Contents

Network Security and Cyber Attacks

Turning Active TLS Scanning to Eleven ........................................... 3
Wilfried Mayer and Martin Schmiedecker

Slow TCAM Exhaustion DDoS Attack ............................................ 17
Túlio A. Pascoal, Yuri G. Dantas, Iguatemi E. Fonseca,
and Vivek Nigam

Evasive Malware Detection Using Groups of Processes .................... 32
Gheorghe Hâjmâșan, Alexandra Mondoc, Radu Portase,
and Octavian Creț

A Malware-Tolerant, Self-Healing Industrial Control System Framework ... 46
Michael Denzel, Mark Ryan, and Eike Ritter

Process Discovery for Industrial Control System Cyber Attack Detection ... 61
David Myers, Kenneth Radke, Suriadi Suriadi, and Ernest Foo

Security and Privacy in Social Applications and Cyber Attacks Defense

Secure Photo Sharing in Social Networks ...................................... 79
Pablo Picazo-Sanchez, Raúl Pardo, and Gerardo Schneider

Context-Dependent Privacy-Aware Photo Sharing Based on Machine
Learning ......................................................................................... 93
Lin Yuan, Joël Theytaz, and Touradj Ebrahimi

3LP: Three Layers of Protection for Individual Privacy in Facebook .... 108
Khondker Jahid Reza, Md Zahidul Islam, and Vladimir Estivill-Castro

A Framework for Moving Target Defense Quantification .................. 124
Warren Connell, Massimiliano Albanese, and Sridhar Venkatesan

Private Queries and Aggregations

Query Privacy in Sensing-as-a-Service Platforms ............................ 141
Ruben Rios, David Nuñez, and Javier Lopez

Secure and Efficient k-NN Queries .............................................. 155
Hafiz Asif, Jaideep Vaidya, Basit Shafiq, and Nabil Adam
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure and Trustable Distributed Aggregation Based on Kademlia</td>
<td>171</td>
</tr>
<tr>
<td><em>Stéphane Grumbach and Robert Riemann</em></td>
<td></td>
</tr>
<tr>
<td><strong>Operating System and Firmware Security</strong></td>
<td></td>
</tr>
<tr>
<td>HyBIS: Advanced Introspection for Effective Windows Guest Protection</td>
<td>189</td>
</tr>
<tr>
<td><em>Roberto Di Pietro, Federico Franzoni, and Flavio Lombardi</em></td>
<td></td>
</tr>
<tr>
<td>Detection of Side Channel Attacks Based on Data Tainting in Android</td>
<td>205</td>
</tr>
<tr>
<td><em>Mariem Graa, Nora Cuppens-Boulahia, Frédéric Cuppens, Jean-Louis Lanet, and Routa Moussaileb</em></td>
<td></td>
</tr>
<tr>
<td>The Fuzzing Awakens: File Format-Aware Mutational Fuzzing on Smartphone Media Server Daemons</td>
<td>219</td>
</tr>
<tr>
<td><em>MinSik Shin, JungBeen Yu, YoungJin Yoon, and Taekyoung Kwon</em></td>
<td></td>
</tr>
<tr>
<td>Towards Automated Classification of Firmware Images and Identification of Embedded Devices</td>
<td>233</td>
</tr>
<tr>
<td><em>Andrei Costin, Apostolis Zarras, and Aurélien Francillon</em></td>
<td></td>
</tr>
<tr>
<td>Runtime Firmware Product Lines Using TPM2.0</td>
<td>248</td>
</tr>
<tr>
<td><em>Andreas Fuchs, Christoph Krauß, and Jürgen Repp</em></td>
<td></td>
</tr>
<tr>
<td><strong>User Authentication and Policies</strong></td>
<td></td>
</tr>
<tr>
<td>On the Use of Emojis in Mobile Authentication</td>
<td>265</td>
</tr>
<tr>
<td><em>Lydia Kraus, Robert Schmidt, Marcel Walch, Florian Schaub, and Sebastian Möller</em></td>
<td></td>
</tr>
<tr>
<td>EmojiTCHA: Using Emotion Recognition to Tell Computers and Humans Apart</td>
<td>281</td>
</tr>
<tr>
<td><em>David Lorenzi, Jaideep Vaidya, Achyuta Aich, Shamik Sural, Vijayalakshmi Atluri, and Joseph Calca</em></td>
<td></td>
</tr>
<tr>
<td>Assisted Authoring, Analysis and Enforcement of Access Control Policies in the Cloud</td>
<td>296</td>
</tr>
<tr>
<td><em>Umberto Morelli and Silvio Ranise</em></td>
<td></td>
</tr>
<tr>
<td>Capturing Policies for BYOD</td>
<td>310</td>
</tr>
<tr>
<td><em>Joseph Hallett and David Aspinall</em></td>
<td></td>
</tr>
</tbody>
</table>
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
   Jean-François Couchot, Raphaël Couturier, and Michel Salomon

