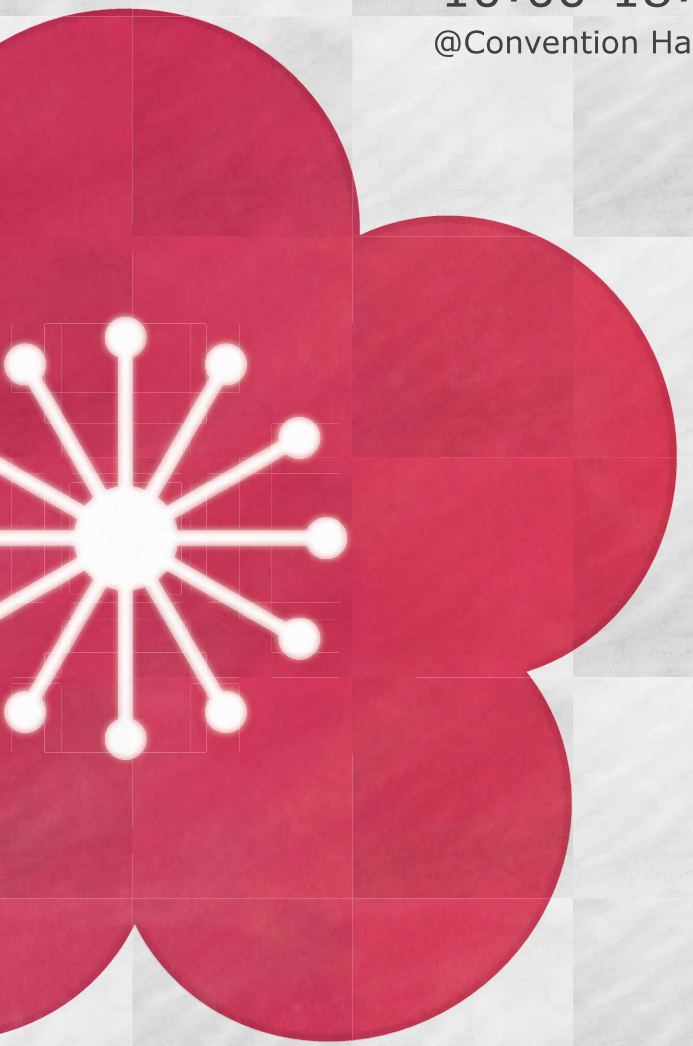
Taiwan - Japan Workshop

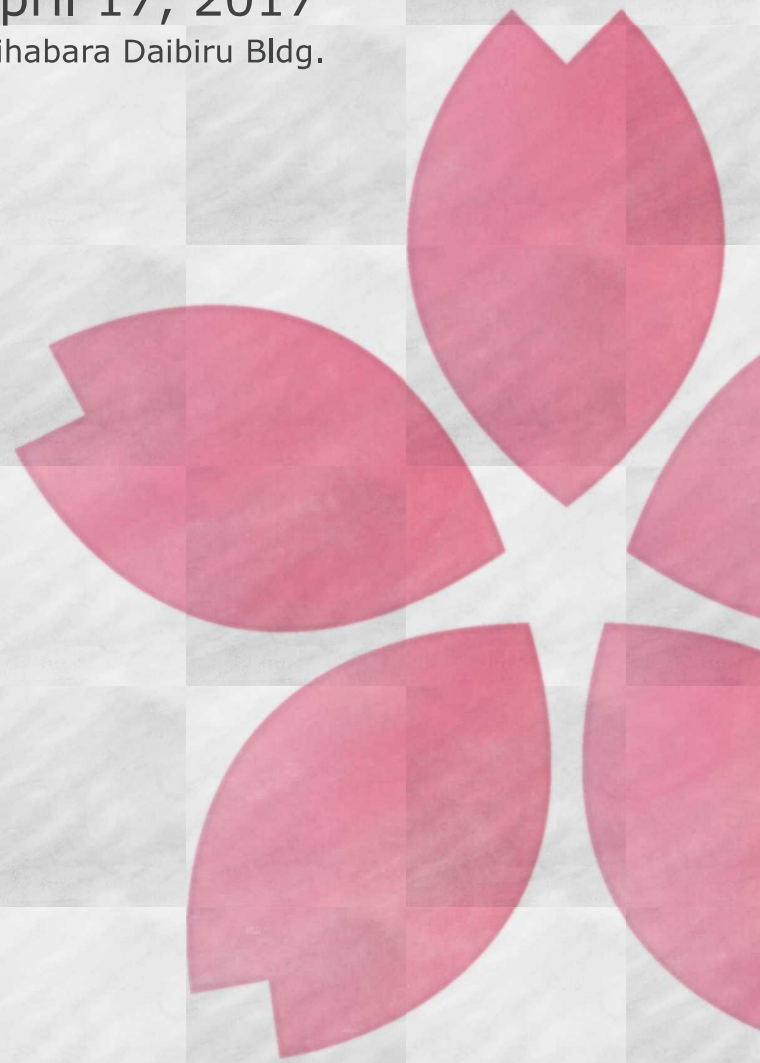
on

"Security and Dependability Technologies for IoT Devices" 2017

10:00-18:00, April 17, 2017

@Convention Hall 5B, Akihabara Daibiru Bldg.





中華民國科技部
Ministry of Science and Technology, R.O.C.

