SICW
Singapore International
Cyber Week

INTERNATIONAL
IOT SECURITY ROUNDTABLE

8 October 2020

PROGRAMME GUIDE

HELD IN

SG singapore
Passion Made Possible

ORGANISED BY

CSA SINGAPORE

EVENT PARTNER

image engine

SICW Singapore International Cyber Week

INTERNATIONAL IOT SECURITY ROUNDTABLE

8 October 2020

SICW INTERNATIONAL IOT SECURITY ROUNDTABLE

DATE 8 October 2020 **TIME** 3.00pm – 5.20pm

The event serves as a platform that brings together representatives from the public and private sector as well as the academia to galvanise global efforts towards a secure IoT ecosystem. It provides an avenue for countries to push the envelope in addressing the challenges of IoT security resulting from the proliferation of IoT and the lack of security provisioning in such devices.

8 OCTOBER 2020 – INTERNATIONAL IOT SECURITY ROUNDTABLE

TIME	PROGRAMME
1500 – 1510 (10 min)	**OPENING ADDRESS** **Dr. Janil Puthucheary** Senior Minister of State, Ministry of Communications and Information, SMS-in-charge of Cybersecurity
1510 – 1525 (15 min)	**1ST KEYNOTE : IoT Security Measures** **Mr. Yasuo Tawara** Director-General for Cybersecurity, Ministry of Internal Affairs and Communication, Japan
1525 – 1540 (15 min)	**2ND KEYNOTE : Secure IoT Ecosystem: Can we make it happen?** **Mr. Hudi Zack** Chief Executive Director, Technology Unit, Israeli National Cyber Directorate
1540 – 1555 (15 min)	**3RD KEYNOTE : Securing Industrial IoT in Operational Environment** **Mr. Paul Forney** Chief Security Architect, Schneider Electric
1555 – 1600 (5 min)	**Intermission**
1600 – 1720 each **Panellist** (10 min) **Discussion** (40 min)	**PANEL DISCUSSION** *Moderated by:* **Mr. Goh Eng Choon** President (Cybersecurity Systems Group), Info-Security, ST Engineering i. **IoT Security Reference Architecture** **Prof. Lam Kwok Yan** Professor, School of Computer Science and Engineering, Director, Nanyang Technopreneurship Centre, Nanyang Technological University ii. **Identity Management of IoT devices** **Mr. Francis D'Souza** Head of Strategy for Analytics & IoT Solutions, Thales iii. **Software Security Assurance in a post-COVID era** **Mr. Brian Fletcher** Director (Policy), BSA (the Software Alliance) iv. **Protecting enterprise and consumers using Collaborative AI** **Prof. Nicholas Allott** Founder/CEO, NquiringMinds

KEYNOTE SPEAKERS

Mr. Yasuo Tawara

Director-General for Cybersecurity, Ministry of Internal Affairs and Communications of Japan

IOT SECURITY MEASURES

Cyberthreats in IoT devices have been globally increasing in recent years. MIC Japan amended the rule in order to address the issue and started the nation-wide project, called "NOTICE", for identifying the vulnerable IoT devices on the Internet last year, which has been drawing a lot of attention from other countries. This presentation introduces our policy initiatives to ensure IoT security including the NOTICE project.

Biography

Mr. Yasuo Tawara joined the Ministry of Internal Affairs and Communications (MIC), Japan in 1988. He has been in charge of ICT policy for more than thirty years, consistently. Mr. Yasuo Tawara was appointed as Director-General for Cybersecurity, Ministry of Internal Affairs and Communications of Japan, MIC. He has been in his current position as Director-General for Cybersecurity since July 2020.

Mr. Hudi Zack

Chief Executive Director Technology Unit, Israeli National Cyber Directorate

SECURE IOT ECO-SYSTEM – CAN WE MAKE IT HAPPEN?

The rapidly evolving IoT arena creates many opportunities but also presents an enormous attack surface which to date holds the IoT technology's users completely exposed. This unfortunate situation enables perpetrators with various malicious motivations to exploit the weaknesses of this complex eco-system and breach the IoT platforms. Mr. Zack's presentation will discuss some of the unique challenges that prevent the different stakeholders from making meaningful progress despite significant efforts that were invested in this area over the last decade. It also tries to outline some new ideas as to government entities' contribution that, if further developed and adopted, can improve IoT resiliency in the national level.

Biography

Since early 2018 Hudi Zack is leading the Technology Unit in INCD, in charge of all the R&D activities in the directorate. Hudi brings to INCD over 30 years of experience in leading Hi-tech business and technology organizations, demonstrating both strategic and execution excellence.

