Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

07-Dec-2005

English - Or. English

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

DSTI/ICCP/REG(2005)13
Unclassified

## Working Party on Information Security and Privacy

# APEC-OECD WORKSHOP ON SECURITY OF INFORMATION SYSTEMS AND NETWORKS: SUMMARY

**Korea, 5-6 September, 2005**

Contact: Anne Carblanc; Tel: 33-1 45 24 93 34

JT00195652



English - Or. English

**APEC-OECD WORKSHOP ON SECURITY OF INFORMATION SYSTEMS AND NETWORKS**
**Held in Seoul, Korea, on 5-6 September 2005**

## Summary

1. APEC and the OECD held a joint workshop on security of information systems and networks on 5-6 September 2005 in Seoul, Korea, in conjunction with the 32nd APEC TEL meeting. The objectives of the joint workshop were to:

- Exchange policy relevant information on strategies in OECD and APEC for developing a culture of security in the digital economy and information society.
- Share experience on effective initiatives for implementing security policies, practices, measures and procedures.
- Identify and prioritise future OECD and APEC co-operation initiatives to continue addressing security issues. Outline the mechanisms for such co-operation in the mid- and longer-term.

2. The workshop drew some 120 participants from APEC and OECD economies, including policymakers and representatives from business and civil society communities.

### Opening Session

3. **Dr. Inuk Chung**, Chair of the APEC TEL Working Group, welcomed the participants to the workshop. He gave a brief overview of the history and work items of the APEC TEL e-security task group (eSTG). He stressed that APEC and OECD shared common goals, and that the OECD Guidelines for the security of information systems and networks had been incorporated in APEC's work. Outreach was a priority for APEC TEL work in the coming years, and would be a subject of discussion at the upcoming eSTG meeting.

4. **Jung-Hyup Kang**, Director General for Information Infrastructure and Security, Ministry of Information and Communication, Korea, welcomed the participants on behalf of the Korean Government. He underlined the growing importance of security of information systems and networks, as most economic and social activities today relied on the Internet. Security was a global issue, and a collaborative effort was needed for finding solutions together, although both APEC and the OECD had already made valuable progress in the area of security of information systems and networks. Korea remained committed to play a part in the fight against online cyber threats.

### Keynote presentations

5. **Nobuo Tanaka**, Director for Science, Technology and Industry at the OECD, underlined that trust and security were among the key challenges to promoting information and communication technology and economic growth. Information and communication technologies had played a pivotal role in economic growth and productivity. He outlined examples of the contribution of ICT-using services to productivity in selected OECD countries. While ICT and e-commerce continued to spread, and access by households and

individuals had steadily increased between 2001 and 2004, real business use was still comparably low. Among other things, demand had been held back by a lack of security and trust. Fostering trust and security was among the six OECD priorities for international co-operation in ICT areas.

6. To try to estimate the size of the problem in the field of trust and security, ongoing OECD work on "Indicators for Trust" aimed at measuring the importance of trust on line, to evaluate the impact of OECD policy in this area, and guide further action. An OECD report to be declassified in the coming weeks reviewed available official and private/semi-official statistical resources on ICT and Trust.

7. Security and trust had been a constant strategic priority on the agenda of the OECD since the OECD Turku Conference in 1997. After 9/11, the OECD adopted the "2002 Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security". The Security Guidelines had had an impact at the regional and global levels, as well as at the national level in OECD member countries. The OECD promoted the exchange of best practices and dialogue between governments and with business and civil society, and had, among other things, issued two reports on the implementation of the Guidelines in member countries (in 2003, and 2005 – the latter to be declassified in the coming weeks).

8. Among the main themes that had emerged from these reports, international co-operation had been identified as a key component and was pursued in various regional fora. Global co-operation was indeed essential for realising a truly global culture of security for information systems and networks, as the systems and networks to be secured were global by nature.

9. **Hong-Sub Lee**, President of the Korea Information Security Agency (KISA) remarked that information security was the greatest challenge to be faced before the potential of the information society in the 21st century would be realized. Unless the Internet was safe, economic prosperity, quality of life, safety and security could not be guaranteed. While Korea was leading in terms of growth in IT infrastructure and applications, it was also among the very first faced with the challenges of managing increasing numbers of reported Internet security incidents. Mr. Lee gave an overview of response and prevention efforts in Korea conducted by the Korea Internet Security Center (KISC) responsible for the network security of the private sector. A video shown to the participants in the workshop outlined KISC's respective activities.

10. In APEC TEL, the work of the e-Security Task Group (eSTG) was covering the promotion of e-commerce as well as cyber crime, network security, and the protection of critical infrastructures. Currently, APEC TEL was working on a strategy to ensure a trusted, secure and sustainable online environment, building on APEC's earlier work.

11. APEC TEL also had carried out different projects to make the global network environment safer, including an effort to provide best practices and guidelines against spam, and for secure international e-commerce transactions. Furthermore, APEC TEL was also working towards strengthening cyber response capabilities of its members by providing a CERT training program. In December 2004, a security incident handling drill had been held between Korea, Japan and China – the first joint security incident response drill at an international level. A second international security incident drill would be held in December 2005 and more APEC member economies were expected to participate.

12. The APEC-OECD joint workshop presented a good opportunity to share knowledge and experiences on steps required to secure the global network.

**APEC and OECD strategies for security**

13. **Keith Besgrove**, Vice-Chair of the Working Party on Information Security and Privacy (WPISP) of the OECD started his presentation on OECD strategies for cyber security referring to the "commons", tracts of community owned land in England. The boundaries of this land were known, and security was based on mutual trust. Other types of commons included the 'high seas' which had been considered a commons to support international trade routes and fishing. To protect it, governments had developed International Conventions on the Law of the Sea. Air space was another commons, which had become increasingly regulated to facilitate air travel. The Internet could be seen as the "new commons" – and like the English Commons, the High Seas, and international airspace, no one owned the Internet. However, like the commons before it the Internet had attracted abusers: Cyber-crime and cyber-terrorism were very real threats, and there was a clear emerging need for rules of behaviour in this new commons.

