The Hope for Today’s... IT Practitioners.

24 – 25 February 2003
9am – 5pm
Lecture Theatre 27
National University of Singapore

Guest-of-Honour:
Dr N Varaprasad
Deputy President, NUS
Security Conference Summit 2003
“The Hope for Today’s IT Practitioners” is

Jointly organized by:

Centre for Industrial Mathematics, NUS

Department of Mathematics, NUS

Co-hosted by:

Quantiq International Pte Ltd

In collaboration with:

Centre for System Security Research, NUS

Law Department, School of Business, SMU

Exhibitors:
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conference Programme</td>
<td>1</td>
</tr>
<tr>
<td>Speakers’ Abstracts &amp; Biodata</td>
<td>3</td>
</tr>
<tr>
<td>Science Faculty Map</td>
<td>18</td>
</tr>
<tr>
<td>Exhibition Floor Plan</td>
<td>19</td>
</tr>
</tbody>
</table>
MONDAY, 24 FEBRUARY 2003
“SECURITY - FINANCIAL & LEGAL PERSPECTIVES”

0845: Registration

0915: Opening Address
Dr N Varaprasad, Deputy President, NUS

Session Chair: Harald Niederreiter

0930: Security Beyond Lean
Chien Siang Yu, IT Director, Ministry of Home Affairs

1015: Break

1030: 3D Secure Architecture for Credit Cards
Eric Trotter, Director, Emerging Technology Risk Management, VISA International Pte Ltd

1115: MasterCard SecureCode
T. V. Seshadri, Head of Technology & Operations, South East Asia, MasterCard International

1200: Lunch

Session Chair: Chien Siang Yu

1330: Technology Risks & Security in eBanking and ePayment Systems
Tony Chew, Director, Technology Risk Supervision, Monetary Authority of Singapore

1415: Singapore’s Legal Infrastructure for E-Security
Harry S K Tan, Director, Centre for Asia Pacific Technology Law & Policy (CAPTEL), NTU

1500: Break

1515: Transnational Issues in Cybercrime
Daniel Seng, Faculty of Law, NUS & Director of Research, Technology Law Development Group, Singapore Academy of Law

1600: Legal Issues in Electronic Surveillance and E-Privacy
Mary Wong, Department of Law, School of Business, SMU

1645: Panel discussion
Chair: Harald Niederreiter, NUS

1700: End of day
TUESDAY, 25 FEBRUARY 2003
“DIGITAL WARFARE, THREATS AND COUNTERMEASURES”

0845: Registration

Session Chair: Roger Tan C E
0930: Security Standards, Evaluation Criteria and Security Assurance
Chi-Hung Chi, Director, Centre for Systems Security Research, NUS
1015: Break
1030: Hacking Demonstration - War-Driving, War-Dialing, Hacking into WLAN
S C Leung, Chairman, Professional Information Security Association
1115: Clues, Vandalism, Litter Sendmail Trojan Mail
Paul Henry, Vice President, Worldwide Operations, CyberGuard Corporation
1200: Lunch

Session Chair: Tony Chew
1330: Understanding the Intrusion Management Timeline
Andre Yee, Vice President, Engineering, Network Flight Recorder Security
1415: Avoiding Soft Security - Using hardware to protect authentication, encryption and digital signatures
Nicko van Someren, Chief Technology Officer, nCipher
1500: Break
1515: Network Availability, Optimisation and Security
Roy Zisapel, Chief Executive Officer, RADWARE
1600: Panel discussion
Chair: Harald Niederreiter, NUS
1615: End of day
Security Beyond Lean  
Chien Siang Yu  
IT Director  
Ministry of Home Affairs

ABSTRACT OF TALK
The speech will examine how the future knowledge-based economy would evolve to demand security in a fundamental and highly optimised way. In recent years, our dependency with regards to the wired world has not diminished but in fact has been accelerating, despite the recession. The prospect of a surprise outage affecting the Internet and hence, national IT infrastructure is no longer be a faint possibility.

