

# Contents

## Mobile Security I

|   |    |
|---|----|
| AppShield: Enabling Multi-entity Access Control Cross Platforms<br>for Mobile App Management . . . . .    | 3  |
| <i>Zhengyang Qu, Guanyu Guo, Zhengyue Shao, Vaibhav Rastogi,<br/>Yan Chen, Hao Chen, and Wangjun Hong</i> |    |
| H-Binder: A Hardened Binder Framework on Android Systems . . . . .  | 24 |
| <i>Dong Shen, Zhangkai Zhang, Xuhua Ding, Zhoujun Li, and Robert Deng</i>                                 |    |
| Exploiting Android System Services Through Bypassing Service Helpers. . . .                               | 44 |
| <i>Yacong Gu, Yao Cheng, Lingyun Ying, Yemian Lu, Qi Li, and Purui Su</i>                                 |    |
| Secure Keyboards Against Motion Based Keystroke Inference Attack . . . . .                                | 63 |
| <i>Shaoyong Du, Yue Gao, Jingyu Hua, and Sheng Zhong</i>  |    |

## Network Security

|  |     |
|--|-----|
| Cloud-Based Privacy-Preserving Parking Navigation<br>Through Vehicular Communications . . . . .                | 85  |
| <i>Jianbing Ni, Kuan Zhang, Xiaodong Lin, Yong Yu,<br/>and Xuemin (Sherman) Shen</i>                           |     |
| TruSDN: Bootstrapping Trust in Cloud Network Infrastructure . . . . .  | 104 |
| <i>Nicolae Paladi and Christian Gehrman</i>  |     |
| Key Update at Train Stations: Two-Layer Dynamic Key Update<br>Scheme for Secure Train Communications . . . . . | 125 |
| <i>Sang-Yoon Chang, Shaoying Cai, Hwajeong Seo, and Yih-Chun Hu</i>  |     |
| Faulty Node Repair and Dynamically Spawned Black Hole Search . . . . .   | 144 |
| <i>Wei Shi, Mengfei Peng, Jean-Pierre Corriveau, and William Lee Croft</i>                                     |     |

## Applied Cryptography

|  |     |
|--|-----|
| Attribute-Based Encryption with Granular Revocation . . . . .                        | 165 |
| <i>Hui Cui, Robert H. Deng, Xuhua Ding, and Yingjiu Li</i>                           |     |
| Tokenisation Blacklisting Using Linkable Group Signatures . . . . .                  | 182 |
| <i>Assad Umar, Iakovos Gurulian, Keith Mayes,<br/>and Konstantinos Markantonakis</i> |     |

Privacy-Preserving Multi-pattern Matching . . . . . 199  
*Tao Zhang, Xiuhua Wang, and Sherman S.M. Chow*

Parallel and Dynamic Structured Encryption . . . . . 219  
*Russell W.F. Lai and Sherman S.M. Chow*

**ATCS Workshop - Session 1**

Secure IoT Using Weighted Signed Graphs . . . . . 241  
*Pinaki Sarkar and Morshed Uddin Chowdhury*

A Multi-protocol Security Framework to Support Internet of Things . . . . . 257  
*Biplob R. Ray, Morshed U. Chowdhury, and Jemal H. Abawajy*

Tinder Me Softly – How Safe Are You *Really* on Tinder? . . . . . 271  
*Mark Carman and Kim-Kwang Raymond Choo*

Biometric Authentication Using Facial Recognition . . . . . 287  
*Mozammel Chowdhury, Junbin Gao, and Rafiqul Islam*

Platform as a Service (PaaS) in Public Cloud: Challenges  
 and Mitigating Strategy . . . . . 296  
*Fidel Ikundi, Rafiqul Islam, and Peter White*

**ATCS Workshop - Session 2**

Architecture Support for Controllable VMI on Untrusted Cloud . . . . . 307  
*Jiangyong Shi and Yuexiang Yang*

IacCE: Extended Taint Path Guided Dynamic Analysis of Android  
 Inter-App Data Leakage . . . . . 317  
*Tianjun Wu and Yuexiang Yang*

A Multi-layer Model to Detect Spam Email at Client Side . . . . . 334  
*Kamini (Simi) Bajaj*

**Cloud Security**

Access Control Management for Secure Cloud Storage . . . . . 353  
*Enrico Bacis, Sabrina De Capitani di Vimercati, Sara Foresti,  
 Stefano Paraboschi, Marco Rosa, and Pierangela Samarati*

Attribution of Economic Denial of Sustainability Attacks in Public Clouds. . . 373  
*Mohammad Karami and Songqing Chen*

A Secure and Fast Dispersal Storage Scheme Based on the Learning with Errors Problem . . . . . 392  
*Ling Yang, Fuyang Fang, Xianhui Lu, Wen-Tao Zhu, Qiongxiao Wang, Shen Yan, and Shiran Pan*

ase-PoW: A Proof of Ownership Mechanism for Cloud Deduplication in Hierarchical Environments . . . . . 412  
*Lorena González-Manzano, Jose Maria de Fuentes, and Kim-Kwang Raymond Choo*

**Web Security and Privacy**

Website Forensic Investigation to Identify Evidence and Impact of Compromise . . . . . 431  
*Yuta Takata, Mitsuaki Akiyama, Takeshi Yagi, Takeshi Yada, and Shigeki Goto*