14. The objective of the 2002 OECD Security Guidelines was to guide the development of consistent national policies to help address security threats and vulnerabilities in a global interconnected society, while preserving important societal values such as privacy and individual freedom. The guidelines were aimed at developing a "Culture of Security" across society, so that security became an integral part of the way individuals, businesses, and governments used ICT and conducted online activities. Mr. Besgrove gave a brief overview of the nine principles of the Guidelines, and described the results from a 2005 OECD survey on the current state of the implementation of the Guidelines in OECD member countries, and the main areas identified for further progress.

15. He underlined that in securing information systems and networks, international co-operation beyond regional boundaries was crucial, and that exchanges such as this workshop were needed to lead to the global collaboration required to protect the Internet as an important resource.

16. **Shamsul Jafni Shafie**, Head of the Information and Network Security Department in the Monitoring and Enforcement Division of the Malaysian Communications and Multimedia Commission, gave an overview of the APEC strategies for security of information systems and networks.

17. APEC's main strategy documents in the area of cyber security were the APEC Cyber security Strategy (2002), and the LIMA Declaration, which would be presented at the next Economic Leaders' Meeting in Busan (Korea) in November 2005.

18. The APEC Cyber security Strategy was focused on the global use of networks for common communications, and identified six areas for APEC economies to focus on: *i*) Legal, *ii*) Information Sharing, *iii*) Development of security and technical guidelines, *iv*) Public awareness, *v*) Development of human resources, and *vi*) Wireless technologies.

19. The LIMA Declaration recognised the importance of ensuring the security and integrity of the APEC region's communications infrastructure, in particular the Internet, in order to bolster the trust and confidence of users and enable the continued advancement of this infrastructure. He said he would also encourage all economies to study the CoE Convention on Cyber crime (2001), and endeavour to enact a comprehensive set of laws relating to cyber security and cyber crime consistent with international legal instruments, including the United Nations General Assembly Resolution 55/63 (2000) and the CoE Convention on Cyber crime.

20. The programme of action adopted by APEC TEL included continuing work to develop a strategy to promote a trustworthy, secure and sustainable online environment. It would also aim at strengthening effective response capabilities among APEC economies. APEC economies would further their efforts to combat cyber crime, including malicious activities that attack the network infrastructure and misuse of that

infrastructure; and to promote capacity building to counter the threat of cyber crime. APEC TEL would develop a set of guidelines to protect against attacks on the electronic information systems of essential infrastructure and services.

**Plenary Session 1: Key Challenges**

21. **Prof. William Caelli** from the Queensland University of Technology in Australia reported on trends and challenges in security of information systems and networks. He stated that one of the main themes in 2005 was the reaction of governments regarding the situation of market failure with regard to information security. As reported recently in the New York Times, the uptake of e-business seemed to be going down because of fear of security risks. This development was to be welcomed, as it might finally provoke reactions from industry that may not happen otherwise. This phenomenon of "market failure" was a consequence of "laissez-faire" public policy, absence of regulation of the ICT industry and low demand for security features from ICT purchasers.

22. While widely used microprocessor technology had been designed with basic security in mind, these basic features were not used in commodity operating systems or middleware products. Instead, simplistic structures had been invoked, associated with high security risks. As a result, the personal computer and the server systems based around it, were not suitable for safe and secure business transactions or e-government usage without substantial security enhancements, including add-in hardware components.

23. The main threats came from limitations in basic and widespread ICT computer systems, the base, also, and from the data communications infrastructure itself, for example router operating systems. Some of these problems would for example be addressed in Microsoft's "Palladium/NGSCB" project that effectively isolated security relevant processes to a specific sub-operating system. However, this structure would only be available two years from now or later – and even then current installations would not be able to take advantage of it.

24. It was also decisive to make existing security standards such as the "Common Criteria" better and more industry relevant, and to enforce government purchasing policy for security evaluated systems to create the necessary lead. Further activities would be needed to make the Common Criteria applicable in the SME environment. As of today, the Common Criteria had to be regarded as a failure with respect to technology for everyday use.

25. Referring to the widespread attitude of manufacturers and service providers to blame the inability of users to take the necessary steps to secure their systems, Prof. Caelli underlined that it was time to stop blaming users, and start to blame vendors. Security instructions often were just too demanding and complicated for users, especially those not having a technical background, to be able or expected to follow them. He outlined a number of further challenges for the development of security of information systems and networks posed in the areas of research and development, as well as in education, training and certification of IT security professionals. Security in mobile devices, and more generally, security of "embedded devices" (including household items, once these would be connected to networks), would develop as an important further issue. International security standards were also needed in this field. Hardening existing operating systems was another important step to take.

26. **Ms. Nor'Azuwa Muhamad Pahri**, consultant at the Mimos Consulting Group, Malaysia, gave a presentation on the protection of essential infrastructures and services. Cyber security was vital for the continuity of critical infrastructure services and ensuring business continuity. Eventually, a failure of these critical infrastructures would affect the economy, and even defence. The different critical infrastructures were increasingly interdependent.

27. Thinking of cyber attacks as the disease, protection measures would resemble medicine. As with health, prevention should also in the cyber sector be preferred to cures after the event. Cyber security challenges included a lack of security awareness, knowledge and skills, a lack of understanding of research and development requirements (including the definition of objectives, identification of key areas, and prioritisation), and reluctance to share security incident information. Components for fostering cyber security could be identified and grouped into different categories. Awareness would for example be a prerequisite for using security best practices and efficient technologies. Education could contribute to providing competent knowledge and skills to handle and respond to cyber attacks.

28. Ms. Pahri outlined examples for available technological solutions, including authentication, cryptography, access control, system integrity, audit, and monitoring security audit tools. Minimum security requirements and security controls needed to be deployed and a process to be put in place to validate the security level of products and services before the procurement. Co-operation with R&D institutions to address existing cyber security threats would be an additional component, as well as using existing security standards, for example ISO 17799, and ISO 15408. Regular security audits should be conducted within and across the sectors.

