PROGRAM GUIDE

ICT-EURASIA 2013
INFORMATION & COMMUNICATION TECHNOLOGY-EURASIA CONFERENCE

SPECIAL TRACK ASIAARES 2013
THE 2013 ASIAN CONFERENCE ON AVAILABILITY, RELIABILITY AND SECURITY

Supported by

ifip

ASEA UNINET
Asean-European University Network, founded in 1994

oead

TU WIEN
TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology

EURASIA-PACIFIC UNINET

secure
sba-research.org

UNIVERSITAS GADJAH MADA
Yogyakarta, INDONESIA
www.ugm.ac.id

TABLE OF CONTENTS

PROGRAM OVERVIEW

	MONDAY, 25.03.		TUESDAY, 26.03.		WEDNESDAY, 27.03.	
Time	Lecture Hall A	Time	Lecture Hall A	Lecture Hall B	Lecture Hall A	Lecture Hall B
		08:00 - 17:00	REGISTRATION		REGISTRATION	
		09:00 - 10:30	Opening		ICTEurAsia 3	AsiaARES 3
10:30 - 17:00	REGISTRATION	10:30 - 11:00	Break		Break	
11:00 - 12:30	PhD Symposium	11:00 - 12:30	Keynote *Prof. Dr. Josef Küng*		ICTEurAsia 4	AsiaARES 4
12:30 - 13:30	Lunch	12:30 - 13:30	Lunch		Lunch	
13:30 - 15:00	PhD Symposium	13:30 - 15:00	ICTEurAsia 1	AsiaARES 1	ICTEurAsia 5	AsiaARES 5
15:00 - 15.30	Break	15:00 - 15.30	Break		Break	
15:30 - 17:00	PhD Symposium	15:30 - 17:00	ICTEurAsia 2	AsiaARES 2	ICTEurAsia 6	AsiaARES 6
			Welcome Dinner *19.00 / UGM*			

	THURSDAY, 28.03.		FRIDAY, 29.03.	
Time	Lecture Hall A	Lecture Hall B	Lecture Hall A	Lecture Hall B
08:00 - 17:00	REGISTRATION		REGISTRATION	
09:00 - 10:30	ICTEurAsia 7		Tour to the Ancient Temple Borobudur + Lunch *Meeting point: 08.30 / UGM*	
10:30 - 11:00	Break			
11:00 - 12:30	ICTEurAsia 8	AsiaARES 7		
12:30 - 13:30	Lunch			
13:30 - 15:00	AsiaARES 8	AsiaARES 9		
15:00 - 15.30	Break			
15:30 - 17:00	AsiaARES 10	AsiaARES 11		
	Conference Dinner + Ramayana Ballet *Busses will depart at 17.00 from UGM*			

MONDAY, MARCH 25, 2013

10:30-17:00 Registration Desk is opened

11:00-12:30 PhD Symposium 1
Location: Lecture Hall A

12:30-13:30 Lunch Break

13:30-15:00 PhD Symposium 2
Location: Lecture Hall A

15:00-15:30 Coffee Break

15:30-17:00 PhD Symposium 3
Location: Lecture Hall A

TUESDAY, MARCH 26, 2013

08:00-17:00 Registration Desk is opened

09:00-10:30 Plenary Session
Opening by Representatives of the Conference Committee, Republic Austria, IFIP, Asea-Uninet and UGM
Location: Lecture Hall A

10:30-11:00 Coffee Break

11:00-12:30 Plenary Session
Keynote
Location: Lecture Hall A

Techniques and Trends in Databases
Prof. Dr. Josef Küng, Johannes Kepler University Linz, Austria

12:30-13:30 Lunch Break

13:30-15:00 Parallel Sessions
ICTEurAsia 1: Cloud and Internet Computing
Location: Lecture Hall A

1. Indonesian Digital Natives: ICT Usage Pattern Study across Different Age Groups
   Neila Ramdhani, Wisnu Wiradhany

   Abstract. Since its first appearance on early 2000's at the U.S, the idea that a new generation of students called digital natives or net generation has entered the world has been widely discussed by parents and educators alike. It is said that this generation think, socialize, and act differently; and they will alter roles and regulation of work and educational institutes. Now, at the second decade of the 21st century, Indonesia has to ready herself to meet this new generation. In this paper, we compared information and technology (ICT) access, activities within ICT, investment on ICT, and attitude towards ICT between five hundred Indonesian in three different groups: those who born before the 1980s; those who born between 1980s to 1989's, and those who born after the 1990s by ANOVA. We found that there were no difference on information and technology (ICT) access, activities, investment on ICT, and attitude towards ICT between the groups.

2. A Genetic Algorithm for Power-Aware Virtual Machine Allocation in Private Cloud
   HUNG Nguyen Quang, NAM Nguyen Hoai, NIEN Pham Dac , Nguyen Huynh Tuong, Nam Thoai

   Abstract. Energy efficiency has become an important measurement of scheduling algorithm for private cloud. The challenge is trade-off between minimizing of energy consumption and satisfying Quality of Service (QoS) (e.g. performance or resource availability on time for reservation request).

We consider resource needs in context of a private cloud system to provide resources for applications in teaching and researching. In which users request computing resources for laboratory classes at start times and non-interrupted duration in some hours in prior. Many previous works are based on migrating techniques to move online virtual machines (VMs) from low utilization hosts and turn these hosts off to reduce energy consumption. However, the techniques for migration of VMs could not use in our case. In this paper, a genetic algorithm for poweraware in scheduling of resource allocation (GAPA) has been proposed to solve the static virtual machine allocation problem (SVMAP). Due to limited resources (i.e. memory) for executing simulation, we created a workload that contains a sample of one-day timetable of lab hours in our university. We evaluate the GAPA and a baseline scheduling algorithm (BFD), which sorts list of virtual machines in start time (i.e. earliest start time first) and using best-fit decreasing (i.e. least increased power consumption) algorithm, for solving the same SVMAP. As a result, the GAPA algorithm obtains total energy consumption is lower than the baseline algorithm on simulated experimentation.

3. Cloud-Based E-Learning : A Proposed Model and Benefits by Using E-Learning Based on Cloud Computing for Educational Institution
Nungki Selviandro, Zainal Arifin Hasibuan

Abstract. The increasing research in the areas of information technology have a positive impact in the world of education. The implementation of e-learning is one of contribution from information technology to the world of education. The implementation of e-learning has been implemented by several educa-tional institutions in Indonesia. E-Learning provides many benefits such as flexibility, diversity, measurement, and so on. The current e-learning applications required large investments in infrastructure systems regardless of commercial or open source e-learning application. If the institution tended to use open source e-learning application it would need more cost to hire professional staff to maintain and upgrade the e-learning application. It can be challenging to implement e-learning in educational institutions. Another problem that can arise in the use of e-laerning trend today is more likely to institution building their own e-learning system itself. If two or more institutions are willing to build and use an e-learning so they can minimize the expenditure to develop the system and share learning materials more likely happened. This paper discuss the current state and challenges in e-learning and then explained the basic concept and previous proposed architectures of cloud computing. In this paper authors also proposed a model of cloud-based e-learning that consists of five layer, namely: (1) infrastructure layer; (2) platform layer; (3) application layer; (4) access layer; and (5) user layer. In addition to this paper we also illustrated the shift paradigm from conventional e-learning to cloud-based e-learning and described the expected benefits by using cloud-based e-learning.

13:30-15:00 Parallel Sessions

AsiaARES 1: Dependable Systems and Applications 1

Location: Lecture Hall B

1. Secure and Verifiable Outsourcing of Sequence Comparisons *(virtual)*
Yansheng Feng, Xiaofeng Chen, Hua Ma

Abstract. With the advent of cloud computing, secure outsourcing techniques of sequence comparisons are becoming increasingly valuable, especially for clients with limited resources. One of the most critical functionalities in data outsourcing is verifiability. However, there is very few secure outsourcing scheme for sequence comparisons that the clients can verify whether the servers honestly execute a protocol or not. In this paper, we tackle the problem by integrating the technique of garbled circuit with homomorphic encryption. As compared to existing schemes, our proposed solution enables clients to efficiently detect the dishonesty of servers. In particular, our construction re-garbles the circuit only for malformed responses and hence is very efficient. Besides, we also present the formal analysis for our proposed construction.

2. Based Secure Data-Level Access Control
Nisreen Alam Aldeen, Gerald Quirchmayr

Abstract. System-level access control methodologies depending on Perimeter Protection proofed their efficiency in the past, but the appearance of many new significant developments in digital communications highlighted the limitations of this approach. Increased concerns about the compatibility of system-level access control mechanism with new distributed and ubiquitous environments are turning aspirations towards de-perimeterisation protection and data level access control as solutions. This research does therefore try to make a contribution to privacy protection based on already advanced data-level access control work, such as the SPIDER project. The solution developed in this research suggests an X.509 certification extension to fit the data-level access control requirements, and proposes a new design for application structure in order to improve the identification and authentication-based secure data-level access control process.

