks ......................... 417
Aron Laszka, Benjamin Johnson, Jens Grossklags, and Mark Felegyhazi

Majority Is Not Enough: Bitcoin Mining Is Vulnerable ..................... 436
Ittay Eyal and Emin Gün Sirer

Bitcoin Anonymity

BitIodine: Extracting Intelligence from the Bitcoin Network ............. 457
Michele Spagnuolo, Federico Maggi, and Stefano Zanero

An Analysis of Anonymity in Bitcoin Using P2P Network Traffic ........ 469
Philip Koshy, Diana Koshy, and Patrick McDaniel

Mixcoin: Anonymity for Bitcoin with Accountable Mixes ................. 486
Joseph Bonneau, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A. Kroll, and Edward W. Felten

Author Index ........................................................................... 505