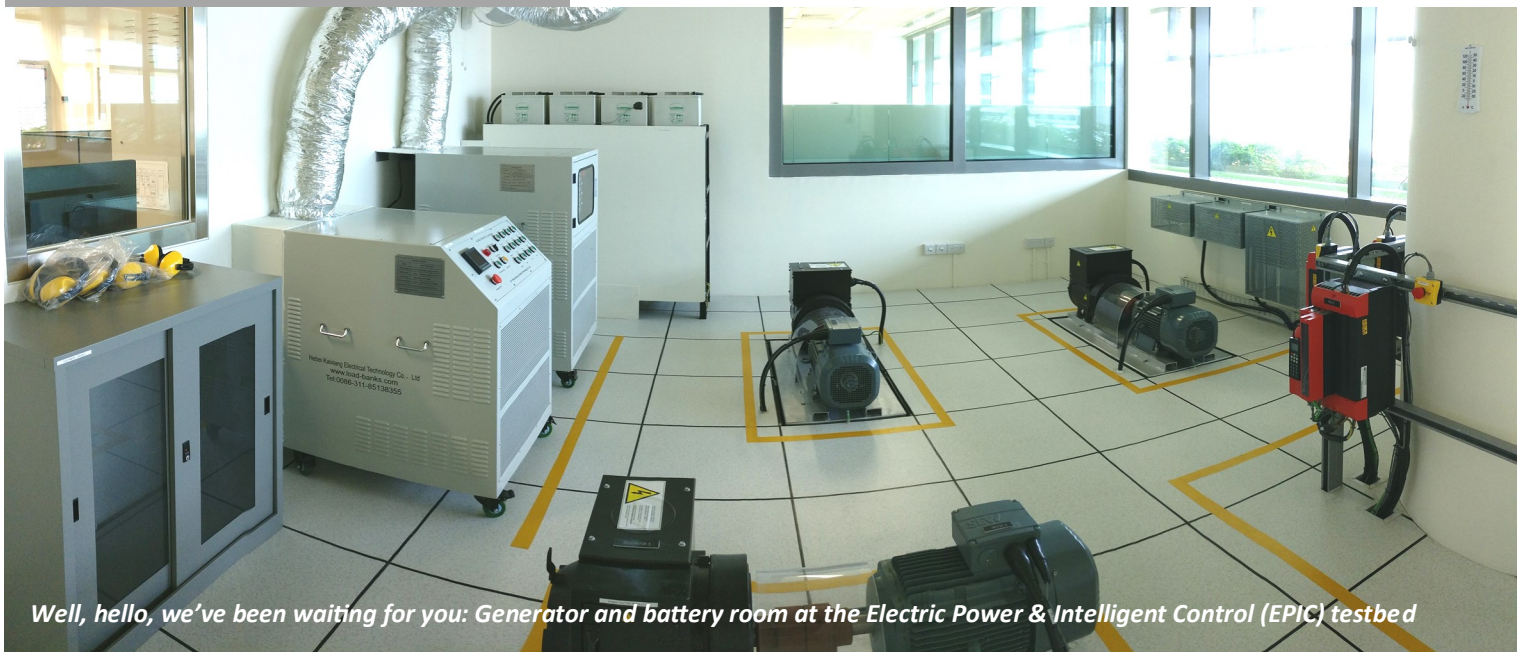
An iTrust Newsletter Apr - Jun 2017 | Issue 9

iTrust Times

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT

From Centre Director's Desk



Well, hello, we've been waiting for you: Generator and battery room at the Electric Power & Intelligent Control (EPIC) testbed

Dear Reader:

Greetings from iTrust!

Welcome to the 9th issue of iTrust Times. This issue also marks the second anniversary of iTrust Times that offers its readers a glimpse into iTrust. Thanks to Mark Goh who has steadfastly worked to ensure that no issue is missed and no one who likes to browse this newsletter misses it.