SecWeb: Privacy-Preserving Web Browsing Monitoring with  $w$ -Event Differential Privacy . . . . . 454  
*Qian Wang, Xiao Lu, Yan Zhang, Zhibo Wang, Zhan Qin, and Kui Ren*

A Behavioral Biometrics Based Approach to Online Gender Classification. . . 475  
*Nicolas Van Balen, Christopher T. Ball, and Haining Wang*

Unique on the Road: Re-identification of Vehicular Location-Based Metadata . . . . . 496  
*Zheng Xiao, Cheng Wang, Weili Han, and Changjun Jiang*

**System Security**

BINDNN: Resilient Function Matching Using Deep Learning . . . . . 517  
*Nathaniel Lageman, Eric D. Kilmer, Robert J. Walls, and Patrick D. McDaniel*

TZ-SSAP: Security-Sensitive Application Protection on Hardware-Assisted Isolated Environment . . . . . 538  
*Yanhong He, Xianyi Zheng, Ziyuan Zhu, and Gang Shi*

SQLite Forensic Analysis Based on WAL . . . . . 557  
*Yao Liu, Ming Xu, Jian Xu, Ning Zheng, and Xiaodong Lin*

Impact of Environment on Branch Transfer of Software. . . . . 575  
*Jianming Fu, Yan Lin, and Xu Zhang*

**Mobile Security II**

DroidClassifier: Efficient Adaptive Mining of Application-Layer Header  
for Classifying Android Malware . . . . . 597  
*Zhiqiang Li, Lichao Sun, Qiben Yan, Witawas Srisa-an,  
and Zhenxiang Chen*

GreatEatlon: Fast, Static Detection of Mobile Ransomware. . . . . 617  
*Chengyu Zheng, Nicola Dellarocca, Niccolò Andronio, Stefano Zanero,  
and Federico Maggi*

Data Flow Analysis on Android Platform with Fragment  
Lifecycle Modeling . . . . . 637  
*Yongfeng Li, Jinbin Ouyang, Shanqing Guo, and Bing Mao*

Alde: Privacy Risk Analysis of Analytics Libraries  
in the Android Ecosystem . . . . . 655  
*Xing Liu, Sencun Zhu, Wei Wang, and Jiqiang Liu*

**Hardware Security**

FROPUF: How to Extract More Entropy from Two Ring Oscillators  
in FPGA-Based PUFs . . . . . 675  
*Qinglong Zhang, Zongbin Liu, Cunqing Ma, Changting Li,  
and Lingchen Zhang*

Extracting More Entropy for TRNGs Based on Coherent Sampling . . . . . 694  
*Jing Yang, Yuan Ma, Tianyu Chen, Jingqiang Lin, and Jiwu Jing*

A Very Compact Masked S-Box for High-Performance Implementation  
of SM4 Based on Composite Field . . . . . 710  
*Hailiang Fu, Guoqiang Bai, and Xingjun Wu*

Security Analysis of Vendor Customized Code in Firmware  
of Embedded Device . . . . . 722  
*Muqing Liu, Yuanyuan Zhang, Juanru Li, Junliang Shu, and Dawu Gu*

**Poster Session**

POSTER: Security Analysis of Personal Unmanned Aerial Vehicles . . . . . 743  
*Peng Chen and Hao Chen*

Modeling User Browsing Activity for Application Layer DDoS  
Attack Detection . . . . . 747  
*TungNgai Miu, Chenxu Wang, Daniel Xiapu Luo, and Jinhe Wang*

POSTER: A Framework for IoT Reprogramming . . . . . 751  
*Nian Xue, Lulu Liang, Jie Zhang, and Xin Huang*

Privacy Preserving Data Classification Using Inner Product Encryption . . . . . 755  
*Damien Ligier, Sergiu Carpov, Caroline Fontaine, and Renaud Sirdey*

POSTER: Location Privacy Using Homomorphic Encryption . . . . . 758  
*Peizhao Hu and Siyu Zhu*

SDNGuardian: Secure Your REST NBIs with API-Grained Permission  
 Checking System . . . . . 762  
*Kailei Ren, Qiang Wei, Zehui Wu, and Qingxian Wang*

POSTER: A Novel Wavelet Denoising Method Based on Robust Principal  
 Component Analysis in Side Channel Attacks. . . . . 766  
*Juan Ai, Zhu Wang, Xinping Zhou, and Changhai Ou*

Exploitation of NetEm Utility for Non-payload-based Obfuscation  
 Techniques Improving Network Anomaly Detection . . . . . 770  
*Ivan Homoliak, Martin Teknos, Maros Barabas, and Petr Hanacek*

POSTER: Non-intrusive Face Spoofing Detection Based on Guided  
 Filtering and Image Quality Analysis. . . . . 774  
*Fei Peng, Le Qin, and Min Long*

**Author Index** . . . . . 779



<http://www.springer.com/978-3-319-59607-5>

Security and Privacy in Communication Networks  
12th International Conference, SecureComm 2016,  
Guangzhou, China, October 10-12, 2016, Proceedings  
Deng, R.; Weng, J.; Ren, K.; Yegneswaran, V. (Eds.)  
2017, XV, 781 p. 256 illus., Softcover  
ISBN: 978-3-319-59607-5