TRUSTED SYSTEMS

3RD INTERNATIONAL CONFERENCE ON TRUSTED SYSTEMS

PROGRAMME

INTURST 2011

International Exchange Center

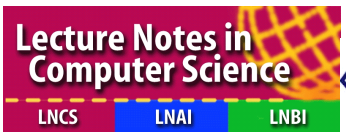
Beijing Institute of Technology

Beijing, P. R. China

November 27-29, 2011

北京理工大學
BEIJING INSTITUTE OF TECHNOLOGY

the Administrative Committee
of Zhongguangcun Haidian
Science Park



Springer

MESSAGE FROM THE GENERAL/PC CHAIRS

Welcome to INTRUST 2011, the Third International Conference on Trusted Systems. The conference programme consists of 22 paper presentations and a workshop, titled "Asian Lounge on Trust, Security and Privacy", which includes 6 keynote speakers: Graeme Proudler (Hewlett-Packard Labs & TCG), Huanguo Zhang (Wuhan University), Moti Yung (Columbia University & Google), Wenbo Mao (DaoliCloud), Yanan Hu (Broadband Wireless IP Standard Group), and Kouichi Sakurai (Kyushu University). Many thanks are due to all the paper presenters and keynote speakers. We hope every participant enjoys the conference and has a lovely time in Beijing.

Robert Deng, Heyuan Huang and Chris Mitchell,
General Chairs
Liqun Chen, Moti Yung and Liehuang Zhu,
Program Chairs

PROGRAMME CONTENTS

INTRUST SCHEDULE, SUNDAY, NOVEMBER 27, 2011

8:00 – 9:00 Registration

9:00 – 9:30 Opening Remarks

SESSION 1 - 2 9:30 A.M – 12:30 P.M

9:30 – 11:00 Session 1: Trusted Services – chaired by Rui Xue

Johannes Winter, Paul Wiegele, Martin Pirker and Ronald Tögl. *A flexible software development and emulation framework for ARM TrustZone*

Chunhua Chen, Chris J. Mitchell and Shaohua Tang. *Building general purpose security services on trusted computing*

Gina Kounga and Liqun Chen. *Enforcing Sticky Policies with TPM and Virtualization Technologies*

Coffee Break 11:00 – 11:30

11:30 – 12:30 Session 2: Mobile Trusted Systems – chaired by Chunhua Chen

Jan-Erik Ekberg and Sandeep Tamrakar. *Mass transit ticketing with NFC mobile phones*

David Derler, Klaus Potzmader, Johannes Winter and Kurt Dietrich. *Anonymous Ticketing for NFC-enabled Mobile Phones*

Lunch 12:30 – 14:00

SESSION 3 - 4 14:00 P.M – 17:30 P.M

14:00 – 15:30 Session 3: Security Analysis (I) – chaired by Lejian Liao

Qinggang Yue, Feng Liu and Rui Xue. *Some Improvements to the Cost-Based Framework for Analyzing Denial of Service Attacks*

Wei Li, Dawu Gu, Zhiqiang Liu, Ya Liu and Xiaohu Huang. *Fault Detection of the MacGuffin Cipher against Differential Fault Attack*

Zijian Zhang, Lejian Liao, Cong Guo and Hongyuan Wang. *Computationally Sound Symbolic Analysis of EAP-TNC Protocol*

Tea Break 15:30 – 16:00

16:00 – 17:30 Session 4: Cryptographic Aspects (I) – chaired by Moti Yung

Yiyuan Luo, Xuejia Lai and Zheng Gong. *Indifferentiability of Domain Extension Modes for Hash Functions*

Michał Koza, Przemyslaw Kubiak, Lukasz Krzywiecki and Miroslaw Kutylowski. *Restricted Identification Scheme and Diffie-Hellman Linking Problem*

Kun Peng. *A Simple And Efficient Exclusion Proof Scheme*

Dinner 18:30 – 20:30

INTRUST SCHEDULE, MONDAY, NOVEMBER 28, 2011

Workshop: Asian Lounge on Trust, Security and Privacy

KEYNOTE 1 - 3 9:30 A.M – 12:10 P.M

9:00 – 10:00 Keynote 1: Graeme Proudler (Senior Researcher of Hewlett-Packard Laboratories; Technical Committee Chairman of Trusted Computing Group) – chaired by Liqun Chen

Revisiting the Trusted Platform Module

Abstract: This presentation describes some of the concepts, constraints and opportunities that will determine the TCG's next generation Trusted Platform Module. While not describing an actual TPM architecture, the material gives some insights into the operation of future TPMs.