3. On the efficiency modelling of cryptographic protocols by means of the Quality of Protection Modelling Language (QoP-ML) *(virtual)*
Bogdan Ksiezopolski, Damian Rusinek, and Adam Wierzbicki

Abstract. The problem of efficiency in the IT systems is now widely discussed. One of the factors affecting the performance of IT systems is implementation and maintaining a high level of security. In many cases the guaranteed security level is too high in relation to the real threats. The implementation and maintenance of this protection level is expensive in terms of both productivity and financial costs. The paper presents the analysis of TLS Handshake protocol in terms of quality of protection performed by the Quality of Protection Modelling Language (QoP-ML). The analysis concerns efficiency.

15:00-15:30 Coffee Break

15:30-17:00 Parallel Sessions
ICTEurAsia 2: E-Society 1
Location: Lecture Hall A

1. Translating the Idea of the eGovernment One-Stop-Shop in Indonesia
Fathul Wahid

Abstract. This study aims to understand how the idea of an eGovernment one-stop-shop (OSS) has been translated into a new setting. Since the beginning of 2000, this idea has been implemented in a variety of ways by Indonesian local governments. Using an interpretive case study in the city of Yogyakarta, the study revealed that the specificity of each setting influences the translation process of the idea of OSS during its institutionalization. It also identified a set of editing rules used during the translation process. These include the editing rules concerning context (e.g., internal readiness); logic (e.g., corruption eradication); and formulation (e.g., standardized processes). The study also found that the idea translation was not a single round process.

2. A Practical Solution Against Corrupted Parties and Coercers in Electronic Voting Protocol over the Network
Nguyen Thi Ai Thao, Dang Tran Khanh

Abstract. In this paper, we introduce a novel electronic voting protocol which is resistant to more powerful corrupted parties and coercers than any previous works. They can be the voting authorities inside the system who can steal voters' information and the content of their votes, or the adversaries outside who try to buy the votes, and force voters to follow their wishes. The worst case is that the adversaries outside collude with all voting authorities inside to destroy the whole system. In previous works, authors suggested many complicated cryptographic techniques for fulfilling all security requirements of electronic voting protocol. However, they cannot avoid the sophisticated inside and outside collusion. Our proposal prevents these threats from happening by the combination of blind signature, dynamic ballots and other techniques. Moreover, the improvement of blind signature scheme together with the elimination of physical assumptions makes the newly proposed protocol faster and more efficient. These enhancements make some progress towards practical security solution for electronic voting system.

3. Early-Detection System for Cross Language (Translated) Plagiarism
   Khabib Mustofa, Yosua Albert Sir

Abstract. The implementation of internet applications has already crossed the language border. It has, for sure, brought lots of advantages, but to some extent has also introduced some side-effect. One of the negative effects of using these applications is cross-languages plagiarism, which is also known as *translated plagiarism*. In academic institutions, translated plagiarism can be found in various cases, such as: final project, theses, papers, and so forth. In this paper, a model for web-based early detection system for translated plagiarism is proposed and a prototype is developed. The system works by translating the input document (written in Bahasa Indonesian) into English using Google Translate API components, and then search for documents on the World Wide Web repository which have similar contents to the translated document. If found, the system downloads these documents and then do some preprocessing steps such as: removing punctuations, numbers, stop words, repeated words, lemmatization of words, and the final process is to compare the content of both documents using the modified sentence-based detection algorithm (SBDA). The results show that the proposed method has smaller error rate leading to conclusion that it has better accuracy.

15:30-17:00 Parallel Sessions

AsiaARES 2: Dependable Systems and Applications 2

Location: Lecture Hall B

1. DiffSig: Resource Differentiation based Malware Behavioral Concise Signature Generation
   Huabiao Lu, Baokang Zhao, Xiaofeng Wang, Jinshu Su

Abstract. Malware obfuscation obscures malware into a different form that's functionally identical to the original one, and makes syntactic signature ineffective. Furthermore, malware samples are huge and growing at an exponential pace. Behavioral signature is an effective way to defeat obfuscation. However, state-of-the-art behavioral signature, behavior graph, is although very effective but unfortunately too complicated and not scalable to handle exponential growing malware samples; in addition, it is too slow to be used as real-time detectors. This paper proposes an anti-obfuscation and scalable behavioral signature generation system, DiffSig, which voids information-flow tracking which is the chief culprit for the complex and inefficiency of graph behavior, thus, losing some data dependencies, but describes handle dependencies more accurate than graph behavior by restrict the profile type of resource that each handle dependency can reference to. Our experiment results show that DiffSig is scalable and efficient, and can detect new malware samples effectively.

2. On Identifying Proper Security Mechanisms

Jakub Breier, Ladislav Hudec

Abstract. Selection of proper security mechanisms that will protect the organization's assets against cyber threats is an important non-trivial problem. This paper introduces the approach based on statistical methods that will help to choose the proper controls with respect to actual security threats. First, we determine security mechanisms that support control objectives from ISO/IEC 27002 standard and assign them meaningful weights. Then we employ a factor analysis to reveal dependencies among control objectives. Then this knowledge can be reflected to security mechanisms, that inherit these dependencies from control objectives.

3. Identity Management Lifecycle - Exemplifying the Need for Holistic Identity Assurance Frameworks
   Jostein Jensen

Abstract. Many governments around the world have a strategy to make electronic communication the primacy choice for interaction between the citizens and public services. Identity management makes the foundation for secure and trusted communication, and government frameworks for authentication and identity assurance are therefore developed to support the strategies. This paper examines three existing authentication and identity assurance frameworks, and is a good example to show the importance of specifying assurance frameworks that takes a holistic view of the identity management lifecycle and related threats.

19:00 Social Event 1

Welcome Dinner at the Universitas Gadjah Mada

supported by the Universitas Gadjah Mada

WEDNESDAY, MARCH 27, 2013

08:00-17:00 Registration Desk is opened

09:00-10:30 Parallel Sessions
ICTEurAsia 3: E-Society 2
Location: Lecture Hall A

1. End-to-End Delay Performance for VoIP on LTE System in Access Network
   Liang Shen Ng, Noraniah Ismail, Tutut Herawan

   Abstract. The desire Quality of Service (QoS) of Voice over Internet Protocol (VOIP) is of growing importance for research and study Long Term Evolution (LTE) is the last step towards the 4th generation of cellular networks. This revolution is necessitated by the unceasing increase in demand for high speed connection on LTE networks particularly for under variable mobility speed for VoIP in the LTE. This paper mainly focuses on performance of VOIP and the impact of resource limitations in the performance of Access Networks particularly important in regions where Internet resources are limited and the cost of improving these resources is prohibitive. By determine rate communication quality, is determined by end to end delay on the communication path, delay variation, packet loss. These performance indicators can be measured and the contribution in the access network can be estimated using simulation tool OPNET Modeler in varying mobility speed of the node. The overall performance of VOIP thus greatly improved significantly by deploying OPNET Modeler.

2. TransWiki: Supporting Translation Teaching
   Robert P. Biuk-Aghai, Hari Venkatesan

   Abstract. Web-based learning systems have become common in recent years and wikis, websites whose pages anyone can edit, have enabled online collaborative text production. When applied to education, wikis have the potential to facilitate collaborative learning. We have developed a customized wiki system which we have used at our university in teaching translation in collaborative student groups. We report on the design and implementation of our wiki system and an evaluation of its use.

3. Physicians' Adoption of Electronic Medical Records: Model Development Using Ability – Motivation - Opportunity Framework
   Rajesri Govindaraju, Aulia Hadining, Dissa Chandra

   Abstract. The benefits of electronic medical record (EMR) adoption by medical personnel, such as physicians, and medical organizations have been discussed in previous studies. However, most of medical personnel and organizations still use traditional paper-based medical records or use EMR ineffectively. This study aims to develop a model of EMR adoption among physicians and analyse the factors influencing the adoption. The model is developed base on Ability, Motivation, and Opportunity (AMO), adapted AMO, and Motivation-Ability Framework. Ten hypotheses were developed in this study. The next part of the study will be done to operationalize and empirically test the model using a survey method.

09:00-10:30 Parallel Sessions

AsiaARES 3: Dependable Systems and Applications 3

Location: Lecture Hall B

1. UVHM: Model Checking based Formal Analysis Scheme for Hypervisors
   Yuchao She, Hui Li, Hui Zhu

   Abstract. Hypervisors act a central role in virtualization for cloud computing. However, current security solutions, such as installing IDS model on hypervisors to detect known and unknown attacks, can not be applied well to the virtualized environments. Whats more, people have not raised enough concern about vulnerabilities of hypervisors themselves. Existing works mainly focusing on hypervisors' code analysis can only verify the correctness, rather than security, or only be suitable for open-source hypervisors. In this paper, we design a binary analysis tool using formal methods to discover vulnerabilities of hypervisors. In the scheme, Z notation, VDM, B, Object-Z or CSP formalism can be utilized as suitable modeling and specification languages. Our proposal sequently follows the process of disassembly, modeling, specification, and verification. Finally, the effectiveness of the method is demonstrated by detecting the vulnerability of Xen-3.3.0 in which a bug is added.