In the early part of 2017 we have received international recognition of the work done by iTrust researchers. Congratulations to (a) David Yau, Yang Li (ADSC), and Rui Tan (NTU) for winning the best paper award at IPSN 2017 for their paper "Natural Timestamping Using Powerline Electromagnetic Radiation," (b) Martin Ochoa, Nils Tippenhauer, Yuval Elovici and their co-authors from Ben Gurion University for winning the best paper award for "SIPHON: Towards Scalable High-Interaction Physical Honeypots" at the ACM Asia Conference on Computer and Communications Security, and (c) the best Poster Paper Award (Internet of Things Track) for the paper "ProfilIoT: A Machine Learning Approach for IoT Device Identification Based on Network Traffic Analysis" at the ACM Symposium on Applied Computing.

The third Secure Cyber Physical (SCy-Phy) Systems Week will be held at iTrust during June 5-9, 2017. Nils Tippenhauer is leading a team of faculty, researchers, and staff to organize various events during the week. This edition of SCy-Phy week will include an extended 2-day Think-in session, a SUTD Security Showdown'17 (S317) event, invited talks, and outreach events. Keynote address at the Think-in session will be delivered by Mr Neil Hershfield, U.S. Department of Homeland Security, Deputy Director, Industrial Control Systems Cyber Emergency Response Team.

I am happy to report that the fourth iTrust testbed, namely, the Electric Power and Intelligent Control (EPIC), is now complete and available to researchers. A formal opening of the testbed by Mr Ng Wai Choong, Chief Executive, Energy Market Authority, is scheduled for May 22, 2017.

On behalf of iTrust, I convey my deepest condolences to family members of COL Charles Ngoh Sien Sen who passed away on March 25, 2017. Col Charles oversaw all activities of iTrust. He was a true friend and led the growth of iTrust since his attachment. We will miss him!

That's all for now folks! Thanks for browsing this newsletter!

Best wishes,

Aditya Mathur
Professor and Head of Information Systems Technology and Design Pillar, and
Centre Director, iTrust

In This Issue

Events

Since 2015, the **Secure Cyber-Physical Systems (SCy-Phy) Week** has been held annually at SUTD. Over the past two years, 20 international cyber security experts from renowned academic institutions and companies had been invited as guest speakers. This year promises another 12. SCy-Phy Systems Week will run from 5 to 12 June.

SCy-Phy Systems Week 2017

SCy-Phy 2017 will encompass an extended **two-day Think-in** event for an in-depth discussion on pressing CPS issues and innovative solutions (we heard you!), the return of the highly successful **SUTD Security Showdown'17 (S317)**, and a number of invited talks, training sessions and outreach workshop for students. Visit https://itrust.sutd.edu.sg for updates on SCy-Phy Systems Week 2017.

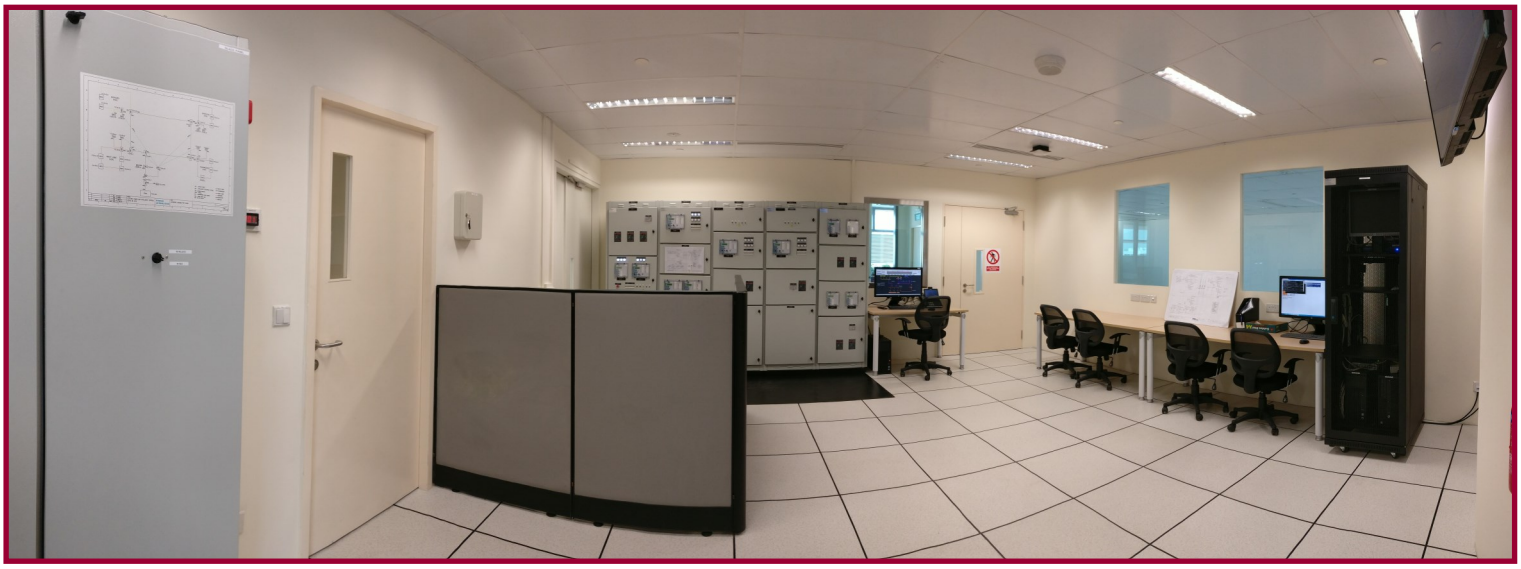
The S317 consists of two main phases, an online qualifier, and a live event held at SUTD. During the live event, participants will have a chance to attack our SWaT testbed with the goal to reach a number of defined challenges. A technical report on the first S3 event, held in 2016, can be found at iTrust's website.

