



## Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA CHINESE TAIPEI JAPAN MALAYSIA NEW ZEALAND SINGAPORE SOUTH KOREA THAILAND



# RECENT SECURITY DEVELOPMENT

**ABSTRACT**

This short paper provides an update on the progress of SC 27 work, as a follow-up to the previous paper published in Volume 3 of the Proceedings titled 'An International Common Language for Information Security - An update on ISMS standards'.

**1. New International Standard on Accreditation of Certification Bodies on ISMS**

Since last February, SC 27 Working Group 1 (WG 1) has been busy revising the accreditation standard EA 7/03. This work is being carried out as a joint project with experts from International Accreditation Forum (IAF) and ISO Committee on Conformity Assessment (CASCO). The revised version is being numbered as ISO/IEC 27006 - Requirements for the accreditation of bodies providing certification of information security management systems. The document has now been circulated to the National Bodies for a Final Committee Draft (FCD) ballot with the expectation to have a published standard by end of 2006. This revised version takes into account the new version of ISO Guide 62, that is ISO/IEC 17021 - Conformity assessment -- Requirements for bodies providing audit and certification of management system (currently in development stage), and more on ISMS guidance for accreditation bodies and certification bodies.

Work on ISO/IEC 27000 Information security management system fundamentals and vocabulary has now started and a first working document is expected to be circulated for review and comment over the next few months. ISO/IEC 27003-27005 are all progressing and are currently at the following stages of development:

- ISO/IEC 27003 Information security management system implementation guidance is currently at 2nd Working Draft (WD);
- ISO/IEC 27004 Information security management measurements is currently at 4th WD and is expected to go out for a 1st Committee Draft (CD) during the next six months; and
- ISO/IEC 27005 Information security risk management is current out for a 2nd CD ballot.

The Disaster Recovery services standard ISO/IEC 24762 Guidelines for information and communications technology disaster recovery services is being circulated as a first CD ballot.

## 2. **WG 1 and Its New WG**

With effect from May 2006, SC 27 has also restructured its working groups. WG 1 is now split into two WGs:

- WG 1 ISMS Standards (Convenor is Ted Humphreys, United Kingdom); and
- WG 4 ISMS Techniques and Services Supporting Guidelines (Convenor is Meng-Chow Kang, Singapore).

The scope of WG 4 covers the development of ISMS standards and guidelines supporting the ISO/IEC 27000 series of standards (i.e. 27000-27009). This also includes work on:

- Disaster Recovery and Business Continuity;
- Cyber Security; and
- Outsourcing.

National Bodies are encouraged to continue support the development of these security standardization initiatives, and in particular, to also contribute and participate in the new WG activities.

### **Mr Ted Humphreys**

*Chartered Fellow of BCS CITP, CISM  
Convenor of ISO/IEC JTC 1/SC 27/WG 1*

*Director  
XiSEC Consultants Ltd, UK*

*Visiting Professor  
Korea University*



Ted Humphreys (Chartered Fellow of the BCS - FBCS CITP, CISM) is the Director of XiSEC Consultants Ltd, a UK company providing Information Security Management consultancy services around the world. He has been an expert in the field of information security and risk management for more than 27 years. During this time, he has worked for major international companies (in Europe, North America and Asia), as well as organizations such as the European Commission and the OECD.

Ted, the internationally acknowledged father and management guru (and some say spiritual leader) of the ISO/IEC 17799 and ISMS (BS 7799) standards and the global BS 7799 certification movement, has been the Editor of BS 7799 Part 1:1999, ISO/IEC 17799:2000, the 1999 and 2002 editions of BS 7799 Part 2 the ISMS standard and the EA 7/03 the ISMS accreditation guidelines. He is the Founder and Director of the ISMS International User Group and is responsible for the International Register of BS 7799/ISMS Certificates. In 2002 he was honoured with the Secure Computing Lifetime Achievement Award. This international award recognizes his noteworthy achievements in shaping and promoting the development and standardization of information security management BS 7799 best practice standards.

# Identity Metasystem - A New Perspective And Architecture On Digital Identity

Mr Meng-Chow Kang

## ABSTRACT

The issues and dilemma of digital identity have been a constant challenge to businesses, governments, and individuals on the Internet. The lack of an identity infrastructure has been a key contributor to many of these challenges, which has facilitated various forms of identity-based cybercrimes such as phishing and scam emails. This paper discusses the principles of digital identity, and presents the concept of an identity metasystem as a way forward to address the digital identity challenges. The identity metasystem establishes a set of standards-based Web Services protocols that support the principles (or laws) of digital identity for achieving interoperability between multiple identity systems securely, with consistent human integration and user experiences.

## 1. Introduction

In the annual RSA conference held in San Jose in February 2006, Bill Gates, Microsoft's Chairman and Chief Software Architect, discussed how Microsoft is aligning its efforts around a security architecture that will create and support four key principles to establish trust in computing and realize the full potential of an interconnected world. The four principles involve building a **trust ecosystem** that engenders trust and accountability between people, business and code; **engineering for security**, infusing security thinking at every step in the process of developing software; **simplifying security** for IT professionals, developers, and consumers by reducing complexity through implementing security-conscious interfaces, tools and guidance, and eliminating unnecessary user intervention; and promoting **fundamentally secure platform**, including devices and networks, that have confidentiality, integrity, availability, and accountability built-in.