2. SA4WSs: a Security Architecture for Web Services *(virtual)*
   Lingxia Liu, Dongxia Wang, Jinjing Zhao, Minhuan Huang

   Abstract. With the rapid development and wide application of the Web services, its security flaws and vulnerabilities are increasing. Security has become one of the key issues to constrain the development of Web services technology. In this paper, we focus on how to build a security architecture for Web services to meet the security requirements of Web service applications. On the basis of analyzing the existing methods, a new security implementation approach for Web services is proposed to meet both the common security requirements of Web services platform and the specific security requirements of Web service applications. Then a security architecture for Web services is proposed. The architecture supports separating the functional implementations of Web service from the non-functional implementation of Web service, and ensures the portability of the platform.

3. Verifying Data Authenticity and Integrity in Server-Aided Confidential Forensic Investigation
   Shuhui Hou, Ryoichi Sasaki, Tetsutaro Uehara, Siuming Yiu

   Abstract. With the rapid development of cloud computing services, it is common to have a large server shared by many different users. As the shared server is involved in a criminal case, it is hard to clone a copy of data in forensic investigation due to the huge volume of data. Besides, those users irrelevant to the crime are not willing to disclose their private data for investigation. To solve these problems, Hou et al. presented a solution to let the server administrator (without knowing the investigation subject) cooperate with the investigator in performing forensic investigation. By using encrypted keyword(s) to search over encrypted data, they realized that the investigator can collect the necessary evidence while the private data of irrelevant users can be protected from disclosing. However, the authenticity and integrity of the collected evidence are not considered there. The authenticity and integrity are two fundamental requirements for the evidence admitted in court. So in this paper, we aim to prove the authenticity and integrity of the evidence collected by the existing work. Based on commutative encryption, we construct a blind signature and propose a "encryption-then-blind signature with designated verifier" scheme to tackle the problem.

10:30-11:00 Coffee Break

11:00-12:30 Parallel Sessions

ICTEurAsia 4: Knowledge Management 1

Location: Lecture Hall A

1. A Data-Driven Approach Toward Building Dynamic Ontology
   Dhomas Hatta Fudholi, Wenny Rahayu, Eric Pardede, Hendrik

Abstract. Ontology has been emerged as a powerful way to share common understanding, due to its ability to chain limitless amount of knowledge. In most cases, groups of domain expert design and standardize ontology model. Unfortunately, in some cases, domain experts are not yet available to develop an ontology. In this paper, we extend the possibilities of creating a shareable knowledge conceptualization terminology in uncommon domain knowledge where a standardized ontology developed by groups of experts is not yet available.
Our aim is to capture knowledge and behaviour which is represented by data. We propose a model of automatic data-driven dynamic ontology creation. The created ontology model can be used as a standard to create the whole populated ontology in different remote locations in order to perform data exchange more seamlessly. The dynamic ontology has a feature of a real-time propagation from the change in the data source structure. A novel delta script is developed as the base of propagation. In order to complete the model, we also present an information of application support in the form of Jena API mapping for propagation implementation.

2. Estimation of Precipitable Water Vapor Using an Adaptive Neuro-Fuzzy Inference System Technique
   Wayan Suparta, Kemal Maulana Alhasa

Abstract. Water vapor has an important role in the global climate change development. Because it is essential to human life, many researchers proposed the estimation of atmospheric water vapor values such as for meteorological applications. Lacking of water vapor data in a certain area will a problem in the pre-diction of current climate change. Here, we reported a novel precipitable water vapor (PWV) estimation using an adaptive neuro-fuzzy inference system (ANFIS) model that has powerful accuracy and higher level. Observation of the surface temperature, barometric pressure and relative humidity from 4 to 10 April 2011 has been used as training and the PWV derived from GPS as a testing of these models. The results showed that the model has demonstrated its ability to learn well in events that are trained to recognize. It has been found a good skill in estimating the PWV value, where strongest correlation was observed for UMSK station (r = 0.95) and the modest correlation was for NTUS station (r = 0.73). In general, the resulting error is very small (less than 5%). Thus, this model approach can be proposed as an alternative method in estimating the value of PWV for the location where the GPS data is inaccessible.

3. Using Semantic Web to Enhance User understandability for Online Shopping License Agreement
   Muhammad Asfandeyar, A Min Tjoa

Abstract. Normally, a common user sign license agreement without understanding the agreement. License agreements are a form of information, which describes product's usage and its terms and conditions. Habitually, users agree with it but without understanding. In the today's information age, there is no integration of license agreements with any current technology. The contents of license agreements are out of scope for search engines. Management of license agreements using Semantic Web is a multi-disciplinary challenge, involving categorization of common features and structuring the required information in such semantics that is easily extendable and fulfilling the requirements of common user.
In this paper construction of Semantic Web model for Online Shopping license agreement is discussed. The user requirements facilitate the construction of License Ontological model. Moreover,

rules are used to capture the complex statements of “terms and conditions”. Finally, an explicit semantic model for agreements is constructed that facilitates users’ queries.

11:00-12:30 Parallel Sessions

AsiaARES 4: Dependable Systems and Applications 4

Location: Lecture Hall B

1. A Variant of Non-Adaptive Group Testing and its Application in Pay-Television via Internet

   Thach V. Bui, Thuc D. Nguyen

   Abstract. In non-adaptive group testing (NAGT), the time for decoding is a crucial problem. Given an unknown string x 2 f0; 1gN with at most d ones, the problem is how to determine xi = 1 using as few tests as possible so that x can be decoded as fast as possible. A NAGT can be represented by a t N matrix. Although we do not know x, this matrix, which is called d-disjunct matrix, can reconstruct it exactly. In this paper, we consider a general problem, in which x is an array of N non-negative integer elements and has up to d positive integers. From nonrandom construction, we prove that we can decode a d-disjunct matrix, which is built from [n; k]q-Reed-Solomon codes and identity matrix Iq, and recover x defined above in poly(d) t log2 t + O(d3n log(d logN)) with t = O(d2 log2 N). We also discuss this problem when x contains negative integer elements. Pay-Television internet-based can be applied these results directly. Since the number of customers is very large, our system must be prevented from illegal buyers. This problem is called traitor tracing. To the best of our knowledge, this is the first result that raises a variant of NAGT and gets how to trace traitors without using probability.

2. A Proposal on Security Case based on Common Criteria

   Shuichiro Yamamoto, Tomoko Kaneko, Hidehiko Tanaka

   Abstract. It is important to assure the security of systems in the course of development. However, lack of requirements analysis method to integrate security functional requirements analysis and validation in upper process often gives a crucial influence to the system dependability. For security requirements, even if extraction of menaces was completely carried out, insufficient countermeasures do not satisfy the security requirements of customers.
   In this paper, we propose a method to describe security cases based on the security structures and threat analysis. The security structure of the method is de-composed by the Common Criteria (ISO/IEC15408).

3. A Test Case Generation Technique for VMM Fuzzing *(virtual)*

   Xiaoxia Sun, Hua Chen, Jinjing Zhao, Minhuan Huang

   Abstract. In this paper, we first give a short introduction to the security situation of virtualization technology, and then analyze the implementation challenges of the CPU virtualization component of a hybrid system virtual machine with support of running a guest machine of the IA-32 instruction set. Based on a formal definition of the CPU’s execution state, we propose a fuzzing test case generation technique for both the operands and operators of instructions, which can be applied to fuzz testing the virtual machine monitor (VMM) of a hybrid system virtual machine.

12:30-13:30 Lunch Break

13:30-15:00 Parallel Sessions

ICTEurAsia 5: Knowledge Management 2

Location: Lecture Hall A

1. On Efficient Processing of Complicated Cloaked Regions for Location Privacy Aware Nearest-Neighbor Queries
   Ngo Chan Nam, Dang Tran Khanh

   Abstract. The development of location-based services has brought not only conveniences to users' daily life but also great concerns about users' location privacy. Thus, privacy aware query processing that handles cloaked regions has become an important part in preserving user privacy. However, the state-of-the-art private query processors only focus on handling rectangular cloaked regions, while lacking an efficient and scalable algorithm for other complicated cloaked region shapes, such as polygon and circle. Motivated by that issue, we introduce a new location privacy aware nearest-neighbor query processor that provides efficient processing of complicated polygonal and circular cloaked regions, by proposing the Vertices Reduction Paradigm and the Group Execution Agent. In the Vertices Reduction Paradigm, we also provide a new tuning parameter to achieve trade-off between answer optimality and system scalability. Finally, experimental results show that our new query processing algorithm outperforms previous works in terms of both processing time and system scalability.

