Contents

IoT Security

ECDSA on Things: IoT Integrity Protection in Practise .......................... 3
   Johannes Bauer, Ralf C. Staudemeyer, Henrich C. Pöhls,
   and Alexandros Fragkiadakis

Identity in the Internet-of-Things (IoT): New Challenges and Opportunities . . 18
   Kwok-Yan Lam and Chi-Hung Chi

A Lightweight Method for Accelerating Discovery of Taint-Style
Vulnerabilities in Embedded Systems ............................................. 27
   Yaowen Zheng, Kai Cheng, Zhi Li, Shiran Pan, Hongsong Zhu,
   and Limin Sun

Cloud Security

A Self-adaptive Hopping Approach of Moving Target Defense
to thwart Scanning Attacks .......................................................... 39
   Duohe Ma, Cheng Lei, Liming Wang, Hongqi Zhang, Zhen Xu,
   and Meng Li

Research on Security Algorithm of Virtual Machine Live Migration
for KVM Virtualization System ...................................................... 54
   Wei Fan, Zhujun Zhang, Tingting Wang, Bo Hu, Sihan Qing,
   and Degang Sun

Towards Efficient Re-encryption for Secure Client-Side Deduplication
in Public Clouds ................................................................. 71
   Lei Lei, Quanwei Cai, Bo Chen, and Jingqiang Lin

Applied Cryptography

The Security of Individual Bit for XTR ............................................. 87
   Kewei Lv, Si-wei Ren, and Wenjie Qin

On the Robustness of Learning Parity with Noise ................................ 99
   Nan Yao, Yu Yu, Xiangxue Li, and Dawu Gu

The Linear Complexity and 2-Error Linear Complexity Distribution
of 2ⁿ-Periodic Binary Sequences with Fixed Hamming Weight .............. 107
   Wenzhi Pan, Zhenzhen Bao, Dongdai Lin, and Feng Liu
The Variant of Remote Set Problem on Lattices .......................... 124
   Wenwen Wang, Kewei Lv, and Jianing Liu

Compression-Based Integral Prior Classification for Improving
Steganalysis ................................................................. 134
   Viktor Monarev, Ilja Duplischev, and Andrey Pestunov

Group Verification Based Multiple-Differential Collision Attack ....... 145
   Changhai Ou, Zhu Wang, Degang Sun, Xinpeng Zhou, and Juan Ai

Attack Behavior Analytics

A Transparent Learning Approach for Attack Prediction Based on User
Behavior Analysis ....................................................... 159
   Peizhi Shao, Jiuming Lu, Raymond K. Wong, and Wenzhuo Yang

Application of Stylometry to DarkWeb Forum User Identification .... 173
   Thanh Nghia Ho and Wee Keong Ng

SECapacity: A Secure Capacity Scheduler in YARN ..................... 184
   Chuntao Dong, Qingni Shen, Lijing Cheng, Yahui Yang,
   and Zhonghai Wu

Authentication and Authorization

Integrity and Authenticity Protection with Selective Disclosure Control
in the Cloud & IoT ..................................................... 197
   Christoph Frädrich, Henrich C. Pöhls, Wolfgang Popp,
   Noëlle Rakotondravony, and Kai Samelin

MultiPol: Towards a Multi-policy Authorization Framework for RESTful
Interfaces in the Cloud ............................................... 214
   Yang Luo, Tian Puyang, Wu Luo, Qingni Shen, Anbang Ruan,
   and Zhonghai Wu

Provably Secure Identity-Based Identification and Signature Schemes
with Parallel-PVR ..................................................... 227
   Bo Song and Yiming Zhao

Engineering Issues of Cryptographic and Security Systems

Assessment of Efficient Fingerprint Image Protection Principles
Using Different Types of AFIS ........................................... 241
   Martin Draschl, Jutta Hämmerle-Uhl, and Andreas Uhl