Consequently, a whole host of security challenges have been thrown forth and we would need to urgently and efficiently craft the right strategies to cope with them. In addition, we have to get back to basics and align ourselves to international developments and recent IT Security advances. Although there might be no easy answer, the right step forward would be to make security easy to deploy like a low cost commodity and take all available security technologies to new heights when it comes to flexibility and ductility. In any case, we can no longer afford to keep security efforts on the lean.

ABOUT THE SPEAKER
Mr Yu was trained at Siemens Research Laboratory and IBM R&D Laboratory in Boblingen, Germany. He was actively involved in IT management and the IT security industry for over 20 years. As EDP with the Ministry of Defence from 1982 to 1986, he introduced IDM STAIRS, the freetext system and invented numerous security systems, e.g. diskless workstations. He also started an IBM mainframe group and managed its operations.

During this period, he developed the first HP terminal emulation PC software running on a NEC PC, the first high quality electric typewriter driven word processor and wrote disassemblers. Besides, he also founded the MS DOS Special Interest Group.

After he transferred to the Ministry of Home Affairs in 1986, Mr Yu started the Special Projects Team, which is in charge of classified work. He also developed the first of its kind embedded system technology that allows realtime systems to be implemented in a high level programming language instead of assembler.

Meanwhile, Mr Yu was also the computer security consultant to numerous national level projects such as the Cashcard project, the Electronic Road Pricing project and so on. He was also the lead technical investigator for the government enquiry into the nation-wide telecommunications exchange blackout at the Singapore Telecoms.

Over the years, Mr Yu led the team that developed the first secure email system in Singapore, Singapore’s first PC security system and pioneered the implementation of public key systems for the Singapore government. He also invented the smart card readers, cryptography systems and more efficient protocols throughout the years. For all his works, Mr Yu was awarded the Silver Medal for Public Administration.

Mr Yu is also a speaker for numerous government events on IT Security, Knowledge Management and Project Management, e.g. IDA Security Day, Keynote for Governmentware programmes, NUS IT Security events and so on. He is also a prolific writer for local IT magazines.
3D Secure Architecture for Credit Cards

Eric Trotter
Director, Emerging Technology Risk Management
VISA International Pte Ltd

ABSTRACT OF TALK
• Current and future threats and challenges
• Security solutions for existing channels (ATM and POS)
• Implementing a secure eCommerce and mCommerce business
• Leveraging chip cards to secure the payments infrastructure
• Increasing importance of data security

ABOUT THE SPEAKER
Eric Trotter has been involved in the Payments industry for over 16 years from both a vendor, Bank and Card Association perspective. His primary focus over this period has been in the development of new payment systems based on emerging technologies.

He started off working in Japan for a leading POS and ATM vendor before joining Visa in London developing and implementing Retail Payment solutions for Banks throughout the European and Middle East Regions. He also represented Visa on several domestic, European and International standards committees for Banking and Payments standards.

He moved to Singapore in 1992 to join Visa Asia Pacific initially responsible for the Visa Network connections to over 150 Banks in the region. He then spent several years implementing chip card solutions including managing the implementation of the Visa Cash stored value card in Hong Kong in 1996. Subsequently he spent 6 months in Malaysia providing consulting to Bank Negara, Malaysia on the design and implementation of the Multi Application Smart Card project.

Eric now heads up the Emerging Technology and Product Risk Review group which focuses on technology risk management and security of B2C, B2B e-Commerce, mobile Commerce and chip based products as well as the more traditional Banks’ ATM and POS systems. He was responsible for the development of a PKI based security architecture for B2B e-Commerce products and currently represents Visa on the Singapore PKI forum and eCommerce Security standards committee.
Securing Online Payment with 3-D Secure

Edward Lodens
Regional Manager, e-Commerce Risk
Visa International Asia-Pacific

ABSTRACT OF TALK
Despite the recent boom in the number of e-commerce transactions, recent studies indicate that some buyers are not using payment cards on the Internet as often as they do in the physical world, in part because of security concerns. A recent survey revealed that nearly 85 percent of users cited security concerns as the number one deterrent for conducting e-commerce (Frederick Schneiders Research, 2001). To realize the huge potential of the new e-commerce payment channels, Visa is committed to raising confidence in online-payment security.

