The 10th International Conference on Network and System Security (NSS 2016)

Taipei, Taiwan

September 28-30, 2016

Organized By

The Chinese Cryptology and Information Security Association (CCISA)

NSS 2016 Committees

Sponsored By

Springer (LNCS)

Microsoft

TEND micro

Taiwan Information Security Center (TWISC)

TWISC@NTUST

National Taiwan University of Science and Technology

National Dong Hwa University

Chang Gung University

Program of NSS 2016

Wednesday, 28th September, 2016

Time	Session	Location
08:20-08:50	Welcome Opening	
08:50-10:05	NSS Session I: Cloud Computing Security	VF, Shih-Cyuan Room (十全軒)
10:05-10:25	Coffee Break	
10:25-12:00	NSS Session II: System Security	VF, Shih-Cyuan Room (十全軒)
12:00-13:00	Lunch (Eastern and Western Cuisine)	Grand Garden Restaurant (松鶴餐廳)
13:00-14:55	NSS Session III: Security Protocol	VF, Shih-Cyuan Room (十全軒)
14:55-15:15	Coffee Break	
15:15-16:30	NSS Session IV: Security Policy and Access Control	VF, Shih-Cyuan Room (十全軒)

NSS Session I: Cloud Computing Security, **Session Chair: Raylin Tso**

- 08:50-09:15, Raylin Tso. Two-in-One Oblivious Signatures Secure in the Random Oracle Model
- 09:15-09:40, Kai He, Jian Weng, Joseph Liu, Wanlei Zhou and Jia-Nan Liu. Efficient Fine-Grained Access Control for Secure Personal Health Records in Cloud Computing
- 09:40-10:05, Shashank Gupta and Brij Gupta. An Infrastructure-Based Framework for the Alleviation of JavaScript Worms from the OSN in Mobile Cloud Platforms

NSS Session II: System Security, **Session Chair: Fei Xu**

- 10:25-10:50, Qiumao Ma, Wensheng Zhang and Jinsheng Zhang. DF-ORAM: A Practical Dummy Free Oblivious RAM to Protect Outsourced Data Access Pattern
- 10:50-11:15, Wenjuan Li, Weizhi Meng, Lam-For Kwok and Horace Ho Shing Ip. PMFA: Toward Passive Message Fingerprint Attacks on Challenge-based Collaborative Intrusion Detection Networks
- 11:15-11:40, Yen-Lung Lai, Zhe Jin, Bok-Min Goi, Tong-Yuen Chai and Wun-She Yap. Iris Cancellable Template Generation based on Indexing-First-One Hashing
- 11:40-12:00, Fei Xu, Pinxin Liu, Jianfeng Yang, Jing Xu. The Design and Implementation of Multi-Dimensional Bloom Filter Storage Matrix (Short Paper)

NSS Session III: Security Protocol, Session Chair: Tomasz Hyla

- 13:00-13:25, Gang Sheng, Chunming Tang, Wei Gao and Ying Yin. MD-VC Matrix: An Efficient Scheme for Publicly Verifiable Computation of Outsourced Matrix Multiplication
- 13:25-13:50, Wei-Ting Lu, Wei Wu, Shih-Ya Lin, Min-Chi Tseng and Hung-Min Sun. A System of Shareable Keyword Search on Encrypted Data
- 13:50-14:15, Sherman S. M. Chow, Russell W.F. Lai, Xiuhua Wang and Yongjun Zhao. Privacy Preserving Credit Systems
- 14:15-14:35, Tomasz Hyla and Jerzy Pejas. Secure Outsourced Bilinear Pairings Computation for Mobile Devices. (Short Paper)
- 14:35-14:55, Kewei Lv, Ke Wang and Qin Wenjie. Improved Security Proofs for Modular Exponentiation Bits. (Short Paper)

NSS Session IV: Security Policy and Access Control, **Session Chair: Chien-Lung Hsu**

- 15:15-15:40, Prosunjit Biswas, Ravi Sandhu and Ram Krishnan. An Attribute Based Protection Model for JSON Documents
- 15:40-16:05, Maanak Gupta and Ravi Sandhu. The GURA-G Administrative Model for User and Group Attribute Assignment
- 16:05-16:30, Asma Alshehri and Ravi Sandhu. On the Relationship between Finite Domain ABAM and PreUCONA

Thursday, 29th September, 2016

Time	Session	Location
08:30-09:30	Keynote Speech I: Applications of Multimedia Security and Forensic Techniques for Secure Communication, Protection and Detection of Data Content (Anthony T.S. Ho, University of Surrey, UK)	12F, Kunlun Hall (崑崙廳)
09:30-10:30	Keynote Speech II: Privacy-Preserving Big Data Analysis (Atsuko Miyaji, Osaka University/JAIST/CREST, Japan)	12F, Kunlun Hall (崑崙廳)
10:30-11:00	Coffee Break	
11:00-12:00	Keynote Speech III: Staying Secure in a Cloud-First Mobile-First World (Eric Lam, Director for Asia, Enterprise Cybersecurity Group, Microsoft)	12F, Kunlun Hall (崑崙廳)
12:00-12:50	Lunch (Cantonese Cuisine)	Golden Dragon

