

Contents

Cloud and IoT Security

A Generic Construction of Secure-Channel Free Searchable Encryption with Multiple Keywords	3
<i>Keita Emura</i>	
Experiences in Trusted Cloud Computing.	19
<i>Ian Oliver, Silke Holtmanns, Yoan Miche, Shankar Lal, Leo Hippeläinen, Aapo Kalliola, and Sowmya Ravidas</i>	
Private Membership Test Protocol with Low Communication Complexity . . .	31
<i>Sara Ramezani, Tommi Meskanen, Masoud Naderpour, and Valtteri Niemi</i>	
Adaptively Secure Hierarchical Identity-Based Encryption over Lattice	46
<i>Leyou Zhang and Qing Wu</i>	
Risk Modelling of Blockchain Ecosystem	59
<i>Igor Kabashkin</i>	

Network Security

Exploiting AUTOSAR Safety Mechanisms to Launch Security Attacks	73
<i>Ahmad M.K. Nasser, Di Ma, and Sam Lauzon</i>	
CookiesWall: Preventing Session Hijacking Attacks Using Client Side Proxy	87
<i>Somanath Tripathy and Praveen Kumar</i>	
Mixed Wavelet-Based Neural Network Model for Cyber Security Situation Prediction Using MODWT and Hurst Exponent Analysis.	99
<i>Fannv He, Yuqing Zhang, Donghang Liu, Ying Dong, Caiyun Liu, and Chensi Wu</i>	
Detecting DNS Tunneling Using Ensemble Learning.	112
<i>Saeed Shafieian, Daniel Smith, and Mohammad Zulkernine</i>	
Survey on Big Data Analysis Algorithms for Network Security Measurement	128
<i>Hanlu Chen, Yulong Fu, and Zheng Yan</i>	

Platform and Hardware Security

A Practical Method to Confine Sensitive API Invocations on Commodity Hardware	145
<i>Donghai Tian, Dingjun Qi, Li Zhan, Yuhang Yin, Changzhen Hu, and Jingfeng Xue</i>	
Hardware and Software Support for Transposition of Bit Matrices in High-Speed Encryption	160
<i>Patrick Eitschberger, Jörg Keller, and Simon Holmbacka</i>	
An Android Vulnerability Detection System	169
<i>Jiayuan Zhang, Yao Yao, Xiaoqi Li, Jian Xie, and Gaofei Wu</i>	
DNA-Droid: A Real-Time Android Ransomware Detection Framework	184
<i>Amirhossein Gharib and Ali Ghorbani</i>	
Exploring Energy Consumption of Juice Filming Charging Attack on Smartphones: A Pilot Study	199
<i>Lijun Jiang, Weizhi Meng, Yu Wang, Chunhua Su, and Jin Li</i>	

Crypto and Others

A Generic yet Efficient Method for Secure Inner Product.	217
<i>Lihua Wang, Takuya Hayashi, Yoshinori Aono, and Le Trieu Phong</i>	
Randomization Can't Stop BPF JIT Spray	233
<i>Elena Reshetova, Filippo Bonazzi, and N. Asokan</i>	
EEG-Based Random Number Generators	248
<i>Dang Nguyen, Dat Tran, Wanli Ma, and Khoa Nguyen</i>	
Safety of $ABAC_{\alpha}$ Is Decidable	257
<i>Tahmina Ahmed and Ravi Sandhu</i>	
Implementation of Bitsliced AES Encryption on CUDA-Enabled GPU	273
<i>Naoki Nishikawa, Hideharu Amano, and Keisuke Iwai</i>	

Authentication and Key Management

Cryptanalysis and Improvement of an Identity-Based Proxy Multi-signature Scheme	291
<i>Jayaprakash Kar</i>	
The Time Will Tell on You: Exploring Information Leaks in SSH Public Key Authentication	301
<i>Joona Kannisto and Jarmo Harju</i>	

Lightweight Deterministic Non Interactive (ni) Hierarchical Key Agreement Scheme (KAS)	315
<i>Pinaki Sarkar</i>	
A State Recovery Attack on ACORN-v1 and ACORN-v2	332
<i>Deepak Kumar Dalai and Dibyendu Roy</i>	
International Workshop on Security Measurements of Cyber Networks (SMCN-2017)	
A Quantitative Method for Evaluating Network Security Based on Attack Graph	349
<i>Yukun Zheng, Kun Lv, and Changzhen Hu</i>	
SulleyEX: A Fuzzer for Stateful Network Protocol	359
<i>Rui Ma, Tianbao Zhu, Changzhen Hu, Chun Shan, and Xiaolin Zhao</i>	
A Detecting Method of Array Bounds Defects Based on Symbolic Execution	373
<i>Chun Shan, Shiyu Sun, Jingfeng Xue, Changzhen Hu, and Hongjin Zhu</i>	
Machine Learning for Analyzing Malware	386
<i>Yajie Dong, Zhenyan Liu, Yida Yan, Yong Wang, Tu Peng, and Ji Zhang</i>	
Optimal Attack Path Generation Based on Supervised Kohonen Neural Network	399
<i>Yun Chen, Kun Lv, and Changzhen Hu</i>	
Defenses Against Wormhole Attacks in Wireless Sensor Networks	413
<i>Rui Ma, Siyu Chen, Ke Ma, Changzhen Hu, and Xiajing Wang</i>	
A Systematic Analysis of Random Forest Based Social Media Spam Classification	427
<i>Mohammed Al-Janabi and Peter Andras</i>	
Application Research on Network Attacks and Defenses with Zachman Framework	439
<i>Chensi Wu, Yuqing Zhang, and Ying Dong</i>	
A Novel Approach to Network Security Situation Assessment Based on Attack Confidence	450
<i>Donghang Liu, Lihua Dong, Shaoqing Lv, Ying Dong, Fannv He, Chensi Wu, Yuqing Zhang, and Hua Ma</i>	
A Discrete Wavelet Transform Approach to Fraud Detection	464
<i>Roberto Saia</i>	

