truevent US

BLUESPACE

18 - 20 FEBUARY 2014 | KUALA LUMPUR, MALAYSIA

*Hacking and cybercrime is costing the global economy between **USD300,000,000** to **USD1,000,000,000** annually*

McAfee and the Center for Strategic and International Studies, July 22, 2013

Why you cannot miss this event

What's more boring than sitting at a conference for two days on end when the speakers are up there showcasing and dazzling you with uber cool tools that you can't wait to get back to experiment with? Probably the commute back and the additional wait to get back to your machine. **BlueSPACE** is a stripped out, no-nonsense – and no holds barred – platform for you, the vanguards of information, to experience the best defense techniques available today while preparing for the breach tomorrow. It is a unique "think from a hacker perspective "event where the best of minds in the hacking world along with policy-makers and government security officials meet face to face to experience the best techniques available today to protect your computer network. Defense, as they say, is the best offense.

Key Features of This Event:

- **Hardening** your system like you never knew you could
- **Identifying** vulnerabilities in your system and constructing safeguards
- **Evaluating** the best counter measures for different attack vectors
- **Fortifying** your networks and dummy-proofing it against internal breaches
- **Leveling** up your ninja defense skills
- **Detecting, deflecting and defeating** intrusions and unauthorised access
- **Immersing** yourself in live demo, simulations and live hacking to enhance your learning experiences

Who should attend:

This conference is designed for:

- Chief Information Officers
- Chief Information Security Officers
- Chief Technology Officers
- Directors of IT
- Directors of Information Security
- Security Systems Managers and Engineers
- Security Architects
- Security Analysts
- Security Auditors
- IT Managers and Engineers
- IT Infrastructure Managers

Key Industries

- Oil and Gas
- Petrochemical and Chemical
- Banking and Finance
- Stock Exchange
- Government Agencies and Ministries
- Law Enforcement
- Military
- Manufacturing
- FMCG
- Semiconductor
- Technology
- Electronics
- Telecommunications
- Power and Utilities
- Healthcare
- Pharmaceuticals
- Airlines and Airports
- Media and Broadcasting
- Logistics
- Transportation
- Ports
- Shipping and Maritime
- Online Portals
- Casinos
- Betting and Gaming

Supporting Organisations

CyberSecurity MALAYSIA
An agency under MOSTI

ispa.MY
Information Security Professionals Association of Malaysia

The Information Security Professional Association of Malaysia (ISPA) established strategically to address nation's need in building quality Information Security professionals. This is the only association in Malaysia that supports the development of Information Security at the moment. Focus areas ranges from competency and capability development, professional development, certification, lifelong learning and knowledge enhancement.

The setup is inline with the government's vision on the strategy for Cyber Security acculturation and capacity building, encompasses a set of common objective to inculcate the culture and building up capacities and capabilities of Information Security professionals.

FEATURING EXPERT TECHNICAL LIVE DEMO BY:

Wayne Burke
CSO
Sequrit CSI, Holland
**Featured in SecureNinja TV:Forging IT Security Experts*

Mohd Zabri Adil Talib
Head of Digital Forensics
Cyber Security Malaysia, Malaysia
**Honoree of Managerial Professional for Information Security Project(s) Category from Asia Pacific Information Security Leadership Achievements (ISLA) 2011 by International Information Systems Security Certification Consortium (ISC)²*

Christopher Low
Founder
ThinkSECURE, Singapore

Dr SPT Krishnan Scientist
Institute of Infocomm, Singapore

Dr Desmond Devandran
CEO-Asia Pacific
Foresec Academy, Malaysia

Hazlin Abdul Rani
Specialist, Cyber Technology Research Department
Cyber Security Malaysia, Malaysia

Muslim Mansor
Forensic Analyst
SHELL, Malaysia
**Honoree of Information Security Practitioner from Asia Pacific Information Security Leadership Achievements (ISLA) 2012 by by International Information Systems Security Certification Consortium (ISC)²*
**Instructor of the Year 2012 by Global EC Council Award*

Fahad Ehsan
Associate Director- Security Research and Analytics
UBS, Singapore

FEATURING EXPERT DEEP DIVE SIMULATION BY:

Mahmud Ab Rahman
Information Security Researcher
NetbyteSEC, Malaysia

FEATURING WORKSHOP BY:

Kiran Karnad
Software Penetration Tester
MIMOS, Malaysia
**Past speaker of AusCert 2013 in Australia*
**Nominee of Information Security Innovation Award (ISIF) Asia Awards 2013*

FEATURING RENOWNED EXPERTS BY:

Pierre Noel
Chief Security Officer & Advisor
Microsoft Asia, Singapore

Murari Kalyanarami
Global Head of Service Architecture & Integration
British American Tobacco, Malaysia

Han Ther Lee
Regional IT Security Compliance Manager
British American Tobacco, Malaysia

