CONTENTS

Welcome Message……2

Notes……3

Announcement……4

Conference Venue……5

Agenda……6

Introduction of Keynote Speakers……8

Introduction of Plenary Speaker……12

Session Schedule……13

WELCOME

Dear Distinguished Delegates,

Welcome to 2016 4th International Conference on Information and Network Security (ICINS 2016) and The 8th International Conference on Information and Multimedia Technology (ICIMT2016). The conference group would like to thank all the Conference Chairs, Program Chairs and the technical Committees. Their high competence and professional advice enable us to prepare the high-quality program. We hope all of you have a wonderful time at the conference and also in Kuala Lumpur.

We believe that by this conference, you can get more opportunity for further communication with researchers and practitioners with the common interest in Information, Network Security and Multimedia Technology.

In order to hold more professional and significant international conferences, your suggestions are warmly welcomed. We look forward to meeting you again next time.

Best Regards!

Conference chairs

Prof. Nabil EL Kadhi

University of Buraimi, Sultunate of Oman

Prof. Mohamed Othman,

Universiti Putra Malaysia, Malaysia

NOTES

- ✧ Please arrive at the designated conference room 30 minutes earlier, in case some authors are not able to make the presentation on time.
- ✧ You can also register at any working time during the conference.
- ✧ The organizer won't provide accommodation, and we suggest you make an early reservation.
- ✧ Please get the notification for your paper printed out and it is required when you register on desk.
- ✧ One best presentation will be selected from each session and the author of best presentation will be awarded the certificate.
- ✧ Get your presentation PPT or PDF files prepared.
- ✧ Regular oral presentation: about 15 minutes (including Q&A).
- ✧ Keynote speech: about 40 minute (including Q&A).
- ✧ Plenary speech: about 30 minutes (including Q&A)
- ✧ Laptop (with MS-Office & Adobe Reader), projector & screen, laser sticks will be provided by the conference organizer.
- ✧ Please keep your belongings (laptop and camera etc.) with you.

ANNOUNCEMENT

- Publication for International Conference on Information and Network Security:

  * **International Conference Proceedings Series by ACM**

- Publication for International Conference on Information and Multimedia Technology:

  *__Journal of Advances in Information Technology__

  *__Journal of Media & Mass Communication__

*For the journal publication schedule, some authors could not get the journal on conference site. We'll post the journal after publication. A U Disk including all registered papers will be handed out to the delegates.

***Attention:**

One best presentation will be selected from each session and the author of excellent presentation will be awarded the certificate at dinner banquet.

Conference Organizing Committee

VENUE

Ambassador Row Hotel Suites by Lanson Place

Add: 1, Jalan Ampang Hilir 55000 Kuala Lumpur, Malaysia

Ambassador Row Hotel Suites by Lanson Place is Only ten minutes from the Petronas Twin Towers and Golden Triangle, Ambassador Row Hotel Suites by Lanson Place is located in the heart of the diplomatic quarter with comfortable one to three bedroom suites.

Contact:

Tel: (60) 3 4253 2888
Fax: (60) 3 4253 1773
Email: enquiry.arkl@lansonplace.com

The organizer won't provide accommodation, and we suggest you make an early reservation. Please send email or call phone numbers above to book the room, and don't forget to mention IACSIT conference.

AGENDA

First Day				
Dec. 28	**Lobby**	**10:00-17:00**	**Registration and conference materials collection**	
Second Day				
Dec. 29 9:00-12:00	**Tembusu I (Level 2)**	**9:00-9:10**	**Opening**	**Prof. Nabil EL KADHI University of Buraimi, Sultunate of Oman**
		9:10-9:50	**Keynote Speech I**	**Prof. Chin-Chen Chang IEEE and IET Fellows, Feng Chia University, Taiwan**
		**9:50-10:10**	**Coffee Break& Group Photo**	
	Tembusu I (Level 2)	**10:10-10:50**	**Keynote Speech II**	**Prof. Mohamed Othman Universiti Putra Malaysia, Malaysia**
		10:50-11:30	**Keynote Speech III**	**Prof. Nabil EL KADHI University of Buraimi, Sultunate of Oman**
		11:30—12:00	**Plenary Speech**	**Prof. Shihab A. Hameed IIUM University Malaysia, Malaysia**
Dec. 29 12:00-13:30	***Lunch @ Restaurant***			
Dec. 29 13:30-18:30	**Tembusu I (Level 2)**	**13:30-15:45**	**Session I**	**Information Security And Technology** --9 Presentations
		**15:45-16:00**	**Coffee Break**	
	Tembusu I (Level 2)	**16:00-18:30**	**Session II**	**Computer Science And Information Engineering** --10 Presentations
Dec. 29 18:30-20:30	***Dinner @ Restaurant***			

AGENDA

Schedule for Visiting on Dec.30

Time: 9:00-17:00

One-day Visiting	
9:00am	Assemble at Lobby
10:00 am	Famous Scenic Spots
13:00	Lunch
14:00-17:00	Famous Scenic Spots
17:00	End of tour

Route

Genting, India Temple of Kuala Lumpur, KLCC, Sunway

Attention:

✧ The cost of one-day tour is 50USD per person for conference participants and 60USD for companion.