29. Ms. Pahri stressed that measures for cyber security of critical infrastructures must include technology, people, processes and policy components. She recommended that the APEC TEL Cyber Security Strategy should focus on, but not be limited to, the development of cyber security policy and guidelines, promoting awareness and increasing the efficiency of security training, co-ordinating information sharing and security incident response processes and co-operation among CERT at an international level, and interaction between the public and private sectors.

**Plenary Session 2: Spyware**

30. **Richard W. Downing**, Senior Counsel in the Computer Crime and Intellectual Property Section at the US Department of Justice, reported on the results from the APEC e-Security Task Group (eSTG) Questionnaire on Spyware. With respect to identifying the attributes of spyware, it was very clear from the responses that there was no single accepted definition of spyware. Most definitions included some mix of the following factors: *i)* software installed without the knowledge and consent of the user, *ii)* software that secretly gathers information stored on or sent through the computer, *iii)* software that secretly sends information back to an outside person, and *iv)* software that interferes with the computer's functioning (such as by displaying ads or resetting "home pages"). Some respondents had supplied examples, such as key loggers, data harvesters, navigation hijackers, tracking cookies, remote control tools, or Internet dialers. An important point was how to define spyware so as to include the harmful or annoying aspects, and avoid legitimate or beneficial software (for example, the downloading of patches without prior consent should be excluded from the definition).

31. As regards the scope of the problem, respondents had reported varying perceptions of "level of threat". While most saw spyware as a growing problem, it had been difficult to collect specific data on the incidence of spyware.

32. Only some respondents advocated new laws and regulations. Worries included difficulties in defining spyware, and the desirability of creating a unified policy on spam, phishing, malicious code in addition to spyware. It was pointed out that much spyware came from other economies, and that there was a need for a global response. Some respondents pointed out that the Convention on Cybercrime (2001) already contained provisions that addressed some types of spyware.

33. All respondents suggested that international co-ordination of work would help to address the problem, and also avoid the duplication of efforts. International organisations could help to define the

problem, assist in raising awareness, and provide a mechanism for discussion of governments' role in addressing the issue. International law enforcement co-operation mechanisms could be used to help address the problem.

34. **Seow Hiong Goh**, Director, Software Policy (Asia) with the Business Software Alliance (BSA) focused on the nature of spyware. He underlined that there was a fine line between spyware and adware. Intrusion channels for spyware included shipping with other applications. Spyware could also be installed through clicking on links or attachments in e-mail messages, via "chat" programs, or unknowingly downloaded from a Web site via exploits. It could also be carried as part of malicious code in viruses or worms. Adware was usually bundled and installed with "free" applications. These were for example made available on Web sites targeting young audiences (*e.g.* "smiley icons" offered for download), and installed through Web browser "drive-bys" or "trick pop-ups".

35. In combating cyber threats, it was important to target criminals, and not technology. Legitimate online services and future innovations should not be stifled. Sufficient funding and resources should be ensured for enforcement authorities, to keep pace with criminal counterparts. Penalties, including fines and imprisonment, should be increased to deter illegal activity, for example fraud, theft and extortion. To discourage future acts, the worst offenders needed to be punished.

36. Private sector solutions also played an important part in an effective overall spyware protection regime and defence against cyber threats. National policies should build upon and encourage the market-driven framework that was already in place, including technological tools.

37. **Andrew Maurer** from the Online Policy, Information Economy Division in the Department of Communications, Information Technology and the Arts in Australia, focused his presentation on policy issues faced by governments. He briefly described existing spyware technology, and its possible uses. That same technology however was also used for other – beneficial, legitimate and quasi-legitimate – purposes. Mr. Maurer gave an overview of the activities of the Australian Government with respect to spyware to date.

38. To develop a common understanding of the problem, clear and consistent definitions were needed. Possible counter strategies included information and education, industry partnerships, technology, legal responses, and international activity. Stratagems were needed for removing and preventing spyware, and the Australian Government had made available respective information on a Web site (www.nospyware.net.au), including fact sheets and a brochure.

39. With respect to appropriate technological responses, techniques useful against other e-security threats would also aid against spyware. It was important to take a proactive, rather than a reactive stance. Any legal responses needed to be targeted at behaviours and outcomes rather than at technology. Spyware aided to commit "old" crimes in a new environment, and thus case law and precedents were needed. Finally, international action also required a shared understanding of spyware, adware and malware. In law enforcement co-operation, it was important to follow the money trail, and continuously exchange knowledge and expertise.

40. **Kim Duffy**, CEO with Internet Security Systems (ISS), underlined that attacker knowledge and sophistication had grown with better attacking tools available. Today, one in every three companies had detected spyware on their network. More than 7 000 spyware programs were known to exist. Spyware could indeed undermine security, through searching and sending confidential information, deleting or modifying registry settings, key logging, disabling of (security) software applications, the installation of back doors, or taking control over peripherals. Spyware also had a cost, be it financial or in terms of resources, for example computer and network resources, or employee productivity.

41. With respect to countermeasures, prevention was always more efficient than reactive approaches. Periodic "search and destroy", typical of free spyware utilities, came too late for many, and relied on the diligence of users. Preventive measures could involve multilayered technologies, for example URL filtering (to prevent user access to known distributors of spyware applications), intrusion prevention (to prevent ActiveX installers and "phone home" communications), virus prevention (to prevent browser hijackers and key loggers), and application and communication control (to prevent "rogue" application installation and "phone home" communications).

42. **Aaron T. Hackworth** from the CERT Coordination Center at the Software Engineering Institute of the Carnegie Mellon University (Pittsburgh, PA) gave a brief description of common types of spyware, of its users and of data that could be collected though its use. Impacts included damaging consumer faith, but also reduction in productivity. He underlined that spyware was a financially driven industry. Among the key actions to be taken for long-term reduction of spyware were public education, building a strong legal and policy environment with consistent enforcement, international co-operation, and improved system architectures, that would in particular remove the value of exposed data, and not expose valuable data.