国立研究開発法人
科学技術振興機構
Japan Science and Technology Agency

Taiwan-Japan Workshop on "Security and Dependability Technologies for IoT Devices" 2017

Monday April 17, 2017

at Convention Hall 5B, Akihabara Daibiru Bldg., Tokyo

10:00– 10:25	Welcome Remarks	● MOST representatives: Dr. Wanjiun Liao, Director General of Department of Engineering and Technologies, MOST ● JST representative: Ms. Yoshiko Shirokizawa, Executive Director of JST ● Local host: Prof. Yoshio Tanaka, Director of Information Technology Research Institute, AIST
10:25– 10:35	Group Photo	
10:35-10:45	Tea Break	

Oral Presentations			
Time	No	Speaker, Affiliation	Project Title
Session Chair: ***Dr. Yoshio Tanaka, AIST***			
10:45 – 11:30	O-1	***Dr. Akihiro Nakao****, Professor, Interfaculty Initiative in Information Studies, The University of Tokyo* *and* ***Dr. Wei-Chung Teng****, Associate Professor, Department of Computer Science and Information Engineering, National Taiwan University of Science and Technology*	Research on Identification of Devices and Application for Improving Security in SDN enabled IoT/Cloud System
11:30 – 12:15	O-2	***Dr. Nei Kato****, Professor, Graduate School of Information Sciences, Tohoku University* *andy* ***Dr. Phone Lin****, Professor, Department of Computer Science & Information Engineering, National Taiwan University*	Identify Management towards Internet of Things(IoT) on Machine Type Communications(MTC): Efficiency & Security
12:15– 13:15	Lunch (invitation only)		
13:15– 14:00	O-3	***Dr. Yoshio Tanaka****, Director, Information Technology Research Institute, National Institute of Advanced Industrial Science and Technology* *and* ***Dr. Weicheng Huang****, Research Fellow, National Center for High Performance Computing, National Applied Research Laboratories*	IoT Security Management System with Unclonable Devices

14:00–14:45	O-4	***Dr. Masakazu Soshi**, Associate Professor, Graduate School of Information Sciences, Hiroshima City University* **As deputy for Prof. Atsuko Miyaji of Osaka University, Japanese side PI of the project* *and* ***Dr. Chien-Lung Hsu**, Professor, Department of Information Management, Chang Gung University*	New Lightweight Cryptosystems for IoT devices and application to eHealth Environments in Taiwan
14:45– 15:00		Tea Break	
15:00–15:45	O-5	***Dr. Haruo Yokota**, Professor, Department of Computer Science, School of Computing, Tokyo Institute of Technology* *and* ***Dr. Chia-Mu Yu (co-PI) ,** Assistant Professor* *Department of Computer Science and Engineering, National Chung Hsing University* *As deputy for Prof. Sy-Yen Kuo of National Taiwan University, the Taiwan-based PI of the project*	Reliable compromise-resilient mechanisms for managing the data integrity and privacy of heterogeneous IoT devices
15:45 – 16:15	O-6	***Dr. Hiroaki Kikuchi**, Professor, School of Interdisciplinary Mathematical Sciences, Meiji University* *and* ***Dr. Chun-I Fan**, Professor, Department of Computer Science and Engineering, National Sun Yat-sen University*	Secure IoT-Based Information Platform with Privacy-Preserving Data Mining on Big Data for M-Healthcare

Poster Presentations			
Time	No	Speaker, Affiliation	Poster Title
16:15-17:15	P-1	Dr. Shin-Tyng Lee, Department of Information Management, Chang Gung University	Attribute-based Encryption Scheme and Conference Key Distribution System
	P-2	Dr. Kuo-Hui Yeh, Department of Information Management, Chang Gung University	Walk as Who I Am: A Transparent Authentication System with Plantar Bio-features on Wearables-based IoT Netwroks
	P-3	Dr. Kuniyasu Suzaki , Senior Researcher, Information Technology Research Institute, National Institute of Advanced Industrial Science and Technology	IoT Software Management based on HSM (Hardware Security Module)

	P-4	Dr. SeongHan Shin, Senior Researcher, Information Technology Research Institute, National Institute of Advanced Industrial Science and Technology (AIST)	How to Provide MQTT with Security
	P-5	Ms. Nesrine Berjab, Master Student, Department of Computer Science, School of Computing, Tokyo Institute of Technology	Exploring Multivariate Sensor Attribute and Spatio-Temporal Correlation to Identify Outliers for a WSN Intrusion Detection
	P-6	Shikhar, Master Student, Graduate School of Information Sciences, Tohoku University	Optimal Group Paging-Based Energy Saving in Cellular Internet of Things (IoT)
	P-7	Dr. Chunhua Su, Assistant Professor , Graduate School of Engineering, Osaka University	Light-weight Cryptographic Primitives for IoT Devices
	P-8	Dr. Ping Du, Project Assistant Professor , the University of Tokyo	Identificationof Malicious Processes in IoT devices using FLARE
	P-9	Ms. Xuping Huang, Researcher, Meiji University	Authentication-Secured Watermarking Method for Multiple Tampering Positions Detection and Identification
17:15-17:25	Presentation of Best Poster Paper Award		
17:25-17:35	Closing Remarks	Dr. Lu-Sheng Hong, Director of Science and Technology Division, Taipei Economic and Cultural Representative Office in Japan	
18:15-20:15	Dinner Meeting at "Chef's Table R&D" (invitation only)		

(Site visit schedule applicable to the Taiwanese delegation members only)

Tuesday April 18, 2017 –Site Visit to KDDI and NICT

8:00 Meet JST officials (**Clement Ng, Ryuichiro Kawai**) at the **lobby of Hotel Sunroute Plaza Shinjuku** and board bus to KDDI

10:30-12:00 **Arrive at KDDI Research, Inc.**

Agenda
- 10:30-11:00 Introduction to KDDI
- 11:00-11:20 Privacy Overview
- 11:20-11:40 Security Overview
- 11:40-12:00 IoT Security Presentation

12:00-13:30 **Networking Lunch at KDDI**

13:30 Transfer by bus to NICT

15:00-16:30 **Arrive at National Institute of Information and Communications Technology (NICT)**

Agenda
- 15:00-15:25 Introduction to NICT
- 15:25-16:05 Introduction to NICTER – An R&D Project against Cyber Attacks
- 16:05-16:25 Q&A
- 16:30-16:50 Visit to Exhibition Room

17:00 Transfer by bus from NICT to Hotel

18:00 Arrive at hotel

18:30 **Meet at Hotel Lobby**

19:00-21:00 **Banquet at "Higashiyama" in Shinjuku**

Wednesday April 19, 2017 – Site Visit to AIST

8:45 Meet with JST officials at the **lobby of Hotel Sunroute Plaza Shinjuku** and board bus to AIST

10:20 (AIST) **Arrive at National Institute of Advanced Industrial Science and Technology**

