

Contents

Payment Systems

Digital Check Forgery Attacks on Client Check Truncation Systems	3
<i>Rigel Gjomemo, Hafiz Malik, Nilesh Sumb, V.N. Venkatakrishnan, and Rashid Ansari</i>	
Security Protocols and Evidence: Where Many Payment Systems Fail	21
<i>Steven J. Murdoch and Ross Anderson</i>	
The Ghosts of Banking Past: Empirical Analysis of Closed Bank Websites	33
<i>Tyler Moore and Richard Clayton</i>	

Case Studies

Hawk and Aucitas: e-Auction Schemes from the Helios and Civitas e-Voting Schemes	51
<i>Adam McCarthy, Ben Smyth, and Elizabeth A. Quaglia</i>	
Sex, Lies, or Kittens? Investigating the Use of Snapchat's Self-Destructing Messages	64
<i>Franziska Roesner, Brian T. Gill, and Tadayoshi Kohno</i>	
On the Awareness, Control and Privacy of Shared Photo Metadata	77
<i>Benjamin Henne, Maximilian Koch, and Matthew Smith</i>	
Outsmarting Proctors with Smartwatches: A Case Study on Wearable Computing Security.	89
<i>Alex Migicovsky, Zakir Durumeric, Jeff Ringenberg, and J. Alex Halderman</i>	

Cloud and Virtualization

A Secure Data Deduplication Scheme for Cloud Storage	99
<i>Jan Stanek, Alessandro Sorniotti, Elli Androulaki, and Lukas Kencl</i>	
Confidentiality Issues on a GPU in a Virtualized Environment	119
<i>Clémentine Maurice, Christoph Neumann, Olivier Heen, and Aurélien Francillon</i>	

Elliptic Curve Cryptography

Elligator Squared: Uniform Points on Elliptic Curves of Prime Order as Uniform Random Strings	139
<i>Mehdi Tibouchi</i>	
Elliptic Curve Cryptography in Practice	157
<i>Joppe W. Bos, J. Alex Halderman, Nadia Heninger, Jonathan Moore, Michael Naehrig, and Eric Wustrow</i>	

Privacy-Preserving Systems

Practical Secure Decision Tree Learning in a Teletreatment Application.	179
<i>Sebastiaan de Hoogh, Berry Schoenmakers, Ping Chen, and Harm op den Akker</i>	
Scaling Private Set Intersection to Billion-Element Sets	195
<i>Seny Kamara, Payman Mohassel, Mariana Raykova, and Saeed Sadeghian</i>	
Efficient Non-Interactive Zero Knowledge Arguments for Set Operations.	216
<i>Prastudy Fauzi, Helger Lipmaa, and Bingsheng Zhang</i>	
Garbled Searchable Symmetric Encryption	234
<i>Kaoru Kurosawa</i>	

Authentication and Visual Encryption

Efficient and Strongly Secure Dynamic Domain-Specific Pseudonymous Signatures for ID Documents	255
<i>Julien Bringer, Hervé Chabanne, Roch Lescuyer, and Alain Patey</i>	
A Short Paper on How to Improve U-Prove Using Self-Blindable Certificates	273
<i>Lucjan Hanzlik and Kamil Kluczniak</i>	
Attack on U-Prove Revocation Scheme from FC'13 - Passing Verification by Revoked Users.	283
<i>Lucjan Hanzlik, Kamil Kluczniak, and Mirosław Kutylowski</i>	
Sample or Random Security – A Security Model for Segment-Based Visual Cryptography	291
<i>Sebastian Pape</i>	

Network Security

You Won't Be Needing These Any More: On Removing Unused Certificates from Trust Stores	307
<i>Henning Perl, Sascha Fahl, and Matthew Smith</i>	

Challenges in Protecting Tor Hidden Services from Botnet Abuse	316
<i>Nicholas Hopper</i>	
Identifying Risk Factors for Webserver Compromise	326
<i>Marie Vasek and Tyler Moore</i>	
Mobile System Security	
Drone to the Rescue: Relay-Resilient Authentication using Ambient Multi-sensing	349
<i>Babins Shrestha, Nitesh Saxena, Hien Thi Thu Truong, and N. Asokan</i>	
On the (In)Security of Mobile Two-Factor Authentication	365
<i>Alexandra Dmitrienko, Christopher Liebchen, Christian Rossow, and Ahmad-Reza Sadeghi</i>	
MoP-2-MoP – Mobile Private Microblogging	384
<i>Marius Senfileben, Mihai Bucicoiu, Erik Tews, Frederik Armknecht, Stefan Katzenbeisser, and Ahmad-Reza Sadeghi</i>	
Incentives, Game Theory and Risk	
Privacy Preserving Tâtonnement: A Cryptographic Construction of an Incentive Compatible Market	399
<i>John Ross Wallrabenstein and Chris Clifton</i>	
Estimating Systematic Risk in Real-World Networks	417
<i>Aron Laszka, Benjamin Johnson, Jens Grossklags, and Mark Felegyhazi</i>	
Majority Is Not Enough: Bitcoin Mining Is Vulnerable	436
<i>Ittay Eyal and Emin Gün Sirer</i>	
Bitcoin Anonymity	
BitIodine: Extracting Intelligence from the Bitcoin Network	457
<i>Michele Spagnuolo, Federico Maggi, and Stefano Zanero</i>	
An Analysis of Anonymity in Bitcoin Using P2P Network Traffic	469
<i>Philip Koshy, Diana Koshy, and Patrick McDaniel</i>	
Mixcoin: Anonymity for Bitcoin with Accountable Mixes	486
<i>Joseph Bonneau, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A. Kroll, and Edward W. Felten</i>	
Author Index	505