

Inhaltsverzeichnis

Biometrics and Digital Signatures

- Busch Christoph, Abt Sebastian, Nickel Claudia, Korte Ulrike, Zhou Xuebing**
Biometrische Template-Protection-Verfahren und Interoperabilitätsstrategien 1
- Busch Christoph, Hartung Daniel**
Biometrische Nachrichten-Authentisierung 13
- Hühnlein Detlef, Roßnagel Heiko, Zibuschka Jan**
Diffusion of Federated Identity Management 25

Dependability and Fault-Tolerance

- Güdemann Matthias, Ortmeier Frank**
Quantitative Model-Based Safety Analysis: A Case Study 37
- Messmer Roman, Keller Jörg**
Real-Time Fault-Tolerant Routing in High-Availability Multicast-Aware Video Networks 49
- Distler Tobias, Kapitza Rüdiger, Reiser Hans P.**
State Transfer for Hypervisor-Based Proactive Recovery of Heterogeneous Replicated Services 61

Security Systems

- Kastl Wolfgang, Loimayr Thomas**
A Parallel Computing System with Specialized Coprocessors for Cryptanalytic Algorithms 73
- Weis Rüdiger, Schüler Brian, Flemming Stefan A.**
Towards Secure and Reliable Firewall Systems based on MINIX3 85
- Kiltz Stefan, Hildebrandt Mario, Altschaffel Robert, Dittmann Jana**
A Transparent Bridge for Forensic Sound Network Traffic Data Acquisition 93

Multimedia Security

- Christlein Vincent, Riess Christian, Angelopoulou Elli**
A Study on Features for the Detection of Copy-Move Forgeries 105
- Kirchner Matthias**
Lineare Zeilen- und Spaltenprädiktoren zur Erkennung von Bildskalierungen 117
- Schäfer Marcel, Berchtold Waldemar, Steinebach Martin, Zmudzinski Sascha, Heilmann Margareta, Katzenbeisser Stefan**
Collusion-Secure Fingerprint Watermarking for Real World Applications 129

Reactive Security

- Rietz René, Schmerl Sebastian, Vogel Michael, König Hartmut**
Iterative präzisionsbewertende Signaturgenerierung 141
- Hoppe Tobias, Holthusen Sönke, Tuchscheerer Sven, Kiltz Stefan, Dittmann Jana**
Sichere Datenhaltung im Automobil am Beispiel eines Konzepts zur forensisch sicheren Datenspeicherung 153
- Spreitzenbarth Michael, Holz Thorsten**
Towards Secure Deletion on Smartphones 165
- Göbel Jan**
Amun: Automatic Capturing of Malicious Software 177
- Göbel Jan, Trinius Philipp**
Towards Optimal Sensor Placement Strategies for Early Warning Systems 191
- Trinius Philipp, Willems Carsten, Holz Thorsten, Rieck Konrad**
A Malware Instruction Set for Behavior-Based Analysis 205

Theory and Practice of Cryptography

- Stelte Björn, Saxe Björn**
State-of-the-Art Kryptoverfahren für drahtlose Sensornetze –
Eine Krypto-Bibliothek für MantisOS 217

Kühn Ulrich
On Security Protocols for Desktop Sharing 229

Schneider Michael, Buchmann Johannes
Extended Lattice Reduction Experiments Using the BKZ Algorithm 241

Development of Secure Systems

Schwab Fabian, Findeisen Alexander, Sakal Peter, Pohl Hartmut
Bedrohungsmodellierung (Threat Modeling) in der Softwareentwicklung 253

Pöhls Henrich C.
Why Showing One TLS Certificate is not Enough -
Towards a Browser Feedback for Multiple TLS Certificate Verifications 265

Ristig Christian, Fritzsche René, Siemers Christian
WatchCop - Safer Software Execution through Hardware/Software Co-Design 277

Models and Metrics for Secure Systems

Schryen Guido
A Fuzzy Model for IT Security Investments 289

Heumann Thomas, Türpe Sven, Keller Jörg
Quantifying the Attack Surface of a Web Application 305

Böhme Rainer, Pötzsch Stefanie
Social Lending aus der Perspektive des Datenschutzes 317

Network Security

Sovis Pavol, Kohlar Florian, Schwenk Jörg
Security Analysis of OpenID 329

Schrank Michael, Braun Bastian, Johns Martin, Posegga Joachim
Session Fixation - The Forgotten Vulnerability? 341

**Baecher Paul, Fischlin Marc, Gordon Lior, Langenberg Robert,
Lützwow Michael, Schröder Dominique**
CAPTCHAs: The Good, the Bad, and the Ugly 353