

# Contents

## Wireless Security and Privacy

Dandelion - Revealing Malicious Groups of Interest in Large Mobile Networks . . . . .	3
<i>Wei Wang, Mikhail Istomin, and Jeffrey Bickford</i>	
Distance-Based Trustworthiness Assessment for Sensors in Wireless Sensor Networks . . . . .	18
<i>Jongho Won and Elisa Bertino</i>	
Isolation of Multiple Anonymous Attackers in Mobile Networks. . . . .	32
<i>Brian Ricks and Patrick Tague</i>	
No Place to Hide that Bytes Won't Reveal: Sniffing Location-Based Encrypted Traffic to Track a User's Position . . . . .	46
<i>Giuseppe Ateniese, Briland Hitaj, Luigi Vincenzo Mancini, Nino Vincenzo Verde, and Antonio Villani</i>	

## Smartphone Security

Compartmentation Policies for Android Apps: A Combinatorial Optimization Approach . . . . .	63
<i>Guillermo Suarez-Tangil, Juan E. Tapiador, and Pedro Peris-Lopez</i>	
Android Botnets: What URLs are Telling Us . . . . .	78
<i>Andi Fitriah Abdul Kadir, Natalia Stakhanova, and Ali Akbar Ghorbani</i>	

## Systems Security

Unraveling the Security Puzzle: A Distributed Framework to Build Trust in FPGAs. . . . .	95
<i>Devu Manikantan Shila, Vivek Venugopalan, and Cameron D. Patterson</i>	
DisARM: Mitigating Buffer Overflow Attacks on Embedded Devices . . . . .	112
<i>Javid Habibi, Ajay Panicker, Aditi Gupta, and Elisa Bertino</i>	
Service in Denial – Clouds Going with the Winds . . . . .	130
<i>Vit Bukac, Vlasta Stavova, Lukas Nemec, Zdenek Riha, and Vashek Matyas</i>	

**Application Security**

RouteMap: A Route and Map Based Graphical Password Scheme for Better Multiple Password Memory . . . . .	147
<i>Weizhi Meng</i>	
Indicators of Malicious SSL Connections . . . . .	162
<i>Riccardo Bortolameotti, Andreas Peter, Maarten H. Everts, and Damiano Bolzoni</i>	
Multi-constrained Orientation Field Modeling and Its Application for Fingerprint Indexing. . . . .	176
<i>Jinwei Xu and Jiankun Hu</i>	

**Security Management**

A Framework for Policy Similarity Evaluation and Migration Based on Change Detection . . . . .	191
<i>Jaideep Vaidya, Basit Shafiq, Vijayalakshmi Atluri, and David Lorenzi</i>	
MT-ABAC: A Multi-Tenant Attribute-Based Access Control Model with Tenant Trust . . . . .	206
<i>Navid Pustchi and Ravi Sandhu</i>	
Managing Multi-dimensional Multi-granular Security Policies Using Data Warehousing . . . . .	221
<i>Mahendra Pratap Singh, Shamik Sural, Vijayalakshmi Atluri, Jaideep Vaidya, and Ussama Yakub</i>	

**Applied Cryptography**

CLKS: Certificateless Keyword Search on Encrypted Data . . . . .	239
<i>Qingji Zheng, Xiangxue Li, and Aytac Azgin</i>	
Secure Cloud Storage for Dynamic Group: How to Achieve Identity Privacy-Preserving and Privilege Control . . . . .	254
<i>Hui Ma and Rui Zhang</i>	
GP-ORAM: A Generalized Partition ORAM. . . . .	268
<i>Jinsheng Zhang, Wensheng Zhang, and Daji Qiao</i>	
Anonymous Evaluation System. . . . .	283
<i>Kamil Klucznik, Lucjan Hanzlik, Przemysław Kubiak, and Mirosław Kutyłowski</i>	