Visa has developed a secure online payment protocol called 3-D Secure. It has been created to address the issue of cardholder authentication and provide buyers, sellers and member financial institutions greater confidence in the security of the e-commerce environment. With 3-D Secure, card issuers can authenticate cardholders in the virtual world as readily as in face-to-face transactions thereby reducing the instances of fraudulent transactions or cardholder’s denial of valid charges.

ABOUT THE SPEAKER
Edward Lodens joined Visa International, in January 1998. Originally based in Sydney, Australia he re-located to Singapore two years ago to take up regional responsibilities.

As part of Visa’s Y2K readiness programme in Asia Pacific, Edward was heavily involved to ensure the readiness of Visa’s systems and Members in the Australia / New Zealand Sub-Region to meet the Y2K challenge.

Edward was responsible for all risk management and security related matters as part of Visa’s Olympic Sponsorship program for the Sydney 2000 Games.

In his current position Edward’s responsibilities include product risk and technical security for new and emerging payment channels as well as compliance and the development of best practices.

Edward has gained a Bachelor of Engineering (Chemical) from the University of Sydney and a Graduate Diploma in Applied Finance and Investment (Treasury) from the Securities Institute of Australia.
MasterCard SecureCode

T V Seshadri
Head of Technology & Operations, South-East Asia
MasterCard International

ABSTRACT OF TALK
• Guaranteed Payments for E-Commerce Transactions
• Introducing MasterCard SecureCode
• Issuer choice of authentication options
• PC Authentication Program
• Chip Authentication Program
• MasterCard 3-D Secure Implementation
• Merchants adopting MasterCard SecureCode
• MasterCard Guaranteed Payment Milestones
• Implementation approach
• Liability Shift Mandate
• Example: Consumer Registration & Shopping Experience

ABOUT THE SPEAKER
T.V. Seshadri is Vice President & Country Manager, Singapore for MasterCard International. He is also Head of Technology & Operations for the company across South East Asia.

As Vice President & Country Manager, Mr Seshadri provides key direction and insight to achieve MasterCard’s business objectives for Singapore. He holds overall responsibility for all aspects of MasterCard’s country operations with the specific aim of promoting the MasterCard family of brands. Mr Seshadri’s core portfolio includes forging close business alliances with member institutions, enhancing MasterCard’s brand awareness and increasing the usage and acceptance of MasterCard cards. In his role as Head of Technology & Operations, South-East Asia, Mr Seshadri oversees technology and process innovations for the region and provides direct support to leading regional and local financial institutions on technology and operations issues.

During his five years with MasterCard, Mr Seshadri has been credited with many successes including, spearheading the strategic and tactical introduction of many innovative card products and programs, introducing new payment alternatives and launching payment initiatives in the area of e-commerce, m-commerce & smart cards. Through his close partnerships with financial institutions he has played an important role in helping them realize the benefits of improved operations processing, enhanced systems and efficiency gains.

Prior to joining MasterCard, Mr Seshadri worked with Bank of America in its offices in India and its Asia Pacific headquarters in Hong Kong. Through his 11-year tenure with the bank, he managed a broad range of portfolios with an extensive focus on retail product management.