An Automatic Vulnerabilities Classification Method Based on Their Relevance	475
<i>Hao Zhang, Kun Lv, and Changzhen Hu</i>	
A Novel Threat-Driven Data Collection Method for Resource-Constrained Networks.	486
<i>Jing Li, Lihua Yin, Yunchuan Guo, Chao Li, Fenghua Li, and Lihua Chen</i>	
International Workshop on Security in Big Data (SECBD-2017)	
OE-CP-ABE: Over-Encryption Based CP-ABE Scheme for Efficient Policy Updating	499
<i>Jialu Hao, Jian Liu, Hong Rong, Huimei Wang, and Ming Xian</i>	
Privacy-Preserving Stochastic Gradient Descent with Multiple Distributed Trainers.	510
<i>Le Trieu Phong</i>	
3rd International Workshop on 5G Security and Machine Learning (IW5GS-2017)	
IPsec and IKE as Functions in SDN Controlled Network	521
<i>Markku Vajaranta, Joona Kannisto, and Jarmo Harju</i>	
Probabilistic Transition-Based Approach for Detecting Application-Layer DDoS Attacks in Encrypted Software-Defined Networks	531
<i>Elena Ivannikova, Mikhail Zolotukhin, and Timo Hämäläinen</i>	
Concealing IMSI in 5G Network Using Identity Based Encryption	544
<i>Mohsin Khan and Valteri Niemi</i>	
A Formal Approach for Network Security Policy Relevancy Checking	555
<i>Fakher Ben Ftima, Kamel Karoui, and Henda Ben Ghezala</i>	
Area-Dividing Route Mutation in Moving Target Defense Based on SDN . . .	565
<i>Huiting Tan, Chaojing Tang, Chen Zhang, and Shaolei Wang</i>	
Covert Channels Implementation and Detection in Virtual Environments	575
<i>Irina Mihai, Cătălin Leordeanu, and Alecsandru Pătraşcu</i>	
Subscriber Profile Extraction and Modification via Diameter Interconnection	585
<i>Silke Holtmanns, Yoan Miche, and Ian Oliver</i>	

5G Slicing as a Tool to Test User Equipment Against Advanced Persistent Threats	595
<i>Lauri Isotalo</i>	
Mind Your Right to Know: On De-anonymization Auditability in V2X Communications	604
<i>Tommi Meskanen, Masoud Naderpour, and Valteri Niemi</i>	
2nd International Workshop on Security of the Internet of Everything (SECIOE-2017)	
A Denial of Service Attack Method for IoT System in Photovoltaic Energy System	613
<i>Lulu Liang, Kai Zheng, Qiankun Sheng, Wei Wang, Rong Fu, and Xin Huang</i>	
Improving Alert Accuracy for Smart Vehicles.	623
<i>Chia-Mei Chen, Gu-Hsin Lai, Yen-Chih Kuo, and Tan-Ho Chang</i>	
Hardware Secured, Password-based Authentication for Smart Sensors for the Industrial Internet of Things.	632
<i>Thomas W. Pieber, Thomas Ulz, Christian Steger, and Rainer Matischek</i>	
Towards Dependably Detecting Geolocation of Cloud Servers	643
<i>Leo Hippelainen, Ian Oliver, and Shankar Lal</i>	
Tor De-anonymisation Techniques	657
<i>Juha Nurmi and Mikko S. Niemelä</i>	
Coincer: Decentralised Trustless Platform for Exchanging Decentralised Cryptocurrencies	672
<i>Michal Zima</i>	
Enhancing Resilience of KPS Using Bidirectional Hash Chains and Application on Sensornet	683
<i>Deepak Kumar Dalai and Pinaki Sarkar</i>	
μ Shield: Configurable Code-Reuse Attacks Mitigation For Embedded Systems	694
<i>Ali Abbasi, Jos Wetzels, Wouter Bokslag, Emmanuele Zambon, and Sandro Etalle</i>	
A Role-Based Access Control System for Intelligent Buildings.	710
<i>Nian Xue, Chenglong Jiang, Xin Huang, and Dawei Liu</i>	
Access Control Model for AWS Internet of Things	721
<i>Smriti Bhatt, Farhan Patwa, and Ravi Sandhu</i>	

Privacy Verification Chains for IoT	737
<i>Noria Foukia, David Billard, and Eduardo Solana</i>	
Platform for Detection of Holes in the Bogotá D.C. Road Network and Exposure of the Information in a Web Environment	753
<i>Rendon Sánchez Angel Mecías, Salcedo Parra Octavio José, and Correa Sánchez Lewys</i>	
Author Index	761

Network and System Security

11th International Conference, NSS 2017, Helsinki,
Finland, August 21–23, 2017, Proceedings

Yan, Z.; Molva, R.; Mazurczyk, W.; Kantola, R. (Eds.)

2017, XVIII, 762 p. 214 illus., Softcover

ISBN: 978-3-319-64700-5