

Table of Contents

Finacial Cryptography and Data Security (FC 2011)

Collective Exposure: Peer Effects in Voluntary Disclosure of Personal Data	1
<i>Rainer Böhme and Stefanie Pötzsch</i>	
It's All about the Benjamins: An Empirical Study on Incentivizing Users to Ignore Security Advice	16
<i>Nicolas Christin, Serge Egelman, Timothy Vidas, and Jens Grossklags</i>	
Evaluating the Privacy Risk of Location-Based Services	31
<i>Julien Freudiger, Reza Shokri, and Jean-Pierre Hubaux</i>	
Selections: Internet Voting with Over-the-Shoulder Coercion-Resistance	47
<i>Jeremy Clark and Urs Hengartner</i>	
Malice versus AN.ON: Possible Risks of Missing Replay and Integrity Protection	62
<i>Benedikt Westermann and Dogan Kesdogan</i>	
Absolute Pwnage: A Short Paper about the Security Risks of Remote Administration Tools	77
<i>Jay Novak, Jonathan Stribley, Kenneth Meagher, and J. Alex Halderman</i>	
A Protocol for Anonymously Establishing Digital Provenance in Reseller Chains (Short Paper)	85
<i>Ben Palmer, Kris Bubendorfer, and Ian Welch</i>	
Impeding Individual User Profiling in Shopper Loyalty Programs	93
<i>Philip Marquardt, David Dagon, and Patrick Traynor</i>	
Beyond Risk-Based Access Control: Towards Incentive-Based Access Control	102
<i>Debin Liu, Ninghui Li, XiaoFeng Wang, and L. Jean Camp</i>	
Authenticated Key Exchange under Bad Randomness	113
<i>Guomin Yang, Shanshan Duan, Duncan S. Wong, Chik How Tan, and Huaxiong Wang</i>	

Oblivious Outsourced Storage with Delegation	127
<i>Martin Franz, Peter Williams, Bogdan Carbunar, Stefan Katzenbeisser, Andreas Peter, Radu Sion, and Miroslava Sotakova</i>	
Homomorphic Signatures for Digital Photographs	141
<i>Rob Johnson, Leif Walsh, and Michael Lamb</i>	
Revisiting the Computational Practicality of Private Information Retrieval	158
<i>Femi Olumofin and Ian Goldberg</i>	
Optimal One Round Almost Perfectly Secure Message Transmission (Short Paper)	173
<i>Mohammed Ashraful Alam Tuhin and Reihaneh Safavi-Naini</i>	
A New Approach towards Coercion-Resistant Remote E-Voting in Linear Time	182
<i>Oliver Spycher, Reto Koenig, Rolf Haenni, and Michael Schl�pfer</i>	
An Attack on PUF-Based Session Key Exchange and a Hardware-Based Countermeasure: Erasable PUFs	190
<i>Ulrich R�hrmair, Christian Jaeger, and Michael Algasinger</i>	
Peeling Away Layers of an RFID Security System	205
<i>Henryk Pl�tz and Karsten Nohl</i>	
Might Financial Cryptography Kill Financial Innovation? – The Curious Case of EMV	220
<i>Ross Anderson, Mike Bond, Omar Choudary, Steven J. Murdoch, and Frank Stajano</i>	
hPIN/hTAN: A Lightweight and Low-Cost E-Banking Solution against Untrusted Computers	235
<i>Shujun Li, Ahmad-Reza Sadeghi, S�ren Heisrath, Roland Schmitz, and Junaid Jameel Ahmad</i>	
Certified Lies: Detecting and Defeating Government Interception Attacks against SSL (Short Paper)	250
<i>Christopher Soghoian and Sid Stamm</i>	
Proximax: Measurement-Driven Proxy Dissemination (Short Paper)	260
<i>Damon McCoy, Jose Andre Morales, and Kirill Levchenko</i>	
BNymble: More Anonymous Blacklisting at Almost No Cost (A Short Paper)	268
<i>Peter Lofgren and Nicholas Hopper</i>	

Towards Secure Bioinformatics Services (Short Paper)	276
<i>Martin Franz, Björn Deiseroth, Kay Hamacher, Somesh Jha,</i> <i>Stefen Katzenbeisser, and Heike Schröder</i>	
Quo Vadis? A Study of the Evolution of Input Validation Vulnerabilities in Web Applications	284
<i>Theodoor Scholte, Davide Balzarotti, and Engin Kirda</i>	
Re-evaluating the Wisdom of Crowds in Assessing Web Security	299
<i>Pern Hui Chia and Svein Johan Knapskog</i>	
Mercury: Recovering Forgotten Passwords Using Personal Devices	315
<i>Mohammad Mannan, David Barrera, Carson D. Brown,</i> <i>David Lie, and Paul C. van Oorschot</i>	
Author Index	331