Mr Seshadri holds a Masters degree in Industrial Engineering.
Technology Risks & Security in eBanking and ePayment Systems

Tony Chew
Director, Technology Risk Supervision
Monetary Authority of Singapore

ABSTRACT OF TALK
Technology developments, and in particular the Internet, have propelled major innovations in the way financial systems operate and how they tap different markets throughout the world. In parallel with this phenomenon, the significance of technology risks and digital security has been escalating due to the increasing deployment of new technologies in banking and payment systems. As an ever growing number of new or revamped financial institutions’ systems assimilate Internet accessibility, information security and technology risk management issues are becoming more pressing and complex.

Security vulnerabilities and threats relating to computer systems and networks are burgeoning in sophistication and magnitude. The diversity and density of technology risks have increased exponentially, to the extent that financial institutions should take a fresh look at their capacity and the control processes they have to address these risks. As a result of recent security incidents, hacking exploits and virus outbreaks, there is greater awareness of the need to strengthen systems security and improve contingency planning, especially in relation to incident response capability, business continuity preparedness and disaster recovery back-up systems.

MAS has developed a set of guidelines to assist financial institutions in recognizing and understanding the dynamism and plethora of computer system, Internet and web application vulnerabilities and threats, and the actions they should take to manage these risks and exposures, including cyber crimes, internal and external threats, viruses, worms, all forms of hacking and potential acts of terrorism.

The guidelines are designed to promote sound processes in managing technology risks and the implementation of security practices. Financial institutions should establish and maintain robust technology risk management policies and practices, including strong security measures to protect their information assets. The aim of the guidelines is to encourage financial institutions to take appropriate actions to meet the following objectives:

- Delineate responsibility for safety and soundness.
- Establish responsibility for managing technology risks.
- Nurture a risk awareness culture.
- Rectify security vulnerabilities and weaknesses.
- Conduct vulnerability and security assessment.
- Invest in system reliability and integrity.
- Prepare for contingencies and disruptions.
- Educate customers on security precautions.
- Manage outsourcing risks.

MAS will take a keen interest in the efforts of financial institutions in complying with the guidelines. Where necessary, the financial institutions can adapt the guidelines taking into account their operational diversity and the different markets in which they run their business.
ABOUT THE SPEAKER
Tony is the director of technology risk supervision in the Specialist Risk Supervision Department at the Monetary Authority of Singapore. His division is responsible for carrying out supervisory and regulatory functions in respect of computer systems, networks and technology developments in the banking, insurance and securities industries.

Tony began his professional career as a Chartered Accountant, specialising in financial accounting, computer auditing and information systems consulting for over 12 years. Subsequently, he took up senior management positions in the private sector as well as in the banking industry for over 10 years.

In addition to being a frequent speaker at infosec forums and technology conferences, Tony has maintained a keen interest in academic pursuits. Recently, he participated as a guest lecturer at the National University of Singapore in its inaugural undergraduate course on “Introduction to Cybercrime”

He had also taught at the University of Technology, Sydney as a part-time lecturer from 1992 to 1996. The courses he conducted, both at undergraduate and post-graduate levels, included computer auditing, investment analysis and financial management accounting.

In addition to accountancy and audit qualifications, Tony has a Bachelor of Commerce from the University of New South Wales, and a graduate diploma in Data Processing and a Master of Business in Applied Finance from the University of Technology, Sydney.

Singapore’s Legal Infrastructure for E-Security
Harry SK Tan
Director, Centre for Asia Pacific Technology Law & Policy (CAPTEL)
Nanyang Business School, NTU

ABSTRACT OF TALK
Singapore has historically been early adopters of new information technologies. To enhance the continued adoption of new technologies, the infrastructure put together by the Singapore government for a first class environment for new technology business is second to none. This includes the legal infrastructure. In this session, we see how Singapore has addressed the variety of concerns arising from electronic security and look at the specific provisions that recognises the use of technologies for securing information to the prosecution of new cyber crime offences.