2. Mobile Collaboration Technology in Engineering Asset Maintenance – What Technology, Organisation and People Approaches are required?
   Faisal Syafar, Jing Gao

   Abstract. Engineering asset maintenance consists of coordinated activities and practices for retaining or restoring a piece of equipment, machine, or system to specified operable conditions to achieve its maximum useful life. An integrated high-level maintenance comprising multiple sub-systems requires the collaboration of many stakeholders including multiple systems and departments. Several of specialised technical, operational and administrative systems have been invested by engineering asset organisations to enhancing their asset management and maintenance systems, however there is no common ground among engineering asset organisations about what are collaborative maintenance are required for adoption/implementation. The lack of systematic approach, together with the lack of specific requirements to implement mobile collaborative maintenance requests a comprehensive framework for guiding engineering organisation to implement of new mobile technologies that meet all maintenance collaboration requirements. This research proposes to develop an appropriate mobile collaboration framework based on Delphi and Case Study investigation.

3. Information Systems Strategic Planning for a Naval Hospital
   Hery Muljo, Bens Pardamean

   Abstract. This article discusses the Information System (IS) strategic planning for a naval hospital in Indonesia. Its purpose is to improve competitive advantage among hospitals through the addition of new services and products that would lead to improvements in the current patient services. The merging of Hospital Information System (HIS), Radiology Information System (RIS), and Laboratory Information System (LIS) into a single network with a concept of telemedicine is the main topic of this article. The hospital's website is also developed with medical tourism in mind, which attracts more patients, generating more revenue for the hospital.

13:30-15:00 Parallel Sessions

AsiaARES 5: Cryptography 1

Location: Lecture Hall B

1. New Ciphertext-Policy Attribute-Based Access Control with Efficient Revocation *(virtual)*
   Xingxing Xie, Xiaofeng Chen, Hua Ma, Jin Li

   Abstract. Attribute-Based Encryption (ABE) is one of the promising cryptographic primitives for fine-grained access control of shared out-sourced data in cloud computing. However, before ABE can be deployed in data outsourcing systems, it has to provide efficient enforcement of authorization policies and policy updates. However, in order to tackle this issue, efficient and secure attribute and user revocation should be supported in original ABE scheme, which is still a challenge in existing work. In this paper, we propose a new ciphertext-policy ABE (CP-ABE) construction with efficient attribute and user revocation. Besides, an efficient access control mechanism is given based on the CP-ABE construction with an outsourcing computation service provider.

2. Provably Secure and Subliminal-Free Variant of Schnorr Signature *(virtual)*
   Yinghui Zhang, Hui Li

   Abstract. Subliminal channels present a severe challenge to information security. Currently, subliminal channels still exist in Schnorr signature. In this paper, we propose a subliminal-free variant of Schnorr signature. In the proposed scheme, an honest-but-curious warden is introduced to help the signer to generate a signature on a given message, but it is disallowed to sign messages independently. Hence, the signing rights of the signer is guaranteed. In particular, our scheme can completely close the subliminal channels existing in the random session keys of Schnorr signature scheme under the intractability assumption of the discrete logarithm problem. Also, the proposed scheme is proved to be existentially unforgeable under the computational Diffie-Hellman assumption in the random oracle model.

3. Anonymous Lattice-Based Broadcast Encryption *(virtual)*
   Adela Georgescu

   Abstract. In this paper we propose a lattice-based anonymous broadcast encryption scheme obtained by translating the broadcast encryption scheme of Paterson et al. [7] into the lattices environment. We use two essential cryptographic primitives for our construction: tag-based hint systems secure under Ring-LWE hardness and IND-CCA secure cryptosystem under LWE-hardness. We show that it is feasible to construct anonymous tag-based hint systems from Ring-LWE problem for which we use a variant with "small" secrets known to be as hard as regular Ring-LWE. We employ an IND-CCA-secure public key encryption scheme from LWE [12] for the PKE component of the anonymous broadcast encryption scheme.

15:00-15:30 Coffee Break

15:30-17:00 Parallel Sessions

ICTEurAsia 6: Security and Privacy

Location: Lecture Hall A

1. Semantic-aware Obfuscation for Location Privacy at Database Level
   Thu Le, Dang Tran Khanh

   Abstract. Although many techniques have been proposed to deal with location privacy problem, which is one of popular research issues in location based services, some limitations still remain and hence they cannot be applied to the real world. One of the most typical proposed techniques is obfuscation that preserves location privacy by degrading the quality of user's location information. But the less exact information, the more secure and the less effective services can be supported. Thus the goal of obfuscated techniques is balancing between privacy and quality of services. However, most of obfuscated techniques are separated from database level, leading to other security and performance issues. In this paper, we introduce a new approach to protect location privacy at database level, called Semantic B^{ob}-tree, an index structure that is based on B^{dual}-tree and B^{ob}-tree and contains semantic aware information in its nodes. It can achieve high level of privacy and keep up the quality of services.

2. Practical Constructions of Face-based Authentication Systems with Template Protection Using Secure Sketch
   Dang Tran Tri, Quynh Chi Truong, Dang Tran Khanh

   Abstract. Modern mobile devices (e.g. laptops, mobile phones, etc.) equipped with input sensors open a convenient way to do authentication by using biometrics. However, if these devices are lost or stolen, the owners will confront a highly impacted threat: their stored biometric templates, either in raw or transformed forms, can be extracted and used illegally by others. In this paper, we propose some concrete constructions of face-based authentication systems in which the stored templates are protected by applying a cryptographic technique called secure sketch. We also suggest a simple fusion method for combining these authentication techniques to improve the overall accuracy. Finally, we evaluate accuracy rates among these constructions and the fusion method with some existing datasets.

3. Code Based KPD Scheme With Full Connectivity: Deterministic Merging *(virtual)*
   Pinaki Sarkar, Aritra Dhar

   Abstract. Key PreDistribution (KPD) is one of the standard key management techniques of distributing the symmetric cryptographic keys among the resource constrained nodes of a Wireless Sensor Network (WSN). To optimize the security and energy in a WSN, the nodes must possess common key(s) between themselves. However there exists KPDs like the Reed Solomon (RS) code based schemes, which lacks this property. The current work proposes a deterministic method of overcoming this hazard by merging exactly two nodes of the said KPD to form blocks. The resultant merged block network is fully connected and comparative results exhibit the improvement achieved over existing schemes. Further analysis reveal that this concept can yield larger networks with small key rings.

15:30-17:00 Parallel Sessions

AsiaARES 6: Cryptography 2

Location: Lecture Hall B

1. On the Security of an Authenticated Group Key Transfer Protocol Based on Secret Sharing *(virtual)*
   Ruxandra F. Olimid

   Abstract. Group key transfer protocols allow multiple parties to share a common secret key. They rely on a mutually trusted key generation center (KGC) that selects the key and securely distributes it to the authorized participants. Recently, Sun et al. proposed an authenticated group key transfer protocol based on secret sharing that they claim to be secure. We show that this is false: the protocol is susceptible to insider attacks and violates known key security. Finally, we propose a countermeasure that maintains the benefits of the original protocol.

2. A Block Cipher Mode of Operation with Two Keys *(virtual)*
   Yi-Li Huang, Fang-Yie Leu, Jing-Hao Yang

   Abstract. In this paper, we propose a novel block cipher mode of operation (BCMO for short), named Output Protection Chain (OPC for short), which as a symmetric encryption structure is different from other existing BCMOs in that it employs two keys, rather than one key, to protect the output of the mode. The security threats of chosen-plaintext attacks on three existing common BCMOs, including the Cipher Feedback mode (CFB), the Output Feedback mode (OFB), and the Counter mode (CTR), are also analyzed. After that, we explain why the OPC mode (or simply the OPC) can effectively avoid chosen-plaintext attacks, and why its security level is higher than those of CFB, OFB, and CTR.

3. Modified Efficient & Secure Dynamic ID-based User Authentication Scheme *(virtual)*
   Toan Thinh Truong, Minh Triet Tran, Anh Duc Duong

   Abstract. Communication is necessary operations in wireless environments. Therefore, we must have a secure remote authentication to defend transactions against illegitimate adversaries in such risky channel. Smart card is one of methods that many schemes used due to its convenience. Recently, Khurram Khan has proposed an enhancement scheme using smart card to recover some pitfalls in Wang et al.'s scheme. They claimed that their scheme remedy those security flaws. Nevertheless, we point out that Khan et al.'s scheme cannot protect user's anonymity. Besides, it does not achieve secret key forward secrecy and cannot resist denial of service attack due to values stored in server's database. Consequently, we present an improvement to their scheme to isolate such problems.