Central in the trust ecosystem is the notion of digital identities, in which the trustworthiness and accountability of individuals, devices, and software code on the other end of a connection are relied upon. Without trustworthy and accountable<sup>1</sup> identity, users have been tricked into divulging private and confidential information. As reported by the Anti-Phishing Working

<sup>1</sup> Accountability can be as simple as a loss of reputation or expulsion from a group, or as severe as a conviction for a criminal act.

Group<sup>2</sup>, the number of web sites involved in phishing<sup>3</sup> activities has grown in the previous year by more than 300 percents to 7,195 in December 2005, from 1,707 in December 2004. In the same period, the number of unique reported phishing incidents has grown from 8,829 to 15,244, clearly highlighting identity theft as one of the major challenges on the Internet today. Similarly, with fraudulent claims of identities that could not be differentiated from valid identities, businesses have also been scammed to execute transactions and deliver services to fraudulent organizations and individuals resulting in substantive financial losses and impacts on reputation<sup>4</sup>. In the United Kingdom's National High Tech Crime Unit (NHTCU) survey<sup>5</sup> conducted in 2005, theft of information or data, including customer lists and personal information were ranked amongst the top nine categories of high-tech crimes reported.

The weaknesses in current digital identities can be attributed to a basic neglect in that **Internet was built without a way to know who and what you are connecting to**<sup>6</sup>. Everyone offering Internet services therefore need to provide its own identity system. For ease of implementation and manageability, simple user name and password scheme of identification and authentication remains the most common today. While other more secure forms of identity authentication systems have also been implemented, such as using smart cards and biometrics to provide greater security assurance, many were not designed and built to interoperate easily as well. User interfaces receiving sensitive and private information from users do not provide a means for them to evaluate the authenticity and trustworthiness of the sites behind them. Users were taught to recognize and trust a web site based on the security lock depicting use of the Secure Socket Layer (SSL) protocol, which however only

<sup>2</sup> The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and email spoofing. There are more than 1,300 companies and government agencies participating in the APWG and more than 2,100 members. APWG publishes a monthly phishing activity trend report that can be downloaded from APWG web site at <http://www.antiphishing.org/>

<sup>3</sup> Phishing refers to the stealing of personal identity information such as user name, password, social security numbers, financial account credentials, and credit card numbers. Phishing attacks normally use social engineering schemes in the form of 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging personal information. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Malicious software such as Trojan keylogger and Spyware are also often deployed in users' PC to steal personal information directly.

<sup>4</sup> For example, see Munir Kotadia (2003), 'Internet fraudsters sentenced to 15 years', CNETAsia, 24 November 2003. Available online at <http://www.asia.cnet.com/newstech/security/0,39001150,39159062,00.htm>.

<sup>5</sup> [http://www.nhtcu.org/media/documents/publications/8817\\_Survey.pdf](http://www.nhtcu.org/media/documents/publications/8817_Survey.pdf)

<sup>6</sup> Kim Cameron (2005), 'The Law of Identity', Microsoft Corporation. Available online at: <http://www.identityblog.com/stories/2005/07/25/thelaws.html>

provides security for data during transmission, but not at either ends of the communications. With the growing numbers of identity systems, the multiplicity of accounts and passwords, users must keep track and remember result not only in frustrations, but insecure practices such as reusing account names and passwords at many websites.

On the other hand, attempts to provide a single identity system for multiple applications across a wide variety of businesses, such as the Microsoft's .NET Passport system, which has been successfully used for identifying and authenticating more than 250 million Hotmail<sup>7</sup> users, and provides simplified access and management, could not meet the requirements for many other businesses and usage contexts, and provide different trust level to meet different security policies and business rules of all applications effectively. From this and many other similar initiatives, we can logically deduce that universal adoption of a single digital identity system or technology is unlikely ever to occur.

In countries where citizens are issued with national identification cards (NIC), in which each citizen has a unique identifier (NID) assigned, the NID uses a data format that enables certain personal data to be decoded. For example, in Singapore, the year of birth is used as the first two digits of the NID for all citizens that are born in 1968 and later. In Korea, the NID includes digits identifying the location (province) and date of birth, as well as the gender. For ease of implementation and identification, a number of systems on the Internet have used such NID directly as user identifier, resulting in some users' concerns over their personal data privacy when such identifiers are not given similar protections like user passwords. Compromise of the security of those systems may impact the privacy of the individuals, since more personal information can be decoded from the NID used in the system.

## 2. The Laws of Digital Identity

The needs for multiple identity systems to co-exist and interoperate, and at the same time provides a way for users to be able to handle multiple digital identities easily, just like handling the many physical cards that they carry in their wallets, with adequate security safeguards of personal information related to each identity system are fundamentals to any universally adoptable and sustainable identity architecture.

<sup>7</sup> <http://www.hotmail.com/>

In recent years, on the Internet, led by Kim Cameron<sup>8</sup>, a number of Net citizens have begun codifying these fundamental principles (along with a number of others) into a proposed set of 'Laws of Identity'. The Laws<sup>9</sup> were proposed, debated, and refined through a long-running, open, and continuing dialogue on the Internet. They are:

**1) User Control and Consent**

Identity systems must only reveal information identifying a user with the user's consent;

**2) Minimal Disclosure for a Constrained Use**

The identity system must disclose the least identifying information possible, as this is the most stable, long-term solution;

**3) Justifiable Parties**

Identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship;

**4) Directed Identity**

A universal identity system must support both 'omni-directional' identifiers for use by public entities and 'unidirectional' identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles;

**5) Pluralism of Operators and Technologies**

A universal identity solution must utilize and enable the interoperation of multiple identity technologies run by multiple identity providers;

**6) Human Integration**

Identity systems must define the human user to be a component of the distributed system, integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks; and

<sup>8</sup> Kim Cameron (2005), 'The Law of Identity', Microsoft Corporation. Available online at: <http://www.identityblog.com/stories/2005/07/25/thelaws.html>

<sup>9</sup> The Laws of Identity are discussed in more detail in The Laws of Identity whitepaper. To join in the discussion of the Laws of Identity, visit [www.identityblog.com](http://www.identityblog.com).