ABOUT THE SPEAKER
Associate Professor Harry Tan is the Director of Centre for Asia Pacific Technology Law & Policy (CAPTEL - http://captel.ntu.edu.sg). Prof Harry Tan is a Fulbright Scholar. He was awarded the Fulbright Scholarship in 1999 by the Council of International Exchange of Scholars and the Fulbright Commission in Washington, US. He is also a Visiting Scholar at Berkeley Centre for Law & Technology at University of California, Berkeley, where he carried out his further research in the field of the Development of Law & Regulation of E-Commerce.
He is the principal lecturer of the "E-Business: Law Policy & Strategy" course at the Nanyang Business School's MBA Programme and he also teaches the undergraduate course, Law of Information & Technology.

Prof Tan is also regularly involved in presenting papers and public seminars at internationally renowned venues. In 1999, he was invited to deliver a public paper at Stanford University’s Japan US Centre for Management of Technology. Over the past five years, Prof Tan had been involved in advisory roles and conducting industry executive development programmes on management of legal risks in electronic commerce and information technology and consultant to local internet banks and law firms. Most recently in November 2002, he led the CAPTEL expert team in a two day executive training on “Primer on Cyberlaws: e-Governance Policy and Regulatory Framework” for ASEAN Ministers and Permanent Secretaries.

He was also a consultant to FORTUNE as the Consulting Editor for the "FORTUNE Reader's Guide Programme", a periodical that focuses on current business trends, case studies and issues His current research interest is in the development of the law and regulation of Electronic Commerce and its impact on businesses. In addition to being a legal advisor to the Computer Centre at NTU, he is also the associate editor and web-master for the Asia Business Law Review. He has also authored several journal articles on E-Business Law, Cybercrime and E-Fraud.

He has an online consultancy practice at http://ByteLawyer.com and together with the related site http://E-Business-Law.com, he maintains a public information service on the developments of E-Business Law.

Transnational Issues in Cybercrime

Daniel Seng

Visiting Associate Professor, Law Faculty, NUS & Director of Research, Technology Law Development Group, Singapore Academy of Law

ABSTRACT OF TALK

Hackers and cybercriminals recognise and honour no national boundaries. The “Slammer” worm - which caused the most recent worldwide Internet attack - set a new speed record for spreading through the Internet. Within 10 minutes of its release, it had infected 75,000 vulnerable hosts around the world. Computers from countries as far away as USA, UK, Japan, Australia, Canada, Taiwan, China and South Korea were affected, and the total cost of the damage it caused is still being tallied. These incidents are bound to cause countries to examine the possibility of international cooperation and coordination to investigate, prosecute and combat cybercrimes. This presentation examines these possibilities and briefly discusses the Council of Europe’s Convention on Cybercrime, whose signatories include 26 CoE member states as well as the United States, Canada, Japan and South Africa.
ABOUT THE SPEAKER

Daniel Seng, an advocate and solicitor, is a Visiting Associate Professor with the Faculty of Law, National University of Singapore, and concurrently, Director of Research, Singapore Academy of Law. He was, until recently, a Partner at Rajah & Tann and Head of its Technology Practice Group. He graduated from the National University of Singapore in 1992 where he obtained a first class and subsequently read for his Master of Laws in Oxford University in 1994, where he also obtained a first class and was the Rupert Cross prize winner that year. He was a Justices’ Law Clerk of the Supreme Court of Singapore in 1995. Daniel was formerly a Senior Lecturer with the Faculty of Law at the National University of Singapore, where he taught information technology law, telecommunications law, evidence and procedure and banking law. He has presented numerous papers at various local, regional and international conferences and written articles on information technology law and evidence. He was one of the joint authors of the Butterworths Annotated Statutes of Singapore: Evidence volume.

Daniel is a member of various governmental committees that were responsible for various legislative reforms in the area of Information Technology law in Singapore, including the Computer Misuse Act, the Copyright Act, the Electronic Transactions Act, the Evidence Act, the Layout Designs of Integrated Circuits Act and the Model Data Protection Code for the Private Sector. He is a member of the Technology Law Development Group, and IT law think tank formed by the Academy of Law and a member of the National Internet Advisory Committee Legal Subcommittee. He is also a domain name panellist for the Singapore Domain Name Dispute Resolution Service.

