Table of Contents

Social Authentication: Harder Than It Looks 1
Hyoungshick Kim, John Tang, and Ross Anderson

The MVP Web-Based Authentication Framework (Short Paper) 16
Sonia Chiasson, Chris Deschamps, Elizabeth Stobert, Max Hlywa, Bruna Freitas Machado, Alain Forget, Nicholas Wright, Gerry Chan, and Robert Biddle

A Birthday Present Every Eleven Wallets? The Security of Customer-Chosen Banking PINs 25
Joseph Bonneau, Sören Preibusch, and Ross Anderson

The Postmodern Ponzi Scheme: Empirical Analysis of High-Yield Investment Programs 41
Tyler Moore, Jie Han, and Richard Clayton

Deploying Secure Multi-Party Computation for Financial Data Analysis (Short Paper) 57
Dan Bogdanov, Riivo Talviste, and Jan Willemson

Cryptographic Rule-Based Trading (Short Paper) 65
Christopher Thorpe and Steven R. Willis

Efficient Private Proximity Testing with GSM Location Sketches 73
Zi Lin, Denis Foo Kune, and Nicholas Hopper

Metrics for Measuring ISP Badness: The Case of Spam (Short Paper) 89
Benjamin Johnson, John Chuang, Jens Grossklags, and Nicolas Christin

Congestion-Aware Path Selection for Tor 98
Tao Wang, Kevin Bauer, Clara Forero, and Ian Goldberg

Attacking the Washington, D.C. Internet Voting System 114
Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman

Security Audits Revisited 129
Rainer Böhme

Efficient, Compromise Resilient and Append-Only Cryptographic Schemes for Secure Audit Logging................................ 148
Attila A. Yavuz, Peng Ning, and Michael K. Reiter

Bibliografische Informationen
http://d-nb.info/1024629260

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

On Secure Two-Party Integer Division 164
Morten Dahl, Chao Ning, and Tomas Toft

A Non-interactive Range Proof with Constant Communication 179
Rafik Chaabouni, Helger Lipmaa, and Bingsheng Zhang

Privacy-Preserving Stream Aggregation with Fault Tolerance 200
T.-H. Hubert Chan, Elaine Shi, and Dawn Song

Dynamic Accumulator Based Discretionary Access Control for Outsourced Storage with Unlinkable Access (Short Paper) 215
Daniel Slamanig

Privacy Enhanced Access Control for Outsourced Data Sharing 223
Mariana Raykova, Hang Zhao, and Steven M. Bellovin

Designing Privacy-Preserving Smart Meters with Low-Cost Microcontrollers 239
Andres Molina-Markham, George Danezis, Kevin Fu, Prashant Shenoy, and David Irwin

Memory-Efficient Garbled Circuit Generation for Mobile Devices 254
Benjamin Mood, Lara Letaw, and Kevin Butler

Oblivious Decision Programs from Oblivious Transfer: Efficient Reductions 269
Payman Mohassel and Salman Niksefat

UC-Secure Searchable Symmetric Encryption 285
Kaoru Kurosawa and Yasuhiro Ohtaki

CTL: A Platform-Independent Crypto Tools Library Based on Dataflow Programming Paradigm 299
Junaid Jameel Ahmad, Shujun Li, Ahmad-Reza Sadeghi, and Thomas Schneider

A Cache Timing Attack on AES in Virtualization Environments 314
Michael Weiß, Benedikt Heinz, and Frederic Stumpf

Softer Smartcards: Usable Cryptographic Tokens with Secure Execution 329
Franz Ferdinand Brasser, Sven Bugiel, Atanas Filyanov, Ahmad-Reza Sadeghi, and Steffen Schulz

The PACE|AA Protocol for Machine Readable Travel Documents, and Its Security 344
Jens Bender, Özgür Dagdelen, Marc Fischlin, and Dennis Kügler

Oblivious Printing of Secret Messages in a Multi-party Setting 359
Aleksander Essex and Urs Hengartner

Reverse Fuzzy Extractors: Enabling Lightweight Mutual Authentication for PUF-Enabled RFIDs 374
Anthony Van Herrewege, Stefan Katzenbeisser, Roel Maes, Roel Peeters, Ahmad-Reza Sadeghi, Ingrid Verbauwhede, and Christian Wachsmann

CommitCoin: Carbon Dating Commitments with Bitcoin (Short Paper) 390
Jeremy Clark and Aleksander Essex

Bitter to Better — How to Make Bitcoin a Better Currency 399
Simon Barber, Xavier Boyen, Elaine Shi, and Ersin Uzun

Author Index 415