✧ Please keep your belongings with you.

Schedule for Tutorial on Dec.31

Venue: Tembusu I (Level 2)

Time: 10:00-17:00

10:00-12:00	Tutorial Registration
12:00-13:30	Lunch @ Restaurant
13:30:00-15:00	Topic I： Wireless Network Security
15:00-15:30	Coffee Break
15:30-17:00	Topic II: Security for Personal Communication Systems
18:00-20:00	Dinner@ Restaurant

KEYNOTE

Prof. Chin-Chen Chang

IEEE and IET Fellows, Feng Chia University, Taiwan

Professor C.C. Chang was born in Taichung, Taiwan on Nov. 12th, 1954. He obtained his Ph.D. degree in computer engineering from National Chiao Tung University. He's first degree is Bachelor of Science in Applied Mathematics and master degree is Master of Science in computer and decision sciences. Both were awarded in National Tsing Hua University. Dr. Chang served in National Chung Cheng University from 1989 to 2005. His current title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from Feb 2005.

Prior to joining Feng Chia University, Professor Chang was an associate professor in Chiao Tung University, professor in National Chung Hsing University, chair professor in National Chung Cheng University. He had also been Visiting Researcher and Visiting Scientist to Tokyo University and Kyoto University, Japan. During his service in Chung Cheng, Professor Chang served as Chairman of the Institute of Computer Science and Information Engineering, Dean of College of Engineering, Provost and then Acting President of Chung Cheng University and Director of Advisory Office in Ministry of Education, Taiwan.Professor Chang's specialties include, but not limited to, data engineering, database systems, computer cryptography and information security. A researcher of acclaimed and distinguished services and contributions to his country and advancing human knowledge in the field of information science, Professor Chang has won many research awards and

KEYNOTE

honorary positions by and in prestigious organizations both nationally and internationally. He is currently a Fellow of IEEE and a Fellow of IEE, UK. On numerous occasions, he was invited to serve as Visiting Professor, Chair Professor, Honorary Professor, Honorary Director, Honorary Chairman, Distinguished Alumnus, Distinguished Researcher, Research Fellow by universities and research institutes. He also published over 1,100 papers in Information Sciences. In the meantime, he participates actively in international academic organizations and performs advisory work to government agencies and academic organizations..

KEYNOTE

Prof. Nabil EL KADHI
University of Buraimi, Sultunate of Oman

Professor Nabil EL KADHI works as Deputy Vice-Chacellor for Academic Affairs in University of Buraimi, Sultunate of Oman now. He has 13 years of experience in management-high education and research units. He assumed various positions starting from project manager and department head to lab director, Dean and recently Provost at AMA International University Bahrain. Professor EL KADHI has more than 20 years of teaching experience in higher education institutions. He has a PhD in Computer Sciences “formal verification of cryptographic protocols (INRIA Rocquencourt France (1998-2000) with the initiative Verified Internet Protocols and the European project TASK)”. He started his professional activities early 90th as a lecturer, programmer and IT manager in public/private institutions. He worked at EPITCH-Paris (2000-2008); he was major stone in developing EPITECH Curricula and research activities. Professor EL KADHI contributed to several industrial projects: Artificial intelligence, automatic translation, secure payment, smart card use, Automation, Mechatronics and Robotics As vice-president of KnK Partner, a think tank to bridge the gap between universities and corporate, he developed, managed 3 specialized Master degrees. As a manager and strategic leader, he successfully conduct various QA and accreditations with various scopes: institutional, programme review and international accreditations Professor EL KADHI has more than 50 International publications indexed by ACM, IEEE, DBLP and others, he is reviewers in various engineering and computer sciences international scientific journals. He is considered today as one among the international specialist in cyber security.

KEYNOTE

Prof. Mohamed Othman

Universiti Putra Malaysia, Malaysia

Mohamed Othman received his PhD from the Universiti Kebangsaan Malaysia with distinction (Best PhD Thesis in 2000 awarded by Sime Darby Malaysia and Malaysian Mathematical Science Society). Now, he is a Professor in the Faculty of Computer Science and Information Technology, Universiti Putra Malaysia (UPM). He is also an associate researcher at the Lab of Computational Science and Mathematical Physics, Institute of Mathematical Research (INSPEM), UPM. He published more than 230 International journals and 230 proceeding papers. He currently has 1947 (\textit{h}-index=18) and 759 (\textit{h}-index=12) citations based on Google Scholar and Scopus, respectively. He is a member of IEEE Malaysia Section, IEEE Communications Society (ComSoc), IEEE Computer Society and Malaysian Mathematical Sciences Society. His main research interests are in the fields of high speed network, parallel and distributed algorithms, software defined networking, network design and management, wireless network (MPDU- and MSDU-Frame aggregation, TCP Performance, MAC layer, resource management, network security, and traffic monitoring) and scientific telegraph equation and modeling.