He is listed in the Guide to the World’s Leading Information Technology Advisers 1999-2000 Edition, a Euromoney Legal expert guides publication and he is acclaimed as one of the prominent intellectual property lawyers in Singapore in AsiaLaw Profiles 2001. He has also been recognised as a leading lawyer in the technology practice area in AsiaLaw Leading Lawyers 2000 and as a leading lawyer in intellectual property practice area in Asia Law Leading Lawyers 2001.

Legal Issues in Electronic Surveillance E-Privacy

Mary Wong

Department of Law, School of Business

Singapore Management University

ABSTRACT OF TALK

Developments in surveillance technology and their deployment by law enforcement agencies, corporations and individuals have given rise to concerns over the legal limits of the use of such technology. One of the main concerns is the impact of such technology on privacy. Much media attention, and some legal disputes, have been focused on the existence and boundaries of electronic privacy rights, particularly in the United States after September 11, 2001, and also in light of policy concerns over crime prevention and anti-terrorism measures.

This talk will outline the various forms of surveillance technology that have been identified as raising particular privacy concerns, and trace the legal issues and proposed legal solutions in relation to resolving the tension between privacy, technology and security.
Ms Wong is an Associate Professor of Law at the Singapore Management University, and concurrently Special Counsel to the US law firm of Morrison & Foerster LLP, where she is associated with its Technology Transactions Group. Prior to joining the Singapore Management University, Ms. Wong was a tenured Senior Lecturer at the Faculty of Law, National University of Singapore. Ms Wong graduated with an LL.B (Honours) degree from the National University of Singapore, where she was the top student in her class, winning the Adrian Clark Memorial Gold Medal, the Leow Chia Heng Prize and the External Examiners’ Special Cash Prize. She also holds an LL.M degree from the University of Cambridge (England).

Ms Wong was resident in Morrison & Foerster’s New York office for several years, during which time she also served a term of secondment to its Brussels office. At Morrison & Foerster, Ms Wong works primarily with technology companies and Internet-based businesses, focusing on transactions relating to intellectual property rights, Internet law and electronic commerce. She has worked extensively on technology law and policy issues relating to electronic signatures, online privacy and domain names. Ms Wong also advises clients on legal and international developments relating to intellectual property and Internet law and policy. She works closely with the Morrison & Foerster offices in Europe and Asia, where her background and experience have enabled her to provide clients and colleagues with a comparative legal and cultural perspective on various laws, national policies and business matters.

Ms Wong has represented Morrison & Foerster as a speaker at various international conferences in the United States, Canada, Europe, Japan and Singapore. She has also conducted seminars and courses for lawyers and entrepreneurs, such as the “Immersion in Information Technology Law” certification program in Singapore and the “Building a Successful New Media Business” program series in New York.

As a law professor, Ms Wong teaches specialist courses in information technology law, electronic commerce law and Internet law and policy. She has published numerous articles and has also co-written commissioned reports for the National Computer Board in Singapore on digital media and a National Information Infrastructure, and co-authored a book on intellectual property rights in Singapore for Kluwer Law International. Ms Wong continues to organize conferences, workshops and other programs, to bring together academics, legal practitioners, government officials and industry professionals in such fields as intellectual property and technology law. One project that Ms Wong is particularly proud of is her work with the USAID Program and the University of San Francisco Cambodia Law Project in 1996, on a pilot project for legal capacity building in Cambodia.

Ms Wong is admitted to practice as an advocate and solicitor of the Supreme Court of Singapore. She has also been trained as a mediator in intellectual property disputes at the World Intellectual Property Organization (WIPO) and is currently a member of the Singapore Government’s E-Commerce Consultative Committee, in which capacity she has represented Singapore at meetings of the UNCITRAL Working Group for Electronic Commerce in New York.
Security Standards, Evaluation Criteria and Security Assurance

Chi-Hung Chi
Associate Professor
Centre for Systems Security Research, NUS

ABSTRACT OF TALK
Security is a balancing Act; one wants neither too little nor too much. Both management and IT professionals need guidance as to when they have enough.