Research Focus

Electric Power & Intelligent Control testbed

iTrust proudly presents to our collaborators, researchers and readers its fourth testbed — the Electric Power and Intelligent Control (EPIC)! This newest fixture, fully operational since late-Mar 2017, adds to a panoply of world class testbeds at iTrust that have borne much fruit in the form of know-hows, toolkits, publications and patents, as well as generated interest from local and international academia, industry and government agencies.

EPIC comprises four stages of Generation, Transmission, Micro-grid, and Smart Home. Each stage has its own switches, PLCs, power supply unit, protection and communication systems in a fibre optic ring network. High-availability Seamless Redundancy and Media Redundancy Protocol (MRP) switches are used in the ring network for redundancy purposes. EPIC uses the IEC 61850 communication protocol for electrical substation and automation systems. Generic object oriented substation event (GOOSE) and Manufacturing message specification (MMS) are used in EPIC ring network for data transfer between relays and SCADA.



Room with a view: EPIC's control room where the SCADA server and distribution board are located

The Generation stage consists of power source from SUTD's grid, three generators, photovoltaic cells (PV) and batteries. An autotransformer is used to step up the voltage from the transmission to distribution station before consumption. Smart meters with Advanced Metering Infrastructure (AMI) are installed at several locations throughout the EPIC grid to measure the kWH consumed by generators, PV and the autotransformer.

WAGO is selected as the PLC to control the opening/ closing of breakers and loading. Communications in EPIC are divided into five sections: Generation, Transmission, Micro-Grid, Smart Home and SCADA. 114 PV cells are installed on the rooftop, with inverters to convert the solar power to electrical energy and feed it into the testbed. Batteries are used to supplement power supply to EPIC in the event of a blackout or low energy conversion owing to cloud cover.

EPIC is connected, and can supply power, to the Secure Water Treatment (SWaT) and Water Distribution (WADI) testbeds. The addition of EPIC adds a jewel to the crown: these three interconnected testbeds give researchers a unique platform to investigate how and what types of cascading effects that cyber attacks on an upstream power plant can have on downstream critical infrastructure, and ways to shore up their security and resilience. EPIC will also support experimental investigation into the cyber security aspects of the distributed cyber components controlling the physical components such as generators and transformers. We invite interested parties to conduct collaborative research with us in this newest fixture!

Close quarters: EPIC's transformer and inverter room

ACM Asia Conference on Computer and Communications Security 2017

Four papers were presented at AsiaCCS, in Abu Dhabi, UAE. In **"SIPHON: Towards Scalable High-Interaction Physical Honeypots"**, research assistant Amit Tambe elaborated on the SIPHON architecture. Seven network devices, presented as 85 real IoT devices on the Internet acting as honeypots recorded over 400 brute-force login attempts via more than 1,800 distinct credentials, from which 11 attempts were successful. Based on the amount of traffic, it was confirmed that location mattered when it came to how attractive a target is to an attacker. **The paper received the Best Paper Award.** Well done!