PLENARY

Prof. Shihab A. Hameed

IIUM University Malaysia, Malaysia

Dr. Shihab A. Hameed is a Full Professor of Computer and Information Engineering in Department of Electrical and Computer Engineering, IIUM University Malaysia. He is a Senior Member in several professional Societies (IEEE, IACSIT, IACSE, ARISE). He is a Member of Board of Study for Computer and Information Engineering Program. Prof Hameed obtained his PhD in Computer from UKM University. He has More than Thirty Five years of Industrial and Educational Experience. His Research Interest is Mainly in Software Engineering and Quality, Healthcare and Medical Applications, Multimedia and Mobile Apps, Professional Ethics, Green ICT and E-Waste, Surveillance and Monitoring Systems. Prof Hameed Supervising Tens of PhD and Master Students, Leading or participating in Funded Research Projects and Research Groups, He has more than 200 Publications including Books, Chapters of Books, Research Papers Published in Indexed or Referred Journals and International Conferences. Prof Hameed Granted a Patent and obtains more than Twenty Five Medals and Rewards for Innovative and advanced Research work. He is participating as keynote speaker or Member of Organizing and Technical Committees for Tens of International Conferences. He participate in assessing articles for several indexed or Referred Journals.

Keynote Speeches

Time: 9:00-12:00

Location: Tembusu I (Level 2)

Opening Remarks 9:00-9:10	 **Prof. Nabil EL KADHI** **University of Buraimi, Sultunate of Oman**
Keynote Speech I 9:10-9:50	 **Prof. Chin-Chen Chang** IEEE and IET Fellows, Feng Chia University, Taiwan **Turtle Shell Based Information Hiding Mechanism** ***Abstract***—Steganography is the science of secret message delivery using cover media. A digital image is a flexible medium used to carry a secret message because the slight modification of a cover image is hard to distinguish by human eyes. In this talk, I will introduce some novel steganographic methods based on different magic matrices. Among them, one method that uses a turtle shell magic matrix to guide cover pixels' modification in order to imply secret data is the newest and the most interesting one. Experimental results demonstrated that this method, in comparison with previous related works, outperforms in both visual quality of the stego image and embedding capacity. In addition, I will introduce

	some future research issues that derived from the steganographic method based on the magic matrix.

Coffee Break & Group Photo
9:50-10:10

Keynote Speech II 10:10-10:50	**Prof. Mohamed Othman** Universiti Putra Malaysia, Malaysia
Keynote Speech III 10:50-11:30	 **Prof. Nabil EL KADHI** University of Buraimi, Sultunate of Oman **Information Security - Yesterday, Today and Tomorrow** ***Abstract*—**Information Security is one of the major concerns of corporate and users since the last decade. Having more connectivities exposes us to more risks; and having more flexibilities and more mobilities in our common life may subject us to encounter more attackers and malicious users or to be even victims of spywares and viruses. Moreover, having more tools and software in our computers and systems also lead to more vulnerability to distributed and dynamic attacks. There are various range of technologies available now and the society has

	evolved from the small local network to the wide area network; from the wired to the wireless connections; and from the owned resources to the cloud-shared ones. These are among the many changes that led to a complete paradigm shift in information security. Techniques of protection detection, prevention and correction have been drastically improved. Attacks, threats and risks have been also growing in a phenomenal way - from a simple hacker challenging the 'world' to prove his superiority to well-organized actions with various social and economic aspects and effects; or from an automated attack to cyber criminality passing by the hacktivism. These reflect the complete paradigm shift that we are facing today. The talk aims to address the technical, economic and social aspects of information security and communication threats. From the fundamental theories (in brief) to their commercial and practical applications, we will browse a large scope of technical, social and commercial aspects. The talk includes information about, but not limited to fundamental security services; cryptography and cryptology; human factors and legal issues; network attacks and vulnerabilities, password cracking, injection attacks and web vulnerabilities
Plenary Speech 11:30-12:00	 **Prof. Shihab A. Hameed** IIUM University Malaysia, Malaysia **Green ICT for Better Human Life**

	***Abstract*—**Seven decades of rapid development in computing and ICT make it an efficient and effective driving force toward better human life. ICT industry has an appreciated contribution to the global economy associating with innovation, invention and rapid development of almost all the aspect of human life (Education, Health, Industry, Entertainment, Agriculture, Business, etc.). On the other hand, global environment and human life facing serious challenges related to human health and life style, climate change and global warming, and unwise consumption and management of resources. The diversity and rapid increasing of ICT usage in our life leads to more energy consumption and environmental problems, which has negative impact on economy, human health, and life style. The expected ICT consumption of energy for the next few years will be about 15% of the total consumption worldwide. This make ICT industry shared responsibility for global CO2 emissions and environmental problems. Therefore, many developed countries are establishing Green ICT policies and strategies to eliminate environmental and human health problems. Shortage and weakness of Green ICT policies or strategies in developing countries requires adoption of an effective one that leads to wise ICT usage and energy consumption. Ethical and moral values should integrate with technical aspects to have effective strategies for green ICT that leads to better human life.