This presentation will review standards and measures for information protection and security. It will treat the advantages and limitations of each and make recommendations for their use.

ABOUT THE SPEAKER
Associate Professor Chi-Hung Chi involved in the Centre for Systems Security Research, Multimedia Information Laboratory and Centre for Internet Research. He holds of 6 US patents and consultant to a number of industries on their internet infrastructure setup and deployment. Associate Professor Chi worked in Philips Laboratories and IBM (Poughkeepsie) in the US.

War -Driving, Wireless LAN Risks and Defense

S C Leung
Chairman
Professional Information Security Association (Hong Kong)

ABSTRACT OF TALK
Wireless LAN (WLAN) has liberated us from the tie of cables in network access. At the same time, it also changed the traditional concept of perimeter, both in physical and logical sense. With just an affordable WLAN card and some available free software tools, users (and hackers) can discovery and connect to a WLAN network everywhere. They can do whatever a user with a physical connection to a network port can do. Your control of network access might be broken without you being informed and the activity not being logged!

The problem is further escalated by the lack of security in most factory default configuration found everywhere in the city. Determined malicious hacker can even launch attack to secured WLAN via vulnerabilities of the current WLAN technology.

In this talk we will highlight the general approach of war driving, the security risks of the current WLAN implementations and the best practices of defense. Live demonstration is included.

Outline
• War Driving: vulnerability assessment or hacking?
• WLAN Risks & Protection Strategies
• WLAN Live Demonstration
ABOUT THE SPEAKER
Mr. SC Leung has over 10 years of working experience in the IT field serving Internet solution provider, banking, the telecommunication industries and outsourcing services. His previous assignments covered architectural design, security assessment, business contingency planning, region-wide standard and policies compilation. He is currently the Senior Consultant of the Hong Kong Computer Emergency Response Team Coordination Centre.

Mr. Leung is a frequent speaker in information security seminar and conferences. He holds several professional qualifications, including Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA) and Certified Business Continuity Professional (CBCP).

He serves as the Chairperson of the Professional Information Security Association, a not-for-profit organization for information security professionals, since it was founded in 2001.

PISA’s WLAN Security Team (Mr. Jim Shek, Mr. Alan Tam and Mr. W.S. Young) had conducted the first War Driving Study in Hong Kong in July 2002. The study was widely reported in local and international media to heighten the attention of the security of wireless LAN in Hong Kong.

SC Leung can be reached at sc.leung@pisa.org.hk

Clues, Vandalism, Litter Sendmail Trojan Trail
Paul Henry
Vice President, Worldwide Operations
CyberGuard Corporation

ABSTRACT OF TALK
Computer forensics today plays an important part in prosecuting the commiters of cybercrime. This forensics workshop will cover topics that addresses what properties will determine an evidence. What is computer forensics all about and how do people typically use and abuse computer systems. The workshop will also explore how to interpret and validate evidence. What limitation and obstacle do forensics expert face and the presentation of evidence. This workshop is meant for audiences who have at least some years of technical experience with computer security.

ABOUT THE SPEAKER
Paul brings with him more than 20 years experience in security and safety controls in high-risk environments such as nuclear power plants and industrial boiler sites. He is currently the Managing Director of Asian Operations, CyberGuard Corporation, Florida, USA.
Over the years, Paul has worked and developed security projects for National Banking System in Saudi Arabia, Department of Defense's Satellite Data Project, USA, and NTT Data in Japan. He has also been engaged several times to speak at network security engagements and presented his white papers on Firewall Architectures, Intrusion Methodology, Enterprise Security and Managed Security Services. An accomplished author, Paul has written many technical papers on Port Scanning Basics, Buffer Over-Runs, Firewall Architectures and Burner Management and Process Controls for nuclear power plants.