PhD student Chuadhry Mujeeb Ahmed presented **"Model Based Attack Detection Scheme for Smart Water Distribution Networks".** The paper detailed a case study on a model-based attack detection procedures for CPS and simulation of a water distribution network. Using EPANET data and sub-space identification techniques, an input-output Linear Time Invariant model for the network was obtained, which in turn was used to **estimate the evolution of the system dynamics and for attack detection.**

In **"IoTScanner: Detecting Privacy Threats in IoT Neighborhoods"** research assistant Sandra Siby presented the use of a scanner that performs **local reconnaissance of existing wireless infrastructure and participating nodes**. Other than enumerating such devices and identifying connection patterns, the IoTScanner could be used to investigate metrics - while maintaining privacy - that could be used to classify devices and identify privacy threats in an IoT neighborhood. The long term goal is to turn the IoTScanner into a convenient hand-held device.

Postdoc researcher Vinay Sachidananda in **"Let the Cat Out of the Bag: A Holistic Approach Towards Security Analysis of the Internet of Things"** presented preliminary efforts in the **security analysis for IoT devices,** using such penetration testing methodologies as port scanning, fingerprinting, and vulnerability scan - via a security IoT testbed. Design, requirements and the architecture to support security analysis in the testbed were also discussed. More complex security analysis by developing new attack and defence models are being planned.

SUTD and BGU researchers collaborated to develop a novel method adopting machine learning on network traffic analysis to identify IoT devices in a given organisation. A poster on the work, **ProfilIoT**, was presented at the conference in Marrakech, Morocco, and they were rewarded with the **Best Poster Paper Award (Internet of Things Track).** Well done!

Research assistant Toh Jing Hui's paper on **"Cyber Security Patrol – Detecting Fake and Vulnerable WiFi-Enabled Printers"** demonstrated how an application the team developed could be used to detect unsecured wireless connection, mimic a printer's Wi-Fi connectivity and then steal print jobs undetected. A video that demonstrates one of the use cases can be found here: https://www.youtube.com/watch?v=aJ2ZG04BrjM. Provisional patent was filed for the resulting technology, ProfilIoT (see below).

Cyber Security Training Workshop

iTrust conducted two training workshops on **Introduction to Cyber Security** for about 100 professionals from the Defence Science and Technology Agency (DSTA) in Feb. The topics covered were comprehensive: cryptography, security in hard- and software, network, OS, IoT, ICS and cloud. Self-assessment quizzes also helped ingrain the participants' learning experience. Asst Profs Martin Ochoa and Nils Tippenhauer, experts in cyber security, were the workshop conductors.

Asst Prof Martin Ochoa walks through the participants on the challenges in cybersecurity

Provisional Patents

In addition to the those reported in the previous issue, iTrust has applied for **provisional application for two more technology inventions** in the IoT sphere. These are described below.

ProfilIoT (Singapore Application No.: 10201701692Y)

Inventors: Yair Meidan, Michael Bohana, Asaf Shabtai,

Juan Guarnizo, Martín Ochoa, Nils Tippenhauer, Yuval Elovici

With a significant proliferation of IoT devices and their integration into systems, it is necessary to identify them in cooperatives networks. ProfilIoT, therefore, provides a flexible, generic, and efficient solution to evolve IoT landscape in different environments. This novel method **uses network traffic analysis to distinguish between IoT and non-IoT devices**. Moreover, the performed analysis could not be easily avoided by attackers due to advanced statistics metrics and machine learning techniques used to profile accurately each element connected to a network. ProfilIoT can recognise IoT devices with an effectiveness of 99%, and is flexible to be implemented in any organisation. This is jointly developed by researchers from iTrust, Singapore University of Technology and Design and Ben-Gurion University of the Negev (Israel).

