

Inhaltsverzeichnis

Mobile Geräte

- Hugo Gascon, Sebastian Uellenbeck, Christopher Wolf, Konrad Rieck**
*Continuous Authentication on Mobile Devices by Analysis of Typing
Motion Behavior* 1
- Andreas Kurtz, Markus Troßbach, Felix Freiling**
Snoop-it: Dynamische Analyse und Manipulation von Apple iOS Apps 13
- Irfan Altiok, Sebastian Uellenbeck, Thorsten Holz**
GraphNeighbors: Hampering Shoulder-Surfing Attacks on Smartphones 25

Web Security

- Nadina Hintz, Markus Engelberth, Zinaida Benenson, Felix Freiling**
*Phishing still works: Erfahrungen und Lehren aus der Durchführung
von Phishing-Experimenten* 37
- Ben Stock, Sebastian Lekies, Martin Johns**
*DOM-basiertes Cross-Site Scripting im Web: Reise in ein
unerforschtes Land* 53
- Andreas Mayer, Vladislav Mladenov, Jörg Schwenk**
On the Security of Holder-of-Key Single Sign-On 65

Practitioners Track: Sichere Anwendungen

Andreas Brinner, Rene Rietz

Verbesserung der Netzsicherheit in virtualisierten Umgebungen mit Hilfe von OpenFlow 79

Achim Brucker, Uwe Sodan

Deploying Static Application Security Testing on a Large Scale 91

Stefan Meier, Günther Pernul

Einsatz von digitaler Forensik in Unternehmen und Organisationen . . . 103

Practitioners Track: Angewandte Kryptographie

Patrick Grofig, Martin Haerterich, Isabelle Hang, Florian Kerschbaum, Mathias Kohler, Andreas Schaad, Axel Schroepfer, Walter Tighzert

Experiences and observations on the industrial implementation of a system to search over outsourced encrypted data. 115

Jürgen Fuß, Bernhard Greslehner-Nimmervoll, Wolfgang Kastl, Robert Kolmhofer

Effizienteres Bruteforcing auf einem heterogenen Cluster mit GPUs und FPGAs 127

Practitioners Track: Sichere Infrastrukturen

Carl-Heinz Genzel, Richard Sethmann, Olav Hoffmann, Kai-Oliver Detken

Sicherheitskonzept zum Schutz der Gateway-Integrität in Smart Grids 137

Christian Freckmann, Ulrich Greveler

IT-Sicherheitsaspekte industrieller Steuerungssysteme 149

Kirsten Brox, Anastasia Meletiadou

Security-Awareness-Programm unter Berücksichtigung viraler Marketingmethoden 157

Angewandte Kryptographie

Frederik Armknecht, Matthias Hamann, Matthias Krause
Hardware Efficient Authentication based on Random Selection 169

Stefan Rass, Peter Schartner
Chameleon-Hashing für Interaktive Beweise der Verfügbarkeit dynamischer Daten in der Cloud 187

Christoph Sibinger, Tilo Müller
Verwendung von Festplattenvollverschlüsselung im geschäftlichen und privaten Umfeld 201

Multimedia Sicherheit

Andreas Westfeld
Angriffe auf eine Spreizspektrummethode für Audio-Steganographie . 217

Oren Halvani, Martin Steinebach, Svenja Neitzel
Lässt sich der Schreibstil verfälschen um die eigene Anonymität in Textdokumenten zu schützen? 229

Michael Hanspach, Michael Goetz
Recent Developments in Covert Acoustical Communications 243

E-Commerce und Mobile Anwendungen

Sebastian Luhn, Ina Bruns, Rainer Böhme
Consumer Participation in Online Contracts – Exploring Cross-Out Clauses 255

Roland Rieke, Maria Zhdanova, Jürgen Repp, Romain Giot, Chrystel Gaber
Verhaltensanalyse zur Erkennung von Missbrauch mobiler Geldtransferdienste 271

| | |
|---|-----|
| Steffen Bartsch, Bernhard Berger, Eric Bodden, Achim Brucker, Jens Heider, Mehmet Kus, Sönke Maseberg, Karsten Sohr, Melanie Volkamer | |
| <i>Zertifizierte Datensicherheit für Android-Anwendungen auf Basis statischer Programmanalysen</i> | 283 |
| Practitioners Track: Quantitative Risikoanalyse | |
| Erik Tews, Christian Schlehuber | |
| <i>Quantitative Ansätze zur IT-Risikoanalyse</i> | 293 |
| Wolfgang Boehmer | |
| <i>Bestimmung des technical-Value at Risk mittels der bedingten Wahrscheinlichkeit, Angriffsbäumen und einer Risikofunktion</i> | 305 |
| Angriffe und Forensik | |
| Steffen Wendzel, Viviane Zwanger, Michael Meier, Sebastian Szlósarczyk | |
| <i>Envisioning Smart Building Botnets</i> | 319 |
| Sven Kälber, Andreas Dewald, Steffen Idler | |
| <i>Forensic Zero-Knowledge Event Reconstruction on Filesystem Metadata</i> | 331 |
| Andreas Ekelhart, Bernhard Grill, Elmar Kiesling, Christine Strauß, Christian Stummer | |
| <i>Komplexe Systeme, heterogene Angreifer und vielfältige Abwehrmechanismen: Simulationsbasierte Entscheidungsunterstützung im IT-Sicherheitsmanagement</i> | 345 |

Forensik

Peter Frühwirt, Peter Kieseberg, Christoph Hochreiner, Sebastian Schrittwieser, Edgar Weippl
InnoDB Datenbank Forensik Rekonstruktion von Abfragen über Datenbank-interne Logfiles 363

Dominik Herrmann, Karl-Peter Fuchs, Hannes Federrath
Fingerprinting Techniques for Target-oriented Investigations in Network Forensics 375

Dominik Brodowski, Andreas Dewald, Felix Freiling, Steve Kovács, Martin Rieger
Drei Jahre Master Online Digitale Forensik: Ergebnisse und Erfahrungen 391

Zuverlässige Systeme & Kritische Infrastrukturen

Sebastian Szlósarczyk, Steffen Wendzel, Jaspreet Kaur, Michael Meier, Frank Schubert
Towards Suppressing Attacks on and Improving Resilience of Building Automation Systems - an Approach Exemplified Using BACnet 407

Johannes Formann
An efficient approach to tolerate attackers in fault-tolerant systems . . . 419

Rafael Accorsi, Julius Holderer, Thomas Stocker, Richard Zahoransky
Security Workflow Analysis Toolkit 433

Western European Workshop on Research in Cryptology 2013

| | |
|--|-----|
| Tobias Nilges, Jörn Müller-Quade, Matthias Huber <i>Structural Composition Attacks on Anonymized Data</i> | 443 |
| Marika Mitrengová <i>Multi-LHL protocol</i> | 461 |
| Eleftheria Makri, Maarten H. Everts, Sebastiaan de Hoogh, Andreas Peter, Harm op den Akker, Pieter Hartel, Willem Jonker <i>Privacy-Preserving Verification of Clinical Research</i> | 481 |