Contents

Wireless Security and Privacy

Dandelion - Revealing Malicious Groups of Interest in Large Mobile Networks .............................................. 3
   Wei Wang, Mikhail Istomin, and Jeffrey Bickford

Distance-Based Trustworthiness Assessment for Sensors in Wireless Sensor Networks .............................................. 18
   Jongho Won and Elisa Bertino

Isolation of Multiple Anonymous Attackers in Mobile Networks ................................................................. 32
   Brian Ricks and Patrick Tague

No Place to Hide that Bytes Won’t Reveal: Sniffing Location-Based Encrypted Traffic to Track a User’s Position ................................................................. 46
   Giuseppe Ateniese, Briland Hitaj, Luigi Vincenzo Mancini, Nino Vincenzo Verde, and Antonio Villani

Smartphone Security

Compartmentation Policies for Android Apps: A Combinatorial Optimization Approach .............................................. 63
   Guillermo Suarez-Tangil, Juan E. Tapiador, and Pedro Peris-Lopez

Android Botnets: What URLs are Telling Us ................................................................. 78
   Andi Fitriah Abdul Kadir, Natalia Stakhanova, and Ali Akbar Ghorbani

Systems Security

Unraveling the Security Puzzle: A Distributed Framework to Build Trust in FPGAs .............................................. 95
   Devu Manikantan Shila, Vivek Venugopal, and Cameron D. Patterson

DisARM: Mitigating Buffer Overflow Attacks on Embedded Devices ................................................................. 112
   Javid Habibi, Ajay Panicker, Aditi Gupta, and Elisa Bertino

Service in Denial – Clouds Going with the Winds ................................................................. 130
   Vit Bukac, Vlasta Stavova, Lukas Nemec, Zdenek Riha, and Vashek Matyas
**Application Security**

RouteMap: A Route and Map Based Graphical Password Scheme for Better Multiple Password Memory

*Weizhi Meng*

Indicators of Malicious SSL Connections

*Riccardo Bortolameotti, Andreas Peter, Maarten H. Everts, and Damiano Bolzoni*

Multi-constrained Orientation Field Modeling and Its Application for Fingerprint Indexing

*Jinwei Xu and Jiankun Hu*

**Security Management**

A Framework for Policy Similarity Evaluation and Migration Based on Change Detection

*Jaideep Vaidya, Basit Shafiq, Vijayalakshmi Atluri, and David Lorenzi*

MT-ABAC: A Multi-Tenant Attribute-Based Access Control Model with Tenant Trust

*Navid Pustchi and Ravi Sandhu*

Managing Multi-dimensional Multi-granular Security Policies Using Data Warehousing

*Mahendra Pratap Singh, Shamik Sural, Vijayalakshmi Atluri, Jaideep Vaidya, and Ussama Yakub*

**Applied Cryptography**

CLKS: Certificateless Keyword Search on Encrypted Data

*Qingji Zheng, Xiangxue Li, and Aytac Azgin*

Secure Cloud Storage for Dynamic Group: How to Achieve Identity Privacy-Preserving and Privilege Control

*Hui Ma and Rui Zhang*

GP-ORAM: A Generalized Partition ORAM

*Jinsheng Zhang, Wensheng Zhang, and Daji Qiao*

Anonymous Evaluation System

*Kamil Klucznik, Lucjan Hanzlik, Przemyslaw Kubiak, and Miroslaw Kutyłowski*
Cryptosystems

An Efficient Leveled Identity-Based FHE. .............................. 303
  Fuqun Wang, Kunpeng Wang, and Bao Li

Evolving Highly Nonlinear Balanced Boolean Functions with Improved
Resistance to DPA Attacks ........................................... 316
  Ashish Jain and Narendra S. Chaudhari

Related-Key Rectangle Attack on Round-reduced Khudra Block Cipher . 331
  Xiaoshuang Ma and Kexin Qiao

A New Statistical Approach for Integral Attack .............................. 345
  Jiageng Chen, Atsuko Miyaji, Chunhua Su, and Liang Zhao

Short Papers: Cryptographic Mechanisms

Foundations of Optical Encryption: A Candidate Short-Key Scheme ...... 359
  Giovanni Di Crescenzo, Ronald Menendez, and Shahab Etemad

From Pretty Good to Great: Enhancing PGP Using Bitcoin
and the Blockchain ....................................................... 368
  Duane Wilson and Giuseppe Ateniese

A Scalable Multiparty Private Set Intersection .............................. 376
  Atsuko Miyaji and Shohei Nishida

Electronic Contract Signing Without Using Trusted Third Party ............. 386
  Zhiguo Wan, Robert H. Deng, and David Lee

New Message Authentication Code Based on APN Functions and Stream
Ciphers ................................................................. 395
  Teng Wu and Guang Gong

Short Papers: Security Mechanisms

Assessing Attack Surface with Component-Based Package Dependency ...... 405
  Su Zhang, Xinwen Zhang, Xinming Ou, Liqun Chen, Nigel Edwards,
  and Jing Jin

An Abstraction for the Interoperability Analysis of Security Policies ...... 418
  Javier Baliosian and Ana Cavalli

Cryptographically Secure On-Chip Firewalling ................................ 428
  Jean-Michel Cioranesco, Craig Hampel, Guilherme Ozari de Almeida,
  and Rodrigo Portella do Canto
Enforcing Privacy in Distributed Multi-domain Network Anomaly Detection

Christian Callegari, Stefano Giordano, and Michele Pagano

439

Short Papers: Mobile and Cloud Security

De-anonymizable Location Cloaking for Privacy-Controlled Mobile Systems

Chao Li and Balaji Palanisamy

449

First-Priority Relation Graph-Based Malicious Users Detection in Mobile Social Networks

Li Xu, Limei Lin, and Sheng Wen

459

A Study of Network Domains Used in Android Applications

Mark E. Fioravanti II, Ayush Shah, and Shenzhi Zhang

467

Detecting Malicious Activity on Smartphones Using Sensor Measurements

Roger Piqueras Jover, Ilona Murynets, and Jeffrey Bickford

475

A Game Theoretic Framework for Cloud Security Transparency

Abdulaziz Aldribi and Issa Traore

488

Short Papers: Application and Network Security

Let’s Get Mobile: Secure FOTA for Automotive System

Hafizah Mansor, Konstantinos Markantonakis, Raja Naeem Akram, and Keith Mayes

503

VICI: Visual Caller Identification for Contact Center Applications

P. Krishnan and Navjot Singh

511

Performance Analysis of Real-Time Covert Timing Channel Detection Using a Parallel System

Ross K. Gegan, Rennie Archibald, Matthew K. Farrens, and Dipak Ghosal

519

Detecting Malicious Temporal Alterations of ECG Signals in Body Sensor Networks

Hang Cai and Krishna K. Venkatasubramanian

531

Author Index

541