

Contents

Network Security and Cyber Attacks

Turning Active TLS Scanning to Eleven	3
<i>Wilfried Mayer and Martin Schmiedecker</i>	
Slow TCAM Exhaustion DDoS Attack	17
<i>Túlio A. Pascoal, Yuri G. Dantas, Iguatemi E. Fonseca, and Vivek Nigam</i>	
Evasive Malware Detection Using Groups of Processes	32
<i>Gheorghe Hăjmașan, Alexandra Mondoc, Radu Portase, and Octavian Creț</i>	
A Malware-Tolerant, Self-Healing Industrial Control System Framework	46
<i>Michael Denzel, Mark Ryan, and Eike Ritter</i>	
Process Discovery for Industrial Control System Cyber Attack Detection	61
<i>David Myers, Kenneth Radke, Suriadi Suriadi, and Ernest Foo</i>	

Security and Privacy in Social Applications and Cyber Attacks Defense

Secure Photo Sharing in Social Networks.	79
<i>Pablo Picazo-Sanchez, Raúl Pardo, and Gerardo Schneider</i>	
Context-Dependent Privacy-Aware Photo Sharing Based on Machine Learning	93
<i>Lin Yuan, Joël Theytaz, and Touradj Ebrahimi</i>	
3LP: Three Layers of Protection for Individual Privacy in Facebook	108
<i>Khondker Jahid Reza, Md Zahidul Islam, and Vladimir Estivill-Castro</i>	
A Framework for Moving Target Defense Quantification	124
<i>Warren Connell, Massimiliano Albanese, and Sridhar Venkatesan</i>	

Private Queries and Aggregations

Query Privacy in Sensing-as-a-Service Platforms.	141
<i>Ruben Rios, David Nuñez, and Javier Lopez</i>	
Secure and Efficient k-NN Queries	155
<i>Hafiz Asif, Jaideep Vaidya, Basit Shafiq, and Nabil Adam</i>	

Secure and Trustable Distributed Aggregation Based on Kademlia	171
<i>Stéphane Grumbach and Robert Riemann</i>	

Operating System and Firmware Security

HyBIS: Advanced Introspection for Effective Windows Guest Protection	189
<i>Roberto Di Pietro, Federico Franzoni, and Flavio Lombardi</i>	

Detection of Side Channel Attacks Based on Data Tainting in Android Systems	205
<i>Mariam Graa, Nora Cuppens-Boulahia, Frédéric Cuppens, Jean-Louis Lanet, and Routa Moussaileb</i>	

The Fuzzing Awakens: File Format-Aware Mutational Fuzzing on Smartphone Media Server Daemons	219
<i>MinSik Shin, JungBeen Yu, YoungJin Yoon, and Taekyoung Kwon</i>	

Towards Automated Classification of Firmware Images and Identification of Embedded Devices	233
<i>Andrei Costin, Apostolis Zarras, and Aurélien Francillon</i>	

Runtime Firmware Product Lines Using TPM2.0	248
<i>Andreas Fuchs, Christoph Krauß, and Jürgen Repp</i>	

User Authentication and Policies

On the Use of Emojis in Mobile Authentication	265
<i>Lydia Kraus, Robert Schmidt, Marcel Walch, Florian Schaub, and Sebastian Möller</i>	

EmojiTCHA: Using Emotion Recognition to Tell Computers and Humans Apart.	281
<i>David Lorenzi, Jaideep Vaidya, Achyuta Aich, Shamik Sural, Vijayalakshmi Atluri, and Joseph Calca</i>	

Assisted Authoring, Analysis and Enforcement of Access Control Policies in the Cloud.	296
<i>Umberto Morelli and Silvio Ranise</i>	

Capturing Policies for BYOD.	310
<i>Joseph Hallett and David Aspinall</i>	

Applied Cryptography and Voting Schemes

Improving Blind Steganalysis in Spatial Domain Using a Criterion to Choose the Appropriate Steganalyzer Between CNN and SRM+EC.	327
<i>Jean-Francois Couchot, Raphaël Couturier, and Michel Salomon</i>	
BinSign: Fingerprinting Binary Functions to Support Automated Analysis of Code Executables.	341
<i>Lina Nouh, Ashkan Rahimian, Djedjiga Mouheb, Mourad Debbabi, and Aiman Hanna</i>	
Decoy Password Vaults: At Least as Hard as Steganography?	356
<i>Cecilia Pasquini, Pascal Schöttle, and Rainer Böhme</i>	
Election-Dependent Security Evaluation of Internet Voting Schemes	371
<i>Stephan Neumann, Manuel Noll, and Melanie Volkamer</i>	

Software Security and Privacy

Combating Control Flow Linearization	385
<i>Julian Kirsch, Clemens Jonischkeit, Thomas Kittel, Apostolis Zarras, and Claudia Eckert</i>	
Ghost Patches: Fake Patches for Fake Vulnerabilities.	399
<i>Jeffrey Avery and Eugene H. Spafford</i>	
SIMBER: Eliminating Redundant Memory Bound Checks via Statistical Inference	413
<i>Hongfa Xue, Yurong Chen, Fan Yao, Yongbo Li, Tian Lan, and Guru Venkataramani</i>	
Towards Systematic Privacy and Operability (PRIOP) Studies	427
<i>Rene Meis and Maritta Heisel</i>	
Data Minimisation: A Language-Based Approach	442
<i>Thibaud Antignac, David Sands, and Gerardo Schneider</i>	

Privacy

Differentially Private Neighborhood-Based Recommender Systems	459
<i>Jun Wang and Qiang Tang</i>	
Privacy-Enhanced Profile-Based Authentication Using Sparse Random Projection.	474
<i>Somayeh Taheri, Md Morshedul Islam, and Reihaneh Safavi-Naini</i>	

Supporting Privacy by Design Using Privacy Process Patterns	491
<i>Vasiliki Diamantopoulou, Christos Kalloniatis, Stefanos Gritzalis, and Haralambos Mouratidis</i>	
Evaluating the Privacy Implications of Frequent Itemset Disclosure	506
<i>Edoardo Serra, Jaideep Vaidya, Haritha Akella, and Ashish Sharma</i>	
Digital Signature, Risk Management, and Code Reuse Attacks	
Forward-Secure Digital Signature Schemes with Optimal Computation and Storage of Signers.	523
<i>Jihye Kim and Hyunok Oh</i>	
RiskInDroid: Machine Learning-Based Risk Analysis on Android	538
<i>Alessio Merlo and Gabriel Claudiu Georgiu</i>	
Using Fraud Patterns for Fraud Risk Assessment of E-services	553
<i>Ahmed Seid Yesuf, Jetzabel Serna-Olvera, and Kai Rannenberg</i>	
Gadget Weighted Tagging: A Flexible Framework to Protect Against Code Reuse Attacks.	568
<i>Liwei Chen, Mengyu Ma, Wenhao Zhang, Gang Shi, and Dan Meng</i>	
Author Index	585

ICT Systems Security and Privacy Protection
32nd IFIP TC 11 International Conference, SEC 2017,
Rome, Italy, May 29-31, 2017, Proceedings
De Capitani di Vimercati, S.; Martinelli, F. (Eds.)
2017, XVI, 586 p. 159 illus., Hardcover
ISBN: 978-3-319-58468-3