

# iTrust Times

## From Centre Director's Desk



Dear Reader:

Greetings from iTrust, and welcome to the 8th issue of iTrust Times. On behalf of all iTrust-ians, I wish you a happy and prosperous 2017 and Chinese Year of The Rooster!

iTrust researchers and staff enter the new year with many accomplishments to their credit. The 18th High Assurance Systems Engineering (HASE) 2017 symposium is now behind us. For the first time in its 18-year history, HASE was brought to beautiful Singapore. This successful symposium served as host to 57 attendees from 15 countries. HASE was supported by sponsorships from Rhode & Scharwz, RSA, SUTD and TNO. iTrust played a major role in HASE through its sponsorship and providing organisational support all the way from the start of planning the symposium until its last day and beyond! My sincere thanks to all members of the programme and organising committees for their outstanding work. My special thanks to Ray Paul, Bojan Cukic, and Jie Xu for their continued dedication without which HASE would not be possible!

iTrust researchers have been prolific in publishing their outstanding work in top conferences. At the start of this new year, the good news is that we have four accepted papers at the [ACM Asia Conference on Computer and Communications Security \(ASIACCS\) 2017](#). Two papers have also been accepted for presentation at the CysWater workshop on Cyber-Physical Systems for Smart Water Networks. I congratulate Nils Tippenhauer, Stefano Galelli, David Yau, Mujeeb Chuadhary,

Venkata Reddy, and Carlos Murguia, and the international collaborators, for getting their work accepted at these prestigious venues, and encourage iTrust researchers to continue their excellent work.

In 2017 we will witness the addition of a new testbed in iTrust. The Electric Power and Intelligent Control (EPIC) testbed is undergoing its last round of testing. A March 29 inauguration is planned. EPIC will enable iTrust researchers and their international collaborators to broaden focus by including the design of secure power grid in their research agenda. For the curious, details of EPIC's design are available at the iTrust website.

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



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

### In This Issue

- ◆ 18th IEEE High Assurance Systems Engineering (HASE)
- ◆ iTrust Provisional Patents
- ◆ SWaT Security Showdown (S<sup>3</sup>) report
- ◆ SUTD-TNO Letter of Commitment signing

## 18th IEEE International Symposium on High Assurance Systems Engineering

iTrust had the honour of organising and hosting the **18th IEEE International Symposium on High Assurance Systems Engineering (HASE)** from 12 to 14 January 2017. Held at the magnificent Grand Copthorne Waterfront Hotel, this was the first time HASE was held in Singapore, and only the third in Asia since the first HASE in Niagara, Canada in 1996. HASE is sponsored by the IEEE Computer Society.



*Dr Tan Guan Hong at his keynote speech on Day 1 of HASE*

High assurance is of paramount importance to engineers who design and build interdependent complex systems that impact individuals, entire cities and even nations. This year's theme focused on the question **“What design innovation is needed to bring about systems whose operation in accordance with functional and non-functional requirements is assured with a very high probability?”**

Call for papers led to the receipt of 49 papers from 18 countries, with North America leading the pack. After deliberations and reviews by members of the Programme Committee, led by Programme Committee Co-chairs Bojan Cukic and Aditya Mathur, 24 submissions were accepted and categorised as regular (10), short (eight) and student papers (six). These presentations – from North America (13), Europe (six), and Asia-Pacific (five) – were organised into six sessions over three days. The symposium also had the fortune of having two keynote speakers, several invited speakers and industry speakers thrown into the mix

of excellent paper presentations. To top it off, there were also two panel discussions, a workshop on Security issues in Cyber Physical Systems (SecCPS), and a tour of iTrust's world class testbeds.

### Keynote Speakers

Dr Tan Guan Hong is the Senior Director (Smart Nation Systems & Solutions) at the newly formed (Oct 2016) Government Technology Agency of Singapore. His talk **“High System Reliability through Design Innovation”** encouraged practitioners to continually find ways to design and implement end-to-end systems which provide high quality and reliable data. This reduces time, cost, and effort in unnecessarily sifting through noisy data, and thus ensuring a high system reliability. Dr Tan also encouraged practitioners to gain field experience to better appreciate the environment in which their systems are exposed to, thereby designing more robust systems.

In **“Cyber Security & Cyber Physical Systems”**, Dr Sukarno Mertoguno (Programme Officer, The Office of Naval Research) stressed the importance of building cyber resiliency in a cyber physical system. His proposed approach is to develop solutions derived from the physical requirements, which led him to focus on three main areas: network layer, bus layer and controller area. Dr Mertoguno also covered the importance of improving software robustness and efficiency, so as to reduce complexity and wasted memory, and outlined strategies to do so.

