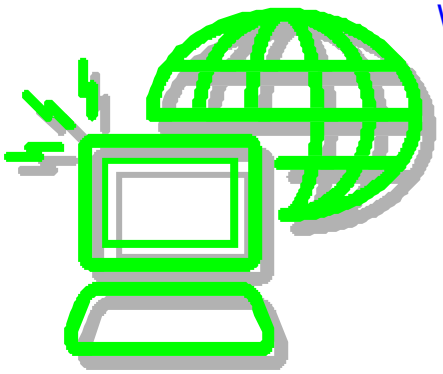
Surviving Security Threats

Wednesday, 27 February 2002
0900hrs to 1700hrs
Lecture Theatre 27
National University of Singapore

Main Host:
National University of Singapore (Department of Mathematics)

Co Host:
Quantiq International Pte Ltd

Participating Vendors:
CyberGuard Corp
Network-1 Security Solutions, Inc.
nCipher Corporation Ltd
NFR Security
PCS Security Pte Ltd
SSH Communications Security Corps
Websense Inc.



Surviving Security Threats

This Seminar's topical coverage addresses a breadth of security technologies and processes, including policy, encryption, applications security, and maintenance, while continually answering the following questions that is critical to network administrators and managers:

- Why is this technology/practice important to a security infrastructure?
- How does this fit into the larger security layer model?
- What basic measures are required to better enhance risk mitigation management?
- How does recent global cyber-terrorist acts affect on future e-businesses?
- Why the need for an Incident Response Team to complete the full picture for Mitigating Risk Management?

Integrating People, Process, Technology Together Securely

Networking and security issues can be very complicated and expensive for business. Security is very important, but enterprising businesses have to manage to balance their needs with what they can afford.

This seminar helps the audience to learn how to determine the risks involved with computer networking and the Internet, and understand the options available to them for securing valuable company information, data and websites. Some topics attempts to explain the costs and complications involved. Some of the security measures covered include encryption, authentication, firewalls, intrusion detection, remote access, host security and server security.

The areas of interest covered goes well beyond a basic explanation of these security topics. It also provides case studies covering security maintenance, vulnerability tests, and security audits and about what to do if and when security is breached. Throughout the seminar topics, the audiences are frequently referred to additional resources where they can find more information as well as offering website URLs where additional information and updates can be found.

This seminar can help government, large and small businesses system administrators to learn what is needed and expected, and help them implement security plans and solutions based on their needs, thus learning to survive security in an insecure cyber world.

Surviving Security Threats

27 February 2002, LT 27, National University of Singapore

PROGRAMME

0900 – 0915	Opening address *Lee Seng Luan* *Professor and Head, Department of Mathematics, NUS*
0915 – 1000	Embracing Security: Be a Survivor, Not a Target *Yu Chien Siang* *Principal Consultant, Ministry of Home Affairs*
1000 – 1015	Break
1015 – 1100	Hacking Tools v2 Live Demonstration *Paul Henry* *Vice President, World Wide Operations, CyberGuard Corp*
1100 – 1145	Security Mechanisms in Database Systems *Tan Kian Lee* *Associate Professor, Department of Computer Science, NUS*
1145 – 1330	Lunch
1330 – 1415	Internet Security Threats - A Regulator's Response *Tony Chew* *Director, Technology Risk Supervision, Monetary Authority of Singapore*
1415 – 1500	Data Integrity and Security Model for Web Intermediary Services *Chi Chi-Hung* *Associate Professor, Department of Computer Science, NUS*
1500 – 1530	Break
1530 – 1615	Security Standards of Network Security: TLS, SSH, IPSEC, MPLS *Jean-Bernard Dumerc* *Vice President, Asia Pacific, SSH Communications Security Corps.*
1615 – 1700	Panel discussion *Chaired by Professor Harald Niederreiter, Department of Mathematics, NUS, with speakers as panel members*

Surviving Security Threats

27 February 2002, LT 27, National University of Singapore

SPEAKERS' SYNOPSIS

KEYNOTE ADDRESS

Yu Chien Siang

Principal Consultant, Ministry of Home Affairs

on

"Embracing Security: Be a Survivor, Not a Target"

Yu Chien Siang is the man at the helm of our nation's informational security, for he holds the distinction for being the leading Computer Security Consultant in the Ministry of Home Affairs.