Agenda
- 10:30-10:40 Introduction to AIST
- 10:40-11:00 IoT Software Management based on HSM
- 11:00-11:20 Related issues to reliability and security
- 11:20-11:40 MiRK: An embedded software kernel for enhancing electro-magnetic noise tolerance
- 11:40-12:00 Introduction of AIST AI Cloud

12:00-12:10 Transfer from AIST to restaurant

12:10-13:30 **Networking Lunch at "Brasserie 2Plats"**

13:30-15:00 Transfer by bus from restaurant to Hotel

O-1 CV (Oral Presentation)

	**Akihiro Nakao**
Job Title:	Professor
Organization:	The University of Tokyo
Major Field:	Computer Science
Education:	Ph.D. Computer Science, Princeton University, USA, 2005. M.Sc. Computer Science, Princeton University, USA, 2000. M.Sc. Engineering, The University of Tokyo, Japan, 1994. B.Sc. Physics, The University of Tokyo, Japan, 1991.
Job history:	The University of Tokyo Professor , Feb. 2014-present. Associate Professor, April 2005-Feb. 2014. The University of Utah, Salt Lake City, UT Adjunct Professor, July 2014-present Adjunct Associate Professor, July 2012-June 2014 International Business Machines, Tokyo, Japan. Researcher, Tokyo Research Laboratory, Tokyo, 1998-March 2005. Engineer, Austin Laboratory, TX, USA, May 1995-Nov. 1995. Engineer, Yamaoto Laboratory, Tokyo, April 1994-March 1998.

O-1 Abstract (Oral Presentation)

Name of Presenter

Akihiro Nakao

Presentation Title

Research on Identification of Devices and Application for Improving Security in SDN enabled IoT/Cloud System

Abstract :

The objective of the collaboration research project is to ensure security and privacy for IoT taking advantage of flexibly programmable communication infrastructure through SDN and NFV technologies. The methodology of the research attempts to resolve the security challenges of IoT from three points of views, (1) application (malware detection, prevention, and elimination) (2) data (personal and privacy data consideration), and (3) device (device identification). The research project has great potential scientific contribution in each aspect above. For application area, identification and classification of legitimate applications and malicious ones require not only sound system design but deep learning within network. For data aspect, identification of personal and private data also requires data mining from a vast amount of information flowing in the network. For device area, one of the most difficult challenges is addressed, namely, identification of devices among trillions of sensors, devices and smartphones that requires both mathematical analysis and system design with universally applicable metrics to a wide variety of devices. The methodologies to be developed in these three aspects of the study certainly contribute to the IoT research community. The mode of cooperation with Taiwanese pertners was carefully designed in such a way that the team is divided into three work groups, each of which corresponds to one of the three aspects of the study, namely, application, data and device.

O-1 CV (Oral Presentation)

	**Wei-Chung Teng**
Job Title:	Associate Professor
Organization:	National Taiwan University of Science and Technology
Major Field:	Network security, Software-Defined Networking, Telepresence systems
Education:	DEng, University of Tokyo, Japan, 2001. M.S. CSIE, National Chiao-Tung University, Taiwan, 1994. B.Sc. CSIE, National Chiao-Tung University, Taiwan, 1992.
Job history:	Associate Professor of Dept. of CSIE, NTUST, Feb. 2014-present. Assistant Professor of Dept. of CSIE, NTUST, Aug. 2003-Jan. 2014. Manager, R&D Division, BOX Solutions Corp., Apr. 2002-Jun. 2003.

O-1 Abstract (Oral Presentation)

Name of Presenter Wei-Chung Teng
Presentation Title Clock Skew Measurement over Networks for Device Identification
Abstract : Accurate clock skew measurements of remote devices over network connections are crucial to device fingerprinting. Although the variant and immeasurable delay in each packet prevents the measurer from getting the real clock offset, the local minimum delays and the majority of delays delineate the clock offset shifts, and are used by existing approaches to estimate the skew. However, events during skew measurement like time synchronization and rerouting caused by switching network interface or base transceiver station may break the trend into multi-segment patterns. To estimate the clock skew in this kind of patterns, two approaches to measure clock skew over networks have been developed in the joint Taiwanese-Japanese research project. The first one is based on Hough transform, and the second one is based on entropy of time offsets. Both approaches will be introduced and compared in the presentation.

O-2 CV (Oral Presentation)

	**Nei Kato**
Job Title:	Professor
Organization:	Graduate School of Information Sciences, Tohoku University
Major Field:	Computer networking, wireless mobile communications, satellite communications, ad hoc & sensor & mesh networks, smart grid, and pattern recognition.
Education:	1986: Bachelor degree, Polytechnic University, Japan 1988: Master degree, Tohoku University, Japan 1991: Doctor degree, Tohoku University, Japan
Job history:	1991-1995: Assistant professor 1996-2002: Associate Professor 2003-Present: Professor 2013: Special Assistant to the President of Tohoku University 2015-Present: Director of Research Organization of Electrical Communication of Tohoku University

Name of Presenter
Phone Lin and Nei Kato

Presentation Title
Identity Management towards Internet of Things (IoT) on Machine Type Communications (MTC): Efficiency & Security

Abstract :
The Internet of Things (IoT) is an emerging area of technology, which is highly anticipated to be capable of connecting trillions of machines for a plethora of exciting applications. Under current networking mechanisms, however, the performance of IoT may suffer from inefficient and non-secure identity (ID) handling and significant signaling overhead due to the trillions of connected devices. As a remedy, our proposal focuses on the efficiency and security strength of ID management for the IoT domain. Based upon our broad research experience, the entire issue will be segmented into three brand new approaches or topics as follows. In the initial topic, an ID management framework based on a grouping ID concept to support device-triggering services will be studied. In the second topic, an efficient scheme using hash functions to reduce both storage and communication overhead for group communication will be investigated. Then, in the third topic, a secure key caching mechanism will be developed to maintain the security strength under reduced signaling requirements. For all our proposed solutions, simulation and analysis will be conducted to provide convincing assessment of the performance. Our comprehensive modeling is anticipated to advance the general understanding of the issue. Additionally, the enhanced ID management and security architecture can be expected to bring advantages to network operators, content providers, and machine-to-machine (M2M) end-users for lower operation cost, higher user-satisfaction, and energy efficiency as well as secure communication, respectively.

