

Contents

Fraud and Deception

Understanding Craigslist Rental Scams	3
<i>Youngsam Park, Damon McCoy, and Elaine Shi</i>	
Graph Analytics for Real-Time Scoring of Cross-Channel Transactional Fraud	22
<i>Ian Molloy, Suresh Chari, Ulrich Finkler, Mark Wiggerman, Coen Jonker, Ted Habeck, Youngja Park, Frank Jordens, and Ron van Schaik</i>	
Android UI Deception Revisited: Attacks and Defenses	41
<i>Earlence Fernandes, Qi Alfred Chen, Justin Paupore, Georg Essl, J. Alex Halderman, Z. Morley Mao, and Atul Prakash</i>	
Introducing Reputation Systems to the Economics of Outsourcing Computations to Rational Workers	60
<i>Jassim Aljuraidan, Lujo Bauer, Michael K. Reiter, and Matthias Beckerle</i>	

Payments, Auctions, and e-Voting

Accountable Privacy for Decentralized Anonymous Payments.	81
<i>Christina Garman, Matthew Green, and Ian Miers</i>	
Private eCash in Practice (Short Paper)	99
<i>Amira Barki, Solenn Brunet, Nicolas Desmoulins, Sébastien Gambs, Saïd Gharout, and Jacques Traoré</i>	
Practically Efficient Secure Single-Commodity Multi-market Auctions.	110
<i>Abdelrahman Aly and Mathieu Van Vyve</i>	
How to Challenge and Cast Your e-Vote	130
<i>Sandra Guasch and Paz Morillo</i>	

Multiparty Computation

VD-PSI: Verifiable Delegated Private Set Intersection on Outsourced Private Datasets	149
<i>Aydin Abadi, Sotirios Terzis, and Changyu Dong</i>	

Confidential Benchmarking Based on Multiparty Computation	169
<i>Ivan Damgård, Kasper Damgård, Kurt Nielsen, Peter Sebastian Nordholt, and Tomas Toft</i>	
Efficiently Making Secure Two-Party Computation Fair.	188
<i>Handan Kılınç and Alptekin Küpçü</i>	
Fast Optimistically Fair Cut-and-Choose 2PC	208
<i>Alptekin Küpçü and Payman Mohassel</i>	
Mobile Malware	
CuriousDroid: Automated User Interface Interaction for Android Application Analysis Sandboxes	231
<i>Patrick Carter, Collin Mulliner, Martina Lindorfer, William Robertson, and Engin Kirda</i>	
DroydSeuss: A Mobile Banking Trojan Tracker (Short Paper)	250
<i>Alberto Coletta, Victor van der Veen, and Federico Maggi</i>	
DroidAuditor: Forensic Analysis of Application-Layer Privilege Escalation Attacks on Android (Short Paper)	260
<i>Stephan Heuser, Marco Negro, Praveen Kumar Pendyala, and Ahmad-Reza Sadeghi</i>	
Social Interaction and Policy	
Discrete Choice, Social Interaction, and Policy in Encryption Technology Adoption (Short Paper).	271
<i>Tristan Caulfield, Christos Ioannidis, and David Pym</i>	
Cryptanalysis	
Failures of Security APIs: A New Case	283
<i>Abdalnaser Algwil and Jeff Yan</i>	
Explicit Optimal Binary Pebbling for One-Way Hash Chain Reversal	299
<i>Berry Schoenmakers</i>	
Factoring as a Service	321
<i>Luke Valenta, Shaanan Cohney, Alex Liao, Joshua Fried, Satya Bodduluri, and Nadia Heninger</i>	
The Self-blindable U-Prove Scheme from FC'14 Is Forgeable (Short Paper)	339
<i>Eric Verheul, Sietse Ringers, and Jaap-Henk Hoepman</i>	

A Sound for a Sound: Mitigating Acoustic Side Channel Attacks on Password Keystrokes with Active Sounds	346
<i>S. Abhishek Anand and Nitesh Saxena</i>	

Surveillance and Anonymity

Leaky Birds: Exploiting Mobile Application Traffic for Surveillance	367
<i>Eline Vanrykel, Gunes Acar, Michael Herrmann, and Claudia Diaz</i>	
Footprint Scheduling for Dining-Cryptographer Networks	385
<i>Anna Krasnova, Moritz Neikes, and Peter Schwabe</i>	

Web Security and Data Privacy

How Anywhere Computing Just Killed Your Phone-Based Two-Factor Authentication	405
<i>Radhesh Krishnan Konoth, Victor van der Veen, and Herbert Bos</i>	
Security Keys: Practical Cryptographic Second Factors for the Modern Web	422
<i>Juan Lang, Alexei Czeskis, Dirk Balfanz, Marius Schilder, and Sampath Srinivas</i>	
Include Me Out: In-Browser Detection of Malicious Third-Party Content Inclusions.	441
<i>Sajjad Arshad, Amin Kharraz, and William Robertson</i>	
A Sensitivity-Adaptive ρ -Uncertainty Model for Set-Valued Data	460
<i>Liuhua Chen, Shenghai Zhong, Li-e Wang, and Xianxian Li</i>	

Bitcoin Mining

Incentive Compatibility of Bitcoin Mining Pool Reward Functions	477
<i>Okke Schrijvers, Joseph Bonneau, Dan Boneh, and Tim Roughgarden</i>	
When Cryptocurrencies Mine Their Own Business	499
<i>Jason Teutsch, Sanjay Jain, and Prateek Saxena</i>	
Optimal Selfish Mining Strategies in Bitcoin	515
<i>Ayelet Sapirshtein, Yonatan Sompolsky, and Aviv Zohar</i>	

Cryptographic Protocols

A Short Paper on Blind Signatures from Knowledge Assumptions	535
<i>Lucjan Hanzlik and Kamil Klucznik</i>	

KBID: Kerberos Bracelet Identification (Short Paper)	544
<i>Joseph Carrigan, Paul Martin, and Michael Rushanan</i>	
Payment Use and Abuse	
The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy	555
<i>Katharina Krombholz, Aljosha Judmayer, Matthias Gusenbauer, and Edgar Weippl</i>	
Refund Attacks on Bitcoin's Payment Protocol	581
<i>Patrick McCorry, Siamak F. Shahandashti, and Feng Hao</i>	
Are Payment Card Contracts Unfair? (Short Paper)	600
<i>Steven J. Murdoch, Ingolf Becker, Ruba Abu-Salma, Ross Anderson, Nicholas Bohm, Alice Hutchings, M. Angela Sasse, and Gianluca Stringhini</i>	
The Bitcoin Brain Drain: Examining the Use and Abuse of Bitcoin Brain Wallets	609
<i>Marie Vasek, Joseph Bonneau, Ryan Castellucci, Cameron Keith, and Tyler Moore</i>	
Author Index	619