Advanced Security Testbed Framework for Internet of Things Devices (Singapore Application No.: 10201609252U)

Inventors: Yuval Elovici, Nils Ole Tippenhauer Asaf Shabtai, and Shachar Siboni

The security testbed for IoT devices is an innovative **security testing framework** whose main objective is to **test an IoT device's security against a set of security requirements**, as well as to test its behavior under various conditions (e.g., when different applications are running). The testbed is designed to simulate environmental conditions in which the tested device might be operated, such as the location, time, lighting, movement, etc., in order to detect possible context-based attacks (i.e., attacks that are designed to be triggered when the device is in a specific state) and data attacks that may occur as a result of sensor manipulation. The testbed employs advanced security tools and mechanisms from several domains, including network security, penetration testing, vulnerability and risk analysis, machine learning for advanced analysis, and more. The security testbed for IoT devices is physically deployed and operated at the IoT Security Lab, located at iTrust.

iTrust Seminar Series

Prof Ahmad-Reza Sadeghi

The emerging and much-touted Internet of Things (IoT) under the slogan "connecting the unconnected" presents a variety of security and privacy challenges in a broad spectrum of application domains, ranging from large-scale smart energy grids to smart vehicles, homes and personal wearable devices.

Prominent among these challenges is the establishment of trust in remote IoT devices typically attained via remote attestation, a distinct security service that aims to ascertain the current state of potentially compromised remote devices. However, recent studies have revealed many security vulnerabilities in embedded devices that are core components of the IoT. On the other hand, established protection measures for traditional computing platforms and networks may not always directly apply to IoT due to their diversity, resource constrains and large scale.

In "Things, Trouble, Trust: On Building Trust in IoT Systems", Prof Ahmad-Reza Sadeghi from Technische Universität Darmstadt on 23 Mar talked about surveying the landscape of the recent research on security architectures and particularly scalable remote attestation schemes for IoT devices. He also discussed their effectiveness and related tradeoffs as well as future research challenges and directions.

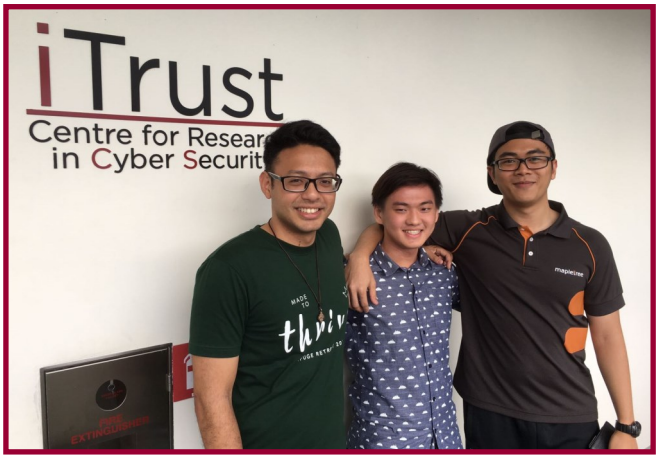
Sebastien Banescu

Software obfuscation transforms code such that it is more difficult to reverse engineer. However, it is known that given enough resources, an attacker will successfully reverse engineer an obfuscated program. Therefore, an open challenge for software obfuscation is estimating the time an obfuscated program is able to withstand a given reverse engineering attack. **Sebastien**

Banescu's talk on "Characterising the Strength of Software Obfuscation Against Symbolic Execution Attacks" presented the key software characteristics for estimating the time needed by symbolic execution attacks, to recover a hidden secret key inside obfuscated software.

Student Internships

iTrust regularly receives internship requests from schools or directly from highly motivated students who are keen to explore or increase their knowledge in cyber security. Two such students, **Riley Hale Aeria** (Singapore Polytechnic) and **Aaron Seah**, while waiting to begin his National Service, interned at iTrust in recent months.



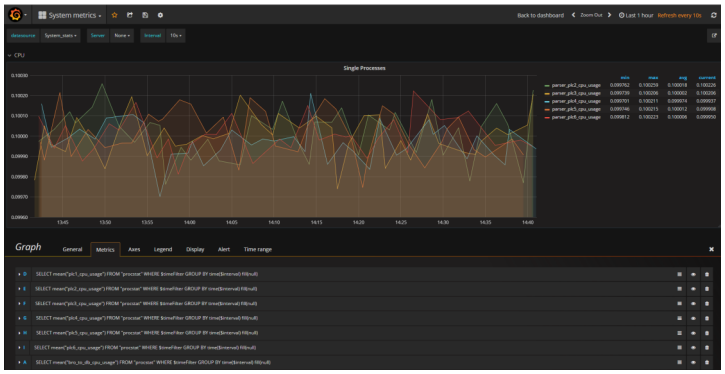
Aaron (center), with his supervisor Research Officer Franciso Furtado (left), and former iTrust intern Muhammad Syuqri

