Program IFIP SEC 2013

Phishing and Organisational Learning: Wayne Kearney and Hennie Kruger.

Key Derivation Function: The SCKDF Scheme: Chai Wen Chuah, Edward Dawson and Leonie Simpson.

Enforcement of Privacy Requirements: Padmanabhan Krishnan and Kostyantyn Vorobyov.

Evolving A Secure Internet: William Caelli, Lam-For Kwok and Dennis Longley.

Program Transformation for Non-interference Verification on Programs with Pointers: Mounir Assaf, Julien Signoles, Frédéric Tronel and Éric Totel.

New Attacks on Song et al.'s Authentication Protocol for Low-cost RFID Tags: Sarah Abughazalah.

Enhancing Click-Draw based Graphical Passwords using Multi-Touch on Mobile Phones: Yuxin Meng, Wenjuan Li and Lam-For Kwok.

A Lightweight Gait Authentication on Mobile Phone Regardless of Installation Error: Thang Hoang and Thuc Nguyen.

Improving Mobile Device Security with Operating System-level Virtualization: Sascha Wessel, Frederic Stumpf, Ilja Herdt and Claudia Eckert.

Extraction of ABNF Rules from RFCs to Enable Automated Test Data Generation: Markus Gruber, Phillip Wieser, Stefan Nachtnebel, Christian Schanes and Thomas Grechenig.

A Viable System Model of Information Security Governance: Establishing a Baseline to Demonstrate the Importance of Direct Feedback Between Governance and Operations Systems: Ezzat Alqurashi, Gary Wills and Lester Gilbert.

Performance Analysis of File Carving Tools: Thomas Laurenson.

Phishing for the truth: A scenario-based experiment of users' behavioural response to emails: Kathryn Parsons, Agata McCormac, Malcolm Pattinson, Marcus Butavicius and Cate Jerram.

Malware Detection using a Cumulative Timeline Approach: Rafiqul Islam, Irfan Altas and Saiful Islam.

Towards Security-enhanced and Privacy-preserving Mashup Compositions: Heidelinde Hobel, Johannes Heurix, Amin Anjomshoaa and Edgar Weippl.

A review of the theory of planned behaviour in the context of information security policy compliance: Teodor Sommestad and Jonas Hallberg.

Screening Smartphone Applications using Behavioral Signatures: Suyeon Lee, Jehyun Lee and Heejo Lee.

Applying DAC principles to the RDF graph data model: Sabrina Kirrane, Alessandra Mileo and Stefan Decker.

Cost-Benefit Evaluation of Malware Proliferation Mitigation Strategies with Epidemiology Modelling and Game Theory: Theodoros Spyridopoulos, George Oikonomou, Theo Tryfonas and Mengmeng Ge.

Sustainable Pseudo-random Number Generator: Huafei Zhu, Wee-Siong Ng and See-Kiong Ng.

Generating Realistic Application Workloads for Mix-Based Systems for Controllable, Repeatable and Usable Experimentation: Karl-Peter Fuchs, Dominik Herrmann and Hannes Federrath.

On Privacy-Preserving Ways to Porting the Austrian eID System to the Public Cloud: Bernd Zwattendorfer and Daniel Slamanig.

An empirical evaluation of the Android Security Framework: Alessandro Armando, Alessio Merlo and Luca Verderame.

A security engineering process approach for the future development of complex aircraft cabin systems: Hartmut Hintze, Benjamin Wiegraefe and Ralf God.

Secure Outsourcing: an investigation of the fit between clients and providers: Gurpreet Dhillon, Romilla Chowdhuri and Filipe Sá-Soares.

Mobile Device Encryption Systems: Peter Teufl, Thomas Zefferer and Christof Stromberger.

Using CIRA for Privacy Risk Analysis of an Identity Management System: Lisa Rajbhandari and Einar Snekkenes.

A Case for Societal Digital Security Culture: Lotfi Ben Othmane, Harold Weffers, Rohit Ranchal, Pelin Angin, Bharat Bhargava and Mohd Murtadha Mohamad.

Performance analysis of scalable attack representation models: Jin B. Hong and Dong Seong Kim.

ADAPT: A Game Inspired Attack-Defense And Performance Taxonomy: Chris Simmons, Sajjan Shiva, Harkeerat Singh Bedi and Vivek Shandilya.

Smartphone Volatile Memory Acquisition for Security Analysis and Forensics Investigation: Vrizlynn Thing and Zheng-Leong Chua.