Lee Hwee Hsiung
Secretariat
Information Security Professionals Malaysia (ISPA), Malaysia
**Winner of Chief Security Officer ASEAN Award 2012*

Mohd Nasir Che Embee
Information Security Manager
Malaysian Electronic Clearing Corporation (MyClear), Malaysia

Goh Su Sim
Threat Insight manager
F-Secure, Malaysia

Tun Abdul Karim Tun Abu Bakar
Senior Technical Expert (IT Security)
Tenaga Nasional Berhad (TNB), Malaysia

CONFERENCE AT A GLANCE

Day One: Tuesday, Feb 18, 2014

Session One
The Google hacking database - A key resource to exposing vulnerabilities

Workshop
Rootkits, Botnets and You

Day Two: Wednesday, Feb 19, 2014

Session One
Security today and tomorrow: Managing threats in the digital age

Session Two
Technical live demo: Malware defense strategies

Session Three
Technical live demo: The essentials of cryptography-how to keep your secrets safe

Session Four
Technical live demo: Offensive hacking and penetration testing

Session Five
Deep dive with simulation: Designing a honeynet from scratch without spending more than your firewall cost

Session Six
Technical live demo: Penetration testing and cyber terrorism through telecommunication network

Session Seven
Technical live demo: Mobile applications and resiliency against attacks

Day Three: Thursday, Feb 20, 2014

Session One
Why typical information security fails: The case for effective defense in depth and the resilience movement from Microsoft perspective

Session Two – Panel discussion
Cyber war and security threats: Penalising hackers who break government regulations and pose threats to the companies and consumers

Session Three
Technical live demo: Analysing web server log files using Google Bigquery to detect anomalies activities

Session Four
Technical live demo: Taking the mystery out of the cloud access and identity management

Session Five
Technical live demo: Securing integrity with forensic computing

Session Six
Technical live demo: Memory forensics and security analytics

Session Seven
The state of net

Day One
Tuesday, 18 February 2014

0800 **Registration and coffee**

0845 **Opening address from the Chairperson**

0900 **Session One**

The Google hacking database - A key resource to exposing vulnerabilities

We all know the power of Google - or do we? Two types of people use Google: normal users like you and me, and the not-so-normal users - the hackers. What types of information can hackers collect from Google? How severe is the damage they can cause? Is there a way to circumvent this hacking? As a security tester, Kiran Karnad uses the GHDB (Google Hacking Database) to ensure their product will not be the next target for hackers. Kiran describes how to effectively use Google the way hackers do, using advanced operators, locating exploits and finding targets, network mapping, finding user names and passwords, and other secret stuff. Kiran provides a recipe of five simple security searches that work. Learn how to automate the Google Hacking Database using Python so security tests can be incorporated as a part of the SDLC for the next product you develop.

0930 **Workshop**

Rootkits, Botnets and You

It's a late Saturday night. Your phone rings and your network guy says your company's network is hacked and that all your customers information is being stolen as you speak! What do you do now?

Malicious software or malware has been around since time immemorial… Errr… since the time computers have been around… They are very polymorphic and so can take the form of a backdoor or a botnets or an info-stealer or even a rootkit or a downloader, launcher, scareware, virus or worm, spam-sender and what have you. As a malware analyst, your work would be to reverse engineer these dangerous "creatures" and ensure your network and machines are no longer vulnerable to them.

So, you've decided to be a malware analyst for more reasons than one!… You find it challenging, every security company needs reverse engineers, cracking up code and tools gives you the high... To be one, you not only need to know how various malwares behave, but also how to reverse engineer them and answer questions such as how can you find which machines are infected, what harm does each type of malware do, and, how can you ensure you are safe now? Etc.

Come and join Kiran as he treads through all these questions and also provides you with a hands-on experience on how you can detect and analyse malware, ensure you understand how it works, dissect it to the core and safeguard your computer and network. We will create a safe yet dangerous environment and host some ugly rootkits and slit them up. No mercy here!!

1200 **End of Day One**

Trainer Profile

Kiran Karnad
Software Penetration Tester
MIMOS, Malaysia
** Past speaker of AusCert 2013 in Australia*
** Nominee of Information Security Innovation Award (ISIF) Asia Awards 2013*

Kiran Karnad is the current Software Penetration Tester at Malaysia Institute of Microelectronic Systems (MIMOS), Malaysia. After more than sixteen years in software testing and implementation, he found his true calling in penetration testing. Proudly calling himself a hands-on lead for information security, Kiran has worked with several Fortune 500 companies and mentored software test teams in multiple geographies. Currently leading the functional and security efforts at MIMOS, Kiran strives to identify process improvement opportunities throughout the organization and to implement them effectively.He has 4 papers selected at IEEE(Institute of Electrical and Electronics Engineers) for presentation.