Lunch @ Restaurant
12:00-13:30

Session I

Information Security and Technology

Time: 13:30-15:45

Location: Tembusu I, Level 2

Chaired by Assoc. Prof. Fredrik Björck

Stockholm University, Sweden

Presentations: NS001, NS007, NS016, NS1009, MT013, NS027, NS025, NS1003, NS034

※Please kindly participate the whole course of the conference to make sure each item sticks to the agenda and runs smoothly.

NS001 13:30-13:45	Performance Comparison between Broadcast Authentication Methods for Vehicular Networks Kanika Grover and **Alvin Lim** Arizona State University, US ***Abstract*—**For authenticating time critical broadcast messages, IEEE 1609.2 security standard for Vehicular Ad hoc Networks (VANETs) suggests the use of secure Elliptic Curve Digital Signature Algorithm (ECDSA). Since ECDSA has an expensive verification in terms of time, most commonly suggested alternate algorithms are TESLA and signature amortization. Unfortunately, these algorithms lack immediate authentication and non-repudiation. Therefore, we introduce a probabilistic verification scheme for an ECDSA-based authentication protocol. Using ns2 simulation tools, we compare the performance of all above-mentioned broadcast authentication algorithms. The results show with our proposed scheme, there is an increase in packet processed ratio over that of all the other algorithms.
NS007 13:45-14:00	Repeated Differential Properties of PRESENT Key Schedules **Alya Geogiana Buja**, Shekh Faisal Abdul Latip and Rabiah Ahmad Universiti Teknologi MARA Malaysia, Malaysia ***Abstract*—**This paper investigates the key schedules of the PRESENT block cipher and studies some repeated differential properties of the key schedules. The concept of repeated differential pattern for PRESENT key schedules are defined and introduced. Our study shows that there is a repeated differential pattern in both PRESENT-80 and PRESENT-128 key schedules. The differential patterns for PRESENT-80 are found repeated until round 28 with at least four bits out of two bytes differential pattern. Meanwhile, for PRESENT-128, the differential patterns are found repeated in all round with at least four bits out of 16-bits initial differential pattern. In addition, the secret keys with the repeated differential pattern have a large number of bytes in common. From the result, we found that the key schedule for PRESENT-80 is more ideal compared to PRESENT-128.

NS016 14:00-14:15	Enhancing Network Security in PPPoE protocol during the logical Local Loop Unbundling **Kushtrim Kelmendi** and Blerim Rexha University of Prishtina, Kosovo ***Abstract*—**Local Loop Unbundling (LLU)is a process which allows the competitive Network Service Providers (NSPs) to use the telecom's incumbent infrastructure to provide the services to their subscribers. In logical LLU, as the traffic passes through the incumbent network infrastructure, security and privacy of the NSP subscribers is of a serious concern. In this paper, we have presented a novel approach to address these concerns, by implementing the encryption on the Point to Point Protocol over Ethernet (PPPoE), in the broadband network, between the NSP Customer Premises Equipment (CPE) and Broadband Network Gateway(BNG) router. First, encryption algorithm is negotiated using the existing protocol Encryption Control Protocol (ECP), during the PPP establishment phase, and after that the PPP packet payload is encrypted using the Advanced Encryption Standard AES, 128 bit version. The encryption key is derived using the first 128 bits of the SHA256 hash of sum of the three key variables: PPPoE SESSION_ID, CPEMAC Address, and CPE serial number, which makes this encryption key unique. The proposed solution is compared to existing protocols.
NS1009 14:15-14:30	IoT Architecture Enabling Dynamic Security Policies Yuhong Li, **Fredrik Björck,** Wenchao Liu Department of Computer and Systems Sciences, Stockholm university, Sweden ***Abstract*---** The Internet of Things (IoT) architecture is expected to evolve into a model containing various open systems, integrated environments, and platforms, which can be programmed and can provide secure services on demand. However, not much effort has been devoted towards the security of such an IoT architecture. In this paper, we present an IoT architecture that supports deploying dynamic security policies for IoT services. In this approach, IoT devices, gateways, and data are open and programmable to IoT application developers and service operators. Fine-grained security policies can be programmed and dynamically adjusted according tousers' requirements, devices' capabilities and networking