		Restaurant (金龍餐廳)
12:50-14:50	NSS Session V: Data Mining for Security Application	VF, Shih-Cyuan Room (十全軒)
14:50-15:10	Coffee Break	
15:10-16:25	NSS Session VI: Network Security and Forensic	VF, Shih-Cyuan Room (十全軒)
18:00-20:30	Banquet	VF, Wu-Fu Room (五福軒)

NSS Session V: Data Mining for Security Application, Session Chair: Yu Wang

- 12:50-13:15, Jinshuo Liu, Yabo Xu, Juan Deng, Lina Wang and Lanxin Zhang. Ld-CNNs: A Deep Learning System for Structured Text Categorization Based on LDA in Content Security
- 13:15-13:40, Zisis Tsiatsikas, Dimitris Geneiatakis, Georgios Kambourakis and Stefanos Gritzalis. Realtime DDoS detection in SIP Ecosystems: Machine Learning tools of the trade
- 13:40-14:05, Mohammad Mamun, Mohammad Rathore, Arash Habibi Lashkari, Natalia Stakhanova and Ali Ghorbani. Detecting Malicious URLs Using Lexical Analysis
- 14:05-14:30, Bailin Xie, Yu Wang, Chao Chen and Yang Xiang. Gatekeeping Behavior Analysis for Information Credibility Assessment on Weibo
- 14:30-14:50, Anisur Rahman, Yue Xu, Kenneth Radke and Ernest Foo. Finding Anomalies in SCADA Logs Using Rare Sequential Pattern Mining. (Short Paper)

NSS Session VI: Network Security and Forensic, **Session Chair: Shi-Cho Cha**

- 15:10-15:35, Toshihiro Yamauchi and Yuta Ikegami. HeapRevolver: Delaying and Randomizing Timing of Release of Freed Memory Area to Prevent Use-After-Free Attacks
- 15:35-16:00, Yosuke Ishikuro and Kazumasa Omote. Privacy-Preserving Profile Matching Protocol Considering Conditions
- 16:00-16:25, Nikolai Hampton and Zubair Baig. A Network Timestamp Verification Mechanism for Forensic Analysis

Friday, 30th September, 2016

Time	Session	Location
09:00-10:00	Keynote Speech IV: Towards Secure Search Over Large Encrypted Datasets (Kui Ren, University at Buffalo, State University of New York, USA)	VF, Shih-Cyuan Room (十全軒)
10:00-10:30	Coffee Break	

10:30-12:10	NSS Session VII: Symmetric Key Cryptography	VF, Shih-Cyuan Room (十全軒)
12:10-13:10	Lunch (Cuisine of Jiangsu and Zhejiang)	Yuan-Yuan Restaurant (圓苑餐廳)
13:10-14:25	NSS Session VIII: Digital Signature	VF, Shih-Cyuan Room (十全軒)
14:25-14:45	Coffee Break	
14:45-16:25	NSS Session IX: Authentication	VF, Shih-Cyuan Room (十全軒)
16:25-16:35	Closing Ceremony	

NSS Session VII: Symmetric Key Cryptography, **Session Chair: Kuo-Yu Tsai**

- 10:30-10:55, Min Hsuan Cheng, Reza Sedaghat and Prathap Siddavaatam. A New Adaptable Construction of Modulo Addition with Scalable Security for Stream Ciphers
- 10:55-11:20, Qianqian Yang, Lei Hu, Siwei Sun and Ling Song. Extension of Meet-in-the-Middle Technique for Truncated Differential and Its Application to RoadRunneR
- 11:20-11:45, Tingting Wang, Man Ho Au and Wei Wu. An Efficient Secure Channel Free Searchable Encryption Scheme with Multiple Keywords
- 11:45-12:10, Fangming Zhao and Takashi Nishide. Searchable Symmetric Encryption Supporting Queries with Multiple-Character Wildcards

NSS Session VIII: Digital Signature, **Session Chair: Man Ho Au**

- 13:10-13:35, Man Ho Au, Kaitai Liang, Joseph K. Liu and Rongxing Lu. While Mobile Encounters with Clouds
- 13:35-14:00, Chao Lin, Fei Zhu, Wei Wu, Kaitai Liang and Raymond Choo. A New Transitive Signature Scheme
- 14:00-14:25, Hiroaki Anada, Sushmita Ruj and Kouichi Sakurai. Expressive Rating Scheme by Signatures with Predications on Ratees

NSS Session IX: Authentication, **Session Chair: Jia-Ning Luo**

- 14:45-15:10, Kamil Kluczniak, Jianfeng Wang, Xiaofeng Chen and Miroslaw Kutylowski. Multi-Device Anonymous Authentication
- 15:10-15:35, Jia-Ning Luo, Ming Hour Yang and Cho-Luen Tsai. A Mobile Device-Based Antishoulder-Surfing Identity Authentication Mechanism
- 15:35-16:00, Chang-Shiun Liu, Li Xu, Limei Lin, Min-Chi Tseng, Shih-Ya Lin and Hung-Min Sun. Mutual Authentication with Anonymity for Roaming Service with Smart Cards in Wireless Communications
- 16:00-16:25, Ishai Rosenberg and Ehud Gudes. Evading System-Calls Based Intrusion Detection Systems (From NSS Session VI: Network Security and Forensic)