

# Contents

## IoT Security

ECDSA on Things: IoT Integrity Protection in Practise . . . . .	3
<i>Johannes Bauer, Ralf C. Staudemeyer, Henrich C. Pöhls, and Alexandros Fragkiadakis</i>	
Identity in the Internet-of-Things (IoT): New Challenges and Opportunities . . .	18
<i>Kwok-Yan Lam and Chi-Hung Chi</i>	
A Lightweight Method for Accelerating Discovery of Taint-Style Vulnerabilities in Embedded Systems . . . . .	27
<i>Yaowen Zheng, Kai Cheng, Zhi Li, Shiran Pan, Hongsong Zhu, and Limin Sun</i>	

## Cloud Security

A Self-adaptive Hopping Approach of Moving Target Defense to thwart Scanning Attacks. . . . .	39
<i>Duohe Ma, Cheng Lei, Liming Wang, Hongqi Zhang, Zhen Xu, and Meng Li</i>	
Research on Security Algorithm of Virtual Machine Live Migration for KVM Virtualization System . . . . .	54
<i>Wei Fan, Zhujun Zhang, Tingting Wang, Bo Hu, Sihan Qing, and Degang Sun</i>	
Towards Efficient Re-encryption for Secure Client-Side Deduplication in Public Clouds . . . . .	71
<i>Lei Lei, Quanwei Cai, Bo Chen, and Jingqiang Lin</i>	

## Applied Cryptography

The Security of Individual Bit for XTR . . . . .	87
<i>Kewei Lv, Si-wei Ren, and Wenjie Qin</i>	
On the Robustness of Learning Parity with Noise . . . . .	99
<i>Nan Yao, Yu Yu, Xiangxue Li, and Dawu Gu</i>	
The Linear Complexity and 2-Error Linear Complexity Distribution of $2^n$ -Periodic Binary Sequences with Fixed Hamming Weight . . . . .	107
<i>Wenlun Pan, Zhenzhen Bao, Dongdai Lin, and Feng Liu</i>	

The Variant of Remote Set Problem on Lattices . . . . .	124
<i>Wenwen Wang, Kewei Lv, and Jianing Liu</i>	
Compression-Based Integral Prior Classification for Improving Steganalysis . . . . .	134
<i>Viktor Monarev, Ilja Duplischew, and Andrey Pestunov</i>	
Group Verification Based Multiple-Differential Collision Attack . . . . .	145
<i>Changhai Ou, Zhu Wang, Degang Sun, Xinping Zhou, and Juan Ai</i>	
<b>Attack Behavior Analytics</b>	
A Transparent Learning Approach for Attack Prediction Based on User Behavior Analysis . . . . .	159
<i>Peizhi Shao, Jiuming Lu, Raymond K. Wong, and Wenzhuo Yang</i>	
Application of Stylometry to DarkWeb Forum User Identification . . . . .	173
<i>Thanh Nghia Ho and Wee Keong Ng</i>	
SECapacity: A Secure Capacity Scheduler in YARN . . . . .	184
<i>Chuntao Dong, Qingni Shen, Lijing Cheng, Yahui Yang, and Zhonghai Wu</i>	
<b>Authentication and Authorization</b>	
Integrity and Authenticity Protection with Selective Disclosure Control in the Cloud & IoT . . . . .	197
<i>Christoph Frädriich, Henrich C. Pöhls, Wolfgang Popp, Noëlle Rakotondravony, and Kai Samelin</i>	
MultiPol: Towards a Multi-policy Authorization Framework for RESTful Interfaces in the Cloud . . . . .	214
<i>Yang Luo, Tian Puyang, Wu Luo, Qingni Shen, Anbang Ruan, and Zhonghai Wu</i>	
Provably Secure Identity-Based Identification and Signature Schemes with Parallel-PVR . . . . .	227
<i>Bo Song and Yiming Zhao</i>	
<b>Engineering Issues of Cryptographic and Security Systems</b>	
Assessment of Efficient Fingerprint Image Protection Principles Using Different Types of AFIS . . . . .	241
<i>Martin Draschl, Jutta Hämmerle-Uhl, and Andreas Uhl</i>	
Medical Record System Using Blockchain, Big Data and Tokenization . . . . .	254
<i>Paul Tak Shing Liu</i>	

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

Optimizing Secure Computation Programs with Private Conditionals . . . . .	418
<i>Peeter Laud and Alisa Pankova</i>	
Automated Security Proof of Cryptographic Support Commands in TPM 2.0 . . . . .	431
<i>Weijin Wang, Yu Qin, Bo Yang, Yingjun Zhang, and Dengguo Feng</i>	
<b>Network Security</b>	
How to Meet Big Data When Private Set Intersection Realizes Constant Communication Complexity . . . . .	445
<i>Sumit Kumar Debnath and Ratna Dutta</i>	
Novel MITM Attacks on Security Protocols in SDN: A Feasibility Study . . .	455
<i>Xin Wang, Neng Gao, Lingchen Zhang, Zongbin Liu, and Lei Wang</i>	
A Practical Scheme for Data Secure Transport in VoIP Conferencing . . . . .	466
<i>Dali Zhu, Renjun Zhang, Xiaozhuo Gu, and Haitao Zhu</i>	
<b>Author Index</b> . . . . .	477

Information and Communications Security  
18th International Conference, ICICS 2016, Singapore,  
Singapore, November 29 – December 2, 2016,  
Proceedings  
Lam, K.Y.; Chi, C.-H.; Qing, S. (Eds.)  
2016, XII, 478 p. 83 illus., Softcover  
ISBN: 978-3-319-50010-2