	environments. The implementation and test results show that new security policies can be created and deployed rapidly and demonstrate the feasibility of the architecture.
MT013 14:30-14:45	A Novel System for Securely Sharing Macros of Spreadsheets of Organizations **Somchai Chatvichienchai** University of Nagasaki, Dept. of Information Security, Nagasaki, Japan ***Abstract***—Modern spreadsheet software provide built-in script languages for developing macros which automate operations on spreadsheets. Typically a macro is stored as a part of the spreadsheet on which it is supposed to operate. Since macros can be created by spreadsheet users who have a few knowledge of computer programing, the macros are widely used by many organization workers. However, macros have the following three drawbacks. The first is overhead cost in maintaining the same macros stored in many spreadsheets. The second is incompatibility of macros among spreadsheet software of different versions and platforms. The third is security risk of macro viruses. The objective of this paper is to propose a spread sheet macro sharing system that can solve these drawbacks. The proposed system eliminates the need of using macro-enabled spreadsheets. During editing a spreadsheet, users can import relevant macro from macro archive into their spreadsheets by macro-import add-in developed by this work. Digital signature is applied to the imported macros to confirm the source of macros and to check whether the macros have not been tampered.
NS027 14:45-15:00	INTELLIGENT INTRUSION DETECTION SYSTEM USING A COMMITTEE OF EXPERTS **Krishnan Subramanian,** Sachin Senthilkumar and Balasubramanian Thiagarajan SVCE, India ***Abstract*--** Intrusion detection plays an important role in today's computer and communication technology. It is of a paramount importance to design a time efficient and accurate Intrusion Detection System (IDS) using the combination of several neural experts forming a Committee of Experts, used to detect and prevent various anomalies. The input to the system is given by the feature extraction of various historic data present in the central database and making a suitable Training

	Data Classifiers. Furthermore, each expert within the committee is assigned a different granularity of data, because the training set is based on its fundamental properties. The experts are designed in such a way that they make accurate predictions using the data. The system provides maximum attack detection success rate and takes the necessary steps in identification of the anomaly.
NS025 15:00-15:15	Challenges in Quantum Key Distribution: A Review **Hong Kah Wing,** Low Tang Jung and Foong Oi Mean Universiti Teknologi PETRONAS, Malaysia ***Abstract*—**Quantum computing is essentially exploiting and harnessing the laws of quantum mechanics to process information. With it, rise the era of a new cryptosystem that has the potential to be unconditionally secure which is known as quantum cryptography. Quantum cryptography uses the properties of quantum mechanics to develop an unbreakable cryptosystem that can never be compromised. Quantum key distribution (QKD), which is an area in quantum cryptography, provides a way for distribution of secure key between two parties. Some of the existing QKD protocols include BB84 protocol, B92 protocol, SARG04 protocol, E91 protocol and many more. In this paper, the trends and challenges in Quantum Key Distribution is reviewed.
NS1003 15:15-15:30	PinTar: A New Keyed Hash Function based on Pseudorandom 2n-to-n bit Compression Function **Zahraddeen Abubakar Pindar ,** Sapiee Haji Jamel, Muhammad Aamir, Mustafa Mat Deris Faculty of Computer Science and Information Technology , UniversitiTun Hussein Onn Malaysia ***Abstract*---**Cryptographic hash functions are used to protect the integrity of information. Hash functions are designed by using existing block ciphers as compression functions. This is due to challenges and difficulties that are encountered in constructing new hash functions from the scratch. However, the key generations for encryption process result to huge computational cost which affects the efficiency of the hash function. This paper a novel, secure and efficient keyed

	hash function based on pseudorandom compression function, that takes in two 2n-bits inputs and produce one n-bit output (2n-to-n bit). In addition, a new keyed hash function with three variants is proposed (PinTar 128 bits, 256 bits and 512 bits) which uses the proposed compression as its underlying building block. Statistical analysis shows that the compression function is an efficient one way random function. Similarly, statistical analysis of the keyed hash function shows that the proposed keyed function has strong avalanche property and is resistant to key exhaustive search attack. The proposed key hash function can be used as candidate for developing security systems.
NS034 15:30-15:45	e-Government and Security Evaluation Tools Comparison for Indonesian e-Government System **Muhammad Sukmana** and Christoph Meinel Hasso Plattner Institut, Germany ***Abstract*---**Electronic Government (e-Government) system nowadays are implemented by majority countries around the world with various reasons, such as to improve the efficiency of government's services to the citizens and increase the accountability of government's process and citizen's trust to avoid corruption. But during the development of e-Government system the security aspect is pushed aside to accommodate the continuous development. Indonesia as one of the countries that pushes hard the development and implementation of e-Government system in all government sectors currently has inadequate e-Government and security evaluation tools to help evaluate the performance and development of Indonesian e-Government system and its security aspect. This paper compares Indonesia's e-Government and its evaluation tools with the available evaluation tools that can be used to help evaluate the current level of Indonesian e-Government system and its security aspect.

Coffee Break & Group Photo
15:45-16:00

Session II

Computer Science and Information Engineering
Information Security and Technology

Time: 16:00-18:30

Location: Tembusu I, Level 2

Chaired by Prof. Somchai Chatvichienchai

Dept. of Information Security, University of Nagasaki, Japan

Presentations: MT002, MT003, MT006, NS019, MT009, NS026, MT014, NS010, NS015, NS018

※Please kindly participate the whole course of the conference to make sure each item sticks to the agenda and runs smoothly.