Understanding the Intrusion Timeline
Andre Yee
Vice President, Engineering
Network Flight Recorder Security

ABSTRACT OF TALK
Intrusion detection and prevention plays a very crucial part in the security defense of an enterprise network. Given the evolution of technology and cyber threats, corresponding detection technologies and methodologies require the necessary enhancement as well. This presentation will address the timeline to which how intrusion management should be done before, during and after an occurrence. It will provide insight to proactive and responding measures.

Agenda:
- Evolution of Security Threats
- Defining the Attack Timeline
- Intrusion Management Continuum
- Intrusion Management Process

ABOUT THE SPEAKER
Andre Yee has over 10 years of management experience in research and product development and is a leading expert in both EAI and B2Bi technologies. Most recently he served as the Vice President of Research and Development for SAGA software. Prior to SAGA Software, Yee was Director of Product Development at Landmark Systems Corporation. Mr. Yee is an experienced speaker in national technology conferences, is the inventor of two US patents and has authored two books on Java and software integration.
Avoiding soft security - using hardware to protect authentication, encryption and digital signatures

Nicko van Someren
Chief Technology Officer
nCipher

ABSTRACT OF TALK
This presentation will look at how cryptography can help to meet a number of the data protection requirements and some of the basics of cryptography, the difference between secret key and public key crypto, encryption, digital certificates and digital signatures. In addition it will look at the role of cryptographic hardware as a best practice security measure - how it is helping organizations meet legislation and compliance issues.

Agenda:
- The proliferation of cryptography
- Vulnerabilities
- Key Finding analyzed
- Best practice for hardware security modules

ABOUT THE SPEAKER
Dr Nicko van Someren, Chief Technology Officer, nCipher. Dr Nicko van Someren co-founded nCipher in 1996. As Chief Technology Officer Nicko leads nCipher's research team and directs the technical development of nCipher products. From 1993 to 1996, Nicko was Technical Director and co-founder of ANT Limited, where he developed hardware products and application software. Before that, he was employed as a Researcher by Xerox EuroPARC and as a Software Engineer by Atari Research and Perihelion Software Limited. Nicko has almost 20 years' experience in cryptography, software and hardware product development, and holds a Doctorate and First Class degree in Computer Science from Trinity College, Cambridge, UK.
ABSTRACT OF TALK
Corporate and carrier security requirements are constantly increasing, and as a result organizations are deploying a full set of security tools to protect their network from viruses and hackers in order to control access to their applications and to defend themselves from Denial of Service (DoS) attacks.
Yet implementing security tools such as firewalls, VPNs, Intrusion Detection Systems, anti-virus and application security devices can create obstacles that interfere with providing complete enterprise security. High network availability is threatened since these security tools are usually software running on general-purpose servers. Multiple single points of failure jeopardize network operation, as each of these tools is usually deployed inline with no redundancy. Decreased performance endangers the complete operation of defense architecture as each of those tools adds a delay; especially as deeper and more thorough application oriented security is needed.

These issues create a strong trade off between security on one hand and availability and performance on the other hand. My presentation will discuss a security and application switching solution that enables the deployment of all standard security tools while accelerating their performance and eliminating downtime. Radware Security Activation solution allows enterprise and carrier customers to simplify network configurations, build scalable security architectures and guarantee enhanced security through Gigabit speed application security and denial of service protection, ensuring that all security tools are fully activated and protecting mission critical data and resources.

ABOUT THE SPEAKER
President and CEO of Radware Inc. Roy is the founder of Radware and has since been improving the features and technology of Radware products to bring it to greater heights. Roy is also a frequent speaker in security events.
To get from LT27 to S14, follow the path on the map (dotted line).
Exhibitors were selected by the organizing committee.