4. Shifting Primes on OpenRISC Processors with Hardware Multiplier *(virtual)*
   Leandro Marin, Antonio J. Jara, and Antonio Skarmeta

   Abstract. Shifting primes have proved its efficiency in CPUs without hardware multiplier such as the located at the MSP430 from Texas Instruments. This work analyzes and presents the advantages of the shifting primes for CPUs with hardware multiplier such as the JN5139 from NX-P/Jennic based on an OpenRISC architecture. This analysis is motivated because Internet of Things is presenting several solutions and use cases where the integrated sensors and actuators are sometimes enabled with higher capabilities. This work has concluded that shifting primes are offering advantages with respect to other kind of primes for both with and without hardware multiplier. Thereby, offering a suitable cryptography primitives based on Elliptic Curve Cryptography (ECC) for the different families of chips used in the Internet of Things solutions. Specifically, this presents the guidelines to optimize the implementation of ECC when it is presented a limited number of registers.

THURSDAY, MARCH 28, 2013

08:00-17:00 Registration Desk is opened

09:00-10:30 Plenary Session
ICTEurAsia 7: Software Engineering 1
Location: Lecture Hall A

1. Software Development Methods in the Internet of Things
   Selo

   Abstract. In the Internet of Things, billions of networked and software-driven devices will be connected to the Internet. They can communicate and cooperate with each other to function as a composite system. This paper proposes the AMG (abstract, model and generate) method for the development of such composite systems. With AMG, the development of software application can be done in an automatic manner, and therefore reducing the cost and development time. The method has been prototyped and tested with use cases.

2. Analyzing Stability of Algorithmic Systems using Algebraic Constructs
   Susmit Bagchi

   Abstract. In general, the modeling and analysis of algorithmic systems involve discrete structural elements. However, the modeling and analysis of recursive algorithmic systems can be done in the form of differential equation following control theoretic approaches. In this paper, the modeling and analysis of generalized algorithmic systems are proposed based on heuristics along with z-domain formulation in order to determine the stability of the systems. The recursive algorithmic systems are analyzed in the form of differential equation for asymptotic analysis. The biplane structure is employed for determining the boundary of the recursions, stability and, oscillatory behaviour. This paper illustrates that biplane structural model can compute the convergence of complex recursive algorithmic systems through periodic perturbation.

3. SAT-Based Bounded Strong Satisfiability Checking of Reactive System Specifications
   Masaya Shimakawa, Shigeki Hagihara, Naoki Yonezaki

   Abstract. Many fatal accidents involving safety-critical reactive systems have occurred in unexpected situations that were not considered during the design and test phases of the systems. To prevent these accidents, reactive systems should be designed to respond appropriately to any request from an environment at any time. Verifying this property during the specification phase reduces development reworking. This property of a specification is commonly known as realizability. Realizability checking for reactive system specifications involves complex and intricate analysis. For the purpose of detecting simple and typical defects in specifications, we introduce the notion of bounded strong satisfiability (a necessary condition for realizability), and present a method for checking this property. Bounded strong satisfiability is the property that for all input patterns represented by loop structures of a given size k, there is a response that satisfies a given specification. We present a checking method based on a satisfiability solver, and report experimental results.

10:30-11:00 Coffee Break

11:00-12:30 Parallel Sessions

ICTEurAsia 8: Software Engineering 2

Location: Lecture Hall A

1. OSMF: A Framework for OSS Process Measurement
   Wikan Danar Sunindyo, Fajar Juang Ekaputra

   Abstract. An Open Source Software (OSS) project can be considered as a new type of business entity involving various roles and stakeholders, e.g., project managers, developers, and users, who apply individual methods. The project managers have the responsibility to manage the OSS development in a way that the OSS product can be delivered to the customers in time and with good quality. This responsibility is challenging, because the heterogeneity of the data collected and analyzed from different stakeholders leads to the complexity of efforts of the project managers to measure and manage OSS projects. In this paper, we propose a measurement framework (OSMF) to enable the project managers to collect and analyze process data from OSS projects efficiently. Initial results show that OSMF can help project managers to manage OSS business processes more efficient, hence improve the decision on OSS project quality.

2. CAPTCHA Suitable for Smartphones
   Yusuke Tsuruta, Mayumi Takaya, Akihiro Yamamura

   Abstract. We propose a CAPTCHA that tells data made by a computer program from one-stroke sketch data given by a human being using embodied knowledge. Utilizing touchscreens of smartphones, we realize this approach and resolve a conceivable inconvenience caused by the existing CAPTCHAs when using smartphones due to the limited display size of smartphones. We implement the proposed technique and analyze its validity, usefulness and security.

3. Algorithms of the Combination of Compiler Optimization Options for Automatic Performance Tuning
   Suprapto, Retantyo Wardoyo

   Abstract. It is very natural when people compile their programs, they would require a compiler that gives the best program performance. Even though today's compiler have reached the point in which they provide the users a large number of options, however, because of the unavailability of program input data and insufficient knowledge of the target architecture; it can still seriously limit the accuracy of compile-time performance models. Thus, the problem is how to choose the best combination of optimization options provided by compiler for a given program or program section. This gives rise the requirement of an orchestration algorithm that fast and effective to search for the best optimization combination for a program. There have been several algorithms developed, such as Exhaustive Search (ES); Batch Elimination (BE); Iterative Elimination (IE); Combined Elimination (CE); Optimization Space Exploration (OSE); and Statistical Selection (SS). Based on those of algorithms, in this paper we proposed Heuristics Elimination (HE) algorithm, a simple algorithm that was mostly inspired by OSE with some differences. The HE algorithm uses a heuristic approach by applying genetic algorithm to find the best combination of compiler's optimization options. It is unlike OSE, however, this proposed algorithm starts from a set of some possible combinations randomly selected, then they are iteratively refined by some genetic operators to find one optimal combination (as the solution).

11:00-12:30 Parallel Sessions

AsiaARES 7: Privacy and Trust Management 1

Location: Lecture Hall B

1. A Simplified Privacy Preserving Message Delivery Protocol in VDTNs
   Youngho Park, Chul Sur, Kyung-Hyune Rhee

   Abstract. In Vehicular Ad Hoc Networks (VANETs), because of high mobility of vehicles and frequent change of road segments, an end-to- end communication path between moving vehicles may not exist unfortunately. As a promising solution to this challenge, for non-realtime constrained VANET applications, store-carry-forward paradigm is considered to deliver a message to a remote destination vehicle effectively through a socialspot in city road environments. So, the behavior of VANET can be modeled as Delay Tolerant Networks, and known as Vehicular Delay Tolerant Networks (VDTNs). Therefore, in this paper, we propose a secure message delivery protocol for protecting receiver-location privacy in socialspot-based VDTNs since location privacy is one of critical security requirements in VANETs. To design a simplified protocol, we eliminate the use of pseudonym-based vehicle identification accompanied with a complex pseudonymous key management. Instead, we introduce an identity-hidden message indexing which enables a receiver vehicle to query a message whose destination is itself to the socialspot RSU without revealing its identity.

2. Supporting Secure Provenance Update by Keeping "Provenance" of the Provenance
   Amril Syalim, Takashi Nishide, Kouichi Sakurai

   Abstract. Provenance of data is a documentation of the origin and processes that produce the data. Many researchers argue that the provenance should be immutable: once a provenance is submitted, it should not be changed or updated. A main reason is that the provenance represents the history of data, and the history should not be altered or changed because it represents the fact in the past. Provenance can be represented by a graph, where each node represents the process executed by a party and an edge represents the relationship between two nodes (i.e. a child node uses the outputs of the parent nodes). A method to ensure that the provenance has not been updated is by using signature chain, where the signatures of the parent nodes are recorded in the children nodes so that any changes to the parent nodes will raise inconsistencies between the parent and the children. However, sticking to the requirement that the provenance should be immutable requires unlimited data storage and also we have problems whenever we need to update the provenance for an accidental error. In this paper, we propose a method that allows updates in the signature chain-based secure provenance, while keeping the signature consistent. The main idea is by keeping the "provenance" of the provenance itself, that is the history of update of the provenance, in the form of the signatures of the previous versions of the nodes. We implement the idea by keeping the signatures of the previous version in a signature tree similar to the Merkle-tree, where the a parent node in tree is the aggregate signature of the children. Using this method, the storage requirement to store signatures is always smaller than the number of updates.

3. Confidentiality-Preserving Query Execution of Fragmented Outsourced Data *(virtual)*
   Anis Bkakria, Frédéric Cuppens, Nora Cuppens-Boulahia, José M. Fernandez

   Abstract. Ensuring confidentiality of outsourced data continues to be an area of active research in the field of privacy protection. Almost all existing privacy-preserving approaches to address this problem rely on heavyweight cryptographic techniques with a large computational overhead that makes inefficient on large databases. In this paper, we address this problem by improving on an existing approach based on a combination of fragmentation and encryption. We present a method for optimizing and executing queries over distributed fragments stored in different Cloud storage service providers. We then extend this approach by presenting a Private Information Retrieval (PIR) based query technique to enforce data confidentiality under a collaborative Cloud storage service providers model.