MT002 16:00-16:15	Mobile Game Developing: Math Mobile Game Learning Model **Hadi Sutopo** Faculty of Computer Science and Communication Science, Institut Teknologi dan Bisnis Kalbis, Jakarta, Indonesia ***Abstract***—This research is intended to develop a mobile multimedia application, specially a mathematics mobile game model for elementary school. This learning model should encourage student's ability to learn mathematics particularly numbers. This research consists of 7 steps such as research and information collecting, planning, developing preliminary product, preliminary field testing, preliminary product revision, main field testing, and operational product revision. Subjects of the research are education, visual communication and computer experts in preliminary field testing, and the elementary school children for implementation revised model in main field testing. The data were analyzed using the analytic descriptive method and interpreted based on the narrative way as research findings. Based on the data of product and learning process taken in the main field testing, most of children could solve the problem on mathematics mobile game, the mathematics mobile game was very useful to support learning, motivate children to learn mathematics, and it could be used for self-learning.
MT003 16:15-16:30	Geometric-based Feature Extraction and Classification for Emotion Expressions of 3D Video Film **Salwa A. Al-agha**,Hilal H. Saleh,Rana F. Ghani University of Technology, Iraq ***Abstract***—Feature extraction is the most significant step in the operation of emotion expressions recognition. Discrimination operation of emotion expressions has gained the attention of many researchers in the field of pattern recognition because of its significant impact on the various aspects of applications, especially in the application of human-computer interaction, both for the image or to the video. Based on pattern recognition theory, the process of facial expression recognition can be divided into features extraction operation and classification operation. In this paper, the geometric-based features extraction operation is used for

	extracting the local characteristics (landmarks) of a set of emotion expressions (anger, happiness, sadness, surprise) for images of BOSPHORUS database as training stage, then the classification operation is done by using of the threshold method (Euclidean distance) between the distances of neutral image and the expression image. The trained system is used for feature extraction and classification for 3D video film (stereoscopic) as testing stage. This method is implemented on 40 3D video films that were recorded, 10 video films for each expression of the four basic emotion; the ratio of discrimination is 85%.
MT006 16:30-16:45	Improving the Performance of a Wireless Presentation System **Gin-Xian KOK**, Khong Neng CHOONG, Danial NAGHSHBANDI, and Mohammad Hilmi MOHD SHARIFF MIMOS Berhad, Malaysia ***Abstract***—In this paper, we study the performance of a wireless presentation system in a scenario called webviewer. In this scenario, the presenter streams the desktop screen of his/her computing device, typically a laptop, to the wireless presentation box, and the wireless presentation box performs a snapshot of the video stream, encodes, and sends the captured image to a list of subscribers called webviewer clients, periodically. We propose an image data transfer rate throttling scheme and compared it with several other schemes. Simulation study showed that the proposed scheme is able to better utilize the available system resource to improve the satisfaction level of the users in a desktop mirroring session.
NS019 16:45-17:00	Information Security Testing Bed based on Game Theory **Tsung-Hui Lu** and Zne-Jung Lee Huafan University, Taiwan ***Abstract***---Information is the core to maintain the operation of an organization. Security of information proved to be the biggest risk on business continuity in government agencies and business entities, whether the threats were comes from natural disaster, hostile entities, external or internal, accidentally or intentionally. In academic, information security has been taught for years. Curriculums on cryptography, defense on protection, testing of maturity and management of internal control help students learned phases of information security but still lacks

	of practical experiences. On-job trainings on employment after education are needed and lead to cost and time consumption. We need an architecture and platform to practice information security in real life while students in school. Architecture makes sure the objective of each curriculum is included into practical and platform exams the knowledge learned from classes. All of this can be achieve through composition of Red, Green and Blue team. On top of teams is script, which categorized scenario of difference cases. Blue team is responsible for defense. By using every concept on how to build up an effective and efficient environment, logical, physical and administrative, blue is suitable for junior student in academy. On the other hand, red team will simulate attack by consist senior student will specific skill on vulnerability and penetration. After that, student can upgrade to green team and judge the condition of simulation based on scripts.
MT009 17:00-17:15	Security Measurement as a Trust in Cloud Computing Selection and Monitoring Abubakar Tom Magira and **Osman Ghazali** University Utara Malaysia,Malaysia ***Abstract***—With the increase in the number of cloud service offerings by the cloud service providers nowadays, selecting the appropriate service provider becomes difficult for customers. This is true, since most of the cloud service providers offer almost similar services at different costs. Thus, making cloud service selection a tedious process for customers. The selection of the cloud services from the security standpoint needs a distinct consideration from both the academia and the industry. Security is an important factor in cloud computing. Thus, any exploited vulnerability will have a negative effect on cloud computing adoption by customers. Hence, little attention has been paid to cloud service monitoring and selection from a security perspective. To solve this issue, we propose a security measurement as a trust (SMaaT) in the cloud computing selection.Finally, we propose Analytical Hierarchical Process (AHP) for service selection from the customers' perspective.
NS026 17:15-17:30	Fast off-site backup and recovery system for HDFS **Yu Wang,** Wei Huang and Hongliang Yu Department of Computer Science and Technology, Tsinghua University, Beijing, China