Before joining INCD, Hudi was the Chief Operating Officer (COO) of Cytegic, a Cyber-Security start-up. Before Cytegic, Hudi founded and led the Cyber activity of Verint (NASDAQ – VRNT). Prior to his tenure in Verint, Hudi filled key senior positions in some of the leading Israeli high-tech companies, including Amdocs (NYSE-DOX) where he served as the Division President of the Billing Product Unit. Prior to Amdocs, Hudi was the COO of Metalink (NASDAQ – MTLK), a fabless semiconductor company.

Hudi holds a master's degree in Electrical Engineering from Tel-Aviv University (Summa Cum Laude) and a bachelor's degree in Mathematics and Physics from the Hebrew University in Jerusalem (Cum Laude, as a member of Talpiot program).

KEYNOTE SPEAKERS

Mr. Paul Forney
Chief Security Architect,
Schneider Electric

SECURING INDUSTRIAL IOT IN THE OPERATIONAL ENVIRONMENT

The industrial Internet of things enables the collection and contextualization of data from sources close to the cyber-physical processes to enterprise level workflows of the business for intelligent analytics and increased responsiveness. In conjunction with a platform that enables Industry 4.0, it has the potential to bring the entire supply chain together with high availability and turn industrial functions into smart operations. Digitization enables the benefits of agile production, optimized scheduling and the ability to give cyber-physical systems the capability to make decisions on their own and perform their tasks as autonomously as possible.

Mr. Paul Forney, chief security architect of Schneider Electric (a global leader of end-to-end industrial products, systems and solutions) highlights the unique challenges of securing this new vision of the future and the fundamental characteristics that must be present in the design to mitigate them.

Biography

In addtion to being the Chief Security Architect for Schneider Electric, Mr. Forney is a founding board member of the ISA Security Compliance Institute (ISCI) which develops the conformance specifications to the IEC 62443 Industrial Control Systems cyber security suite of standards and has held the Co-chair position for the Research and Development Sub-group of the Department of Homeland Security Industrial Control System Joint Working Group. He has been an advisor to the White House Cyber Security Office, the National Security Council, the Department of Justice, the Department of Energy, NERC and FERC.

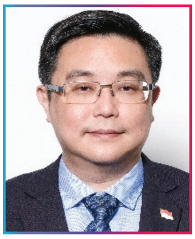
Paul was a primary contributor in the ISA99 WG4 TG6 committee that wrote the IEC 62443-4-1 world wide standard for secure development in industrial automation. He has been a guest speaker on the subject of the Security Development Lifecycle and incident response in industrial control and cyber physical systems at national and international conferences including Microsoft PDC, Gartner, SANS, ICSJWG, AFPM, API, RCMP, S4 and Public Safety Canada. He was given the honor of being the keynote speaker at the NDSS 2020 premier conference for cybersecurity in Academia and as well the CENTCOM conference at the US Central Command. Additionally, he works closely with the ICS/US-CERT/DISA organizations on control system vulnerabilities and forensics with cyber researchers around the globe.

Mr. Forney has been awarded eleven patents in failure prediction for upstream Oil and Gas, power grid balancing and industrial Internet portal technologies; and for thirty years has been involved in the design, security and implementation of SCADA, Event Driven/Service Oriented Architecture (EDA/SOA) and distributed control software and systems for industrial automation.

Paul is a strategic member of the CyManII institute (Cybersecurity for Energy Efficient Manufacturing), funded by a $70M grant from the DOE. He was recently appointed to the Trustworthy and Secure Cyber-Plexus (TSCP) Scientific Advisory Board and has been an active member of the Microsoft Azure Advisory Board. He has served on the Board of Advisors for Cylance, Inc. and Virsec, Inc., two fast growing and innovative cyber security companies.

Paul is a certified Information Systems Security Professional (CISSP), a certified Information Systems Security Architect Professional (ISSAP), a certified Secure Software Lifecycle Professional (CSSLP), a certified Malware Reversal Analyst (GREM) and an accomplished jazz musician.

MODERATOR



Mr. Goh Eng Choon
President, Cybersecurity Systems Group, Info-Security, ST Engineering

Biography

Mr Goh Eng Choon is the President Cybersecurity Systems Group in ST Engineering. A leading cybersecurity company that provides comprehensive suite of future ready solutions for commercial enterprises, government agencies and critical infrastructures.

He has since lead the company to deliver a full spectrum of cybersecurity solutions both in Singapore and abroad. These projects included the build, operations and maintenance of the National Authentication Framework System providing Two Factor Authentication services at the national level for all e-government services and some financial institutions. The company has successfully design, build and operate over 17 Security Operations Centre (SOC) in local and overseas. Abroad, Eng Choon has lead and won the contract to design Sri Lanka's first National SOC for the government of Sri Lanka which was completed in 2017. The Advanced Cybersecurity Operations solution detect and respond to cyber-attacks at both Information Technology (IT) and Operational Technology (OT) networks. It is equipped with cognitive capabilities driven by Threat Intelligence to enhance cyber threat detection with speed and accuracy.