12:30-13:30 Lunch Break

13:30-15:00 Parallel Sessions

AsiaARES 8: Privacy and Trust Management 2

Location: Lecture Hall A

1. Syntactic Analysis for Monitoring Personal Information Leakage on Social Network Services: A Case Study on Twitter
   Dongjin Choi, Pankoo Kim

   Abstract. Social network services such as Twitter and Facebook can be considered as a new media different from the typical media group. The information on social media spread much faster than any other traditional news media due to the fact that people can upload information with no constrain to time or location. Because of this reason, people got fascinated by SNS and it sinks into our life. People express their emotional status to let others know what they feel about information or events. However, there is a high possibility that people not only share information with others, but also they expose personal information unintentionally such as place to live, phone number, date of birth, and more. This will be serious problem if someone has impure mind. It is actually happening in cyber-stalking, offline stalking or others. There are also many spam messages in SNS because of the fact that information in SNS spread much faster than any other media and it is easy to send a message to others. In other words, SNS provides vast backbone environment to spammers to hunt normal pure users. In order to prevent information leakage and detect spam messages, many researchers traditionally have been studied for monitoring email systems, web blogs, and so on. In this paper, we dealt with text message data in Twitter which is one of the most popular social network services over the world in order to reveal various hidden patterns. Twitter data is severely dangerous to organizations and more is that anyone who has Twitter account can access to any users by "following" function. The following function does not require permission from the requested person to confirm to ready their timelines. This study will be focused on the user to whom exchange text messages and what types of information they reciprocated with others by monitoring 50 million tweets on November in 2009 which was collected by Stanford University.

2. Toward Secure Clustered Multi-Party Computation: A Privacy-Preserving Clustering Protocol *(virtual)*
   Sedigheh Abbasi, Stelvio Cimato, Ernesto Damiani

   Abstract. Despite a large amount of research work has been done and a large number of results produced, the deployment of Secure Multi-party Computation (SMC) protocols for solving practical problems in real world scenarios is still an issue. This is mainly due to the complexity of the SMC-based solutions and to the needed assumptions that are not easy to fit to the considered problem. In this paper we propose an innovative approach for the deployment of SMC, providing a tradeoff between efficiency and privacy. In the Secure Clustered Multi-Party Computation (SCMC) approach, a function is more efficiently computed through reducing the number of participants to the SMC protocol by clustering, such that a reasonable privacy leakage inside the cluster is allowed. Toward this direction, this paper verifies the impact and the feasibility of applying different clustering techniques over the participants to a SMC protocol and proposes an effective specifically-tailored clustering protocol.

3. A Real-time Privacy Amplification Scheme in Quantum Key Distribution
   Bo Liu, Baokang Zhao, Dingjie Zou, Chunqing Wu, Ilsun You

Abstract. QKD (Quantum Key Distribution) technology, based on the laws of physics, can create an unconditionally secure key between communication parties. In recent years, researchers draw more and more attention to the QKD technology. Privac amplification is a very significant procedure in QKD system. In this paper, we propose the real-time privacy amplification (RTPA) scheme which converts the weak secret string W to a uniform key that is fully secret from Eve. We implement RTPA scheme based on CLIP (Cvqkd Ldpc experImental Platform) which is connected to the real quantum communication systems. Experimental results show that, our proposed RTPA scheme is very efficient when the bit error rate of quantum channel is lower than 0.06.

13:30-15:00 Parallel Sessions

AsiaARES 9: Network Analysis and Security 2

Location: Lecture Hall B

1. Improved Greedy Forwarding Protocol for VANETs
   Wen Huaqing and Rhee Kyung-Hyune

Abstract. Most researches in the VANETs domain concentrate on the development of communication routing protocols. However, it is not effective to apply the existing routing protocols of MANETs to those of VANETs. In this paper, we propose a new greedy forward routing protocol which leverages real time traffic flow information to create a routing policy. Based on this routing policy, the proposed protocol alleviates the influence of high dynamic topology and decreases the average delivery delay on VANETs.

2. Improved Clustering for Intrusion Detection by Principal Component Analysis with Effective Noise Reduction
   Lu Zhao, Ho-Seok Kang, Sung-Ryul Kim

Abstract. PCA (Principal Component Analysis) is one of the most wildly used dimension reduction technique, which is often applied to identify patterns in complex data of high dimension [1]. In GA-KM [2], we have proposed GA-KM algorithm and have experimented using KDD-99 data set. The result showed GA-KM is efficient for intrusion detection. However, due to the hugeness of the data set, the experiment needs to take a long time to finish. To solve this deficiency, we combine PCA and GA-KM in this paper. The goal of PCA is to re-move unimportant information like the noise in data sets which have high dimension, and retain the variation present in the original dataset as much as possible. The experimental results show that, compared to GA-KM [2], the proposed method is better in computational expense and time (through dimension reduction) and is also better in intrusion detection ratios (through noise reduction).

3. Emulation on the Internet Prefix Hijacking Attack Impaction *(virtual)*
   Jinjing Zhao, Yan Wen

Abstract. There have been many incidents of IP prefix hijacking by BGP pro-tocol in the Internet. Attacks may hijack victim's address space to disrupt network services or perpetrate malicious activities such as spamming and DoS attacks without disclosing identity. The relation between network topology and prefix hijacking influence is presented for all sorts of hijacking events in different Internet layers. The impaction parameter is analyzed for typical prefix hijacking events in different layers. A large Internet emulation environment is constructed and the attack impaction of IP prefix hijacking events are evaluated. The results assert that the hierarchical nature of network influences the prefix hijacking greatly.

4. Architecture of Network Environment for High-risk Security Experimentation *(virtual)*
   Xiaohui Kuang, Xiang Li, Jinjing Zhao

   Abstract. Adequate Environment for conducting security experiments and test under controlled, safe, repeatable and as-realistic-as-possible conditions, are a key element for the research and development of adequate security solutions and the training of security personnel and researchers. In this paper, a new large-scale network experimental environment for high-risk security research was put forward. The main idea was using isolated computing clusters to obtain high levels of scale, manageability and safety by heavily leveraging virtualization technology, separating experiment and control network and multilayer sanitization.

15:00-15:30 Coffee Break

15:30-17:00 Parallel Sessions

AsiaARES 10: Network Analysis and Security 1

Location: Lecture Hall A

1. Trustworthy Opportunistic Access to the Internet of Services *(virtual)*
   Alessandro Armando, Aniello Castiglione, Gabriele Costa, Ugo Fiore, Alessio Merlo, Luca Verderame, Ilsun You

   Abstract. Nowadays web services pervade the network experience of the users. Indeed, most of our activities over the internet consist in accessing remote services and interact with them. Clearly, this can happen only when two elements are available: (i) a compatible device and (ii) a suitable network connection. The recent improvement of the computational capabilities of mobile devices, e.g., tablets and smartphones, seriously mitigated the first aspect. Instead, the inappropriateness, or even the absence, of connectivity is still a major issue. Although mobile, third generation (3G) networks can provide basic connectivity, complex interactions with web services often require different levels of Quality of Service (QoS). Also, 3G connectivity is only available in certain areas, e.g., user's country, and purchasing temporary connection abroad can be very costly. These costs weigh down on the original service price, seriously impacting the web service business model. In this paper we describe the problems arising when considering the orchestration of service-oriented opportunistic networks and we present the assumptions that we want to consider in our context. We claim that our model is realistic mainly for two reasons: (i) we consider state-of-the-art technology and technical trends and (ii) we refer to a concrete problem for service providers.

2. CSP-based General Detection Model of Network Covert Storage Channels *(virtual)*
   Hui Zhu, Tingting Liu, Guanghui Wei, Beishui Liu, Hui Li

   Abstract. A network covert channel is a malicious conversation mechanism, which brings serious security threat to security-sensitive systems and is usually difficult to be detected. Data are hidden in the header fields of protocols in network covert storage channels. In this paper, a general detection model based on formal protocol analysis for identifying possible header fields in net-work protocols that may be used as covert storage channels is proposed. The protocol is modeled utilizing the Communication Sequential Processes (CSP), in which a modified property of header fields is defined and the header fields are classified into three types in accordance to the extent to which their content can be altered without impairing the communication. At last, verification of the model in Transmission Control Protocol (TCP) shows that the proposed method is effective and feasible.

