

Inhaltsverzeichnis

IT Angriffe und IT Grundschutz

Isabel Münch

Internationalisierung der IT-Grundschutz-Zertifizierung 1

Sebastian Gajek, Jörg Schwenk, Christoph Wegener

SSL-VA-Authentifizierung als Schutz vor Phishing und Pharming 6

Simone Dimler, Hannes Federrath, Thomas Nowey, Klaus Plöbß

Awareness für IT-Sicherheit und Datenschutz in der Hochschulausbildung –
Eine empirische Untersuchung 18

Klaus-Peter Kossakowski, Jürgen Sander

CarmentiS Auf dem Weg zu einem deutschen IT-Frühwarnsystem 22

Alexander Becher, Zinaida Benenson, Maximillian Dornseif

Tampering with Motes: Real-World Attacks on Wireless Sensor Networks 26

Thorsten Holz

Learning More About Attack Patterns With Honeypots 30

Seda F. Gürses, Thomas Santen

Contextualizing Security Goals: A Method for Multilateral Security
Requirements Elicitation 42

Biometrie

Tobias Scheidat, Franziska Wolf, Claus Vielhauer

Analyse biometrischer Handschriftverifikation im Kontext von Metadaten 54

Gunter Lassmann, Matthias Schwan

Vertrauenswürdige Chipkartenbasierte Biometrische Authentifikation 66

Violeta Uzunova, Arslan Brömme

On Experiences with (In)direct Marking Techniques for Eye Features within
Evaluation of Irides Recognizing Biometric Authentication Systems 78

Zugriffsmanagement

Latifa Boursas, Wolfgang Hommel

Policy-gesteuerte Datenfreigaben und Trust Management im
organisationsübergreifenden Identitäts-Management 91

Stephan Groß Selbstschützende mobile Systeme	103
Xuebing Zhou, Martin Schmucker, Christopher L. Brown Video Perceptual Hashing Using Interframe Similarity	107
Rüdiger Kügler Softwareschutz durch einen Hardware-Dongle	111

Steganographie and Watermarking

Hans-Georg Eber, Felix C. Freiling Kapazitätsmessung eines verdeckten Zeitkanals über HTTP	115
Andreas Westfeld Steganographie für den Amateurfunk	119
Thomas Vogel, Jana Dittmann, Reyk Hillert, Christian Krätzer Design und Evaluierung von Steganographie für Voice-over-IP	131
Martin Steinebach, Sascha Zmudzinski Robustheit digitaler Audiowasserzeichen gegen Pitch-Shifting und Time-Stretching	143

Anonymität

Lexi Pimenidis A Method for Degradation of Anonymity on Mix Systems for E-Mail and Surfing the WWW	155
Melanie Volkamer, Walter Reinhard, Roland Vogt FUSE - ein Internetwahlsystem für zeitlich unbegrenzt geheime Betriebsratswahlen	159
Sebastian Clauß, Stefan Schiffner Anonymität auf Anwendungsebene	171
Stefan Köpsell Vergleich der Verfahren zur Verhinderung von Replay-Angriffen der Anonymisierungsdienste AN.ON und Tor	183
Sebastian Clauß, Stefan Schiffner, Sandra Steinbrecher, Dogan Kesdogan, Tobias Kölsch, Lexi Pimenidis Identitätsmanagement und das Risiko der Re-Identifikation	188

Signaturanwendungen

Thomas Strang Geographische Authentifikation und Signatur	192
Sebastian Schmerl, Ulrich Flegel, Michael Meier Vereinfachung der Signaturentwicklung durch Wiederverwendung	201
Hermann Strack, Christoph Karich BeGovSAH – Begleitforschung zur Umsetzung des eGovernment-Aktionsplans in Sachsen-Anhalt	213
A. Wiesmaier, U. Rauchschalbe, C. Ludwig, B. Henhagl, M. Ruppert, J. Buchmann Intrinsically Legal-For-Trade Objects by Digital Signatures	218

Workshop QSIG2006 - Qualifizierte elektronische Signaturen in Theorie und Praxis

Thomas Krabichler Das Problem der geringen Verbreitung qualifizierter elektronischer Signaturen – Ursachen und Lösungsansätze aus Sicht der Wirtschaftswissenschaften	222
Tobias Straub, Manuel Hartl, Markus Ruppert Digitale Reisepässe in Deutschland – Prozesse und Sicherheitsinfrastruktur	233
Hanno Langweg Malware Attacks on Electronic Signatures Revisited	244
Detlef Hühnlein, Ulrike Korte Rechtliche Rahmenbedingungen der elektronischen Rechnung	256

Workshop Kryptographie in Theorie und Praxis

Ammar Alkassar, Elena Andreeva, Helger Lipmaa SLC: Efficient Authenticated Encryption for Short Packages	270
Frederik Armknecht, Jörg Brandeis, Egor Ilinykh Experimental results on algebraic attacks on stream ciphers	279
Heiko Stamer Verifikation von Ping-Pong Protokollen in Zeit $O(n^2)$	283

Markus Volkmer, Sebastian Wallner Ein IP-Core Design für Schlüsselaustausch, Stromchiffre und Identifikation auf ressourcenbeschränkten Geräten	294
Danny De Cock, Christopher Wolf, Bart Preneel The Belgian Electronic Identity Card (Overview)	298
Andreas Gaupmann, Christian Schausberger, Ulrich Zehl, Jürgen Ecker Implementing Zero-Knowledge Authentication in OpenSSH	302
Jörn Schweisgut Effiziente elektronische Wahlen mit Observer	306
Björn Fay, Jörn Schweisgut, Christian Tobias Identitätsbasierte Kryptografie - Hindernisse auf dem Weg von der Theorie in die Praxis	317
Ulrich Greveler Patentierung kryptographischer Verfahren, die an Hochschulen entwickelt wurden	329
Max Gebhardt, Georg Illies, Werner Schindler A Note on the Practical Value of Single Hash Collisions for Special File Formats	333
 Special Session Safety	
Fevzi Belli, Christof J. Budnik, Axel Hollmann Holistic Testing of Interactive Systems Using Statecharts	345
Shourong Lu, Wolfgang A. Halang A UML Framework for Safety Mechanisms Based on IEC 61508	357
Christian Diedrich, Jan Krause, Andreas Franke UML based software development under safety constraints	361
Wolfgang Ehrenberger Schichtenbetrachtung bei der Genehmigung von Software aufgrund von Betriebserfahrung	369
Francesca Saglietti Interaktion zwischen funktionaler Sicherheit und Datensicherheit	373