Medical Record System Using Blockchain, Big Data and Tokenization .. 254
   Paul Tak Shing Liu
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is it Good or Bad? Disclosure of Medical Ailments on Twitter</td>
<td>262</td>
</tr>
<tr>
<td>B.S. Vidyalakshmi and Raymond Wong</td>
<td></td>
</tr>
<tr>
<td>Weaknesses in Security Considerations Related to Chaos-Based Image Encryption</td>
<td>278</td>
</tr>
<tr>
<td>Thomas Hütter, Mario Preishuber, Jutta Hämmerle-Uhl, and Andreas Uhl</td>
<td></td>
</tr>
<tr>
<td>Low-Cost Hardware Implementation of Elliptic Curve Cryptography</td>
<td>292</td>
</tr>
<tr>
<td>for General Prime Fields</td>
<td></td>
</tr>
<tr>
<td>Yuan Ma, Qinglong Zhang, Zongbin Liu, Chenyang Tu, and Jingqiang Lin</td>
<td></td>
</tr>
<tr>
<td>Differential Fault Analysis on Midori</td>
<td>307</td>
</tr>
<tr>
<td>Wei Cheng, Yongbin Zhou, and Laurent Sauvage</td>
<td></td>
</tr>
<tr>
<td>Privacy Protection</td>
<td></td>
</tr>
<tr>
<td>Private Boolean Query Processing on Encrypted Data</td>
<td>321</td>
</tr>
<tr>
<td>Hoang Giang Do and Wee Keong Ng</td>
<td></td>
</tr>
<tr>
<td>Privacy Leakage via Attribute Inference in Directed Social Networks</td>
<td>333</td>
</tr>
<tr>
<td>Raymond K. Wong and B.S. Vidyalakshmi</td>
<td></td>
</tr>
<tr>
<td>DynaEgo: Privacy-Preserving Collaborative Filtering Recommender System Based on Social-Aware Differential Privacy</td>
<td>347</td>
</tr>
<tr>
<td>Shen Yan, Shiran Pan, Wen-Tao Zhu, and Keke Chen</td>
<td></td>
</tr>
<tr>
<td>Risk Evaluation and Security</td>
<td></td>
</tr>
<tr>
<td>A Comprehensive Study of Co-residence Threat in Multi-tenant Public PaaS Clouds</td>
<td>361</td>
</tr>
<tr>
<td>Weijuan Zhang, Xiaoqi Jia, Chang Wang, Shengzi Zhang, Qingjia Huang, Mingsheng Wang, and Peng Liu</td>
<td></td>
</tr>
<tr>
<td>The Threat of Virtualization: Hypervisor-Based Rootkits on the ARM Architecture</td>
<td>376</td>
</tr>
<tr>
<td>Robert Buhren, Julian Vetter, and Jan Nordholz</td>
<td></td>
</tr>
<tr>
<td>Towards Trustworthy Smart Cyber-Physical Systems</td>
<td>392</td>
</tr>
<tr>
<td>M.W. David, C.R. Yerkes, M.E. Simmons, and W. Franceschini</td>
<td></td>
</tr>
<tr>
<td>Key Management and Language-Based Security</td>
<td></td>
</tr>
<tr>
<td>Vulnerability and Enhancement on Bluetooth Pairing and Link Key Generation Scheme for Security Modes 2 and 3</td>
<td>403</td>
</tr>
<tr>
<td>Da-Zhi Sun and Xiao-Hong Li</td>
<td></td>
</tr>
</tbody>
</table>
Optimizing Secure Computation Programs with Private Conditionals  
Peeter Laud and Alisa Pankova  

Automated Security Proof of Cryptographic Support Commands in TPM 2.0  
Weijin Wang, Yu Qin, Bo Yang, Yingjun Zhang, and Dengguo Feng  

Network Security  
How to Meet Big Data When Private Set Intersection Realizes Constant Communication Complexity  
Sumit Kumar Debnath and Ratna Dutta  

Novel MITM Attacks on Security Protocols in SDN: A Feasibility Study  
Xin Wang, Neng Gao, Lingchen Zhang, Zongbin Liu, and Lei Wang  

A Practical Scheme for Data Secure Transport in VoIP Conferencing  
Dali Zhu, Renjun Zhang, Xiaozhuo Gu, and Haitao Zhu  

Author Index  

XII Contents