Coffee Break 10:00 – 10:30

10:30 – 11:20 Keynote 2: Huanguo Zhang (Professor of Wuhan University) – chaired by Yongbin Zhou

What is TCM (Trusted Cryptography Module)?

Abstract: Trusted Computing is a novel technology of information security and have obtained great achievements in the last ten years. Before 2004, trusted computing had been developed independently in China. The Architecture and main technical lines of ESM (Embedded Security Module) and SQY14 trusted computer of China were consistent with the specifications of TCG, but also had some differences in which there were some innovations also some lacks. After 2004, China learnt many useful techniques of trusted computing form TCG, also TCG learnt some from China. It is well known that there are some cryptographic lacks in TPM of TCG. Therefore China had published "Cryptographic technology specification for trusted computing" in 2006. This specification had adopted Chinese commerce ciphers and improved the scheme of cryptography of TPM. This specification is not contrary to TCG but cipher localization and optimization. In this specification China had named TPM as TCM (Trusted Cryptography Module). This only accentuates action of cipher in trusted computing. This speech will introduce trusted computing and TCM of China.

11:20 – 12:10 Keynote 3: Moti Yung (Professor of Columbia University & Google Inc.) – chaired by Yongbin Zhou

Aspect of Trustworthiness in System Development

Abstract: Trust is a general term with no accurate definition. However, trustworthy systems are ones which can be better suitable to serve critical tasks and be more acceptable to the public. I will review issues of trust in systems and what is needed to get systems that are more, reliable, acceptable and secure.

Lunch 12:10 – 13:30

KEYNOTE 4 - 6 13:30 P.M – 16:00 P.M

13:30 – 14:20 Keynote 4: Wenbo Mao (CEO of Daoli Limited) – chaired by Graeme Proudler

Trust-Chain-less Trusted Computing Model and Realization

Abstract: The TCG model of trusted computing builds a "chain of trust" by measuring software from the root of trust, code by code, way up to applications. Unfortunately, because this style of software measurement goes through some system management software such as a management console which inevitably involves non-measurable human configuration activities, so far no chain of trust has ever been constructed in any sense of completion. Incompletion of the TCG chain of trust has left an important question unanswered: Why and how a virtualized TPM (vTPM) as a virtual machine deployed by a non-measurable management console is trusted? The industry is in an urgent need of a good answer to this question since not only virtualization computing platforms are getting dominant computing environment for cloud computing, but also trust is a key issue for cloud security. We propose a Trust-Chain-Less trusted computing model for virtualization computing platforms, and achieve a practical realization of mutual trust between the TCB and a vTPM which are separated by a non-measurable or even malicious management console.

14:20 – 15:10 Keynote 5: Yanan Hu (Vice Secretary-General of Broadband Wireless IP Standard Group; Security Architect of China IWNCOMM Co.,Ltd) – chaired by Graeme Proudler

A trusted Network System – Development and Applications

Abstract: In this talk, we will introduce a network system, which is able to provide trusted relationship between a terminal and an access point. This system can cooperate with multiple network constructs, such as WLAN, LAN, RFID, PON, BWM, UWB, etc., to enhance security and reliability of these networks. Our major technical contribution is a trusted third party based authentication mechanism that has been adopted by ISO/IEC in international standards. The presentation will also demonstrate how the system is widely used in various equipments, including mobile phones and laptops.