43. **Alice Hrdy** from the Division of Financial Practices Bureau of Consumer Protection in the Federal Trade Commission, United States, gave a presentation on activities to combat spyware in the United States. A report from a workshop held by the FTC in March 2005 recommended to industry to continue to develop and deploy improved technologies to combat spyware, and to develop industry standards for defining spyware and disclosing information. Key issues in defining spyware included whether the software was distributed with adequate notice and consent, and whether it caused real and serious harm to consumers. Industry should also expand consumer education efforts, and assist in law enforcement. Governments were recommended to increase prosecution under current laws. No new spyware-specific laws were recommended. Governments were recommended to increase prosecution under current laws. Ms. Hrdy outlined examples of recent enforcement activities undertaken by the Federal Trade Commission under these laws against providers of spyware. New proposed legislation would help US enforcement bodies to share investigatory information with enforcement bodies abroad. Governments also were recommended to encourage industry efforts, including technological solutions, and to increase consumer education efforts. Information on spyware was also part of the FTC's ongoing consumer education campaign on information security.

44. **Meng-Chow Kang**, Chief Security & Privacy Advisor for the Asia Pacific Region with the Microsoft Corporation, underlined that spyware was also a cost issue for software companies, as remarkable percentages of support queries they had to deal with were related to spyware problems. He described the functioning of spyware, and offered a classification of spyware based on the potential for harm to consumers. To address spyware challenges, it was important to empower users to make informed decisions of what software was installed and ran on their computers. In particular, prominent notice and opt-in was required for sharing personal information, for programs that display stand-alone ads, and for programs without complete uninstall or disable functionality. Prominent notice and opt-in or opt-out would be adequate for changes to the browser home or search page. Finally, easy user control of stand-alone ad programs should be provided, in particular the ability to stop future ads, as well as visibility into the source of ads.

45. **Kay Chuan Chua**, Government Relations Representative for Asia Pacific and Japan with the Symantec Corporation, reported on the prevalence of spyware and gave examples from different surveys. He underlined that the cost of spyware for end users, and companies would increase with the growing prevalence of spyware. Spyware was creating a crisis of confidence among consumers, as shown by recent surveys. A new comprehensive approach was needed for tackling the problem, and Mr. Chua outlined a risk impact model for evaluating computer applications which would help users to determine whether an

application should be removed from their computer, but the choice would ultimately be left to users. This model takes into account the impact of the computer application on a system performance, ease of its removal, risks it posed to privacy, its stealth nature and its prevalence. Legislation should be technology neutral, and provide exemption for security companies, from lawsuits by spyware/adware companies, and for the technology employed by security companies in protecting users. End-User License Agreements should be enhanced to give clear notice and choice to users regarding the installation of monitoring software on their systems, while allowing for users to be able to remove or uninstall such software easily and completely without damage to the computer or the information stored on it.

46. **Suresh Ramasubramanian**, Coordinator at the Asia Pacific Coalition Against Unsolicited Commercial Email (APCAUCE), reported on the relationship between spyware and spam. Both phenomena were not to be fully removed in the foreseeable future. Activities should therefore be focused on mitigation, rather than looking for ultimate solutions. He advocated a multi- stakeholder, multi-pronged approach addressing short-term goals, besides implementing long-term measures aimed at the mitigation and prevention of spam. At present, massive communication gaps between stakeholders were a major obstacle to co-ordinated action against spam and malware. Mr. Ramasubramanian outlined existing anti-spam initiatives in Asia and at the global level, including APCAUCE, the OECD Spam Task Force, and related activities in the context of WSIS. He advocated that some of these initiatives should merge their efforts, or work jointly, so that their joint skills could be harnessed. This would also widen the outreach of these efforts, as a larger constituency could be approached. Locally based organisations for co-operation, such as APECTEL and APCAUCE were well placed to play a co-ordinating and facilitating role in this process.

47. **Thomas Veit** from the Federal Office for Information Security, Germany, outlined technical and educational strategies for combating spyware. He suggested a definition of spyware that would include bots, Trojans and viruses, while excluding adware and system management software. He outlined trends in the evolution of malicious software. Recently, a change could be noticed from attacks on unspecific targets to specifically targeted actions against certain sectors, organisations, or systems. A comprehensive approach was necessary involving all responsible actors, including governments/organisations, vendors, service providers and citizens. For example, products should have built-in security by design, and should be pre-configured with the appropriate balance between security and functionality. Governments and organisations should implement a comprehensive security framework, and access providers could provide a “secure Internet access package” to their customers.

48. **Mikko Hypponen**, Chief Research Officer with the F-Secure Corp. in Finland, stressed that the attackers had in the last years evolved from kids and hobbyists to professionals and criminals. Many attacks today were aimed at making money, with professional teams of programmers behind them. In the past 19 years, around 140 000 viruses had been detected. He described examples of cases, including a hacker group that had managed to collect a vast number of usage data, with IP numbers, user names, passwords, and credit card numbers. Another attack had targeted customers of 2 700 different Web sites of financial organisations worldwide. Attacks increasingly had an international dimension, and involved parties from different countries requiring strengthened enforcement co-operation across borders. In the future, it was expected that threats and attacks would also spread into the mobile environment. In the past year, 71 instances of malicious code for mobile handsets had been discovered.

***Parallel Session 1 - Reaching out to SMEs and individuals.***

Moderator: **Michael Mudd**, Director of Public Policy for Asia - Pacific at The Computing Technology Industry Association (CompTIA)

49. This parallel session discussed the increased necessity for SMEs and individual users to focus on securing their systems, as a result of their expanding use and deployment of information systems and networks.

50. In the opening presentation **Jan Gessin** from the Asia Oceania Electronic Marketplace Association (AOEMA) underlined that many SMEs were still unaware that they were a possible target for attacks, and even convinced it could never happen to them because their businesses were too insignificant. In parallel, there was low awareness of the risk of assets loss, and even that their information system contained assets that were valuable for their business.

51. **Nick Ellsmore**, from SIFT Australia, focused on the phenomenon of "security fatigue", defined as "desensitisation and risk tolerance within a community or organisation leading to an increased risk exposure". Drivers included information overload, warnings without actualisation, over-shooting risk assessments, and information in the public domain inconsistent with the day to day experience of the community. The phenomenon could be observed in the health sector, as well as with regards to security in traffic. As security fatigue and doubt were propagating through an organisation's culture, it was key to ensure that new initiatives would be taken seriously. Cultural recognition of the importance of information security was necessary to avoid security fatigue. In addition, Mr. Ellsmore highlighted leadership in SMEs as important – founders/owners were to obey the good practice that they preach to their employees.