Eng Choon understood the core success factor to level up the cybersecurity preparedness and competencies in any organisation and countries is to ensure sufficient cybersecurity competent professionals to support the growing demand. Under his leadership, he has initiated the formation of an operational based cybersecurity training modelled from military experience. The 'live firing' experience allows trainees to experience, learn and respond to cyber threats with realism of an actual cyber-attack in an Organisation. In June 2014, the company launched the first cybersecurity training centre in Singapore under the name DigiSAFE Cyber Security Centre which later rebranded to ST Engineering Cybersecurity Academy (STECA), offering IT, OT and Leadership Executive cybersecurity training courses. To date, it has trained more than 150 organisations locally and overseas.

His previous appointments as a military officer in the Singapore Armed Forces (SAF) for 15 years, last appointment being Head of Plans for the Army Integrated Knowledge-based Command and Control Office (Army IKC2 Office). Responsible for all Command, Control, Communications and Computerization (C4) developments across the entire Army and all medium and long term development plans, strategy, budget allocation. Eng Choon was also a Managing Director of an SME specialising in security, command and control.

Eng Choon was awarded a training award by the SAF to attain a Bachelor's degree in Electrical & Electronic Engineering from National University Singapore. He was also awarded a SAF Postgraduate Scholarship in 2001 to attain a Master of Science in Information Studies from Nanyang Technological University. He has also completed the Stanford Executive Programme in Stanford University this 2016. Eng Choon has served as the chairman of Cyber Security Chapter in SG Tech for two years, a premier trade association for the tech industry that develops sustainable initiatives to grow and strengthen the technology industry. He is also appointed by the Minister-In-Charge of Cybersecurity as a member of Cybersecurity Advisory Group (CAG), a group of eminent cybersecurity experts whose expertise may tap upon for cybersecurity issues in the fast evolving cybersecurity landscape including cyber threats that confront Singapore.

PANEL EXPERTS

Prof. Lam Kwok Yan
Professor, School of Computer Science and Engineering, Director, Nanyang Technopreneurship Centre, Nanyang Technological University

IOT SECURITY REFERENCE ARCHITECTURE

IoT systems are generally characterized as large-scale complex distributed systems without a clear notion of network perimeter between the system components. Large-scale geographically distributed deployment of nodes and a diversity of operating environments result in complex threat scenarios. A new security architecture for guiding the design of IoT systems, which is fundamentally different from traditional enterprise security architecture, is needed. To address the characteristics of IoT systems, we adopted an approach that considers the IoT security framework from three complementary viewpoints, namely, Activity-centric (A), Network-centric (N) and Things-centric (T) perspectives. We propose an IoT Security Reference Architecture, linking the three perspectives to assist in comprehending, selecting, and using appropriate security control measures for complex IoT use cases in practice.

Biography

Professor Lam is a Professor of Computer Science at the School of Computer Science and Engineering and Director of the Nanyang Technopreneurship Center, Nanyang Technological University (NTU), Singapore. He is currently the Director of the Strategic Centre for Research in Privacy-Preserving Technologies and Systems (SCRIPTS), and Director of NTU's SPIRIT Smart Nation Research Centre. He served as the Program Chair (Secure Community) of the Graduate College of NTU 2017-2019. Professor Lam has been a Professor of the Tsinghua University, PR China (2002-2010) and a faculty member of the National University of Singapore and the University of London since 1990. He was a visiting scientist at the Isaac Newton Institute of the Cambridge University and a visiting professor at the European Institute for Systems Security. In 1997, he founded PrivyLink International Ltd, a spin-off company of the National University of Singapore, specializing in e-security technologies for homeland security and financial systems. In 2012, he co-founded Soda Pte Ltd which won the Most Innovative Start Up Award at the RSA 2015 Conference. In 1998, he received the Singapore Foundation Award from the Japanese Chamber of Commerce and Industry in recognition of his R&D achievement in Information Security in Singapore. Prof Lam received his B.Sc. (First Class Honours) from the University of London in 1987 and his Ph.D. from the University of Cambridge in 1990. His research interests include Distributed and Intelligent Systems, Multivariate Analysis for Behavior Analytics, Cyber-Physical System Security, Distributed Protocols for Blockchain, Biometric Cryptography, Homeland Security and Cybersecurity.

Mr. Francis D'Souza

Head of Strategy for Analytics & IoT Solutions, Thales

IDENTITY MANAGEMENT OF IOT DEVICES

IoT is creating a revolutionary new way of working and living, powered by a multitude of connected machines and devices, sharing data and turning it into business intelligence.