O-2 CV (Oral Presentation)

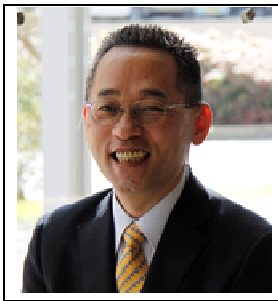
	**Phone Lin**
Job Title:	Professor
Organization:	Department of Computer Science & Information Engineering, National Taiwan University
Major Field:	Machine to Machine (M2M)/Internet of Things (IoT); Software Defined Networks (SDN); HetNet for 5G Networks; Green Communications
Education:	1997.09-2001.01: Ph.D. in Computer Science & Information Engineering, National Chiao Tung University, Hsinchu, R.O.C. 1992.09-1996.06: B.S. in Computer Science & Information Engineering, National Chiao Tung University, Hsinchu, R.O.C.
Job history:	**Current Position** Professor, Department of Computer Science and Information Engineering, and Graduate Institute of Networking and Multimedia, Telecommunications Research Center, Graduate Institute of Medical Device and Imaging, National Taiwan University **Membership** IEEE Fellow through IEEE ComSoc ACM Senior Member **Journal Editor (partial list)** 2016.01-present: Editor, IEEE Network Magazine 2013.07-present: Editor, IEEE Internet of Things Journal (IoT-J) 2011.10-present: Editor, IEEE Wireless Communications Magazine 2010.12-present: Area Editor, Computer Networks Journal (Elsevier) 2006.06-present: Editor, IEEE Transactions on Vehicular Technology **Academic Experience (2014-2016)** 2016.7-8: Visiting Fellow, Princeton University, USA 2015-2016: Officer of Professional Activities, IEEE Taipei Section 2014-2015: Chair, IEEE Vehicular Technology Society (VTS) Taipei Chapter

Name of Presenter:
Phone Lin

Presentation Title: Identity Management towards Internet of Things (IoT) on Machine Type Communications (MTC): Efficiency

Abstract :
Machine-Type Communications (MTC) proposed by the 3GPP working group is an enabling technology for a wide range of applications involving autonomy devices. MTC is actively evolving to support Internet of Things (IoT) and has becomes one of the 5G requirements. In IoT, massive MTC devices will be connected to Internet, which may cause significant overload to networks, such as the wireline and wireless resource, ID resources, and so on. We will focus on the efficiency for the ID management towards IoT on MTC, which are the results of our project in the first two years. The presentation consists of the following two topics: **Topic 1.** In MTC, a device is identified by a unique identifier (ID) in the core network domains (e.g., IMSI and MSISDN in LTE networks), which is the same as that in a human-to-human device. With the unique ID, the MTC Application Server (MTC AS) can deliver the message (i.e., triggering request message) to an MTC device. Because a huge number of MTC devices may coexist in the network, it is challenging to use the limited number of IDs to support huge number of MTC devices. To resolve the issue, we propose an efficient ID management mechanism based on the “ID sharing” concept. The proposed mechanism, based on some criteria, groups MTC devices. The devices in the same group will share the same ID, one of which is allowed to attach to the network at a given time. In other words, the MTC device in the same group needs to attach to the network in turn to wait for the triggering request message from the MTC AS. The proposed mechanism has been filed for ROC and US patents. We also implement a platform to realize the proposed mechanism. **Topic 2.** We discuss how to efficiently and fairly share the network resources among the MTC devices in the same group. As forming resource sharing device groups to be a major solution mitigating instantaneous signaling load, we propose a graph-model based approach to minimize the number of required MTC groups while meeting execution time constraints from IoT applications. The minimization problem is formulated as a variation of bin packing problem with dynamic bin sizes. From the point of view “relaxing dynamic constraints in a group”, a mixed-integer linear programming (MILP) problem can be defined with efficient solvers available. Alternatively, the unique dynamic bin size property can be handled by a specially designed best fit decreasing (BFD) algorithm for a comparable low complexity solution. Compared with conventional grouping criteria such as device feature and location, advantages of group number minimizing strategies are clearly observed.

O-3 CV (Oral Presentation)

	**Yoshio Tanaka**
Job Title:	Director, Information Technology Research Institute
Organization:	National Institute of Advanced Industrial Science and Technology
Major Field:	Distributed Computing Cyber Infrastructure for eScience Cyber Physical System, Cyber Physical Security
Education:	1995: Dr. Eng., Graduate School of Mathematics, Keio University 1989: M.E., Graduate School of Mathematics, Keio University 1987: B.E., Department of Mathematics, Keio University
Job history:	2015.04-present: Director, Information Technology Research Institute, AIST, Japan 2014.04-2015.03: Director, Research Planning Office, IT and Electronics Research Department, AIST, Japan 2008.04-2014.03: Principal Research Scientist, Information Technology Research Institute, AIST, Japan 2006.07-2008.03: Principal Research Scientist, Grid Technology Research Center, AIST, Japan 2002.01-2006.06: Team Leader, Grid Technology Research Center, AIST, Japan 2000.04-2001.03: Researcher, Electrotechnical Laboratory, Japan 1996.04-2000.03: Researcher, Real World Computing Partnership, japan

O-3 Abstract (Oral Presentation)

Name of Presenter

Yoshio Tanaka

Presentation Title

IoT Security Management System with Unclonable Devices

Abstract :