### **7) Consistent Experience Across Contexts**

The unifying identity metasytem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

In essence, these principles must be met for any identity systems to be effective and successful. However, no single system can fulfill all these principles completely. Taken together, the Laws therefore define the architecture of an Identity Metasytem in which the individual (user) is the center of multiplicity of identity systems, with different parties participating in different ways.

### **3. Identity Metasytem**

The identity metasytem, or system of systems, would leverage the strengths of its constituent identity systems, provide interoperability between them, and enable creation of a consistent and straightforward user interface to all of them. The resulting improvements in cyberspace would benefit everyone, making the Internet a safer place with the potential to boost e-commerce, combat phishing, and solve other digital identity challenges.

In the offline world, people carry multiple forms of identification in their wallets, such as driver's licenses or other government-issued identity cards, credit cards, and affinity cards such as frequent flyer cards. People decide which card to use and how much information to reveal in any given situation.

Similarly, the identity metasytem makes it easier for users to stay safe and in control when accessing resources on the Internet. It lets users select from among a portfolio of their digital identities and use them at Internet services of their choice where they are accepted. The metasytem enables identities provided by one identity system technology to be used within systems based on different technologies, provides an intermediary exists that understands both technologies and is willing and trusted to do the needed translations.

It is important to note that the identity metasytem does not compete with or replace the identity systems it connects. Rather, it plays a role analogous to that of the Internet Protocol (IP) in the realm of networking by offering a technology-independent metasytem that

insulated applications from the intricacies of individual network technologies, providing seamless interconnectivity and a platform for including not-yet-invented networks (such as 802.11 wireless, which came into the landscape only a few years ago) into the network metasystem. In the same way, far from competing with or replacing the identity systems it connects, the identity metasystem **relies** on the individual systems to do its work.

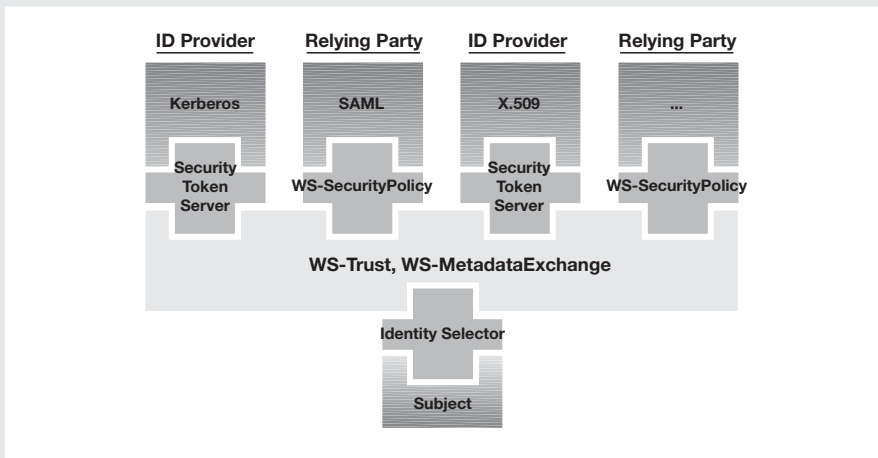
In the identity metasystem, participants will undertake one of the three main roles, namely, **identity providers**, **relying parties**, or **subjects**. In many cases, participants may play more than one role, and often all three. Identity providers are participants who issue digital identities. For example, government might issue identities to citizens for e-government services, like those used in Singapore for online access to the Central Provident Funds (CPF) accounts information; banks might issue identities to consumers for enabling online banking transactions on the Web; and Internet service providers might issue identities to subscribers for broadband or wireless network access services. Relying parties are participants who make use of identities to determine whether an online service could be provided. Again, they include government agencies running e-government services, banks running online banking services, and ISP providing network services, in which all require identities to validate subjects' authenticity and authorization. Subjects, including end users, companies, and organizations, are the individuals and other entities about whose claims are made. Claims refer to pieces of information about the subject that the issuer asserts are valid. For example, an X.509 certificate issued by a Certification Authority, or a Kerberos security token issued by an Active Directory in an organization, is both claims that a subject may use to identify itself to a relying party.

To build an identity metasystem, there must be components in the system to provide a way to represent identities using claims; a means for identity providers, relying parties, and subjects to negotiate and determine mutually agreeable technologies, claims, and requirements; an encapsulation protocol to obtain both claims and requirements dynamically; a means to bridge technology and organizational boundaries using claims transformation; and a consistent user experience across multiple contexts, technologies, and operators.

To realize the identity metasystem, the WS-\* Web Services<sup>10</sup> architecture has been proposed. Figure 1 depicts such an architecture. The encapsulating protocol used for claims

<sup>10</sup> Read more about Web services at <http://msdn.microsoft.com/webservices/>.

transformation is WS-Trust. Negotiations are conducted using WS-MetadataExchange and WS-SecurityPolicy. These protocols enable a technology-neutral identity metasystem to be built which form the ‘backplane’ of the identity metasystem. Like other Web services protocols, they also allow new kinds of identities and technologies to be incorporated and utilized as they are developed and adopted by the industry.