**Cryptosystems**

An Efficient Leveled Identity-Based FHE. . . . .	303
<i>Fuqun Wang, Kunpeng Wang, and Bao Li</i>	
Evolving Highly Nonlinear Balanced Boolean Functions with Improved Resistance to DPA Attacks. . . . .	316
<i>Ashish Jain and Narendra S. Chaudhari</i>	
Related-Key Rectangle Attack on Round-reduced <i>Khudra</i> Block Cipher . . . .	331
<i>Xiaoshuang Ma and Kexin Qiao</i>	
A New Statistical Approach for Integral Attack. . . . .	345
<i>Jiageng Chen, Atsuko Miyaji, Chunhua Su, and Liang Zhao</i>	

**Short Papers: Cryptographic Mechanisms**

Foundations of Optical Encryption: A Candidate Short-Key Scheme . . . . .	359
<i>Giovanni Di Crescenzo, Ronald Menendez, and Shahab Etemad</i>	
From Pretty Good to Great: Enhancing PGP Using Bitcoin and the Blockchain . . . . .	368
<i>Duane Wilson and Giuseppe Ateniese</i>	
A Scalable Multiparty Private Set Intersection . . . . .	376
<i>Atsuko Miyaji and Shohei Nishida</i>	
Electronic Contract Signing Without Using Trusted Third Party . . . . .	386
<i>Zhiguo Wan, Robert H. Deng, and David Lee</i>	
New Message Authentication Code Based on APN Functions and Stream Ciphers . . . . .	395
<i>Teng Wu and Guang Gong</i>	

**Short Papers: Security Mechanisms**

Assessing Attack Surface with Component-Based Package Dependency. . . . .	405
<i>Su Zhang, Xinwen Zhang, Xinming Ou, Liqun Chen, Nigel Edwards, and Jing Jin</i>	
An Abstraction for the Interoperability Analysis of Security Policies . . . . .	418
<i>Javier Baliosian and Ana Cavalli</i>	
Cryptographically Secure On-Chip Firewalling . . . . .	428
<i>Jean-Michel Cioranescu, Craig Hampel, Guilherme Ozari de Almeida, and Rodrigo Portella do Canto</i>	

Enforcing Privacy in Distributed Multi-domain Network Anomaly Detection . . . . .	439
<i>Christian Callegari, Stefano Giordano, and Michele Pagano</i>	

**Short Papers: Mobile and Cloud Security**

De-anonymizable Location Cloaking for Privacy-Controlled Mobile Systems . . . . .	449
<i>Chao Li and Balaji Palanisamy</i>	
First-Priority Relation Graph-Based Malicious Users Detection in Mobile Social Networks . . . . .	459
<i>Li Xu, Limei Lin, and Sheng Wen</i>	
A Study of Network Domains Used in Android Applications . . . . .	467
<i>Mark E. Fioravanti II, Ayush Shah, and Shengzhi Zhang</i>	
Detecting Malicious Activity on Smartphones Using Sensor Measurements . . .	475
<i>Roger Piqueras Jover, Ilona Murynets, and Jeffrey Bickford</i>	
A Game Theoretic Framework for Cloud Security Transparency . . . . .	488
<i>Abdulaziz Aldribi and Issa Traore</i>	

**Short Papers: Application and Network Security**

Let's Get Mobile: Secure FOTA for Automotive System . . . . .	503
<i>Hafizah Mansor, Konstantinos Markantonakis, Raja Naeem Akram, and Keith Mayes</i>	
VICI: Visual Caller Identification for Contact Center Applications . . . . .	511
<i>P. Krishnan and Navjot Singh</i>	
Performance Analysis of Real-Time Covert Timing Channel Detection Using a Parallel System . . . . .	519
<i>Ross K. Gegan, Rennie Archibald, Matthew K. Farrens, and Dipak Ghosal</i>	
Detecting Malicious Temporal Alterations of ECG Signals in Body Sensor Networks . . . . .	531
<i>Hang Cai and Krishna K. Venkatasubramanian</i>	
<b>Author Index</b> . . . . .	541

Network and System Security

9th International Conference, NSS 2015, New York, NY,  
USA, November 3-5, 2015, Proceedings

Qiu, M.; Xu, S.; Yung, M.; Zhang, H. (Eds.)

2015, XIV, 542 p. 126 illus. in color., Softcover

ISBN: 978-3-319-25644-3