The main objective of this research is to develop technologies for building secure IoT infrastructure. We set the two work packages, (1) IoT Security Management (WP1), and (2) key management for unclonable IoT devices (WP2). Many IoT devices are easily created and geologically distributed. One of the key issues in the IoT Security Management is to identify the “trustable” IoT devices. WP1 has developed software management technologies which are based on HSM (Hardware Security Module) as Root of Trust. We use a secure chip named TPM (Trusted Platform Module) or TEE (Trusted Execution Environment) offered by ARM TrustZone. The logs of boot procedure of IoT device are stored in the TPM. The logs could be verified by a Remote Attestation and used to detect an insertion malicious application. The main research topic of WP2 is to develop a key management system for IoT devices. The MQTT (Message Queuing Telemetry Transport) is a ”machine-to-machine” (M2M) / ”Internet of Things” (IoT) connectivity protocol in a publish/subscribe architecture, and was standardized by OASIS. In order to provide MQTT with security, the OASIS standard strongly recommends the MQTT security solution using SSL/TLS. However, this solution entails additional significant communication and computation overheads for certificate validation checks as well as certificate revocation checks to prevent revoked certificates from being used. WP2 has proposed a simple security framework for MQTT (for short, AugMQTT) by incorporating the AugPAKE protocol that is secure against passive attacks, active attacks, and off-line dictionary attacks even with a weak secret (e.g., a password/pin) while achieving measurable efficiency over previous works. As a distinguishing feature, AugMQTT does not require any certificate validation checks and certificate revocation checks on both publishers/subscribers and broker sides. This can simplify the initial setup of publishers/subscribers and the overall procedure of AugMQTT. Implementation details and performance overhead of AugMQTT will be presented.

O-3 CV (Oral Presentation)

	**Weicheng Huang**
Job Title:	Division Director, Software Technology Division
Organization:	National Center for High-performance Computing, Taiwan
Major Field:	Parallel processing, distributed computing, Grid, Cloud, Big Data
Education:	1994 : Ph.D., Aeroanutical & Astronautical Engineering, University of Illinois at Urbana-Champaign 1989 : M.S., Aeroanutical & Astronautical Engineering, University of Illinois at Urbana-Champaign 1984 : B.S., System Engineering & Naval Architecture, National Taiwan Ocean University
Job history:	2012/04 ~ : Research Fellow, Division Director, Software Technology Division, NCHC 2008/09 – 2012/03 : Deputy Director General, NCHC, Taiwan 2010/05 – 2011/12 : Project Director, “National Cloud Computing Platform for Scientific and Technology Research & Development” NCHC/NSC, Taiwan 2008/01 – 2009/09 : Researcher and Program Manager of Grid Computing System and Application Program, NCHC, Taiwan 2005/01 – 2007/12 : Researcher & Division Manager of Parallel and Cluster Processing Division, NCHC, Taiwan 2003/01 – 2004/12 : Researcher & Deputy Division Manger of Grid Computing Division, NCHC, Taiwan 2001/09 – 2002/12 : Associate Researcher & Executive Secretary of National Knowledge Management Grid (KING), NCHC, Taiwan 1998/09 – 2001/09 : Research Scientist and CFD Software Coordinator, National Center for Supercomputing Applications (NCSA), UIUC, USA 2994/08 – 1998/09 : Assistant Research Fellow, Institute of Mathematics, Academia Sinica, Taiwan

O-3 Abstract (Oral Presentation)

Name of Presenter
Weicheng Huang, National Center for High-performance Computing, Taiwan

Presentation Title
Secure Real-Time IoT Analysis on MQTT

Abstract :

The MQTT (Message Queuing Telemetry Transport), which is a connectivity protocol for IoT (Internet of Things), implements a Publisher-Subscriber messaging architecture. Each publisher, such as sensor, can publish its own message to a broker, and the real-time analysis system as a subscriber will connect to a running broker to retrieve messages.

By default, the data transported by the MQTT takes the format of a plain text. However, do to the demand of security of MQTT, the adaptation of the SSL/TLS is recommended. Such a solution requires additional communication and computation overheads for certificate validation checks. A key exchange protocol, the AugPAKE, which is developed in the AIST, is proposed as a remedy for such situation. The AugPAKE has been proven secure against passive attacks, active attacks, and off-line dictionary attacks even with a weak secret. In this demonstration, the AugPAKE is incorporated with the MQTT to provide secure data transmission in the application layer.

Before the data transmission, both the AugPAKE initiator and the responder will negotiate to generate a one-time Cipher key, which is used to encrypt the data to be sent. Furthermore, because a single subscriber can receive data from multiple publishers, an extra session identity, which is generated during the key exchange phase, is adopted to identify the data streamed from different publishers. When the encrypted data arrives at subscriber via MQTT broker, the data is decrypted and then indexed and analyzed by the Splunk. Then, real-time graphs, reports, alerts, dashboards and visualizations can be generated from the searchable data repository.

O-4 CV (Oral Presentation)

	**Masakazu Soshi**
Job Title:	Associate Professor
Organization:	Hiroshima City University
Major Field:	Computer security
Education:	March, 1991: Department of Mechanical Engineering, The University of Tokyo (Bachelor of Engineering) March, 1993: Graduate School of Information Science, The University of Tokyo (Master of Science) March, 1999: Graduate School of Information Systems, The University of Electro-Communications (Doctor of Engineering)
Job history:	1997-1999: Research Associate, The University of Electro-Communications 1999-2003: Research Associate, Japan Advanced Institute of Science and Technology 2003-2007: Research Associate Professor, Japan Advanced Institute of Science and Technology 2007- now: Associate Professor, Hiroshima City University

O-4 Abstract (Oral Presentation)

Name of Presenter
Masakazu Soshi

Presentation Title
New Lightweight Cryptosystems for IoT Devices and Application to eHealth Environments in Taiwan

Abstract :

`IoT' (Internet of Things) environments, where various devices are interconnected via the Internet, have recently been paid much attention to. However, such IoT devices often suffer from limited computational resources and thus we need lightweight and efficient cryptographic primitives for security of the IoT environment. Furthermore, it is now of critical importance to promote good health of people by taking advantage of IoT technology. Therefore, in our Japan-Taiwan joint research project, first, we propose lightweight cryptography and access control techniques for IoT devices. Then, with such technologies, we develop and evaluate eHealth application by using it in Chang Gung Hospital in Taiwan.

In today's talk, I focus on white-box AES implementation proposed in our project. In IoT environments, it is often possible that an attacker illegally obtains an IoT device and then extracts a secret key from it by some means. White-box cryptography tries to make such a secret key exposure extremely difficult even in untrusted environments.

Most of white-box AES implementations proposed so far are based on the techniques by Chow et al. One of the most promising of them is to create a `lookup-table' to obscure the relationship between input and output of a part of AES cryptographic transformation. However, unfortunately, many of the proposed white-box AES implementations have failed by various cryptanalyses.