52. **Sophie Li-Hsuan Liang**, project manager at NII Enterprise Promotion Association (Chinese Taipei) described an information security management system practice in environments with limited resources in Chinese Taipei. The existing BS7799/CNS17800 standards had been redefined for SMEs, and applied in the context of schools. Chinese Taipei was also proposing a Government mandated security program for SMEs including certification as well as training for users, administrators, auditors and trainers.

53. **Sallie McDonald,** Special Assistant to the Assistant Secretary for Infrastructure Protection (USA), presented the US National Cyber Security Alliance (NCSA), a public private partnership including the US Federal Government, private sector companies, trade associations, and educational organisations. Its goal was to provide tools and resources, including a Web portal, to educate and empower home users, small businesses and schools, and colleges and universities with regard to security of their information systems and networks. A national cyber security awareness month was planned, including TV spots, cyber security workshops for small businesses, and a radio campaign on phishing.

54. **Peter Lübkert**, Head of Division, Information Technology and Network Services at the OECD, illustrated the complexity and challenges of establishing and keeping secure ICT environments in an international organisation. Operational security at the OECD followed the principles of the OECD guidelines and the ISO17799 standard. Proportionality and costs were important aspects. With the changing nature of the online environment and evolving threats, perimeter defence alone was not enough. Application security, access control and identity management mattered, as well as network and information transmission security, and end-user and device security. For security solutions, ease of use and simplicity were paramount – for example, too many security passwords might cause risks instead of mitigating them. Emerging technologies that might enhance security of ISN included self-healing systems and devices, and the use of behavioural analysis tools instead of traditional end-user security software.

***Parallel Session 2 - Promoting effective global incident response (the roles of governments and CERTs/CSIRTs)***

Moderator: **Arnold Yoon**, Korean CERT Coordination Center (KRCERT/CC)

55. This parallel session started with a presentation by **Yurie Ito** from JPCERT Coordination Center on the Asian Pacific Computer Emergency Response Team (APCERT), a coalition of at present 17 teams from 13 economies in the Asian-Pacific region. Incident handling among APCERT members had been changing in the last years, following changes in cyber security incidents its members were dealing with. Mr. Ito provided an overview of the practical procedures in APCERTs work. Based on the paradigm that the security of all participating organisations was interdependent, APCERT members formed a "web of trust", and the trust relationship among the participating CERTs had been developed based on long time operational collaboration, including regular face to face meetings between teams. Systematic handling of incidents following a repeatable procedure and an agreement on points of contact (including 24h hotlines and the use of encrypted communication) were highlighted as further key components for successful co-operation. Among other things, a practical incident handling exercise had been conducted in 2004 between China, Korea and Japan, and it was envisioned to expand such exercises to include all members. In the context of ASEAN, APCERT member provided CSIRT training for developing economies. Partners in cross-regional co-operation included the TF-CSIRT and FIRST.

56. **Jiao Xulu**, from the Chinese CNCERT/CC and **Jinhyun Cho** from KrCERT/CC focused on case studies of collaboration between different CERTs/CSIRTs across borders to tackle cyber incidents. Both speakers stressed the growing importance of co-operation and information sharing among CERTs/CSIRTs to mitigate the damage from cyber attacks, and namely for incident early warning.

57. **Vu Quoc Khanh** from the Vietnamese Ministry of Post and Telematics highlighted specific challenges faced in setting up national CERTs in developing economies. With restricted government budgets and small national IT markets, these CERTs had to be set up at a high professional level, but with minimal costs. Support from already established CERTs was crucial, for example through sharing of experience and provision of training.

58. During the discussion, a question was raised from the audience as to where CERTs/CSIRTs would be best located. The panellists shared the view that this would depend on the specific situation, and provided examples for the way their organisation was set up (ranging from being a fully independent organisation or an independent body with partial funding from the government, to being part of a ministry). One panellist suggested that the appropriate location may depend on the respective constituency, for example a CERT/CSIRT focusing on CIP may be best located inside the public administration.

59. Asked what international organisations could do to help CERTs/CSIRTs in fulfilling their tasks, one panellist underlined that international organisations could act as vehicles for presenting the issues linked to the operation of and co-operation among CERTs to political leaders.

***Parallel session 3 - Emerging security threats and the technologies being developed to address them: the Role of R&D***

Moderator: **Keith Besgrove**

60. **Jong Ki Yoo**, Consultant for IBM Business Resilience & Continuity Services provided an overview of facts and figures about the security of information systems and networks, and an assessment of the expected process of maturity of information security over time. He outlined security threats and their origins. While increased collaboration and new business models offered greater business rewards, they also posed greater business risks. Key security trends included the convergence of physical and logical security,

the adoption of federated Identity management, the evolution of real-time threat management systems, and a movement from disaster recovery to business continuity and resiliency. Enterprise-wide security programs were focusing on risk management and governance. Mr. Yoo concluded his presentation with a list of items to consider for minimizsng security risks.

61. **Dr. Kenji Rikitake** from the Security Advancement Group of the National Institute of Information and Communications Technology (NICT) in Japan described a network security incident analysis system for detecting large-scale Internet attacks, aimed at the collaborative monitoring and centralised analysis and handling of networks security incidents among Japanese Internet service providers, to protect the national IT infrastructure. Partners included Telecom-ISAC Japan, as well as members of the Internet security research community. The project included an analysis center for real-time monitoring and analysis, whose required functions were described in detail, as well as examples for analysis methods, and an example of an analysis of a DDoS attack. More expertise and research activity was still needed to better understand the relationship between data trends and actual incidents. While there was also a need for more information sources, legal requirements needed to be observed, including the privacy of network users. A first beta-version of the incident analysis center system was expected to be available by December 2005, full operation of the institution in 2007.