	***Abstract*---** HDFS is designed to store massive scale data on commodity hardware reliably. However, it is still vulnerable to severe site disaster, eg. fire, earthquake. The off-site file system backup is an important strategy for data retention. In this paper, we present an efficient, easy-to-use off-site backup and recovery system for HDFS. The system includes a client based on HDFS v2.3.0 with additional feature of off-site backup, and a remote server with a HDFS cluster to keep the backup data. It supports full backup and regularly incremental backup. Both the metadata alteration and the data blocks alteration will be recorded and transferred to remote backup server. Several techniques are used to improve efficiency and throughput. In our experiment, the average speed of backup is up to 95 MB/s, approaching the theoretical maximum speed of gigabit Ethernet.
MT014 17:30-17:45	A Conceptual Framework for a Problem Resolution Support System (PReSS) **Osama Al Masri** and Mohd Sharifuddin Ahmad College of Graduate Studies, Universiti Tenaga Nasional, Kajang, Malaysia ***Abstract***—Decision-making is the most critical task of management. Organizations use decision support systems (DSS) to improve decision-making by senior managers. Other than those provided by organizational decision support systems, little attention has been given to decision-making in resolving unstructured problems and issues within organizations. More often, such decisions are left to the individual department responsible for the problems for it to resolve often without access to relevant data, information or expertise. These issues are mainly related to daily operational and administrational issues arising out of poor cooperation between departments. This paper proposes a conceptual problem resolution support model utilizing the technique of multi-criteria decision-making (MCDM) to help organizations in identifying, prioritizing and resolving unstructured organizational issues. The paper shows how the MCDM evaluates and validates the proposed solutions to come up with an ideal solution.

NS010 17:45-18:00	Analyzing efficiency of Pseudo-Random Number Generators using Machine Learning **Sumit Kumar** Schneider Electric India Pvt. Ltd. India ***Abstract*—**Random numbers are very important components in cyber security. A main application of random numbers is in the field of cryptography. PKI and TLS based encryption uses random numbers extensively. Other areas include session IDs of web applications, passwords and game of chance. A number of cyber security attacks have happened in the past because of using weak random number generators. Machine learning has been extensively used in pattern identification in a number of areas, including credit card frauds, genomics and face identification. It utilizes a set of algorithms to detect patterns from in a data to perform tasks like classification, clustering and prediction. In this paper, a fast method to test the randomness of a sequence generated by pseudo-random number generator is proposed which tries to take advantages of the pattern identification of machine learning.
NS015 18:00-18:15	Study of Car Dash Cam Security Vulnerabilities **Jaehyun Park**, Hongjin Kim, Junbo Shim, Junseok Kim, Hojin Lee, Jaeyoon Kim, Hyongkyo Kim, Hayeon Ra, Sungjin Hong Korea Information Technology Research Institute BoB Progr, Korea ***Abstract*—**Nowadays, wireless networking features are being used widely, also used in the Car Dash Cams. However, because of the introduction of wireless networking system, it generated a lot of new forms of security vulnerabilities and issues which were not in the conventional Car Dash Cams. This study derives the security vulnerabilities of the Car Dash Cam's firmware which have the wireless networking feature. In addition, by analyzing the packet that is used for communication between the smart phone applications and a Car Dash Cams, this study analyses the bypassing method of authentication and presents the risks of the above vulnerabilities. In the point of view of Car Dash Cams which have the wireless networking feature are not fully discussed before, this study is expected to be a meaningful study.

NS018 18:15-18:30	A High Performance Computing-based Interval Fuzzy Type-2 Model for Web Services' QoS Evaluation: A Review **Mohd Hilmi Hasan,** Jafreezal Jaafar, Izzatdin A. Aziz and Lukman Ab Rahim Universiti Teknologi PETRONAS , Malaysia Abstract--- Web services' QoS evaluation involves high degree of uncertainty due to the unpredictable nature of network. Existing models are not realistic because they apply crisp computation. Hence, a model using Interval Fuzzy Type-2 (IT2) method was proposed in our previous work. IT2 method was selected because it has better ability than Fuzzy Type-1 and crisp methods in handling uncertainties. However, the introduction of an extra component and a degree of freedom has made IT2 method computationally expensive. Therefore, it is proposed that the IT2-based web services' evaluation model to be implemented on high performance computing (HPC) platform. This paper reviews previous research that are related to HPC-based IT2 implementation as well as discusses the implications of the work.