BinSign: Fingerprinting Binary Functions to Support Automated Analysis of Code Executables. ................................. 341
   Lina Nouh, Ashkan Rahimian, Djedjiga Mouheb, Mourad Debbabi,
   and Aiman Hanna

Decoy Password Vaults: At Least as Hard as Steganography? ............... 356
   Cecilia Pasquini, Pascal Schöttle, and Rainer Böhme

Election-Dependent Security Evaluation of Internet Voting Schemes ........... 371
   Stephan Neumann, Manuel Noll, and Melanie Volkamer

Software Security and Privacy

Combating Control Flow Linearization ........................................ 385
   Julian Kirsch, Clemens Jonischkeit, Thomas Kittel, Apostolis Zarras,
   and Claudia Eckert

Ghost Patches: Fake Patches for Fake Vulnerabilities. ........................ 399
   Jeffrey Avery and Eugene H. Spafford

SIMBER: Eliminating Redundant Memory Bound Checks via Statistical Inference ......................................................... 413
   Hongfa Xue, Yurong Chen, Fan Yao, Yongbo Li, Tian Lan,
   and Guru Venkataramani

Towards Systematic Privacy and Operability (PRIOP) Studies ................. 427
   Rene Meis and Maritta Heisel

Data Minimisation: A Language-Based Approach ............................... 442
   Thibaud Antignac, David Sands, and Gerardo Schneider

Privacy

Differentially Private Neighborhood-Based Recommender Systems ............ 459
   Jun Wang and Qiang Tang

Privacy-Enhanced Profile-Based Authentication Using Sparse Random Projection .......................................................... 474
   Somayeh Taheri, Md Morshedul Islam, and Reihaneh Safavi-Naini
Supporting Privacy by Design Using Privacy Process Patterns . . . . . . . . . . . . 491
  Vasiliki Diamantopoulou, Christos Kalloniatis, Stefanos Gritzalis,
  and Haralambos Mouratidis

Evaluating the Privacy Implications of Frequent Itemset Disclosure . . . . . . . . 506
  Edoardo Serra, Jaideep Vaidya, Haritha Akella, and Ashish Sharma

Digital Signature, Risk Management, and Code Reuse Attacks

Forward-Secure Digital Signature Schemes with Optimal Computation
  and Storage of Signers . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 523
  Jihye Kim and Hyunok Oh

RiskInDroid: Machine Learning-Based Risk Analysis on Android . . . . . . . . . . 538
  Alessio Merlo and Gabriel Claudiu Georgiu

Using Fraud Patterns for Fraud Risk Assessment of E-services . . . . . . . . . . . 553
  Ahmed Seid Yesuf, Jetzabel Serna-Olvera, and Kai Rannenberg

Gadget Weighted Tagging: A Flexible Framework to Protect Against Code
  Reuse Attacks . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 568
  Liwei Chen, Mengyu Ma, Wenhao Zhang, Gang Shi, and Dan Meng

Author Index . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 585
ICT Systems Security and Privacy Protection
De Capitani di Vimercati, S.; Martinelli, F. (Eds.)
2017, XVI, 586 p. 159 illus., Hardcover
ISBN: 978-3-319-58468-3