3. A Review of Security Attacks on the GSM Standard *(virtual)*
   Umberto Ferraro Petrillo, Giancarlo De Maio, Giuseppe Cattaneo, Pompeo Faruolo

Abstract. The Global Systems for Mobile communications (GSM) is the most widespread mobile communication technology existing nowadays. Despite being a mature technology, its introduction dates back to the late eighties, it suffers from several security vulnerabilities, which have been targeted by many attacks aimed to break the underlying communication protocol. Most of these attacks focuses on the A5/1 algorithm used to protect over-the-air communication between the two parties of a phone call. This algorithm has been superseded by new and more secure algorithms. However, it is still in use in the GSM networks as a fallback option, thus still putting at risk the security of the GSM based conversations. The objective of this work is to review some of the most relevant results in this field and discuss their practical feasibility. To this end, we consider not only the contributions coming from the canonical scientific literature but also those that have been proposed in a more informal context, such as during hacker conferences.

4. Unconditionally Secure Fully Connected Key Establishment using Deployment Knowledge *(virtual)*
   Sarbari Mitra, Sourav Mukhopadhyay, Ratna Dutta

Abstract. We propose a key pre-distribution scheme to develop a well-connected network using deployment knowledge where the physical location of the nodes are pre-determined. Any node in the network can communicate with any other node by establishing a pairwise key when the nodes lie within each other's communication range. Our proposed scheme is unconditionally secure against adversarial attack in the sense that no matter how many nodes are compromised by the adversary, the rest of the network remains perfectly unaffected. On a more positive note, our design is scalable and provides full connectivity.

15:30-17:00 Parallel Sessions

AsiaARES 11: Multimedia Security 1

Location: Lecture Hall B

1. An Extended Multi-Secret Images Sharing Scheme Based on Boolean Operation
   Huan Wang, MingXing He, Xiao Li

Abstract. An extended multi-secret images scheme based on Boolean operation is proposed, which is used to encrypt secret images with different dimensions to generate share images with the same dimension. The proposed scheme can deal with grayscale, color, and the mixed condition of grayscale and color images. Furthermore, an example is discussed and a tool is developed to verify the proposed scheme.

2. A Data Structure for Efficient Biometric Identification
   Kensuke Baba, Serina Egawa

Abstract. This paper proposes an efficient algorithm for personal identification with biometric images. In identification based on image comparison, the number of comparisons is an important factor to estimate the total processing time in addition to the processing time of a single comparison. Maeda et al. proposed an identification algorithm that reduces the number of comparisons from the linear search algorithm, however the processing time of each comparison is proportional to the number of registered images. The algorithm in this paper is an improvement of the algorithm by Maeda et al. with constant-time image comparisons. This paper evaluates the algorithms in terms of the processing time and the accuracy with practical palmprint images, and proves that the novel algorithm can

reduce the number of image comparisons from the linear search algorithm as the algorithm by Maeda et al. without loss of the accuracy.

3. Image Watermarking Using Psychovisual Threshold Over the Edge
   Nur Azman Abu, Ferda Ernawan, Nanna Suryana, Shahrin Sahib

Abstract. Currently the digital multimedia data can easily be copied. Digital image watermarking is an alternative approach to authentication and copyright protection of digital image content. An alternative embedding watermark based on human eye properties can be used to effectively hide the watermark image. This paper introduces the embedding watermark scheme along the edge based on the concept of psychovisual threshold. This paper will investigate the sensitivity of minor changes in DCT coefficients against JPEG quantization tables. Based on the concept of psychovisual threshold, there are still deep holes in JPEG quantization values to embed a watermark. This paper locates and utilizes them to embed a watermark. The proposed scheme has been tested against various non-malicious attacks. The experiment results show the watermark is robust against JPEG image compression, noise attacks and low pass filtering.

4. The PCA-Based Long Distance Face Recognition using Multiple Distance Training Images for Intelligent Surveillance System
   Hae-Min Moon, Sung Bum Pan

Abstract. In this paper, PCA-based long distance face recognition algorithm applicable to the environment of intelligent video surveillance system is proposed. While the existing face recognition algorithm uses the short distance images for training images, the proposed algorithm uses face images by distance extracted from 1m to 5m for training images. Face images by distance, which are used for training images and test images, are normalized through bilinear interpolation. The proposed algorithm has improved face recognition performance by 4.8% in short distance and 16.5% in long distance so it is applicable to the intelligent video surveillance system.

17:00-22:00 Social Event 2

Conference Dinner and Ramayana Ballet Performance at the Prambanan Temple

→ buses will depart at 17.00 from the Conference Venue (UGM)
→ we will come back at Yogyakarta at around 22.00

FRIDAY, MARCH 29, 2013

08:00-16:00 Social Event 3

Tour to the Ancient Temple Borobudur

Meeting point: 08.30 at the Conference Venue (UGM)

➔ lunch and tour guide included

➔ we will come back to Yogyakarta at around 16.00

Social Events

Welcome Dinner, Tuesday 26th of March

The Welcome Dinner will take place at the Conference Venue (UGM) at 19.00 and is supported by the Universitas Gadjah Mada.

Conference Dinner, Thursday 28th of March

The Conference Dinner will take place at the Prambanan Temple where we will also enjoy a Ramayana Ballet Performance.
Buses will depart directly after the last session at 17.00 from the Conference Venue (UGM). We will come back to Yogyakarta at around 22.00.

Tour to the Ancient Temple Borobudur, Friday 29th of March

We will meet at 08.30 at the Conference Venue (UGM). Buses will take us to Borobudur and will bring us back to Yogyakarata. We will arrive at Yogyakarta at around 16.00. Lunch will be served at Borobudur.

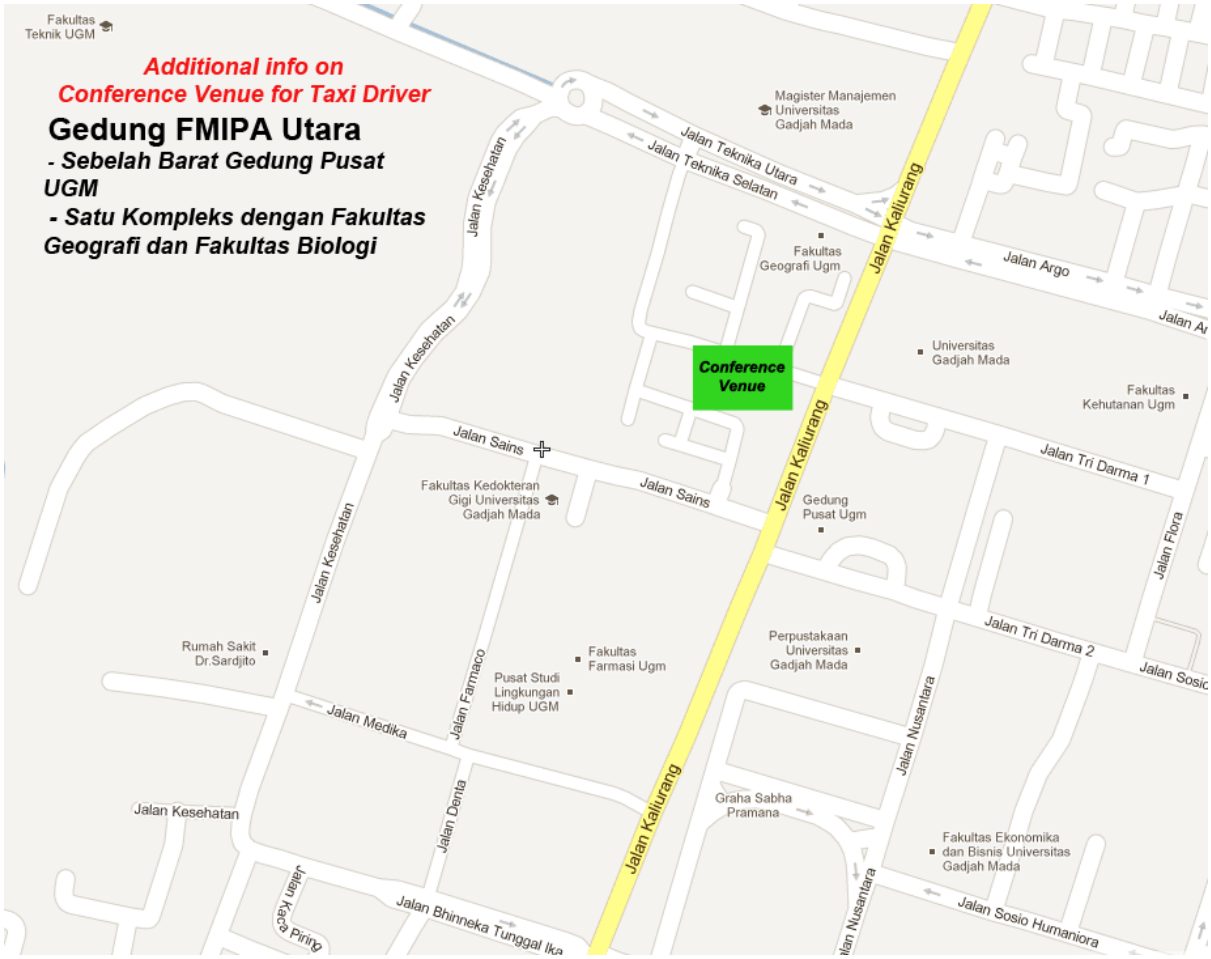
How to get to the Conference Location

From the airport to the Gadjah Mada University (UGM):

The easiest way to get to the conference venue is to take a taxi. We advise to take a “blue bird” taxi, if available. It will cost you less than 10 EUR (less than 125.000 IDR) to get from the airport to the university.