However, the IoT does not come without its challenges. With billions of connected devices, the possibilities of vulnerabilities and cyber-attacks are increasing dramatically. All industries are open to cyber-attacks against critical infrastructures, instigated to steal valuable sensitive data, alter industrial control systems, shut down operations and cause maximum damage. All it takes is one open door and the whole ecosystem can be affected in seconds.

To fully embrace the IoT and its promise of simplicity, optimization and cost efficiency, IoT providers need to mitigate threats at every level of IoT systems. By building a foundation of trust that underpins the entire ecosystem, they can protect what matters, where it matters and when it matters most. IoT Device Identity and its management is at the root of that Trust.

Biography

Mr. Francis D'Souza is Head of Strategy for Analytics & IoT Solutions at Thales. The Business Line supports customers in critical sectors such as energy, healthcare and manufacturing by leveraging Thales' market-leading cellular communication, security and analytics technology and expertise to implement successful digital transformation strategies.

Francis engages with IoT customers in Utilities, Healthcare and Connected Factories around the world. He helps implement strategies which enable cellular IoT roll outs to be successful while ensuring security and RoI, and helping to minimise Total Cost of Ownership (TCO).

Francis has worked in Siemens and Gemalto, which was acquired by Thales in 2019, in a range of roles from telecommunications, IoT, cybersecurity and AI. Besides being a telecoms engineer, he has also served in a variety of roles in sales, product marketing and business strategy in Mumbai, London and Paris.

On weekends, Francis enjoys pottering in his kitchen and trying out traditional Goan recipes. Francis is currently based in Paris.

Singapore International Cyber Week

INTERNATIONAL IOT SECURITY ROUNDTABLE

8 October 2020

PANEL EXPERTS

Prof. Nicholas Allott

Founder & CEO, NquiringMinds

PROTECTING ENTERPRISE AND CONSUMERS USING COLLABORATIVE AI

Your systems can be breached regardless of how strong your defences are. The ability to detect and rapidly respond to incidents is essential. Artificial Intelligence has an important role to play here; there is a broad portfolio of techniques from basic statistics to Deep Learning, which can help detect anomalies and even help implement mitigating strategies. However, these techniques need data at scale, and we will only achieve this through industry collaboration. Professor Allott will give an overview of the most promising AI techniques, technical architecture for the deployment and highlight the international need for collaboration in this area.

Biography

Prof. Nicholas Allott is an IoT Security Foundation Ambassador and CEO of NquiringMinds, a company with deep experience in AI, IOT and security. Nick was formerly the CTO of OMTP, which published over 30 mobile industry technical specifications including TR0/TR1 Trusted Execution Environment, which forms the security basis of many of PC and mobile technologies we use today. He is also the Director of the Webinos Foundation a secure IOT open source collaboration including W3C, Sony, Samsung, BMW, Deutsche Telekom, Telefonica and 20 international organisations. In an independent peer review webinos was deemed to be the most secure of 22 reviewed IOT middleware frameworks. Nick also participates in the UK Governments Secure by Default Expert Group.

Mr. Brian Fletcher

Director (Policy), BSA (the Software Alliance)

SOFTWARE SECURITY ASSURANCE IN A POST-COVID ERA

Software and cloud-based services have been an essential part of the solution for governments and businesses to help communities respond to and recover from the COVID-19 pandemic. As a society we are more reliant than ever before on the security and integrity of software. The global software community is identifying best practices that help software developers address important aspects of software security, including security-by-design principles and secure development lifecycle processes. Based on these, BSA developed the Framework for Security Software to help software development organizations improve the security of products throughout their entire lifecycle. The framework provides a tool for stakeholders, from IOT device manufacturers to policymakers, to evaluate security of IOT software.

Biography

Brian Fletcher is Director, Policy – APAC based in BSA's Singapore Office. Working closely with BSA member companies, he manages BSA's policy and government affairs initiatives in the APAC region, with a focus on Australia, China, India, Japan, Korea, and South East Asian countries.

Prior to joining BSA, he was Director of Government Affairs (APJ) for Symantec Corporation. Prior to joining the private sector he served for 21 years in the Australian Government across a number of portfolios. Most recently he was the inaugural Director of Cyber Security Policy and Relationships in the Australian Cyber Security Centre and before that he served in the Australian Embassy in Washington, DC, as the Counselor Defence and Cyber Policy.

Fletcher has an MBA from the Australian Institute of Business in Adelaide (Australia), and a Bachelor of Science with Honours in Neuroscience from the Australian National University in Canberra. He also holds professional privacy certifications (CIPPE and CIPM) with the International Association of Privacy Professionals.