**Figure 1:** A WS-\* Architecture for the Identity Metasystem

The Security Token Server (STS) implements the WS-Trust protocol and provides support for claims transformation. Relying parties provide statements of requirements, expressed in terms of the WS-SecurityPolicy specification, and made available through the WS-MetadataExchange protocol. The Identity Selector implements the consistent user experience. After being invoked by an application, it performs the negotiation between relying party and identity provider(s), displays the identities of ‘matched’ identity providers and relying parties to the subject (e.g. the end user), obtains claims, and releases them to the application under the supervision of the subject.

#### 4. Realizing the Identity Metasystem

To realize the implementation of the identity metasystem, Microsoft and other industry leaders are working together and investing in a number of areas. For example, Sun Microsystems has demonstrated a version of the STS interoperating with Microsoft’s

Windows CardSpace (identity selector, previously known as 'InfoCard') technology during the May 2006 JavaOne conference. A number of open source developers have also embarked on implementing supports at the different operating systems platforms, web servers, and web browsers technology for the Web Services protocols that have been defined for the metasystem to enable interoperability across various technologies and systems.

## 5. Conclusion

The many security and privacy challenges on the Internet today are the result of the absence of a unifying and architected systems of digital identity and the past ignorance of the Laws of Digital Identity. The widespread adoption and deployment of the identity metasystem has the potential to address these challenges and bring about greater benefits of connectivity by making the online world trustworthy, safer, and easier to use. It is also important to note that the identity metasystem, by itself, addresses only the needs of a trust ecosystem for identity and accountability in the interconnected world. Engineering for security, drive for simplicity, and building fundamentally secure platforms must also be undertaken by the industry in order to realize the full potential of the interconnected world. We will discuss these other elements in future papers.

Note: The biography of the author is available on page 05 at the Preface.

# Security Incidents And Trace-back - Introduction To Network Security Incident Analysis System For Detecting Large-scale Internet Attacks

Mr Koji Nakao

## ABSTRACT

Considering the increase in the dependency of network and current network threats lately, it has become more and more important to provide appropriate network security countermeasures in both network and end-systems. This paper focused on two major activities related to network security development in Japan namely, (a) Network incident analysis, and (b) Trace-back technology.

## 1. Network Incident Analysis

The content of this section is based on the latest result of the research activity in the National Institute of Communication Technology (NICT) in Japan. The research members in NICT are investigating prompt detection of network security incidents and analysis of the incidents in order to protect wide area network infrastructure against DDoS-like threats of large scale and volume attacks. The first stage of the mission of Network Incident Analysis Center for Tactical Emergency Response (NICTER) is to build the incident analysis center.

The NICTER incident analysis system provides a framework to enable integrated analysis of network security incidents using various methods and data sources. NICTER collects data from live information sources such as the internet service providers (ISPs) and other sensor points deployed in Japan. It has the following three objectives:

- 1) Real-time automated analysis for detecting precursor trends;
- 2) In-depth analysis for investigating the detected incidents in details; and
- 3) Prompt security recommendation to the ISPs and users.

NICTER analyzes events<sup>1</sup> which are captured and collected by network monitoring and shows results in order to support decision making by network security analysts. It has two analysis engines, namely macro analysis and micro analysis (see Figure 1). The macro

<sup>1</sup> The event means an occurrence on network which is recorded. E.g. traffic data, logged data and so on.

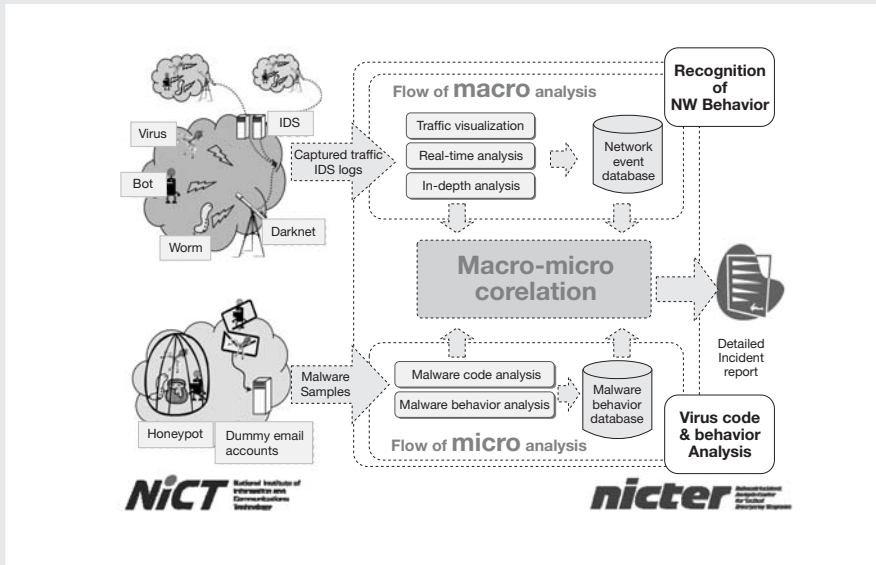


Figure 1: An Overview of NICTER

analysis engine finds out trend of incident on network security and the micro analysis engine examines the details of each incident such as finding out the behavior of malicious code by collecting and analyzing sample code. These two analyses identify relationships between occurrence and reason of the events. The macro analysis confirms an occurrence and the micro analysis pinpoints reasons of incidents such as activity of malicious code. By comparing results of the macro analysis and the micro analysis, a network security analyst at NICTER can find out correlation of these results. It also enables the analyst to determine suitable countermeasures against an attack. Consequently, NICTER provides not only statistical results of network security monitoring but also reports of analytic results of an incident including cause and countermeasure. These reports are published timely for government organizations, companies and users to manage their risks more effectively.