He is a frequent presenter at various conferences and workshops including STARWEST 2012 (USA), STARWEST 2013 (USA), Agile Testing Days (Germany), Be a Testing RockStar (US),AusCERT 2013 (Australia), IEEE (Malaysia), Scopus (Finland) and has conducted workshops through EC Council at various Malaysian Universities. As Kiran is also a certified ASS - Application Security Specialist, he is passionate to develop IT security not limited to the enterprise network but also for the Malaysian community. He is currently nominated for his pioneering project on using GPS and web portal using Phyton & PHP for" Where is my Baby?" by Information Security Innovation Award (ISIF) Asia Awards 2013.

Day Two
Wednesday, 19 February 2014

0800 **Registration and coffee**

0845 **Opening address from the Chairperson**
Murari Kalyanarami Global Head of Service Architecture & Integration
British American Tobacco, Malaysia

0900 **Session One**
Security today and tomorrow: Managing threats in the digital age
The dynamic and competitive nature of changing business and IT landscapes requires a change in mindset for the information security professional. This keynote presentation explores challenges that business and IT "forces " face in terms of impacting the organisational security risk profile, change in skill set requirements and driving business value through information security initiatives.
Murari Kalyanarami Global Head of Service Architecture & Integration
British American Tobacco, Malaysia

0945 **Session Two**
Technical live demo: Malware defense strategies
With various techniques used by cyber attackers to exploit & compromise organisations, to the advancement of exploit kits and malware development kit, many IT Security professionals start to take a serious look at dealing with malware based incidents. This presentation will provide participants with appropriate and best malware defeating tools by reverse engineering on common malwares encountered by major corporations today.
Muslim Mansor Forensic Analyst
SHELL, Malaysia

1045 **Morning refreshments**

1100 **Session Three**
Technical live demo: The essentials of cryptography-How to keep your secrets safe
Cryptography is an indispensable tool for protecting information in computer security systems especially classified data of company financing and privacy of consumer information. Modern cryptography provides a variety of mathematical tools for protecting privacy and security that extend far beyond the ancient art of encrypting messages.

This presentation is designed specifically to allow participants to apply effective methods to encrypt the transport layer data without going into mundane specifics of cryptography. Important areas of modern cryptography are also highlighted, such as latest cryptography algorithm, key management, hashing, and applications as well as a current research in the cryptography field with a special live demo on encrypting the transport layer.
Hazlin Abdul Rani Specialist, Cyber Technology Research Department
Cyber Security Malaysia, Malaysia

1300 **Networking luncheon**

1400 **Session Four**
Technical live demo: Offensive hacking and penetration testing
Mobile hacking and forensics is fast becoming a lucrative and constantly evolving field. The mobile phone industry has been witnessing some unimaginable growth. Some experts say it may even replace computers for those who prefer to send and receive emails. This is definitely an area of digital forensics which will grow in scope and size due to the prevalence and proliferation of mobile devices.

Mobile hacking and forensics are certainly here to stay as every mobile device is different. This presentation is designed to cover the intricacies of manual acquisition (physical vs. logical), advanced analysis using reverse engineering and understanding how popular Mobile OS are hardened to defend against common attacks and exploits.
Wayne Burke CSO
Sequrit CSI, Holland

1445 **Session Five**
Deep dive with simulation: Designing a honeynet from scratch without spending more than your firewall cost
Deploying honeynet is often an overlooked area in the corporate networks whether it is in oil & gas, financial banking, commercial FMCG and telecommunication industry. This presentation will provide deep dive with simulation to design a central honeynet to catch attacks. Delegates will learn valuable lessons in using honeynet as a defense mechanism by embedded devices.
Mahmud Ab Rahman Information Security Researcher
NetbyteSEC, Malaysia

1615 **Afternoon refreshments**

1630 **Session Six**
Technical live demo: Penetration testing and cyber terrorism through telecommunication network
Telecommunication and hacker activities are closely related to cyber terrorism. This presentation will detail the common mistakes that Internet Service Providers (ISP) do that could cost business dearly.
The presentation will highlight the risk in telecommunication industry and how it would impact the entire nation in terms productivity as well as financial loss. In addition, participants will have a great learning experience of the tools and techniques used by the attackers to target telecommunication equipments. Delegates will be guaranteed and awed with how easy penetration to these networks could be done with no special knowledge with a live demonstration.
Dr Desmond Devandran CEO-Asia Pacific
Foresec Academy, Malaysia

1800 **Session Seven**
Technical live demo: Mobile applications and resiliency against attacks
As more and more people increasingly relies on mobile applications in their everyday lives, there is huge increase of information being kept from mobile apps which range from private photos and documents to confidential corporate data and emails. This presentation will cover techniques and tools which can be used to run penetration-tests against any mobile app. The techniques and tools can also be used by those who wish to convince themselves of the security of such apps which are installed in their mobile devices before entrusting personal information / data to said application.
Christopher Low Founder
ThinkSECURE, Singapore