62. **Steven Furnell** from the Network Research Group at the University of Plymouth (United Kingdom) focused on fostering the usability of information security solutions. Security ought to be understandable, and users had to be able to determine and select the protection they required. The technology should also not make unrealistic assumptions about a user's prior knowledge. Furthermore, security needed to be visible, enabling users to find the desired functionality. Users ought to be able to determine whether protection was being applied and to what level. A recent survey among users had revealed a clear majority of respondents had difficulties in using security functions in widespread software products (browser and word processor software). At the same time, some functions had undesirable side effects, *e.g.* a browser set to a "high" security level would not be able to display commonly used web sites, without an indication that this was caused by the security settings chosen. Mr. Furnell outlined a number of guidelines for creating usable security functions and provided examples, including for interface improvement.

63. **Kevin J. Houle** from Carnegie Mellon University's CERT/CC described research and development for artefact analysis, *i.e.* the study of Internet attack tools and malicious code. He explained the roles of malicious code analysis in different contexts, such as incident response, and following attack technology trends, but also for law enforcement and forensics. Malicious code analysis, among other things, contributed to an accurate view of attack systems and evolving capabilities, and an accurate insight into assets targeted and resources used by attackers. However, tools were still immature, and there was a lack of formal training and sufficiently skilled experts. Information sharing also remained a challenge. With regard to goals for R&D, it was important to further reduce analysis time, but also to reduce the time between an attack and possible legal consequences. The focus of R&D needed to be expanded beyond the attack vectors of the day, and instead follow a long-term social approach, looking ahead 5-10 years. R&D investment should be focused on decreasing the value of assets criminals could access.

64. Finally, **Chi-Seng Yu** from the Information and Communication Security Technology Center in Chinese Taipei presented a case study on the discovery of a specific vulnerability unknown before, that allowed malicious software to be installed even in a fully patched environment. For the last two years, the institution had focused on collecting and analysing malicious MS-Office documents, which in many cases exploit well-known vulnerabilities to install spyware or backdoors, most of which were undetectable to antivirus software. The exploit of un-disclosed vulnerabilities added another dramatic magnitude of difficulties in handling zero-day attacks. A possible way forward could be the establishment of efficient and formal vulnerability handling channels between major software manufactures. In addition to educating

end users, more automatic and behaviour-based anti-malicious software tools were needed. Finally, software programmers and architects should be certified with respect to secure coding and design.

***Parallel Session 4 - Comparing legislative and policy approaches to identity management and to security of information systems and networks***

Moderator: **Shamsul Jafni Shafie**

65. **Andrew McEwen Mason** from the consulting firm BSA Ltd (New Zealand) described possible repercussions of trusted computing and digital rights management on the integrity of government-held information. He described the main features of the "trusted computing initiative", and underlined that this technology had a great potential to improve security in a number of areas, including safe storage of passwords, PINs and account numbers, the prevention of spoofing, and the reduction of threats posed by malware. The trusted computing technology might also serve as a platform for digital rights management (DRM) applications. Already today DRM features were integrated into widely-used software products.

66. The New Zealand Government had looked into possible consequences of the introduction of trusted computing and DRM for digital information in the realm of the public administration. There was concern about the integrity of government-held information and processes. Information available today about trusted computing and DRM indicated that the design had not sufficiently taken into account government's requirements in managing information. Main issues were ensuring governments' long-term access to its own information, and the possibility of information being communicated to external parties without explicit knowledge or permission. Among other things, a working group had been established to develop government-wide principles for the use of trusted computing technology, and engage in international consultation and co-operation. The group would also continue to share its work via channels such as the OECD. Up to now, governments internationally did not seem to have been active in evaluating the impact of trusted computing. Finally, the working group would continue its engagement with key ICT industry players to ensure that government requirements were adequately considered in the further development of trusted computing and DRM technology.

67. **Jamie Gillespie**, Senior Security Analyst at the Australian AUSCERT reported on identity theft response arrangements and processes at the operational level in Australia. He outlined the current scope of identity theft in Australia, where financial institutions and their customers formed the primary target. Attack methods included phishing and Trojan malware, and evidence suggested that the perpetrators primarily originated from foreign organised crime. He described the role of the Australian CERT in response to identity theft and mitigating other online threats, and the co-operative arrangements in place at the local and the international levels, in particular for shutting down Web sites used for illegal activities.

68. **Katarina de Brisis**, Senior Advisor at the Ministry of Modernisation, Department of National IT Policy in Norway, focused on identity management in the context of e-government as a potential driver for a culture of security. She outlined current e-government initiatives, and the legal framework and strategy in place for electronic identification enabling e-government in Norway. Among the goals of the "eNorway2009" national IT policy were common solutions for eID/eSignatures, Identity Management, secure electronic service delivery and electronic intergovernmental exchange of information. With regard to the use of PKI-based electronic IDs and -signatures, there was no interoperable infrastructure covering the whole of society available yet. An outline was given of the current usage of PKI in different sectors. The government in Norway is currently developing a common security portal, for securing communication between the government and the public, as well as businesses. The portal will integrate PKI offers in the Norwegian market and provide for seamless interoperability of them. The portal will also support identity management functions and enable single-sign-on to government services. Identity management, defined as a broad administrative area that deals with identifying individuals in a system (such as a country, a

network, or an enterprise) and controlling their access to resources within that system by associating user rights and restrictions with the established identity, was an important concept for e-government, as a prerequisite for the effective roll-out of new electronic services. Remaining challenges however included how to define identity in a "global" context, how to provide for unique identification of physical and legal persons, and how federation in a "global" environment could be achieved, as well as interoperability across heterogeneous IT-platforms.

69. **Takashi Ishitobi**, Assistant Director at the Office of IT Security Policy in the Ministry of Economy, Trade and Industry of Japan outlined the activities for establishing a framework for information security governance in the private sector in Japan. He underlined the need for information security to be recognised as a management task, and gave an overview of the Japanese government's activities to establish information security governance in the national private sector, including the introduction of information security measuring benchmarks, of information security reports and of guidelines for business continuity plans. Mr. Ishitobi also outlined the content of these instruments, which were to be used in the private sector on a voluntary basis.

