NSS 2014

The 8th International Conference on Network and System Security

October 15-17, Xi'an, China

Xi'an Tangcheng Hotel ★★★★

Program

General Co-Chairs

Xiaofeng Chen	Xidian University	China
Dieter Gollmann	Hamburg University of Technology	Germany
Xinyi Huang	Fujian Normal University	China

Program Co-Chairs

Man Ho Au	Hong Kong Polytechnic University	Hong Kong, China
Barbara Carminati	University of Insubria	Italy
C.-C. Jay Kuo	University of Southern California	USA

NSS Steering Chair

Yang Xiang	Deakin University	Australia

Sponsored by:

State Key Lab of ISN, Xidian University, China

National 111 Project for Wireless Networks

Fujian Provincial Key Laboratory of Network Security and Cryptology, Fujian Normal University

Oct. 15, 2014

- Registration (8:30-9:30)
- Opening remarks (9:30-10:00)
- Keynote 1 (10:00-11:00) (Chair: Yang Xiang)
- Coffee Break (11:00-11:30)
- Keynote 2 (11:30-12:30) (Chair: Ravi Sandhu)
- Break for lunch (12:30-14:00)
- Session A1：Cloud Computing (14:00-16:05)

Chair: Man Ho Au

- An Approach for the Automated Analysis of Network Access Controls in Cloud Computing Infrastructures (14:00-14:25)

  Thibaut Probst, Eric Alata, Mohamed Kaâniche and Vincent Nicomette

- Adopting Provenance-Based Access Control in OpenStack Cloud IaaS (14:25-14:50)

  Dang Nguyen, Jaehong Park and Ravi Sandhu

- Identity Privacy-Preserving Public Auditing with Dynamic Group for Secure Mobile Cloud Storage (14:50-15:15)

  Yong Yu, Jianbing Ni, Jiang Deng and Ke Huang

- A Formal Model for Isolation Management in Cloud Infrastructure-as-a-Service (15:15-15:40)

  Khalid Bijon, Ram Krishnan and Ravi Sandhu

- Rational secure two-party computation in social cloud (15:40-16:05)

  Yilei Wang and Qiu-Liang Xu

- Coffee break (16:05-16:30)
- Session A2: Access Control (16:30-18:35)

Chair: Barbara Carminati

- Extending OpenStack Access Control with Domain Trust (16:30-16:55)

  Bo Tang and Ravi Sandhu

- Hierarchical Solution for Access Control and Authentication in Software Defined Networks (16:55-17:20)

  Shuangyu He, Jianwei Liu, Jian Mao and Jie Chen

- A Limited Proxy Re-encryption with Keyword Search for Data Access Control in Cloud Computing

(17:20-17:45)

Zhenhua Chen, Shundong Li, Guomin Min, Yilei Wang and Yunjie Chu

- A Location-based Socially Aware Access Control Framework (17:45-18:10)

  Nathalie Baracaldo, Balaji Palanisamy and James Joshi

- Multi-domain direct anonymous attestation scheme from pairings (18:10-18:35)

  Li Yang, Jianfeng Ma, Wei Wang and Chunjie Cao

- Dinner (18:35-21:00)

Oct. 16, 2014

- Session A3: Network Security (8:30-10:35)

Chair: Joseph K. Liu

- psOBJ: Defending against Traffic Analysis with pseudo-Objects (8:30-8:55)

  Yi Tang, Piaoping Lin and Luo Zhaokai

- Universally Composable secure TNC protocol based on IF-T binding to TLS (8:55-9:20)

  Shijun Zhao, Qianying Zhang and Feng Dengguo

- Revisiting Node Injection of P2P Botnet (9:20-9:45)

  Jia Yan, Lingyun Ying, Yi Yang, Purui Su, Qi Li and Dengguo Feng

- On addressing the imbalance problem: A correlated KNN approach for network traffic classification (9:45-10:10)

  Di Wu, Xiao Chen, Chao Chen, Jun Zhang, Yang Xiang and Wanlei Zhou.

- An entropy approach to anomaly-based network attack detection in network forensics (10:10-10:35)

  Khoa Nguyen, Dat Tran, Wanli Ma and Dharmendra Sharma

- Coffee break (10:35-10:55)
- Session A4: Security Analysis I (10:55-12:35)

Chair: Yong Yu

- Exploiting the Hard-wired Vulnerabilities of Newscast via Connectivity-splitting Attack (10:55-11:20)

  Jakub Muszyński, Sebastien Varrette, Juan Luis Jiménez Laredo and Pascal Bouvry

- A Meet-in-the-Middle Attack on Round-Reduced mCrypton Using the Differential Enumeration Technique (11:20-11:45)

  Yonglin Hao, Dongxia Bai and Leibo Li

- Impossible differential cryptanalysis of LBlock with concrete investigation of key scheduling algorithm (11:45-12:10)

  Jiageng Chen, Yuichi Futa, Atsuko Miyaji and Chunhua Su

- Tighter Security Bound of MIBS Block Cipher Against Differential Attack (12:10-12:35)

  Xiaoshuang Ma, Lei Hu, Siwei Sun, Kexin Qiao and Jinyong Shan

- Lunch Break (12:35-14:00)
- Session A5: PKC I (14:00-16:05)

Chair: Hasini Gunasinghe

- Identity Based Threshold Ring Signature from Lattices (14:00-14:25)