Therefore we propose a white-box AES implementation to enhance security of the techniques proposed by Luo and You, which have not been broken yet as far as we know. To be more specific, we decompose the MixColumns matrix into two randomly chosen submatrices and implement each of them with a lookup table, which now has an extra addition operation of the same 32bit random number. In this manner, our white-box AES implementation functions completely the same way as AES does and can improve security of the white-box AES of Luo and You. However, we have not yet completed analysis of security and performance of our approach.

In this talk, I also give a brief survey on security of IoT environments.

O-4 CV (Oral Presentation)

	**Chien-Lung Hsu**
Job Title:	Professor
Organization:	Chang Gung University
Major Field:	Smart Home, Mobile Commence, Computer and Communication Security, Information Security, Applied Cryptography, Healthcare, Digital Right Management, Auto Identification Technology, User Centered Services
Education:	PhD: Information Management, National Taiwan University of Science and Technology, 2002 MBA: Information Management, National Taiwan University of Science and Technology, 1997 BS: Business Administration, National Taiwan University of Science and Technology, 1995
Job history:	2011/08~ Professor of Department of Information Management, Chang Gung University, Taiwan 2016/08~ Professor of Graduate Institute of Business and Management, Chang Gung University, Taiwan 2016/08~ Adjunct Professor of Department of Visual Communication Design, Ming-Chi University of Technology, Taiwan 2016/08~ Adjunct Professor of Administration, Chang Gung Memorial Hospital, Taiwan 2015/07~ Director of Taiwan Association for Medical Informatics, Taiwan 2014/09~ Program Chairman of Data Science with Industrial Applications for Big Data, Chang Gung University, Taiwan 2007/09~ Program Chairman of Internet of Things (IoT) with Industrial Innovative Applications, Chang Gung University, Taiwan 2007/09~ Program Chairman of Information of Security with Medical Applications, Chang Gung University, Taiwan 2009/08~ Director and Commissioner of Committee of Chinese Cryptology and Information Security Association, Taiwan

Name of Presenter
Chien-Lung, HSU

Presentation Title
New Lightweight Cryptosystems for IoT based eHealth Environments—Project Achievement of the First Year

Abstract :

In this international joint project, the Japan-Taiwan team aims two main objectives. The first objective is to develop lightweight and secure cryptography technologies for IoT portable devices embedded with power-constrained sensors or resource-limited RFID/NFC tags. Our second objective is to design two general-purpose schemes. After that, we will focus on how to efficiently integrate all the proposed cryptographic modules and the associated authentication protocol and intelligent access control scheme into real IoT based eHealth applications at Chang Gung Hospital in Taiwan. We have designed and evaluated an intelligent health promotion system based on serious games with osteoporosis clinical practice guideline and verified acceptance by interview. We also evaluated system's security and implemented secure protocol. Moreover, we proposed a transparent authentication system with plantar bio-features on wearables-based IoT networks. We introduced systems with wearable devices into four field domains, such as Chang Gung Health and Culture Village, and verified acceptance and usability. We have held conferences and hackton, and visited Osaka University, Japan, and University of Central Florida, USA, to communicated with international specialty.

O-5 CV (Oral Presentation)

	**Haruo Yokota**
Job Title:	Professor
Organization:	Tokyo Institute of Technology
Major Field:	Computer Science Data Engineering Dependable Computing
Education:	Bachelors, 1980, Tokyo Institute of Technology, Tokyo Masters, 1982, Tokyo Institute of Technology, Tokyo Ph.D, 1991, Tokyo Institute of Technology, Tokyo
Job history:	1982-1986: Researcher at the Research Center in Institute of New Generation Computer Technology (ICOT) for Japanese 5th Generation Computer Project 1986-1992: Researcher in Fujitsu Laboratories 1992-1998: Associate Professor in Japan Advanced Institute of Science and Technology (JAIST) 1998-2001: Associate Professor at Department of Computer Science in Graduate School of Information Science and Engineering in Tokyo Institute of Technology 2001-2010: Professor at Global Scientific Information and Computing Center of Tokyo Institute of Technology 2010-2015: Professor at Department of Computer Science in Graduate School of Information Science and Engineering of Tokyo Institute of Technology 2016-present: Professor at Department of Computer Science in School of Computing of Tokyo Institute of Technology 2016-present: Associate Dean of School of Computing 2016-present: Councilor of Tokyo Institute of Technology

O-5 Abstract (Oral Presentation)

Name of Presenter

Haruo Yokota

Presentation Title

Progress of the Research on Reliable Compromise-Resilient Mechanism for Managing the Data Integrity and Privacy of Heterogeneous IoT Devices

Abstract :

This joint project between Tokyo Institute of Technology and two Taiwan universities, National Taiwan University and National Chung Hsing University, aims at developing basic technologies to realize the reliable compromise-resilient mechanisms for managing the data integrity and privacy of heterogeneous IoT devices. Under the physical constraints of heterogeneous IoT devices, such as the limited computational performance, we are trying to develop methods for detecting the failed and/or compromised IoT devices and for correcting the data from those devices using spatio-temporal correlation of the data. At the same time, we are trying to develop lightweight security and dependability protection mechanisms to preserve the privacy in the IoT systems.

The Japan-based team is mainly focusing on the detection and correction methods, while the Taiwan-based team is mainly focusing on the lightweight security and dependability protection. However, these teams tightly collaborate to tackle the research subjects from both sides. To move forward with the project, each side researchers often visited the other side institutes. From the start of this project, we totally had six face-to-face meetings to discuss research subjects; three in Japan and three in Taiwan. We also organize a workshop of this project in Tokyo Institute of Technology, named as “The first Japan-Taiwan Workshop on Secure and Dependable IoT Systems”. It had totally 12 participants; six from Japan side and six from Taiwan side. Moreover, a student of the Taiwan-based team had stayed at Tokyo Institute of Technology for 50 days to advance the research actively.