Having completed his 'A' Levels, Aaron was tasked with developing a better understanding of **ransomware** during his two-month internship, with guidance from Research Officer Francisco Furtado. Even without prior coding experience or knowledge, his interest helped him quickly master Python and encryption methods to design and create his own ransomware. This ransomware targeted two main groups of people: corporations and the elderly. Once installed, the ransomware would talk through important directories on the victim's computer and encrypt document (pdf) and picture (png and jpeg) files with 128-bit AES encryption. With the files encrypted, a ransom message will be displayed on the victim's computer until the victim pays the ransom sum, usually in the form of Bitcoins, to a specified PayPal account.

Recent high-profile news of the ransomware WannaCry running amok in computers worldwide drives home the importance of understanding how ransomware works and ways to prevent being held hostage.

Riley is a 3rd year studying pursuing a Diploma in Information Technology at Singapore Polytechnic. Riley's keen interest in cyber security and IoT saw him enrolled as a student researcher with iTrust from Oct 16 to Feb 17. Under the tutelage of iTrust's Senior Specialist Kaung Myat Aung, Riley impressively mastered Python and a suite of protocols in the space of three months, including several **Distributed Message Queuing Protocols** (MQTT, ZeroMQ etc.) and their respective authentication and encryption protocols (CurveZMQ, TLS). The **encryption protocols** ensured that cyber attackers were unable to interrupt or eavesdrop the data collected and transferred. Sensor time series data collected from the SWaT testbed was retrieved and stored using InfluxDB installed on a Raspberry Pi. Together with Telegraf - a plugin-driven server agent for collecting and reporting metrics - and Grafana - an open source **metric analytics and visualisation** suite - the SWaT data was visually represented (see below).

Riley's research has three advantages: (a) it ensures that data collected are transmitted and communicated between devices in a CPS in a secured manner; (b) the trusted data can be used by data scientists for developing more advanced machine learning algorithms; and (c) data visualisation for ICS operators for sense making.

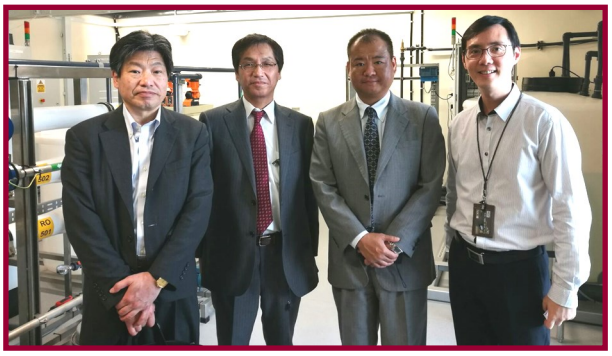


Screenshot of visualised data collected from SWaT

Visits

The past few months saw a steady stream of visitors from across the world, from Japan to Dubai, Brazil and the US.

- **17 & 20 Feb:** **Dubai Electronic Security Center (DESC)**, the government agency responsible for Cyber Security in Dubai, and **NEC Corporation** visited iTrust on 17 and 20 Feb, respectively, to explore collaboration opportunities including joint research projects.



(Left to right): Dr Keiji Yamada, Mr Akira Kon, Mr Takuya Mori with Ivan Lee at the SWaT testbed

- **23 Feb:** During the 12th Technology Working Group (TWG) bilateral meeting between the Singapore Ministry of Defence (MINDEF) with the **US Air Force Research Laboratory (AFRL)**, a tour to iTrust was arranged. The delegation was led by Mr C. Douglas Ebersole, Executive Director of AFRL. Centre Director Prof Aditya Mathur hosted the visit and gave an introduction of iTrust, with the Co-PIs and researchers of iTrust research projects briefing the guests on their work.

Mr C. Douglas Ebersole (first row, center), amongst the delegation from AFRL and MINDEF at the briefing by iTrust

- **28 Feb:** Chairman & CEO Mr Yves Meignié and his team from **VINCI Energies** — a transport infrastructure concession operator — were given a briefing on SUTD and research capabilities as well as a tour of the labs at SUTD, including iTrust's.