NICTER further deals with results from macro and micro analysis engines automatically to evaluate their correlation. As the results of the evaluation, NICTER shows events that are likely to be network security incidents as a task list to a network security analyst. The network security analyst thoroughly investigates each event on the task list, assesses criticality of the event, and creates an incident report. An incident handling system, which is part of NICTER supports these procedures with integrated graphical user interface (GUI) framework. Figure 2 depicts a view of the NICTER operation center.

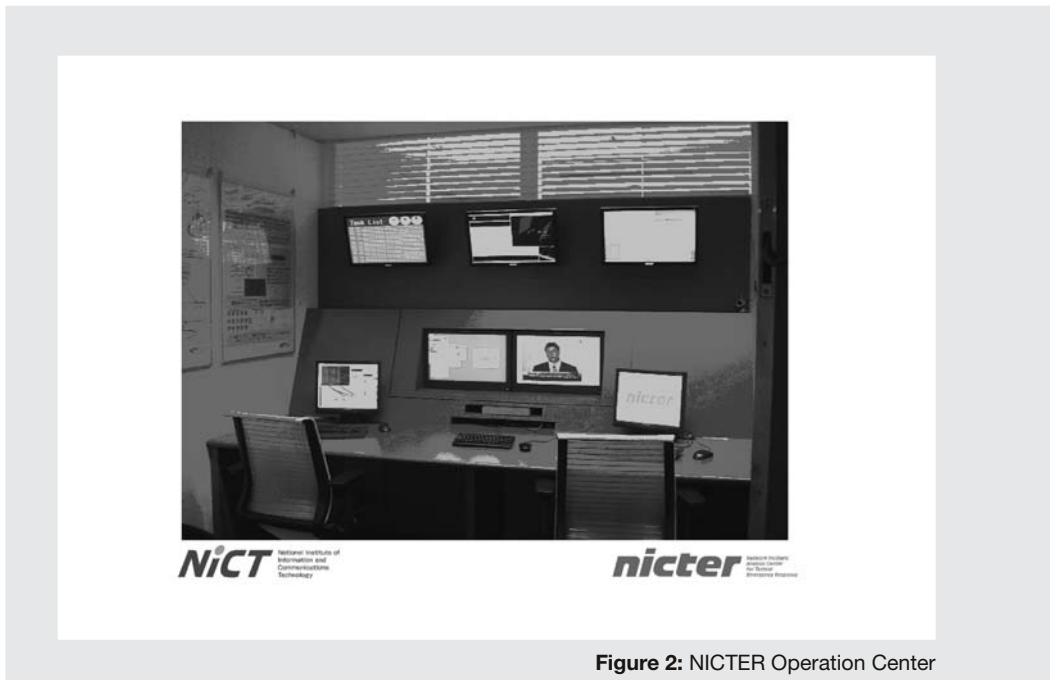


Figure 2: NICTER Operation Center

## 2. Trace-back Technology

As deterrent measures against cyber crimes, it is recognized in Japan that the trace-back technology is an important countermeasure. From 2005, the joint project was established and started to effectively deploy the trace-back system in the Japanese internet environment. The diagrammatic view of the project is shown in Figure 3.

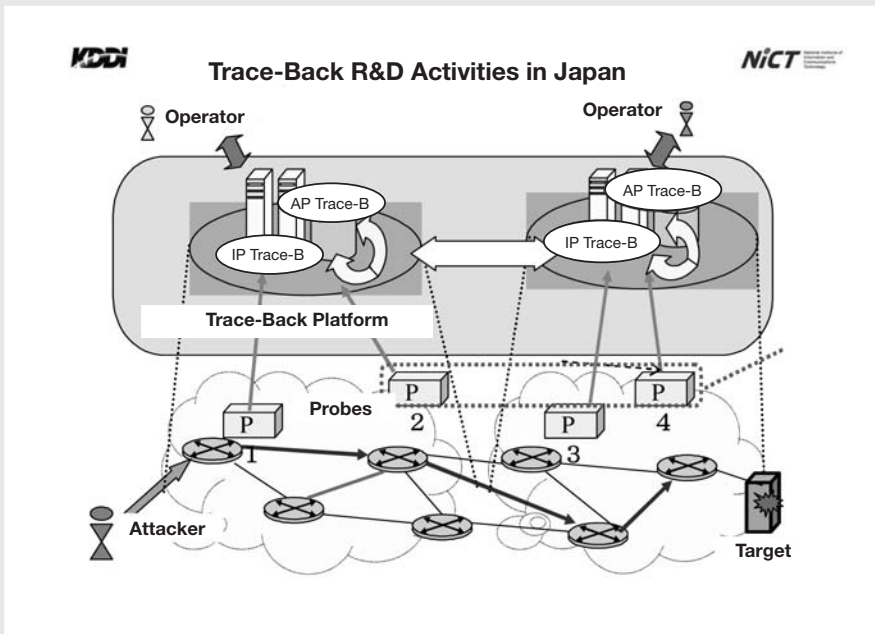


Figure 3: Overview of the Trace-back Project in Japan

### 3. Conclusion

In Japan, network security R&D is recognized as a significant activity to address the current and future network security issues and challenges. Further information regarding the progress and achievements of these projects will be shared at the next and future RAISS Forum meetings.