As a part of research results of this project, we published two papers in international conferences: "Key Management in Internet of Things via Kronecker Product" was presented in the 22nd IEEE Pacific Rim International Symposium on Dependable Computing, and "Impact Analysis for Dos and Integrity Attacks on IoT Systems" in the 7th International Conference on Information Systems and Technologies. Both these papers are co-authored by Japan-based and Taiwan-based teams.

O-5 CV (Oral Presentation)

	**Chia-Mu Yu**
Job Title:	Assistant Professor
Organization:	National Chung Hsing University
Major Field:	Cloud/IoT Security, Data Privacy, Cryptography
Education:	Ph.D. in Electrical Engineering (Computer Science Group) National Taiwan University
Job history:	1. Assistant Professor (2013/8 – 2016/7) Department of Computer Science & Engineering, Yuan Ze University 2. Visiting Professor (2017/1 – 2017/2) Department of Mathematics, University of Padua, Italy 3. Visiting Professor (2016/7 – 2016/9) Department of Computer Science, University of Illinois at Chicago, US 4. Visiting Professor (2015/8 – 2015/9) Department of Mathematics, University of Padua, Italy 5. Visiting Professor (2015/2 – 2015/3) School of Global Information and Telecommunication Studies, Waseda University, Japan 6. Postdoc Researcher (2012/9 – 2013/8) Data-Intensive Systems and Analytics, IBM Thomas J. Watson Research Center, US 7. Visiting Scholar (2012/1 – 2012/8) Electrical and Electronic Engineering Department, Imperial College London, UK 8. Research Assistant (2011/9 – 2012/1) Institute of Information Science, Academia Sinica, Taiwan 9. Visiting Scholar (2010/9 – 2011/9) Harvard School of Engineering and Applied Sciences, Harvard University, US 10. Research Assistant (for obligatory military service) (2004/9 – 2010/9) Institute of Information Science, Academia Sinica, Taiwan

O-5 Abstract (Oral Presentation)

Name of Presenter
Haruo Yokota (Tokyo Tech, Japan) and
Chia-Mu Yu (National Chung Hsing University, Taiwan)

Presentation Title

Research and Development for Secure and Dependable IoT Portable Devices

Abstract :

We first present the progress of our joint project, and show some evidences for our collaboration. After that, we will show the research results from our collaboration, and show our plan on the future collaboration.

We also will spend time on explaining one of our research results. In particular, as the number of everyday objects connected to the Internet grows rapidly, securing these connected devices is a big security challenge. Key establishment in Internet of Things (IoT) becomes a challenging problem when considering the resource constrained IoT devices. In spite of the fact that many clever solutions have been proposed, no practical and suitable scheme has emerged, especially for the extremely large amount of IoT devices in the future. So, we propose a new key establishment scheme for IoT. The scheme is achieved by Kronecker product and satisfies the following conditions. 1) Substantially decreases the amount of data needs to be stored in an IoT device, 2) efficiently compute the pairwise key, 3) no communication is needed during the computation of the keys.

O-6 CV (Oral Presentation)

	**Hiroaki Kikuchi**
Job Title:	Professor
Organization:	Meiji University,
Major Field:	Network security, privacy technology
Education:	He received B. E., M. E. and Ph.D. degrees from Meiji University in 1988, 1990 and 1994. He was a visiting researcher of the school of computer science, Carnegie Mellon University in 1997.
Job history:	After he working in Fujitsu Laboratories Ltd. in 1990, he had worked in Tokai university from 1994 through 2013. He is currently a professor in at Department of Frontier Media Science, School of Interdisciplinary Mathematical Sciences, Meiji University. He is a member of the Institute of Electronics, Information and Communication Engineers of Japan (IEICE), the Information Processing Society of Japan (IPSJ), the Japan Society for Fuzzy Theory and Systems (SOFT), IEEE and ACM. He was a director of IPSJ since 2013. He receives IPSJ Fellow.

O-6 Abstract (Oral Presentation)

Name of Presenter

Hiroaki Kikuchi

Presentation Title

Privacy-Preserving Data Mining on Big Data for Mobile IoT Healthcare

Abstract :

This talk studies the feasibility of privacy-preserving data mining in epidemiological study. As for the data mining algorithm, we focus to a linear multiple regression that can be used to identify the most significant factors among many possible variables, such as the history of many diseases. We try to identify the linear model to estimate a length of hospital stay from distributed dataset related to the patient and the disease information.

In this study, we have conducted experiment using the real medical dataset related to stroke and attempt to apply multiple regression with six predictors of age, sex, the medical scales, e.g., Japan Coma Scale, and the modified Rankin Scale. Our contributions of this study includes (1) to propose a practical privacy-preserving protocols for linear multiple regression with vertically partitioned datasets, and (2) to show the feasibility of the proposed system using the real medical dataset distributed into two parties, the hospital who knows the technical details of diseases during the patients are in the hospital, and the local government who knows the residence even after the patients left hospital. (3) to show the accuracy and the performance of the PPDM system which allows us to estimate the expected processing time with arbitrary number of predictors.

O-6 CV (Oral Presentation)

Chun-I Fan

Job Title:	Professor
Organization:	Department of Computer Science and Engineering, National Sun Yat-sen University
Major Field:	Applied Cryptology, Cryptographic Protocols, and Information and Communication Security

Education:

School Nmae	Country Of Citizenship	Major	Degree	Start and end date
National Chiao Tung University	R.O.C (Taiwan)	Department of Computer Science and Information Engineering	Master	1991 ~ 1993
National Taiwan University	R.O.C (Taiwan)	Department of Electrical Engineering	Doctor	1993 ~ 1998

Job history:

Institution	Department	Title	Start and end date
National Sun Yat-sen University	Dept. of Computer Science and Engineering	Professor	2010 ~ Now
National Sun Yat-sen University	Dept. of Computer Science and Engineering,	Associate Professor	2006 ~ 2010
National Sun Yat-sen University	Dept. of Computer Science and Engineering,	Assistant Professor	2003 ~ 2006
Chunghwa Telecom Co., Ltd	Telecommunication Laboratories	Project Associate Researcher	1999 ~ 2003

Name of Presenter

Chun-I Fan

Presentation Title

Lightweight Authentication Scheme with Dynamic Group Members in IoT Environments

Abstract :