***Plenary Session 3: Reports from the parallel sessions and panel discussion***

70. After a brief report by the moderators on the parallel sessions, the two co-chairs introduced a number of key issues and possible areas for future co-operation between APEC and OECD, which had emerged out of the discussions at the workshop.

71. The following summary also includes the results from the discussion between the panellists and with the audience:

Overarching objectives for future co-operation:

- Continue and intensify co-operation between OECD and APEC.
- Improve information sharing between the two organisations (*e.g.* regular reports on respective activities and linking respective Web sites).
- Increase awareness of policy makers about the importance of online security and trust to economic growth and more broadly to the information society, and
- Join efforts to conduct research and analysis and consolidate data with a view to better understanding the size of the problem and to guide policy makers.

Possible topics for co-operation could be:

**Research and analysis on evolving threats [and counter measures]**

72. The participants noted that both APEC and OECD members have a strong interest in being well informed about the nature of evolving information security threats and counter measures. Opportunities for collaboration in research and analysis that were mentioned included:

- Malware.
- Wireless [and mobile] security, and
- Information sharing and response (to help the stakeholders to be prepared with a focus on SMEs and individuals).

**Meeting the needs of SMEs and individuals**

73. Small enterprises and individuals are more exposed to security risks than the other participants. A consensus emerged during the workshop that while many actions are undertaken to sensitise them to those risks, few known initiatives help them implement tailored and easy-to-use solutions. In addition to continuing to educate/raise awareness of SMEs and individuals about security risks, it is essential to help devise methods for risk analysis and security solutions tailored to their needs.

**Indicators for trust**

74. Ongoing OECD work could be enriched by data on APEC economies.

**Mutual consideration/endorsement of policy and practical guidance on a case by case basis by the appropriate bodies of the respective organisations**

75. With respect to process, governments would collaborate with the private sector and R&D institutions as appropriate. The work would be led by an APEC or OECD member. Expert groups could be established (10 people maximum). Work would essentially be conducted online with face-to-face meetings where necessary.