1930 **End of Day Two**

Day Three
Thursday, 20 February 2014

0800 **Registration and coffee**

0845 **Welcome address from the Chairperson**
Lee Hwee Hsiung Secretariat
Information Security Professionals Malaysia (ISPA), Malaysia

0900 **Session One**
Why typical information security fails: The case for effective defense in depth and the resilience movement from Microsoft perspective
In the midst of a spate of data leakage incidents in both public and private sector, effective strategies should be deployed to prevent catastrophic financial or data loss. Interesting observation point on historical and recent security incidents will be shared to highlight the methods to analyse different layers that ought to be present to prevent common pitfalls in typical information security systems. Delegates will gather important lessons building toward Security 2.0: Information Resilience by understanding the reasoning for information resilience vs. typical information security protection.
Pierre Noel Chief Security Officer & Advisor
Microsoft Asia, Singapore

0945 **Session Two – Panel discussion**
Cyber war and security threats: Penalising hackers who break government regulations and pose threats to the companies and consumers
In response to the ever growing threat of loss of data and national security, many countries in Asia have begun enacting new laws and regulations. This groundbreaking panel discussion will discuss security policies, legal procedures and technological readiness to optimise security.

Moderator
To be announced

Panelists
Han Ther Lee Regional IT Security Compliance Manager
British American Tobacco, Malaysia

Lee Hwee Hsiung Secretariat
Information Security Professionals Malaysia (ISPA), Malaysia

Tun Abdul Karim Tun Abu Bakar Senior Technical Expert (IT Security)
Tenaga Nasional Berhad(TNB), Malaysia

Mohd Nasir Che Embee Information Security Manager
Malaysian Electronic Clearing Corporation (MyClear)

1000 **Morning refreshments**

1015 **Session Three**
Technical live demo: Analysing web server log files using Google BigQuery to detect anomalies activities
Google BigQuery is a web service that allows user to do interactive analysis of massive datasets—up to billions of rows and is predicted to be next big thing in doing interactive data analytics. Google BigQuery is scalable and easy to use that lets security analysts perform on-demand real-time analytics without building the infrastructure first.

In this presentation, the presenter will be sharing his experience of using the Google BigQuery to analyse apache web server log files to detect anomaly activities. The apache web server log files are from a live web portal that the speaker has been maintaining for several years now. The presenter will be showing a live hands-on demo of setting up the analysis work bench, data cleaning, data transformation and detecting potential threats using Google BigQuery. The presenter will also be giving away the software that he created for data cleaning/transformation in addition to the slides. Using this, the attendees can start with Google BigQuery immediately.
Dr.SPT Krishnan Scientist
Institute of Infocomm, Singapore

1145 **Session Four**
Technical live demo: Taking the mystery out of the cloud access and identity management
Managing identities and access control for enterprise applications remains one of the greatest challenges facing IT today especially in the corporate world. This presentation will share the latest tools to secure mechanisms for transmitting the information from the trusted source to the cloud service across user population.
Wayne Burke CSO
Sequrit CSI, Holland

1230 Networking luncheon

1330 **Session Five**
Technical live demo: Securing integrity with forensic computing
Investigators use a variety of techniques and proprietary software forensic applications to examine the copy, searching hidden folders and unallocated disk space for copies of deleted, encrypted, or damaged files. It is about identifying, preserving, analysing and producing evidence that is admissible in court. This presentation will focus on technical overview of designing computer forensic methods to ensure trustworthy and secure systems within all computing applications against internet and network threats.
Mohd Zabri Adil Talib Head of Digital Forensics
Cyber Security Malaysia, Malaysia

1500 **Session Six**
Technical live demo: Memory forensics and security analytics
Memory analysis is a crucial skill while analysing network intrusions. Attackers use rootkits, file wiping, timestamp adjustments, privacy cleaners, and complex malware to hide their tracks. The presenter will share his experience, regarding the challenges faced while setting up a security analytics engine. Memory forensics can also contribute in enhancing the capabilities of security analytics. Security analytics allows security investigation teams to do automated detection of threats, which generally remain undetected by traditional security tools, e.g. SIEM, AV, IDS etc. This presentation will also include live demo showing some of the memory forensics techniques.
Fahad Ehsan Associate Director- Security Research and Analytics
UBS, Singapore

1630 **Afternoon refreshments**

1650 **Session Seven**
The state of net
IT threat landscape and the mobile malware scene has become a norm in Malaysia with the rising cases of infection by computer virus. This presentation will show a malware infection demo in which it highlight how a malware could drop a payload in your system and hijack for money.
Goh Su Sim Threat Insight manager
F-Secure, Malaysia

1750 **End of Day Three**