Note: The biography of the author is available at the end of the paper 'Japan's Status Update' on page 35.



## Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA CHINESE TAIPEI JAPAN MALAYSIA NEW ZEALAND SINGAPORE SOUTH KOREA THAILAND



# PROJECTS DISCUSSION

## 1. Introduction

This is a follow-up from the projects discussion at the 3rd meeting. Discussions were carried out in two concurrent tracks. Track 1 was facilitated by Mr Kin-Chong Chan and track 2 by Mr Tim-Meng Ching, both from the Singapore's Security and Privacy Standards Technical Committee.

## 2. Track 1 Discussion

The projects discussed in track 1 were:

- Risk Assessment Guideline for Systems and Network Administrators; and
- Guideline for the Implementation of Business Continuity Management (new work item).

### 2.1 Risk Assessment Guideline for Systems and Network Administrators

This project was proposed by Thailand [1] and discussed at the 3rd RAISS Forum meeting in Kuala Lumpur, Malaysia. The original proposal was to modify two courses targeted at managers, auditors, and middle-to-higher management to include technical components so that they could be leveraged for training network and systems administrators.

At the Kuala Lumpur meeting, it was agreed to change the proposal to develop a guideline and methodology for risk assessment that are applicable and useful for network and systems administrators. This methodology could later be incorporated into training courses to be carried out by training and education specialists, which would address the objective of the original proposal.

Subsequently, Thailand developed the first draft of the guideline and circulated it to the Forum members for comment in March 2006. The draft guideline specifies 22 processes and the corresponding controls around these processes. The processes and controls were adapted from the controls in ISO/IEC 17799 that are relevant to network and systems administrators and extended to cover many of the controls in greater detail. These processes and controls were presented and discussed at the April 2006 meeting in Jeju.

All participants agreed to review the draft document and provide comment by July/August so that a revised document can be prepared for further discussion at the 5th RAISS Forum meeting.

## 2.2 Guideline for the Implementation of Business Continuity Management

This is a new work item proposed by Malaysia [2] after the 3rd RAISS Forum meeting in Kuala Lumpur. Its purpose is to develop a guideline for the implementation of business continuity management (BCM) which would help organisations implement BCM.

This guideline would take into consideration existing standards, guidelines and other related documents, such as ISO/IEC 27001, NFPA 1600 (US), PAS 56 (UK), HB221 (Australia/New Zealand), BASEL II (Switzerland) and TR 19:2005 (Singapore). This guideline could subsequently be used, in the longer term, as a basis to develop a specification for self-assessment or certification.

Malaysia has volunteered to be the project editor of this guideline and proposed to first develop a glossary that defines the terminology and sets the common language for BCM. The discussion group agreed that this glossary document would be based on the terminologies used in the above reference standards and guidelines.

The next step is to develop the guideline for BCM implementation in compliance with ISO/IEC 27001 and other related standards. This guideline can be developed at the same time that the glossary is being developed. As such, Malaysia will prepare the first drafts of the BCM glossary and implementation guideline to be circulated for comment in July/August 2006 before the 5th RAISS Forum meeting.

It was also suggested during the discussion to accelerate this project where possible, so as to propose this guideline to be further developed into an international standard under ISO.

## 3. Track 2 Discussion

The projects discussed in track 2 were:

- Security Standards Toolkit;
- Application Security Standard; and
- Mutual Recognition of IT Security Certification.

### 3.1 Security Standards Toolkit

At the 3rd RAISS Forum meeting, the idea of a Security Standard Toolkit was mooted to collate all regional standards bodies operating information, processes and best practices into a publication. At the beginning of year 2006, questionnaires were sent to all the members to gather information. At the 4th RAISS Forum meeting, a summary collection of the responses collected were distributed to all members.

So far, Chinese Taipei, Malaysia, Singapore, South Korea and Thailand had submitted their responses. Inputs from Australia and Japan have yet to be received. As such, one of the action items after the meeting is to solicit the inputs from Australia and Japan, and with that, a publication of the responses would be prepared for dissemination to all the members for their reference. Members were also encouraged to submit any write-up or papers that they think would be useful for incorporation into the publication.

A suggestion was to rename this toolkit into a reference guide as the term toolkit seems to give the impression of a software tool. As such, the renaming of this publication will be looked into after this meeting. A suggested title is 'Regional Security Standard Bodies Reference Guide'.

### 3.2 Application Security Standard

At the 3rd RAISS Forum meeting, the idea of creating an Application Security Standard was mooted, as the members agreed that the existence of such a standard will be useful in guiding developers and users on how to reduce the number of application vulnerabilities. An initial draft of the standard was circulated among the members for feedback during February 2006. Upon gathering some inputs, another draft of the standard was circulated to the members on the finalized structure of the standard.

The envisaged Application Security Standard would consist of the following sections:

- i) Part 1 - Security guidelines for application development;
- ii) Part 2 - Security guidelines for application implementation;
- iii) Part 3 - Security guidelines for application management; and
- iv) Part 4 - Security guidelines for application un-installation.

Feedback was solicited from the members and there was no objections on the proposed structure, but there was unanimous agreement that the details are very important to ensure that the standard is not too general in scope, and yet not too detailed that it becomes limiting in nature.

Although there was a suggestion on creating a standard for specific security platform (PDA, mobile phone, web), the current Application Security Standard would not focus on any specific platform or architecture. The reason is that good application development, implementation and management process are generally platform or architecture independent, and this standard should address the general principles and recommend the guidelines.