Yu Chien Siang graduated from a German university as a Data Systems Engineer and also received training from the Siemens Research Laboratory and the IBM R&D Laboratory in Boblingen, Germany. He has been active in the IT management and IT Security industry for over 20 years. During this time, he led numerous IT projects in the IT security aspects at the national level and had been instrumental in evolving their architecture and the basic mechanisms required. Mr Yu also invented unique smart card readers, cryptography systems and more efficient protocols.

He was an ex-President of the Singapore Microcomputer Society, a prolific writer for local IT magazines and a hobbyist programmer that had created more than 60,000 lines of code. One of his proudest achievements was leading a team that won the First Prize for Physics for the Science Fair in 1974.

Surviving Security Threats

27 February 2002, LT 27, National University of Singapore

SPEAKERS' SYNOPSIS

Paul Henry
Vice President, World Wide Operations, CyberGuard Corp
on
"Hacking Tools v2 (Live Demo)"

Paul Henry 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 Vice President of Worldwide 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 events and presented 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* as well as whitepapers on firewall architectures, covert channel attacks, distributed denial of service (DDoS) attacks, common mode noise and common mode rejection, PLC programming and buffer over-runs.

In addition to his CISSP certification, Henry holds numerous other security certifications such as MCP+I, MCSE and CCSA. He is also in demand as a presenter and has delivered keynote speeches at security seminars and conferences worldwide on topics including DDoS attack risk mitigation, firewall architectures, intrusion methodology, enterprise security and managed security services. Paul Henry has also been interviewed by or appeared in a variety of media outlets including NBC Nightly News, CNBC-Asia, *Power Magazine*, *Secure Computing Magazine*, ISA Publication Industrial Computing, the *Miami Herald*, *San Francisco Chronicle* and many others.

Apart from delving into "hacking activities" as part of his role as a *-Hat Hacker"* security consultant, in his leisure, Paul blows up his home servers occasionally with the latest attack tools, studies software exploits and vulnerabilities, and continuously builds up his arsenal of Unix/Linux/Windows hacking tools.

Tony heads the Technology Risk Supervision division of the Market Infrastructure and Risk Advisory Department in MAS, which is responsible for conducting supervisory inspection and regulatory reviews of computer systems and technology developments in the financial sector.

Tony began his professional career as a Chartered Accountant, specializing in financial accounting, computer security 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 a period exceeding 10 years.

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.

Surviving Security Threats

27 February 2002, LT 27, National University of Singapore

SPEAKERS' SYNOPSIS

Chi Chi Hung

Associate Professor, Department of Computer Science, NUS

on

"Data Integrity and Security Model for Web Intermediary Services"

Dr Chi is currently an associate professor in the School of Computing, National University of Singapore. He is also actively involved in the Centre for Systems Security Research, Multimedia Information Laboratory and Centre for Internet Research. Prior to joining NUS, he was with Philips Laboratories and IBM (Poughkeepise) in the U.S. He publishes widely in journals and conferences, holds six U.S. patents, and consults many industries on their Internet infrastructure setup and deployment.

Jean-Bernard Dumerc

Vice President, Asia Pacific, SSH Communications Security Corps.

on

"Security Standards of Network Security: TLS, SSH, IPSEC, MPLS"

Jean-Bernard Dumerc a French National, brings with him more than 15 years of international business experience in telecommunications networks in Asia Pacific, in such fields as radio-communications, optical communications or IP networks. He is responsible for developing the business in Asia Pacific of SSH Communications Security Corp, the world-leading supplier of Internet security software for network security and also act as CEO of SSH Communications Security K.K., the Asian subsidiary of SSH in Tokyo, Japan. Prior to joining SSH in April 2000, he has held previous positions at Alcatel, the European Telecommunication vendor, and was until 1999 Executive Vice President of Alcatel Japan Ltd. He graduated from Institut National des Sciences Appliquées, France, with an MSEE, as well as an MBA from UC Berkeley Extension, USA.