INTRUST 2015 Programme

Sunday December 6

16:00 - 20:00  Registration (1st Floor, GRAND GONGDA JIANGUO HOTEL of Beijing University of Technology)

Monday December 7

08:00-09:00  Registration (3rd Floor Grand Ballroom, GRAND GONGDA JIANGUO HOTEL of Beijing University of Technology)
09:00-09:15  Open remarks
09:15-10:05  Keynote 1 Robert Deng (Singapore Management University)
10:05-10:55  Keynote 2 Wenchang Shi (Renmin University)
10:55-11:15  Tea & Coffee Break
11:15-12:05  Keynote 3 Rob Spiger (Microsoft)
12:05-13:30  Lunch
13:30-15:00  Session 1: Encryptions and Signature I
15:00-15:10  Best Paper Award
15:10-15:40  Tea & Coffee Break
15:40-17:10  Session 2: Encryptions and Signature II
17:30-19:00  Banquet Dinner

Tuesday December 8

09:00-09:50  Keynote 4 Claire Vishik (TCG)
09:50-10:20  Tea & Coffee Break
10:20-11:50  Session 3: Security Model
11:50-13:30  Lunch
13:30-15:00  Session 4: Trusted technologies
15:00-15:30  Tea & Coffee Break
15:30-17:00  Session 5: Software and System Security
17:00-18:30  Dinner
Monday 7\textsuperscript{th} December 2015

8:00  Registration

9:00  Welcome and Opening, chaired by Yongfei Han

Keynotes I, chaired by Yongfei Han
Keynote 1:  9:15-10:05  
Title: Flexible and Scalable Search and Sharing of Encrypted Data in the Cloud  
Speaker: Prof. Robert H. Deng, Singapore Management University, Singapore.
Keynote 2: 10:05-10:55  
Title: Key Techniques for Implementation of Trusted Software Base With Hardware Backing  
Speaker: Prof. Wenchang Shi, Ren Min University of China.
Keynote 3: 11:15-12:05  
Title: Trusted computing technology in Operating System: Win 10  
Speaker: Rob Spiger, Senior Security Strategist, Microsoft Trustworthy Computing Group.

Session 1: Encryptions and Signature I, chaired by Rob Spiger

Paper1: 13:30-14:00  
Privacy-Preserving Anomaly Detection Across Multi-Domain for Software Defined Networks  
Huishan Bian, Liehuang Zhu, Meng Shen, Mingzhong Wang and Chang Xu.

Paper2: 14:00-14:30  
Distributed Multi-user, Multi-key Searchable Encryptions Resilient Fault Tolerance  
Huafei Zhu.

Paper3: 14:30-15:00  
Another Look at Aggregate Signatures: Their Capability and Security on Network Graphs  
Naoto Yanai, Masahiro Mambo, Kazuma Tanaka, Takashi Nishide and Eiji Okamoto.
Best Paper Award: chaired by Robert H. Deng

Session 2 Encryptions and Signature II, chaired by Antonio de La Piedra
Paper4: 15:40-16:10
Universally Composable Oblivious Database in the Presence of Malicious Adversaries.
Huafei Zhu.

Paper5: 16:10-16:40
Public Key Encryption with Distributed Keyword Search
Veronika Kuchta and Mark Manulis.

Paper6: 16:40-17:10
A Signature Generation Approach based on Clustering for Polymorphic Worm
Jie Wang.

Tuesday 8th December 2015
Keynote 4: 09:00-09:50 Keynotes II, chaired by Robert H. Deng
Title:
Speaker: Claire Vishik

Session 3 Security Model, chaired by Veronika Kuchta
Paper7: 10:20-10:50
Computational Soundness of Uniformity Properties for Multi-party Computation based on LSSS
Hui Zhao and Kouichi Sakurai.

Paper8: 10:50-11:20
Attribute-Based Signatures with Controllable Linkability
Miguel Urquidi, Jean Lancrenon, Dalia Khader and Liqun Chen.

Paper9: 11:20-11:50
A Causality-based Model for Describing the Trustworthiness of a Computing Device
Jiun Yi Yap and Allan Tomlinson.

Session 4 Trusted technologies, chaired by Takanori Yasuda
Paper10: 13:30-14:00
An Application-oriented Efficient Encapsulation System for Trusted Software Development
Zheng Tao, Jun Hu, Jing Zhan, Mo Li and Chunzi Chen.

Paper11: 14:00-14:30
Research on Trusted Bootstrap based on the Universal Smart Card
Lin Yan and Jianbiao Zhang.

Paper12: 14:30-15:00
Efficient implementation of AND, OR and NOT operators for ABCs
Antonio de La Piedra.

Session 5 Software and System Security, chaired by Miguel Urquidi

Paper13: 15:30-16:00
Application of NTRU using Group Rings to Partial Decryption Technique
Takanori Yasuda, Hiroaki Anada and Kouichi Sakurai.

Paper14: 16:00-16:30
RbacIP: a RBAC-based Method for Intercepting and Processing Malicious Applications in Android Platform
Jian Ni, Li Lin and Jian Hu.

Paper15: 16:30-17:00
An audit log protection mechanism based on security chip
Guan Wang, Jian Sun, Jun Zhou and Ziyi Wang.