Dinner @ Restaurant
18:30-20:30

POSTERS

NS005	Binary Protection using Dynamic Fine-grained Code Hiding and Obfuscation Meng Wu, Yi Zhang and Xianya Mi National University of Defense Technology, China ***Abstract***--Anti-reverse engineering is one of the core technologies of software intellectual property protection, prevailing techniques of which are static and dynamic obfuscation. Static obfuscation can only prevent static analysis with code mutation done before execution by compressing, encrypting and obfuscating. Dynamic obfuscation can prevent both static and dynamic analysis, which changes code while being executed. Popular dynamic obfuscation techniques include self-modifying codeand virtual machine protection. Despite the higher safety, dynamic obfuscation has its problems: 1) code appear in plain text remains a long time; 2) control flow is exposable; 3) time and space overheads are too big. This paper presents a binary protection scheme using dynamic fine-grained code hiding and obfuscation named dynFCHO. In this scheme, basic blocks to be protected are hidden in original code and will be restored while being executed. Code obfuscation is also implemented additionally to enhance safety. Experiments prove that dynFCHO can effectively resist static and dynamic analysis without destructing original software functions. It can be used on most binary programs compiled by standard compilers. This scheme can be widely used with the advantages of strong protection, light-weight implementation, and good extendibility.
NS008	Penetration Testing on Virtual Environments Teresa Guarda Universidade Estatal da Península de Santa Elena , Portugal ***Abstract***--Since the beginning, computer systems have faced the challenge of protecting the information with which they work, and with the technological development, computational security techniques have become more complex to

	face the potentials attacks. Currently we are facing a war game with the usual two sides, attackers and defenders. The attackers want to have complete control over the systems. In is turn, defenders virtualized systems to maintain the resources safety in case of attack. The attackers have also developed increasingly sophisticated techniques to break such protections, being necessary to anticipate such events, which may be achieved through the application of preventative measures. This may be done by simulating Penetration Testing (PT). PT is an attack on a computer system, using a set of specialized tools that looks for security weaknesses, which eventually may have access to computer's features and data, allowing the discovery of such evidence vulnerability. Virtual Environments have a higher exposure to cyber-attacks. The aim of this paper is propose a framework to provide guidelines for Penetration Testing in Virtual Environments.
NS013	Sym Finder: Privacy Leakage Detection using Symbolic Execution on Android Devices Yu Su, Yan Yu , Yu Qiu, Anmin Fu Nanjing University of Science and Technology, China ***Abstract***--Android system has a large number of users and application markets, but its security situation is worrying. Unlike most of the PC apps, Android apps manipulates private information such as contacts and SMS messages, and leakage of such information may cause great loss to the Android users. Thus, detecting privacy leakage on Android is in urgent need. In this paper, we propose a new approach called SymFinder, which detects privacy leakage vulnerabilities on Android with reverse symbolic execution technology. Unlike dynamic approaches, SymFinder analyzes applications without the need of code execution. Thus, it has a higher coverage and less false negative rate of vulnerabilities, and can avoid the path explosion problem in dynamic analysis. Besides, SymFinder can increase accuracy of vulnerability analysis and reduce false positive rate by recognizing invalid and inaccessible sensitive paths. Experimental results show that, SymFinder can detect the existence of 14 real privacy leakages from a 100 provided application set.
NS1008	A Method of Workfolw Services Fault Recovery Based on Micro Reboot Liang Chen, Dapeng Xiong, ZOU Peng

	Equipment Academy, Beijing, China ***Abstract***--In order to recover the fault caused by key atomic service out of order in workflow service, a new method of Workfolw Services fault recovery based on micro reboot is proposed. It uses atomic service weaved monitoring probes to monitor atomic service faults, and combines with the detection algorithm to locate the faults of workflow service. The construction method of workflow basic structures reboot tree is given, and and the method of data consistency processing is given too. On the basis of the above, a prototype system is designed and implemented to support workflow services fault recovery. The experiment results prove that the proposed method can efficiently detect, locate and recover the fault of workflow service, which greatly improves the availability of workflow services.
NS1012	Causes and Prevention of SQL Injection attacks in modern Web Applications Stephanos Mavromoustakos, Aakash Patel, Kinjal Chaudhary, ParthChokshi,Shaili Patel School of Computer Science, University of Windsor ***Abstract***--SQL injection is one of the major threats to the security of the web applications. Attackers try to gain unauthorized access to the database, which has vital and private information of the users. Many researchers have come up with various techniques and practices to protect the web applications from the attackers. From a pool of techniques available to perform SQL injection, usually not everyone is familiar with every attack. Hence, this kind of attack is still the most prevalent. We have presented the types of attacks in SQL injections and most dominant ways to prevent them.

Academic.net
Academic Conferences Calendar for Academics since 1995

http://www.academic.net/index.html

Academic Conferences Calendar for Academics since 1995
Your smart choice to find academic conferences worldwide

Follow us on **Twitter** by inputting account name: academic.net

Follow us on **Wechat** by scanning the above two-dimensional code

Follow us on **Instagram** by inputting account name: academic.net

Follow us on **Weibo** by scanning the above two-dimensional code

Note

Schedule of Sessions