15:10 – 16:00 Keynote 6: Kouichi Sakurai (Professor of Kyushu University) – chaired by Graeme Proudler

Application of Game Theory for Security Modeling and Analysis in Wireless Networks

(Joint work with Dong Hao and Xiaojuan Liao)

Abstract: Wireless network is vulnerable to various kinds of security threats which have been paid a lot of attention and effort. Traditional wireless network security solutions employ either proactive or reactive security schemes to protect the network against intrusions or attacks from our adversaries. However, these existing security schemes are not very intelligent and rely on ad hoc schemes and experimental work. Theoretical models can be applied to provide security-oriented decision making for the wireless

networks, which makes the security systems more intelligent. In the theoretical security models, the attackers and defenders often have conflicting objective, and have interaction with each other. Game theory provides a rich set of mathematical tools and models for analyzing the multi-agent decision making and finding the multi-criteria optimization solutions. It has recently become prevalent in many engineering applications, notably in wireless network security and insider cooperation models. In this talk, we introduced how game theory can be applied to wireless network security; we also show our current study progress about mitigating attacks in wireless cognitive radio networks by using game theory.

Tea Break 16:00 – 16:30

SESSION 5 16:30 P.M – 17:30 P.M

16:30 – 17:30 Section 5: Security Analysis (II) – chaired by Kouichi Sakurai

Christopher Jämthagen, Martin Hell and Ben Smeets. *A technique for remote detection of certain virtual machine monitors*

Yasaman Rabiee Kenari and Reza Azmi. *Reputation Based Trust Modeling Using Dynamic Neuro-Fuzzy Model in P2P Networks*

Conference Banquet/Best Paper Award 18:30 P.M – 21:00 P.M

INTRUST SCHEDULE, TUESDAY, NOVEMBER 29, 2011

SESSION 6 9:00 A.M – 10:30 A.M

9:00 – 10:30 Session 6: Cryptographic Aspects (II) – chaired by Mirek Kutylowski

Danilo Gligoroski, Rune Steinsmo Oedegaard, Rune Erlend Jensen, Ludovic Perret, Jean-Charles Faugere, Svein Johan Knapskog and Smile Markovski. *MQQ-SIG, An Ultra-fast and Provably CMA Resistant Digital Signature Scheme*

Shin'ichiro Matsuo, Daisuke Moriyama and Moti Yung. *Multifactor Authenticated Key Renewal*

Kimmo Halunen. *Multicollisions and graph-based hash functions*

Coffee Break 10:30 – 11:00

SESSION 7 11:00 A.M – 12:00 A.M

11:00 – 12:00 Session 7: Trusted Networks – chaired by Yanan Hu

Dong Hao, Avishek Adhikari and Kouichi Sakurai. *Mixed-Strategy Game Based Trust Management for Clustered Wireless Sensor Networks*

Thouraya Bouabana-Tebibel. *A trust protocol to secure ad hoc networks*

Lunch 12:00 – 13:30

SESSION 8 13:30 P.M – 14:30 P.M

13:30 – 14:30 Session 8: Implementation – chaired by Weili Han

Patrick Koeberl, Jiangtao Li, Roel Maes, Anand Rajan, Claire Vishik and Marcin Wojcik. *Evaluation of a PUF Device Authentication Scheme on a Discrete 0.13um SRAM*

Pengqi Cheng, Yan Gu, Zihong Lv, Jianfei Wang, Wenlei Zhu, Zhen Chen and Jiwei Huang. *A Performance Analysis of Identity-Based Encryption Schemes*

Tea Break 14:30 – 15:00

SESSION 9 15:00 P.M – 16:00 P.M

15:00 – 16:00 Session 9: Direct Anonymous Attestation – chaired by Shin'ichiro Matsuo

Ernie Brickell, Liqun Chen and Jiangtao Li. *A (Corrected) DAA Scheme Using Batch Proof and Verification*

Qin Yu, Xiaobo Chu, Dengguo Feng, Wei Feng. *DAA Protocol Analysis and Verification*

Closing Remarks 16:00 – 16:10

Buffet Dinner 17:00

END OF INTRUST 2011 SCHEDULE