

Contents

Identity-Embedding Method for Decentralized Public-Key Infrastructure	1
<i>Hiroaki Anada, Junpei Kawamoto, Jian Weng, and Kouichi Sakurai</i>	
Diversification of System Calls in Linux Binaries	15
<i>Sampsa Rauti, Samuel Laurén, Shohreh Hosseinzadeh, Jari-Matti Mäkelä, Sami Hyrynsalmi, and Ville Leppänen</i>	
Outsourced KP-ABE with Enhanced Security	36
<i>Chao Li, Bo Lang, and Jinmiao Wang</i>	
A Simulated Annealing Algorithm for SVP Challenge Through y -Sparse Representations of Short Lattice Vectors	51
<i>Dan Ding and Guizhen Zhu</i>	
Rerandomizable Threshold Blind Signatures	70
<i>Veronika Kuchta and Mark Manulis</i>	
Verifiable Computation of Large Polynomials	90
<i>Jiaqi Hong, Haixia Xu, and Peili Li</i>	
A Characterization of Cybersecurity Posture from Network Telescope Data . . .	105
<i>Zhenxin Zhan, Maochao Xu, and Shouhuai Xu</i>	
Key-Exposure Protection in Public Auditing with User Revocation in Cloud Storage	127
<i>Hua Guo, Fangchao Ma, Zhoujun Li, and Chunhe Xia</i>	
Software Behavior Model Measuring Approach of Combining Structural Analysis and Language Set	137
<i>JingFeng Xue, Yan Zhang, ChangZhen Hu, HongYu Ren, and ZhiQiang Li</i>	
On Cache Timing Attacks Considering Multi-core Aspects in Virtualized Embedded Systems	151
<i>Michael Weiß, Benjamin Weggenmann, Moritz August, and Georg Sigl</i>	
How to Choose Interesting Points for Template Attacks More Effectively? . .	168
<i>Guangjun Fan, Yongbin Zhou, Hailong Zhang, and Dengguo Feng</i>	
NeuronVisor: Defining a Fine-Grained Cloud Root-of-Trust	184
<i>Anbang Ruan and Andrew Martin</i>	

A Privacy-Aware Access Model on Anonymized Data.	201
<i>Xuezhen Huang, Jiqiang Liu, and Zhen Han</i>	
Functional Signatures from Indistinguishability Obfuscation	213
<i>Li Wang, Hongda Li, and Fei Tang</i>	
Lightweight Protocol for Trusted Spontaneous Communication.	228
<i>Przemysław Błaskiewicz, Marek Klonowski, Mirosław Kutylowski, and Piotr Syga</i>	
Using TPM Secure Storage in Trusted High Availability Systems	243
<i>Martin Hell, Linus Karlsson, Ben Smeets, and Jelena Miroslavljevic</i>	
APP Vetting Based on the Consistency of Description and APK.	259
<i>Weili Han, Wei Wang, Xinyi Zhang, Weiwei Peng, and Zheran Fang</i>	
Traitor Tracing Based on Partially-Ordered Hierarchical Encryption	278
<i>Yan Zhu, Dandan Li, and Liguang Yang</i>	
SCIATool: A Tool for Analyzing SELinux Policies Based on Access Control Spaces, Information Flows and CPNs.	294
<i>Gaoshou Zhai, Tao Guo, and Jie Huang</i>	
Faster Pairing Computation on Jacobi Quartic Curves with High-Degree Twists	310
<i>Fan Zhang, Liangze Li, and Hongfeng Wu</i>	
DATAEvictor: To Reduce the Leakage of Sensitive Data Targeting Multiple Memory Copies and Data Lifetimes	328
<i>Min Zhu, Bibo Tu, Ruibang You, Yanzhao Li, and Dan Meng</i>	
Template Attacks Based on Priori Knowledge	346
<i>Guangjun Fan, Yongbin Zhou, Hailong Zhang, and Dengguo Feng</i>	
Some Observations on the Lightweight Block Cipher Piccolo-80	364
<i>Wenyong Zhang, Jiaqi Zhang, and Xiangqian Zheng</i>	
A Memory Efficient Variant of an Implementation of the F_4 Algorithm for Computing Gröbner Bases	374
<i>Yun-Ju Huang, Wei-Chih Hong, Chen-Mou Cheng, Jiun-Ming Chen, and Bo-Yin Yang</i>	
Efficient Public Key Encryption with Field-Free Conjunctive Keywords Search	394
<i>Chenggen Song, Xin Liu, and Yalong Yan</i>	
mOT+: An Efficient and Secure Identity-Based Diffie-Hellman Protocol over RSA Group.	407
<i>Baoping Tian, Fushan Wei, and Chuangui Ma</i>	

Secure $(M + 1)$ st-Price Auction with Automatic Tie-Break 422
 Takashi Nishide, Mitsugu Iwamoto, Atsushi Iwasaki, and Kazuo Ohta

Author Index 439

Keyword Index 441

Trusted Systems

6th International Conference, INTRUST 2014, Beijing,
China, December 16-17, 2014, Revised Selected Papers

Yung, M.; Zhu, L.; Yang, Y. (Eds.)

2015, XIII, 442 p. 83 illus. in color., Softcover

ISBN: 978-3-319-27997-8