**APEC-OECD WORKSHOP ON SECURITY OF INFORMATION SYSTEMS AND NETWORKS**
**5-6 SEPTEMBER 2005**
**SEOUL, KOREA**

**Final List of Participants**

**Ms. Suryahti ABDUL LATIFF**
Infocomm Development Authority Of Singapore - Singapore

**Mr. Muhammad Hanafiah ABDUL RASHID**
Infocomm Development Authority of Singapore - Singapore

**Ms. Nur Sulyna ABDULLAH**
Malaysian Communications and Multimedia Commission - Malaysia

**Mr. Michael BAKER**
AOEMA - Australia

**Mr. Laurent BERNAT**
OECD

**Mr. Keith BESGROVE**
Australian Department of Communications, Information Technology & the Arts - Australia

**Mr.s Jiraporn BHONGSATIERN**
National Telecommunications Commission - Thailand

**Ms. Louise BIGGS**
Australia

**Mr. Henk BRONK**
GOVCERT.NL - Netherlands

**Mr. Guolei CAI**
Ministry of Information Industry - People's Republic of China

**Mr.s Anne CARBLANC**
OECD

**Mr.s Christiane CHASLE**
Government of Canada, Industry Canada - Canada

**Mr.s Ru-Fen (Rhonda) CHEN**
National Information and Communication Security Taskforce - Chinese Taipei

**Ms. Vivian CHEN**
Chunghwa Telecom Int'l business group - Chinese Taipei

**Mr. Jinhyun CHO**
Korea Information Security Agency - Republic of Korea

**Mr. Kay Chuan CHUA**
Symantec Corporation

**Dr Inuk CHUNG**
KISDI (Korea Information Strategy Development Institute) - Republic of Korea

**Mr. Kyung-Ho CHUNG**
Korea Information Security Agency - Republic of Korea

**Mr. Shinnosuke DATE**
Fujitsu Limited as a GBDe Member - Japan

**Mr.s Katarina DE BRISIS**
Ministry of Modernization - Norway

**Mr. Edgar DE LANGE**
Ministry of Economic Affairs (DGTP) - Netherlands

**Ms. Anita DEY**
Federal Communications Commission - United States

**Mr. Kim DUFFY**
Internet Security Systems., Australasia - Australia

**Mr. Daniel DWYER**
CEPU - Australia

**Mr. Nick ELLSMORE**
SIFT Pty Ltd - Australia

**Ms. Jacqueline FAM**
Australian Communications & Media Authority - Australia

**Mr. MARIO FROMOW**
Secretaria de Comunicaciones y Transportes - Mexico

**Dr Steven FURNELL**
University of Plymouth – United Kingdom

**Ms. Janice GESSIN**
AOEMA

**Mr. James GILLESPIE**
AusCERT - Australia

**Mr. Seow Hiong GOH**
Business Software Alliance - Singapore

**Ms. Caroline GREENWAY**
Australia

**Mr. Aaron HACKWORTH**
CERT Coordination Center - United States

**Mr.s Elizabeth Jane HAMILTON**
Industry Canada - Canada

**Mr. Douglas HARTLEY**
Lotte Hotels Korea - Canada

**Mr. Hirosato HAYASHI**
Embassy of Japan in Seoul - Japan

**Ms. Ashley HEINEMAN**
National Telecommunications and Information Administration - United States

**Mr. Pablo HINOJOSA**
COFETEL - Mexico

**Mr.s ALLAN HORSLEY**
Australian Communications and Media Authority - Australia

**Mr. Kevin HOULE**
CERT Coordination Center - United States

**Mr.s Alice HRDY**
Federal Trade Commission - United States

**Mr. Hao HUANG**
China Academy of Telecommunications Research of MII (CATR) - People's Republic of China

**Mr. IAN HUTCHINGS**
Ministry of Economic Development - New Zealand

**Ms. Anna Amalina IMAM BAWEH**
Ministry of Energy, Water and Communications - Malaysia

**Mr. Takashi ISHITOBI**
Ministry of Economy, Trade and Industry - Japan

**Ms. Yurie ITO**
JPCERT/CC - Japan

**Ms. Xulu JIAO**
CNERT/CC - People's Republic of China

**Mr. Youm JONGSUN**
APEC e-Government Research Center - Japan

**Mr. Meng Chow KANG**
Microsoft Operation (S) Pte Ltd - Singapore

**Ms. Rosa KIM**
Korea Information Security Agency - Republic of Korea

**Ms. Soyoung KIM**
Korea Information Security Agency - Republic of Korea

**Ms. Beatrix KOZMA**
U.S. Department of Commerce - United States

**Mr. Axel KRAEMER**
Federal Ministry of the Interior - Germany

**Ms. Crystal LARM**
Industry Canada - Canada

**Ms. Eun-kyeong LEE**
Korea Information Strategy Development Institute (KISDI) - Republic of Korea

**Mr. Hong-Sub LEE**
Korea Information Security Agency - Republic of Korea

**Ms. Lihsuan LIANG**
NII Enterprise Promotion Association - Chinese Taipei

**Mr. Ziping LIU**
Ministry of Information Industry - People's Republic of China

**Mr. Eho-Cheng LO**
National Information Infrastructure Enterprise Promotion Association - Chinese Taipei

**Mr. San LOU**
Office for the Development of Telecommunications and Information Technology

**Mr. Peter LUBKERT**
OECD

**Mr. Andrew MASON**
BSA Limited - New Zealand

**Mr. Kazuyoshi MATSUMOTO**
NICT - Japan

**Mr. Andrew MAURER**
Australian Department of Communications, Information Technology & the Arts - Australia

**Ms. Sallie MCDONALD**
Department of Homeland Security - United States

**Ms. Rojarase MEKSIRIVILAI**
Ministry of Information and Communication Technology - Thailand

**Mr. Sven MOERS**
OECD

**Mr. Michael MUDD**
The Computing Technology Industry Association (CompTIA)

**Ms. Nor'Azuwa MUHAMAD PAHRI**
Mimos Berhad - Malaysia

**Mr. Masayuki NAKATANI**
JPCERT/CC - Japan

**Mr. Ernie NEWMAN**
International Telecom User Group - INTUG

**Ms. pulsiri NINKITSARANONT**
Office of the NTC - Thailand

**Mr. Seiji NINOMIYA**
MIC - Japan

**Prof Toshio OBI**
APEC e-Government Research Center - Japan

**Ms. Monica OCHOA**
APEC Secretariat - Singapore

**Mr. Colin OLIVER**
Department of Communications, Information Technology and the Arts - Australia

**Ms. Jiwon PAIK**
KISDI (Korea Information Strategy Development Institute) - Republic of Korea

**Dr Liu PEI-WEN**
Institute for Information Industry - Chinese Taipei

**Ms. Audrey PLONK**
Department of Homeland Security - United States

**Mr. Theodore POLITES**
The Colony Park Group - Australia

**Mr.s NGUYEN QUYNH ANH**
National institute of Posts and Telematics strategy - Viet Nam

**Mr. Kenji RIKITAKE**
NICT - Japan

**Dr Bo-Hyun SEO**
KISDI (Korea Information Strategy Development Institute) - Republic of Korea

**Mr. ShaMs.ul Jafni SHAFIE**
Malaysian Communications and Multimedia Commission - Malaysia

**Mr.s Elizabeth SHELTON**
U.S. Department of State - United States

**Mr. Kwok-Kei SIN**
OFTA - Hong Kong, China

**Mr.s Rosemary SINCLAIR**
INTUG - Australia

**Mr. Steven STROUD**
Attorney-General's Department - Australia

**Dr IDRIS F. SULAIMAN**
Indonesia Information Technology Federation (IITF) - Indonesia

**Mr. Heru SUTADI**
LPPMI - Indonesia

**Mr.s MARIE SVOBODOVA**
Ministry of Informatics – Czech Republic

**Mr. Fumitake TAKAHASHI**
Ministry of Internal Affairs and Communications - Japan

**Mr. Hiroki TAKASAN**
Global Business Dialogue on Electronic Commerce - GBDe - Japan

**Mr. Makoto TAKEMA**
Ministry of Internal Affairs and Communications - Japan

**Ms. Si Man TANG**
Macao Economic Service

**Ms. Rujira THAMMACHAT**
National Telecommunications Commission - Thailand

**Mr. Nguyen Minh THANG**
Ministry of Posts and Telematics - Viet Nam

**Mr. Richard THWAITES**
INTUG - Australia

**Ms. Jeanette TOM**
TIA - United States

**Mr. CUONG TRAN**
Ministry of Posts and Telematics - Viet Nam

**Mr. Shan-Hsin TSAO**
Chunghwa Telecom Training Institute - Chinese Taipei

**Dr CARLOS VALDEZ**
Ministerio de Transportes y Comunicaciones - Peru

**Mr. THOMAS VEIT**
BSI - Federal Office for Information Security - Germany

**Mr.s SUDAPORN VIMOLSETH**
TOT Public Company Limited - Thailand

**Mr. Alan VINCENT**
NTIA - United States

**Mr. Soon Jae WON**
Korea Information Security Agency - Republic of Korea

**Mr. Ming-Wei (Benson) WU**
National Information Communication Security Taskforce - Chinese Taipei

**Ms. Eva WU**
Institute for Information Industry - Chinese Taipei

**Mr. Kazuya YAMABE**
GBDe - Japan

**Ms. Anne YAU**
Ministry of Economic Development - New Zealand

**Dr Chiunn YEH**
NCHC - Chinese Taipei

**Ms. Hsiao-Feng YEH**
Chunghwa Telecom - Chinese Taipei

**Mr.s Eun Jae YOO**
Korea Information Security Agency - Republic of Korea

**Mr. Chungyoll YOO**
The Quebec Government in Korea - Canada

**Mr. Arnold YOON**
KrCERT/CC, KISA - Republic of Korea

**Mr. Chi-Sheng YOU**
Institute for Information Industry - Chinese Taipei

**Mr. Tanin YOUKHAW**
CAT Telecom Public Company Limited - Thailand

**Mr. Chun Chang YU**
Bureau of Foreign Trade - Chinese Taipei

**Mr. Siu-yee YUNG**
Office of the Telecommunications Authority - Hong Kong, China