In IoT environments, the user may have many devices to connect each other and share the data. Also, the device will not have the powerful computation and storage ability. Many studies have focused on the lightweight authentication between the cloud server and the client in this environment. They can use the cloud server to help sensors or proxies to finish the authentication. However, on the client side, how to create the group session key without the cloud capability is the most important issue in IoT environments. The most popular application network of IoT environments is the wireless body area network (WBAN). In WBAN, the proxy usually needs to control and monitor user's health data transmitted from the sensors. In this situation, the group authentication and group session key generation are needed. In this paper, to provide an efficient and robust group authentication and group session key generation in the client side of IoT environments, we propose a lightweight authentication scheme with dynamic group members in IoT environments. Our proposed scheme can satisfy the properties including the flexible generation of shared group keys, the dynamic participation, the active revocation, the low communication and computation cost, and no time synchronization problem. Also, our scheme can achieve the security requirements, including the mutual authentication, the group session key agreement, and prevent all various well-known attacks.

P-1 Abstract (Poster Presentation)

Name of Presenter

Shin-Tyng, LEE

Presentation Title

Attribute-based Encryption Scheme and Conference Key Distribution System

Abstract :

Ciphertext policy attribute-based encryption, which is also called CPABE, is a cryptographic system that is suitable for cloud storage system access control. In this protocol, every data user has a secret key with his own attributes and utilizes the access structure and data user's attributes to encrypt data. If the data user's attributes correspond to the data owner's access structure, the data user can decrypt the ciphertext and use this data. However, attribute revocation phase and update phase of this protocol need too much computation cost. In this paper, we proposed an attribute-based conference key distribution system. We improved the traditional conference key distribution system that can only use the user's ID to encrypt conference key. Our scheme can use the user's attributes to encrypt conference key and only legitimate conference participants can decrypt conference key to attend conference. The computation cost is less than traditional conference key distribution system, and conference key will not get longer as number of participants grows.

Name of Presenter
Kuo-Hui, YEH

Presentation Title
Walk as Who I Am: A Transparent Authentication System with Plantar Bio-features on Wearables-based IoT Netwroks

Author
Kuo-Hui Yeh, Wayne Chiu, Chunhua Su, Chien-Lung Hsu, Atsuko Miyaji

Abstract :

The comprehensive evolution of information communication technologies on mobile sensing objects has led to a provision of versatile ubiquitous network services embedded with specific-purpose modern sensors and intelligent wearable devices. The universal Internet connectivity of such smart objects brings a new era of ubiquitous application development on the Internet of Things (IoT). Meanwhile, security has been attached tremendous importance. In the past decade, academia and industry have dedicated great efforts on the design of transparent authentication for multi-modal networks. Multiform authentication bio-tokens have been introduced for transparent entity identification and verification. With the rapid growth and universality of wearable devices, in this paper we envision an IoT-based environment with users possessing wearable healthcare (and wellness) related smart objects. A transparent authentication system with plantar bio-features on wearables-based IoT netwroks is then proposed. In brief, this study delivers three major contributions. First, we provide a comprehensive review of transparent authentication in these years and present the state of the art of this interesting research filed. Second, we develop a wearable plantar bio-feature extractor constructed with commercial pressure sensors and the Raspberry Pi platform. The prototype is adopted to retrieve user plantar bio-data as the raw (and training) data in the proposed authentication system. Third, we apply machine learning-based techniques to derive user's plantar bio-features as authentication tokens in the system which will then transparently perform continual (or real-time) entity verification in the background without the user's notices. Based on the experiment results, the proposed authentication system enjoys good computation efficiency and high verification accuracy.

P-9 CV (Poster Presentation)

	**Xuping Huang**
Job Title:	Researcher
Organization:	Meiji University
Major Field:	Information Security, Audio Signal Processing
Education:	She received B.S. and B.A. degrees from the Department of Software Science, Dalian JiaoTong University, China in 2007 and an M.S degree from the Department of Information Science, Graduate School of Iwate Prefectural University, Japan in 2009. Since 2009, she has been a Ph.D. candidate at the Graduate University for Advanced Studies (SOKENDAI), Japan
Job history:	She worked as a research assistant at the National Institute of Informatics (NII), and technical staff at National Institute of Advanced Industrial Science and Technology (AIST), Japan during 2009,5~2014,3. After working as an Assistant Professor in The Kyoto College of Graduate Studies for Informatics (KCGI) during 2014,4 ~2017,3, She is currently a researcher in Meiji University. She is a member of IEICE and IPSJ.

Name of Presenter
Xuping Huang

Presentation Title
Authentication-Secured Watermarking Method for Multiple Tampering Positions Detection and Identification

Abstract :
This method introduces a watermarking method based on spectrum expansion to guarantee the authentication of big data. Security and integrity of data are protected by detection and identification of the tampered positions in details with content-based verification payload embedded imperceptibly and reversibly in advance. Multiple tampered positions can be identified in detail to a frame unit precisely to 0.36 msec. This work has the following achievements that are simultaneously not realized in previous methods: 1) Re-localization the index sampling of non-tampered frames to avoid false detection; 2) Part of the data can be clipped as a target for detection and the remaining reliable data can be reconstructed and reused, and 3) Detection of multiple tampering of data is theoretically achievable. Target application is to protect integrity of big data, including healthcare recordings, military images, police-investigation and testament recordings, etc.

Speakers

Dr. Wei-Chung Teng
(National Taiwan University of Science and Technology)

Dr. Phone Lin
(National Taiwan University)

Dr. Weicheng Huang
(National Center for High Performance Computing)

Dr. Chien-Lung Hsu
(Chang Gung University)

Dr. Chia-Mu Yu
(National Chung Hsing University)

Dr. Chun-I Fan
(National Sun Yat-sen University)

Dr. Akihiro Nakao
(The University of Tokyo)

Dr. Nei Kato
(Tohoku University)

Dr. Yoshio Tanaka
(National Institute of Advanced Industrial Science and Technology)

Dr. Masakazu Soshi
(Hiroshima City University)

Dr. Haruo Yokota
(Tokyo Institute of Technology)

Dr. Hiroaki Kikuchi
(Meiji University)