  Baodian Wei, Yusong Du, Huang Zhang, Fangguo Zhang, Haibo Tian and Chongzhi Gao

- Identity-Based Transitive Signcryption (14:25-14:50)

  Shuquan Hou, Xinyi Huang and Li Xu

- GO-ABE: Group-Oriented Attribute-Based Encryption (14:50-15:15)

  Mengting Li, Xinyi Huang, Joseph K. Liu and Li Xu

- Jhanwar-Barua's Identity-based Encryption Revisited (15:15-15:40)

  Ibrahim Elashry, Yi Mu and Willy Susilo

- A new Multivariate based Threshold Ring Signature scheme (15:40-16:05)

  Jingwan Zhang and Yiming Zhao

- Coffee break (16:05-16:30)
- Session A6: System Security (16:30-18:35)

Chair: Hung-Min Sun

- Countering Ballot Stuffing and Incorporating Eligibility Verifiability in Helios (16:30-16:55)

  Sriramkrishnan Srinivasan, Chris Culnane, James Heather, Steve Schneider and Zhe Xia

- iCryptoTracer: Dynamic Analysis on Misuse of Cryptographic Functions in iOS Applications (16:55-17:20)

  Yong Li, Yuanyuan Zhang, Juanru Li and Dawu Gu

- Formal Verification of Finite State Transactional Security Policy (17:20-17:45)

  Rajamanickam N, Nadarajan R and Atilla Elçi

- Capturing Android Malware Behaviour using System Flow Graph (17:45-18:10)

  Radoniaina Andriatsimandefitra and Valérie Viet Triem Tong

- Evaluating Host-based Anomaly Detection Systems: Implementation of Frequency-based Algorithms on

ADFA-LD (18:10-18:35)

Miao Xie, Jiankun Hu, Xinghuo Yu and Elizabeth Chang

- Dinner (18:35-21:00)

Oct. 17, 2014

Invited talk (8:00-9:00)(Chair: Xiaofeng Chen)

- Coffee break (9:00-9:20)
- Session A7: PKC II (9:20-12:15)

Chair: Xinyi Huang

- A Dynamic Matching Secret Handshake Scheme without Random Oracles (9:20-9:45)

  Yamin Wen and Zheng Gong

- Lightweight Universally Composable Adaptive Oblivious Transfer (9:45-10:10)

  Vandana Guleria and Ratna Dutta

- How to Evaluate Trust Using MMT (10:10-10:35)

  Khalifa Toumi, Ana Cavalli, Wissam Mallouli, Edgardo Montes De Oca and César Andrés

- Certificate-based Condition Proxy Re-encryption (10:35-11:00)

  Jiguo Li, Xuexia Zhao and Yichen Zhang

- A secure obfuscator for Encrypted Blind Signature Functionality (11:00-11:25)

  Xiao Feng and Zheng Yuan

- Attribute-Based Signing Right Delegation (11:25-11:50)

  Weiwei Liu, Yi Mu and Guomin Yang

- A New Public Key Encryption with Equality Test (11:50-12:15)

  Kaibin Huang, Raylin Tso, Yu-Chi Chen, Wangyu Li and Hung-Min Sun

- Lunch Break (12:15-14:00)
- Session A8: Privacy-Preserving and Key Distribution (14:00-16:30)

Chair: Qianhong Wu

- Fingerprint Indexing Based on Combination of Novel Minutiae Triplet Features (14:00-14:25)

  Wei Zhou, Jiankun Hu, Song Wang, Ian Petersen and Mohammed Bennamoun

- Privacy Preserving Biometrics-Based and User Centric Authentication Protocol (14:25-14:50)

  Hasini Gunasinghe and Elisa Bertino

- eCK Secure Single Round ID-based Authenticated Key Exchange Protocols with Master Perfect Forward Secrecy (14:50-15:15)

  Tapas Pandit, Rana Barua and Somanath Tripathy

- Efficient Sub-/Inter-Group Key Distribution for Ad Hoc Networks (15:15-15:40)

  Bo Qin, Linxiao Wang, Yujue Wang, Qianhong Wu, Wenchang Shi and Bin Liang

- A novel hybrid key revocation scheme for wireless sensor networks (15:40-16:05)

  Mengmeng Ge and Kim-Kwang Raymond Choo

- A proposed approach to compound file fragment identification (16:05-16:30)

  Khoa Nguyen, Dat Tran, Wanli Ma and Dharmendra Sharma

- Coffee break (16:30-17:00)
- Session A9: Security Analysis II (17:00-19:05)

Chair: Jin Li

- Formal Analysis of DAA-Related APIs in TPM 2.0 (17:00-17:25)

  Li Xi and Dengguo Feng

- Cryptanalysis on the authenticated cipher Sablier (17:25-17:50)

  Xiutao Feng and Fan Zhang

- A Stochastic Cyber-Attack Detection Scheme for Stochastic Control Systems Based on Frequency-Domain Transformation Technique (17:50-18:15)

  Yumei Li, Holger Voos, Albert Rosich and Mohamed Darouach

- Security Analysis and Improvement of Femtocell Access Control (18:15-18:40)

  Chien-Ming Chen, Tsu-Yang Wu, Raylin Tso and Mu-En Wu

- A Probabilistic Algebraic Attack on the Grain Family of Stream Ciphers (18:40-19:05)

  Pratish Datta, Dibyendu Roy and Sourav Mukhopadhyay

- Dinner (19:05-21:00)