### Invited Speakers

Four invited speakers from the academia and government agencies discussed the **challenges and resilience in systems and infrastructures**. Prof John McDermid (University of York) spoke about the **challenges in identifying and assessing hazards in autonomous vehicles**, and how they could be extended to other domains (air and sea). Assoc Prof Sun Jun (SUTD) presented the **challenges in modelling a water treatment testbed** at SUTD, in which a precise model would help model-based system analysis methods such as model checking. During the industry session, Mr Tan Ee Sin (PUB) presented how Singapore's water agency,

recognising the increasing complexity in interdependent systems, carried out an **evaluation process to provide segregation and systematic redundancy of all critical components** along their functional lines so that no single point of failure should cripple the operation of any one system. Mr Lim Soon Chia (Cyber Security Agency of Singapore) shared Singapore's Cybersecurity Strategy and the government's three-pronged **approach towards securing critical infrastructure in governance, risk assessment and compliance.**

#### iTrust-sponsored Panel Discussions

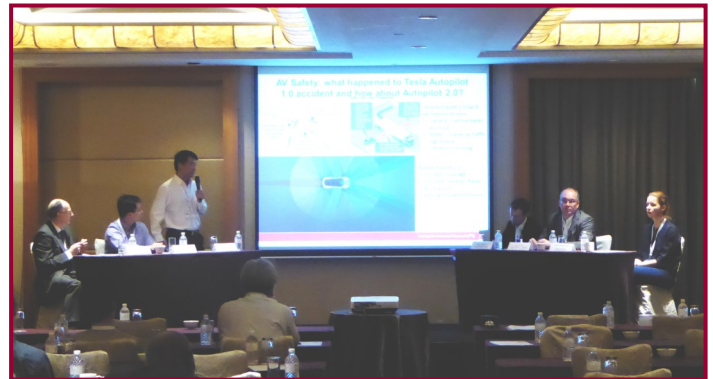
Robert Kooij (TNO) moderated a highly interactive panel discussion on **"High Assurance for Interdependent Critical Infrastructures"**, with a diverse select of panellists from A\*STAR (Christopher Monterola), INTERPOL (Roeland van Zeijst), Missouri University of Science and Technology (Bruce McMillin), and SIM-CI (Dhiradj Djairam). Each panellist gave an overview of their work in relation to critical infrastructure, including from a law enforcement and city planning perspective. The audience was then polled on their views on the challenges in ensuring resilience in critical infrastructure.



*From left: Roeland van Zeijst commenting on the result of one of the poll, with Christopher Monterola, Bruce McMillin, Dhiradj Djairam and moderator Robert Kooij*

On Day 2, Giedre Sabaliauskaite (SUTD) moderated the panel discussion on **"Assurance in the Context of Autonomous Vehicles."** The panelists – Niels de Boer (Energy Research Institute @ NTU), Mario Gleirscher (Technical University of Munich), Bingbing Liu (Insitute for Infocomm Research), Yang Liu (Nanyang Technological University), and John McDermid (University of York) – briefly presented the challenges, modelling and

opportunities in the AV field. This was followed by questions from the audience revolving around the possibility of completely autonomous vehicles, how much time was needed to achieve this, how secure they would be, and their interactions with non-autonomous vehicles.



*Bingbing Liu presenting (standing) on localisation for AV, with (from left) John McDermid, Yang Liu, Mario Gleirscher, Niels de Boer and moderator Giedre Sabaliauskaite*

#### Student paper presentations

Six students presented their research work on topics ranging from **CPS to indoor navigation ontology and access control policies.** The judges — Dr Raymond Paul, Prof Bojan Cukic and Dr Robert Kooij — gave valuable insights and suggestions to the students. After deliberations from the judges, Anusha Thurdimilla (Missouri University of S&T) won the 1st prize in the student paper category. Praneeth Sakhamuri (Ryerson University) and Koyena Pal (SUTD) came in second 2nd and 3rd respectively.

#### Workshop on Security issues in Cyber Physical Systems (SecCPS)

The papers at the half day SecCPS on 14 January discussed **practical and theoretical solutions to securing CPS.** Five papers were accepted by a Technical Programme Committee. The paper titled "Anomaly Detection in Cyber Physical Systems Using Recurrent Neural Networks" by Jonathan Goh, Sridhar Adepu, Marcus Tan and Zi Shan Lee from SUTD won the Best Paper Award, selected based on reviewer comments and scores.