- **22 Mar:** A **senior delegation from the government of Brazil**, accompanied by Custodio Technologies Pte Ltd, visited iTrust to learn our advanced research and contribution to the cybersecurity ecosystem of Singapore. The Brazilian delegation was very impressed by what it saw, and would examine ways to promote similar initiatives in Brazil, including the promotion of future cooperation.

Ivan with the Brazilian and Israeli visitors

- **29 Mar:** As part of iTrust's continuing efforts to engage the Singapore government in Smart Nation initiatives, the **Energy Market Authority's** Deputy Chief Executive Mr Bernard Nee was invited to visit our cyber security testbeds.

Aditya explains iTrust's work to Mr Nee (third from right) with Aditya

- **25 Apr:** A delegation from **Kaspersky Lab** — Mr. Andrey Dukhvalov, Chief Strategy Architect and Head of FutureTech, Mr. Kirill Shiryaev, Global Head of Talent and Mr. Dmitry Postelnik, Head of Education Programs — expressed interest in exploring corporation with SUTD in education and research in cybersecurity including IoT and critical Infrastructure.

Tributes

COL Charles Ngoh Sien Sen

Col Charles, that is how we fondly referred to him, passed away on March 25, 2017. He was the Head SCG3 of the Future Systems and Technology Directorate (FSTD) of the Ministry of Defence (MINDEF). In this capacity, Col Charles oversaw all activities of iTrust. As the Centre Director, I had numerous opportunities to interact with Col Charles. One of the many traits that I admired in him was his patience to hear me out, ask questions, and respond logically to my requests.

He was an ardent supporter of iTrust events such as the Secure Cyber Physical (SCy-Phy) Systems Week and the many outreach programmes conducted by iTrust staff. He was always appreciative of the technologies being developed by iTrust researchers while encouraging us to translate the work into practice. Despite his extremely hectic schedule, and sometimes even when it was months before he met us, he kept track of iTrust activities through his colleagues at MINDEF and transmitted decisions to us through them. Focus on collaboration and technology translation seemed to be his mantra that helped iTrust grow into what it is today!

Col Charles was a true friend of iTrust. All who had interacted with him will miss him dearly.

John Charles Knight

John Knight passed away on February 23, 2017. John was a Professor at the University of Virginia in Charlottesville, USA. He was an invited speaker at the 18th IEEE High Assurance Systems Engineering conference organised by iTrust. Due to illness, he could not make it to the conference. John made numerous contributions to software engineering. One that made headlines relates to N-version Programming. In 1977 Liming Chen and Algirdas Avizienis conjectured that multiple versions of a program, written by independent programmers, will reduce the probability of identical software faults. However, this conjecture failed a statistical test conducted ably by John and Nancy Leveson as reported in their landmark paper titled “An experimental evaluation of the assumption of independence in multi-version programming” that was published in 1986. John contributed significantly to advance the field of Software Engineering through his work in formal methods. He received the prestigious Harlan D. Mills award “…for encouraging software researchers to focus on practical results as well as theory, and for critically analyzing their assumptions and evaluating their research claims.” John will be missed by many who knew him and of his work.

To explore research collaborations and outreach activities, feel free to contact the relevant iTrust staff listed.

iTrust Contact Information

Mr Kaung Myat AUNG, *Senior Specialist (Water)*
kaungmyat_aung@sutd.edu.sg

Prof. Yuval ELOVICI, *iTrust Research Director*
yuval_elovici@sutd.edu.sg

Mr Mark GOH, *Manager, iTrust*
mark_goh@sutd.edu.sg

Mr Ivan LEE, *Senior Associate Director, Cyber Security Technologies*
ivan_lee@sutd.edu.sg

Prof. Aditya P MATHUR, *Professor & Head of Pillar, ISTD Pillar & iTrust Centre Director*
aditya_mathur@sutd.edu.sg

MUHAMED Zhaffi Bin Mohamed Ibrahim, *Specialist (Power)*
zhaffi_ibrahim@sutd.edu.sg

Ms Angie NG
Deputy Manager, iTrust
angie_ng@sutd.edu.sg

Ms Priscilla PANG
Manager, iTrust
priscilla_pang@sutd.edu.sg

iTrust
Centre for Research in Cyber Security
https://itrust.sutd.edu.sg