Address of the Conference Venue (map)

Fakultas MIPA (FMIPA) Universitas Gadjah Mada
Sekip Utara, Bulaksumur, Depok, Sleman
Yogyakarta 55281
INDONESIA



Note:

The additional Info on Conference venue is hopefully helpful for the participants when communicating with taxi driver

ABOUT YOGYAKARTA

Yogyakarta is a major tourist destination in Indonesia. It is the capital city of the province of Yogyakarta Special Region which is in the southern part of the Central Java province, Indonesia.

It is renowned as a centre of classical Javanese fine art and culture such as batik, ballet, drama, music, poetry, and puppet shows. Yogyakarta was the Indonesian capital during the Indonesian National Revolution from 1945 to 1949.

Yogyakarta is a bustling town of some 500,000 people and the most popular tourist destination on Java, largely thanks to its proximity to the temples of Borobudur and Prambanan.

Nickname(s): Kota Pelajar (*Student's City*)
Kota Budaya (*Cultural City*) or Kota Gudeg (*Gudeg City*)

Motto: *Memayu Hayuning Bawono*

Location of Yogyakarta in Indonesia

Coordinates: 7°48'5"S 110°21'52"E

Country	Indonesia
Province	Yogyakarta Special Region
Government	
• **Governor**	ISKS Hamengkubuwono X
• **Mayor**	Haryadi Suyuti
Area	
• City	32.5 km^2 (12.5 sq mi)
• **Metro**	1,114.16 km^2 (430.18 sq mi)
Population (2010)	
• City	388,088
• **Density**	12,000/km^2 (31,000/sq mi)
• Metro	2,389,200
• **Metro density**	2,100/km^2 (5,600/sq mi)
Time zone	WIB (UTC+7)

Weather

The temperature in Yogyakarta tends to be relatively moderate, although high levels of humidity can make the summers in the area seem quite hot. The average summer high temperature is in the nineties degrees Fahrenheit and the average humidity at that time is approximately seventy five percent. Humidity throughout the rest of the year varies between sixty five and eighty five percent. The average temperature throughout the year is a comfortable eighty degrees Fahrenheit, with the average winter low being in the sixties degrees Fahrenheit.

In March Daytime temperatures average between 32°C/90°F and 25°C/77°F.

Despite the fact that it is hotter in the area during the summer, many people travel to Yogyakarta at this time because it also marks the area's dry season. Yogyakarta is a wet environment, with a rainy season which begins in September and continues through May. The heaviest monsoon rains generally last from January through April, with February being the rainiest month.

Websites about travelling to Yogyakarta:

http://wikitravel.org/en/Yogyakarta

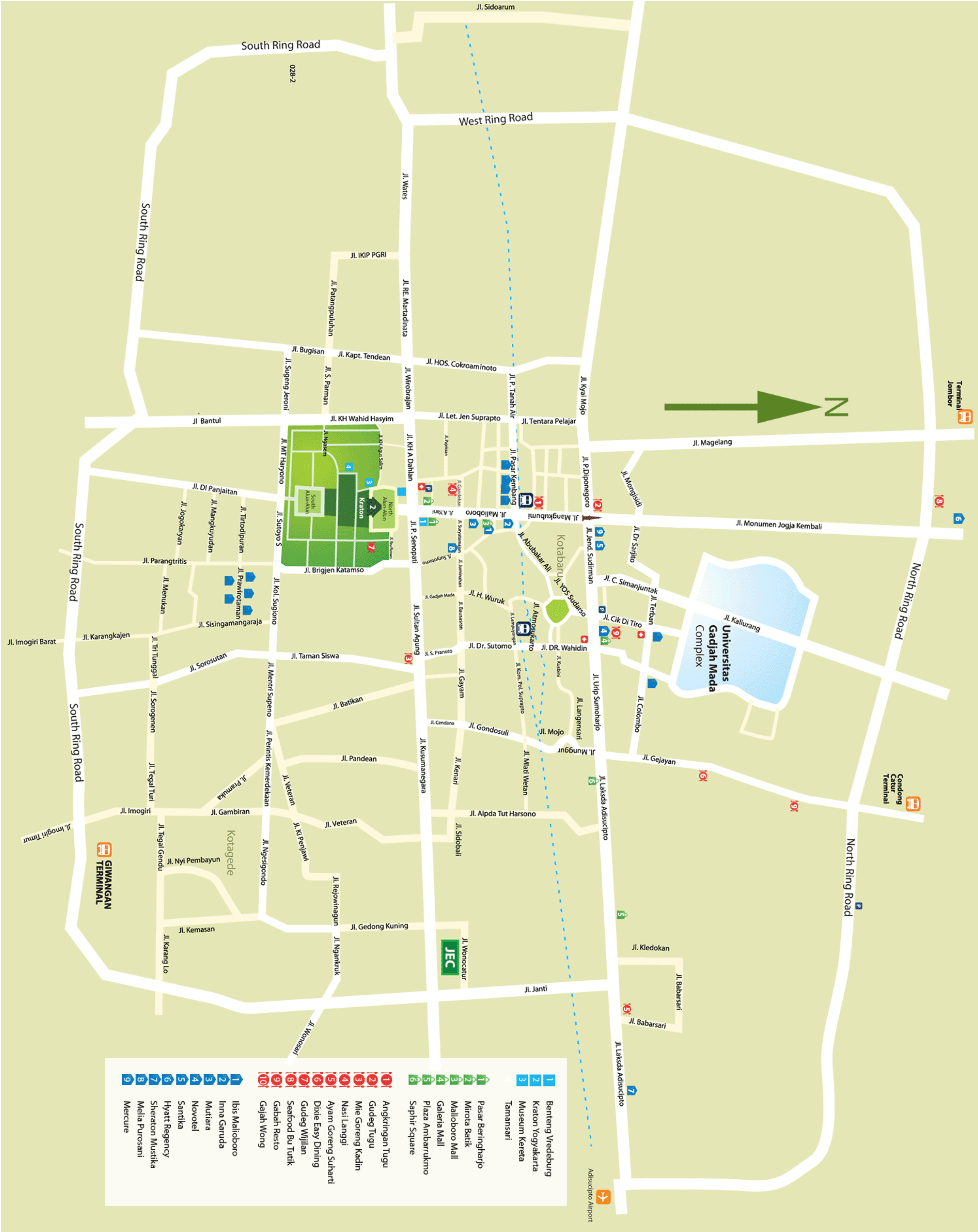
http://www.yogyes.com/

Good to know

1 Euro (EUR) equals about 12,443.38 Indonesian Rupiah (IDR). (there is no guarantee that the rate will be equal from one money changer to another)

For further information on rates please check the currency calculator below:
http://www.x-rates.com/calculator/

City Map


1 Benteng Vredeburg
2 Kraton Yogyakarta
3 Museum Kereta
Tamansari
1 Pasar Beringharjo
2 Mirota Batik
3 Malioboro Mall
4 Galeria Mall
5 Plaza Ambarrukmo
6 Saphir Square
1 Angkringan Tugu
2 Gudeg Tugu
3 Mie Goreng Kadin
4 Nasi Langgi
5 Ayam Goreng Suharti
6 Dixie Easy Dining
7 Gudeg Wijilan
8 Seafood Bu Tutik
9 Gabah Resto
10 Gajah Wong
1 Ibis Malioboro
2 Inna Garuda
3 Mutiara
4 Novotel
5 Santika
6 Hyatt Regency
7 Sheraton Mustika
8 Melia Purosani
9 Mercure
N
South Ring Road
West Ring Road
North Ring Road
Kraton
Kotagede
Kotabaru
Universitas Gadjah Mada Complex
JEC
GIWANGAN TERMINAL
Condong Catur Terminal
Terminal Jombor
Adisucipto Airport

CONFERENCE OFFICE

If you have any questions or need assistance during the conference do not hesitate to contact:

ICT-EurAsia / AsiaARES Conference Office

Yvonne Poul

Tel: +43 699 100 41 066

Email: ypoul@sba-research.org

Local Organizing Committee

Faculty Staff

1. Khabib Mustofa. Phone **+628998997827**, khabib@ugm.ac.id
2. Mardhani Riasetiawan, Phone **+6283869942863**, mardhani@ugm.ac.id
3. Ahmad Ashari, Phone +**62817463205**, ashari@ugm.ac.id

Students

1. Sonia Yunita, Phone +**6283823346009**, soniayunita@gmail.com