Contents

Mobile Security I

AppShield: Enabling Multi-entity Access Control Cross Platforms for Mobile App Management .............................................. 3
Zhengyang Qu, Guanyu Guo, Zhengyue Shao, Vaibhav Rastogi, Yan Chen, Hao Chen, and Wangjun Hong

Dong Shen, Zhangkai Zhang, Xuhua Ding, Zhoujun Li, and Robert Deng

Exploiting Android System Services Through Bypassing Service Helpers. .... 44
Yacong Gu, Yao Cheng, Lingyun Ying, Yemian Lu, Qi Li, and Purui Su

Secure Keyboards Against Motion Based Keystroke Inference Attack .......... 63
Shaoyong Du, Yue Gao, Jingyu Hua, and Sheng Zhong

Network Security

Cloud-Based Privacy-Preserving Parking Navigation Through Vehicular Communications ..................................................... 85
Jianbing Ni, Kuan Zhang, Xiaodong Lin, Yong Yu, and Xuemin (Sherman) Shen

TruSDN: Bootstrapping Trust in Cloud Network Infrastructure .......... 104
Nicolae Paladi and Christian Gehrmann

Key Update at Train Stations: Two-Layer Dynamic Key Update Scheme for Secure Train Communications .......................... 125
Sang-Yoon Chang, Shaoying Cai, Hwajeong Seo, and Yih-Chun Hu

Faulty Node Repair and Dynamically Spawned Black Hole Search .......... 144
Wei Shi, Mengfei Peng, Jean-Pierre Corriveau, and William Lee Croft

Applied Cryptography

Attribute-Based Encryption with Granular Revocation .......................... 165
Hui Cui, Robert H. Deng, Xuhua Ding, and Yingjiu Li

Tokenisation Blacklisting Using Linkable Group Signatures ................. 182
Assad Umar, Iakovos Gurulian, Keith Mayes, and Konstantinos Markantonakis
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy-Preserving Multi-pattern Matching</td>
<td>199</td>
</tr>
<tr>
<td>Tao Zhang, Xiuhua Wang, and Sherman S.M. Chow</td>
<td></td>
</tr>
<tr>
<td>Parallel and Dynamic Structured Encryption</td>
<td>219</td>
</tr>
<tr>
<td>Russell W.F. Lai and Sherman S.M. Chow</td>
<td></td>
</tr>
<tr>
<td>ATCS Workshop - Session 1</td>
<td></td>
</tr>
<tr>
<td>Secure IoT Using Weighted Signed Graphs</td>
<td>241</td>
</tr>
<tr>
<td>Pinaki Sarkar and Morshed Uddin Chowdhury</td>
<td></td>
</tr>
<tr>
<td>A Multi-protocol Security Framework to Support Internet of Things</td>
<td>257</td>
</tr>
<tr>
<td>Biplob R. Ray, Morshed U. Chowdhury, and Jemal H. Abawajy</td>
<td></td>
</tr>
<tr>
<td>Tinder Me Softly – How Safe Are You Really on Tinder?</td>
<td>271</td>
</tr>
<tr>
<td>Mark Carman and Kim-Kwang Raymond Choo</td>
<td></td>
</tr>
<tr>
<td>Biometric Authentication Using Facial Recognition</td>
<td>287</td>
</tr>
<tr>
<td>Mozammel Chowdhury, Junbin Gao, and Rafiqul Islam</td>
<td></td>
</tr>
<tr>
<td>Platform as a Service (PaaS) in Public Cloud: Challenges and Mitigating Strategy</td>
<td>296</td>
</tr>
<tr>
<td>Fidel Ikundi, Rafiqul Islam, and Peter White</td>
<td></td>
</tr>
<tr>
<td>ATCS Workshop - Session 2</td>
<td></td>
</tr>
<tr>
<td>Architecture Support for Controllable VMI on Untrusted Cloud</td>
<td>307</td>
</tr>
<tr>
<td>Jiangyong Shi and Yuexiang Yang</td>
<td></td>
</tr>
<tr>
<td>IacCE: Extended Taint Path Guided Dynamic Analysis of Android Inter-App Data Leakage</td>
<td>317</td>
</tr>
<tr>
<td>Tianjun Wu and Yuexiang Yang</td>
<td></td>
</tr>
<tr>
<td>A Multi-layer Model to Detect Spam Email at Client Side</td>
<td>334</td>
</tr>
<tr>
<td>Kamini (Simi) Bajaj</td>
<td></td>
</tr>
<tr>
<td>Cloud Security</td>
<td></td>
</tr>
<tr>
<td>Access Control Management for Secure Cloud Storage</td>
<td>353</td>
</tr>
<tr>
<td>Enrico Bacis, Sabrina De Capitani di Vimercati, Sara Foresti, Stefano Paraboschi, Marco Rosa, and Pierangela Samarati</td>
<td></td>
</tr>
<tr>
<td>Attribution of Economic Denial of Sustainability Attacks in Public Clouds</td>
<td>373</td>
</tr>
<tr>
<td>Mohammad Karami and Songqing Chen</td>
<td></td>
</tr>
</tbody>
</table>
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, Xinpeng 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
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