This standard does not attempt to create a new software development methodology, but instead supplements the existing software development methodologies in the areas of secure coding. If this standard could be successfully published, it could be used as a basis for the development of application security standard on specific platforms or architectures.

One of the participants from Malaysia queried about the difference of this standard and the Common Criteria standard. The response was that this standard is created for the purpose of developing secure applications without the need of spending large amount of money to certify an application. This would be particularly useful for small in-house developers that might not have the resource to spend on Common Criteria certification.

The next revised standard would be sent to all members for feedback. Members were encouraged to participate actively in contributing ideas and contents to this standard so that it could be used by all the members.

Thailand agreed to be the Co-Editor for this standard.

### **3.3 Mutual Recognition of IT Security Certification**

At the 3rd RAISS Forum meeting, the idea of a mutually recognizing IT security certification among the regional economies was mooted. The objective and benefit of having such mutual recognition scheme is that a company from Economy A that has obtained certain certification would not have to perform similar certification in Economy B, hence achieving cost saving for the company in providing services to, or setting up and running a business in Economy B.

Another perspective is that if both Economies A and B use similar IT security standards, a company operating in Economies A and B can just apply to have one IT security standard certification preformed in one of the Economies, and it can be mutually recognized by both countries, thus avoiding additional operating cost.

From the above two examples, it was suggested that the region could expand their cooperation such that all members can recognize each other's local IT security standards.

Generally, the participants felt that it is a good idea in principle, but the execution could be challenging. At the same time, the legal implication would have to be considered.

At the end of the discussion, it was suggested that as an action plan to move forward, all members would consult their national standards body and check what are the judging criteria that would determine if other members' IT security standards could be recognized.

South Korea volunteered to share their local ISMS standard for recognition by the RAISS Forum members. As such, RAISS Forum would make an assessment of South Korea's local ISMS standard and determine if it is feasible to be used as a trial to work out the mutual recognition process.

#### 4. References

- [1] 'Modified Risk Assessment using a New Logical Way of Thinking', Dr Banchong Harangsri, Dr Komain Pibulyarajana, Doungkamoi Suppotayakorn, Siriwan Apisiridej, Security Standard Research & Development, Thai Computer Emergency Response Team (ThaiCERT), National Electronics and Computer Technology Center (NECTEC), Thailand, 2005.
- [2] 'Project Discussion on Business Continuity/Disaster Recovery', Prabha Ramanathan, Malaysia, 2006.

Note: Track 1 discussion notes is contributed by Kin-Chong Chan and his biography is available at the end of the paper 'Updates from Singapore: Introduction to Biometric Technical Committee & Singapore Standard for Identification' on page 59.

## Mr Tim-Meng Ching

*Co-Chair, Information Security Management Working Group of the Security and Privacy Standards Technical Committee IT Standards Committee, Singapore*

*Regional Security Consultant, Asia Pacific Region  
Lucent Worldwide Services - Professional Services  
Lucent Technologies Singapore Pte Ltd*



Tim-Meng Ching is the Regional Security Consultant of the Lucent Worldwide Services, (Professional Services team), and performs security consulting roles in Asia Pacific and China, Australia and New Zealand. He works with Lucent's sales group, product group, customers and partners to provide practical solutions pertaining to information security issues.

Tim-Meng has nine years of extensive experience in the information security industry. He has performed numerous penetration tests, technical review of systems, network architecture review, information security training, policy review and technical risk management audit. The clients he worked for includes global financial institutions, government bodies, multinational companies, educational institutions and network service providers. Tim-Meng's technical expertise lies in penetration test, wireless and VoIP security, firewall and IDS tuning, network incident handling and analyzing security issues on new technologies.

Prior to joining Lucent, Tim-Meng was the Information Security Officer in a private Swiss Bank, where he was responsible for the management of information security matters for the Singapore and Hong Kong office. He had previously worked in consulting positions for both PricewaterhouseCoopers and KPMG, providing information security services to clients.

Tim-Meng is currently the Co-Chairperson of Information Security Management Working Group (Singapore representative body for ISO/IEC JTC 1/SC 27/WG 1) responsible for developing and reviewing network and application security standards. In the international arena, he is also involved in the ITU-T SG17 security standards discussion groups. He is a regular contributor for Singapore's security professional group, SIG<sup>2</sup>, by performing technical researches and delivering talks to the members. Tim-Meng has also delivered a diverse range of information security topics in several public seminars.

Tim-Meng received his Bachelor of Applied Science degree in Computer Engineering from Nanyang Technological University. He is also a Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA) and a qualified practicing BS 7799 Auditor.



## Regional Asia Information Security Standards Forum Proceedings

AUSTRALIA CHINESE TAIPEI JAPAN MALAYSIA NEW ZEALAND SINGAPORE SOUTH KOREA THAILAND



# APPENDIX

### **Meng-Chow Kang**

#### **1. Introduction**

Although ISO/IEC, ITU, and other international standards bodies have been in operation for many years, regional economies in Asia, except for a few developed nations like Australia, Japan, and Korea, have mainly been the adopters of international security standards. As many regional economies are also new in the security standards arena, and not in the main or core participants or contributors to the development of existing international security standards, they all face unique challenges in various aspects of adoption, and deployment.

Regional economies also face challenges in establishing security standards bodies, cultivating industry involvement and participation, and promulgating knowledge and use of international security standards within their economy, especially when there is limited local security expertise that is familiar with security standards, as well as standards development and deployment.

There are potential benefits or values that we could develop and share across the region, if regional economies begin to share their knowledge, expertise, and more importantly experiences in the area of international security standards adoption and deployment. Emerging economies and new security standards bodies could immediately benefit from the experiences, and eliminate wastages in terms of repeating mistakes and errors that other more matured bodies have gone through previously. Similarly, from a regional perspective, the aggregated learning and experiences could potentially be useful for identifying new directions and needs in security standards development in the international standards communities.

#### **2. Objectives**

The Regional Asia Information Security Standards (RAISS) Forum is therefore proposed to reap the potential benefits and values through regional security standards bodies' participation and collaborations.

The Forum is to act as an overall focal point for the Asian standardization community on information security issues by:

- Providing a platform for sharing of knowledge, exchange of ideas and dialogues on standards related issues, challenges, and directions, in particular, relating to the adoption, deployment, and implementation of ICT related standards in the region;
- Ensuring that the security-related standardization activities in Asia adequately reflect the requirements of the market constituents at a strategic level;
- Providing a mechanism that could be used to follow-up on Asia policy requirements on Information Security standards issues;
- Providing effective co-ordination between organizations of relevant standardization work programmes and their execution;
- Ensuring Asia requirements for standards and standards work in this area are correctly interfaced with international standards activity, and standards activity in other regions, to avoid conflict or duplication of effort; and
- Acting as a strategic communication interface between relevant standards authorities and agencies on international standardization related topics.

### **3. Initial Tasks**

Initially, the RAISS Forum shall:

- Organize workshops & seminars for knowledge sharing and exchange of experiences and information relating to the adoption, deployment, and implementation of standards and promulgation of standards activities in the region;
- Establish liaison with the appropriate standards bodies or authorities/agencies interested in promoting or adopting international standards;

- Consider the implementation aspects of Information Security standards to Asia countries and other relevant Asia policy institutions;
- Consider appropriate proposals to improve Asia countries usage of international information security standards;
- Provide a common view where possible related to information security international standards;
- Create a mailing list for the members to share experience and knowledge in information security standards; and
- Establish a homepage/website for the Forum where reports and recommendations are published.

#### **4. Membership**

The RAISS Forum shall be open to any Asian National Standards bodies/committees/ organizations and their relevant technical groups, and to additional interested parties as specified below.

The Forum shall invite participation of stakeholder interests, including individuals representing:

- Hardware and software manufacturers/vendors;
- Information society service providers;
- Telecommunication service providers;
- Regulatory authorities in Asia;
- Research centres; and
- Academia.

**5. Liaison Activities**

The Forum may appoint electronic or physical liaisons.

**6. Working Methods**

- The initial Chair and possibly a Co-Chair will be nominated by the founding members of the Forum. Further refinement of this Terms of Reference shall consider the period of service for the various appointments in the Forum, and future method of nomination. The current Co-Chairs for the RAISS Forum are Mr Meng-Chow Kang of Singapore, and Mr Koji Nakao of Japan.
- The Secretariat shall be provided by voluntary members of the RAISS Forum, either as a permanent appointment, or follows the terms of appointment of the Chair of the Forum. The current Secretariat is Ms Yean-Lan Thay of IT Standards Committee, Singapore.
- The Forum will work on a voluntary basis.
- Physical meetings may be held as required, but full electronic working facilities shall also be arranged.
- The Forum shall work by consensus; its approved outputs should document any minority views.
- The Forum should focus on adoption of existing international standards.
- The Forum may organize open meetings or seminars on specific topics.
- The Forum role is advisory; its recommendations shall not be binding on the participating organizations.
- The Forum members are encouraged to participate in relevant international and global standardization efforts.
- The Forum shall provide a report on its activities.

## 7. Conclusion

The terms of reference detailed in this paper are essentially a framework to guide the collaboration, coordination, and execution of activities to bring the RAISS Forum forward, and ensure that the underlying objectives of the Forum could be successfully achieved. It is important that participants and members of RAISS Forum continue to maintain and update this guide to ensure its relevance and adequacy to meet the changing demands of IT security standardization, as well as the evolving needs of the Forum as it matures. It would be a failure of the Forum if these terms become the showstoppers to execution and running of the Forum. Ultimately, the knowledge and experiences shared, and open dialogues in the Forum meetings are the key deliverables that would benefit contributing and participating members.

Participation by the various economies in Asia in the initial meeting held on 22 April 2004 in Singapore and the inauguration meeting held on 19 November 2004 in Tokyo, Japan, have both shown the region's recognition of the needs for such a Forum. These needs have been further confirmed at the Panel Discussion session held in Tokyo, which identified future works required for moving forward with the objectives of the RAISS Forum.

## 8. Acknowledgement

This paper was developed in conjunction with the contributions provided by Mr Ariffuddin Aizuddin of National ICT Security and Emergency Response (NISER), Malaysia. I would like to express my deepest appreciation to Mr Aizuddin for his support and contributions to make the RAISS Forum possible. Also thanks to the online members of RAISS Forum Online<sup>1</sup> who have also previously provided feedback to the earlier draft of the terms of reference, in particular, Mr John Snare of Australia, and Prof Jussipekka Leiwo of Singapore.

<sup>1</sup> The online discussion group was set up in MSN Group web site (<http://groups.msn.com/RAISSForum>) as an online forum for ongoing dialogues for coordination of RAISS Forum related activities, as well as continuous discussion on topics relating to security standardization in the region. At the moment, membership to this online group is on invitation only.