## **SUTD-TNO Letter of Commitment Signing**

In April 2016, SUTD and the Netherlands Organisation for

Applied Scientific Research (TNO) signed a Memorandum of Understanding (MoU) to collaborate on research and innovation in cyber security and resilience. After months of intense discussions and collaborations, the MoU has given birth to two concrete projects on two focus areas: Blockchain Security Lab and Design of Secure Critical Infrastructures. On 24 Nov 2016, **SUTD and TNO demonstrated their commitment by signing a letter of commitment (LOC) on these two projects.**



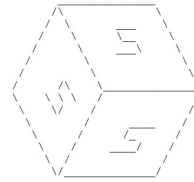
*Signatories at the LOC signing: SUTD Provost Prof Chong Tow Chong (third from left) and TNO CEO Mr Paul de Krom (first from right), with witnesses Minister for the Environment and Water Resources Mr Masagos Zulkifli Bin Masagos Mohamad and Prime Minister of The Netherlands Mr Mark Rutte*

SUTD's signatory to the LOC, Provost Professor Chong Tow Chong, said: "This further commitment between SUTD and TNO underscores the increasing importance of cyber security in the world today. As a research-intensive university focused on technology and design, SUTD will partner with TNO to drive research in blockchain technology, which will help improve financial technology, as well as cybersecurity in critical infrastructures." Mr Paul de Krom, CEO at TNO, added, "Blockchain technology is the future and the driving force behind thousands of startups with all its regulatory, business and societal impacts. Therefore focus on safe and secure Blockchain applications is essential." Together, SUTD and TNO will set up the Blockchain Security Lab at iTrust. By attacking Blockchain technology in a testbed setting, controls are created on how to regulate, design, deploy and certify cyber secure Blockchain applications.

The signing ceremony was witnessed by Mr Masagos Zulkifli Bin Masagos Mohamad, Minister for the Environment and Water Resources and Mr Mark Rutte,

Prime Minister of The Netherlands . Mr Rutte's visit to Singapore was part of a trade mission to South East Asia, and included a Business Round Table where specific partnerships between Singapore and The Netherlands were demonstrated.

## SWaT Security Showdown (S<sup>3</sup>) report



In July 2016, iTrust hosted the first SWaT Security Showdown (S<sup>3</sup>) event during the second Secure Cyber Physical (SCy-Phy) Systems Week, in which ethical cyber attackers from both academic and commercial organisations attempted to hack into iTrust's Secure Water Treatment (SWaT) testbed deployed with several defence mechanisms. This was perhaps the first Capture-The-Flag event targeted at ICS security that used an operational plant as the target. **The aim of S<sup>3</sup> was to (a) assess the robustness of the installed defence mechanisms; (b) compile the attack methodologies used by various cyber attackers; and (c) provide learning points for all parties involved**, in order to build a more robust and secure defence system for Singapore's critical infrastructures.

The event's organisers, Dr Nils Tippenhauer and Dr Martin Ochoa, Assistant Professors at the Information Systems Technology and Design (ISTD) Pillar in SUTD, have since compiled **learning points, results and observations into a concise report**. This report is now available on iTrust's website. In this year's SCy-Phy Systems Week in June 2017, iTrust will be organising a second run of S<sup>3</sup>, with additional challenges and will be larger in scale and longer in duration. Do look out for updates on this at iTrust website!

## 11th International Conference on Critical Information Infrastructures Security

In the previous issue, we featured that Sridhar Adepu, a former Research Assistant with iTrust and now a PhD student at SUTD, presented two papers at the 11th International Conference on Critical Information Infrastructures Security (CRITIS). We are pleased to

announce that Sridhar was **shortlisted as a finalist for the CRITIS Young Award, for the paper titled “A Dataset to Support Research in the Design of Secure Water Treatment Systems”**, which he co-authored with iTrust research scientist Jonathan Goh, Aditya Mathur and Khurum Junejo. Well done, Sridhar!



*Sridhar (center) receiving the award from the organisers*

## Research Focus

iTrust is proud to announce that it has applied for **provisional application for three technology inventions** developed during the course of research work using its testbeds. The three inventions – Water Defence, Argus, and Automated Identification of Unsecure Paths in Network Infrastructures – are described below.

### Water Defence

*Inventors: Sridhar Adepur and Aditya Mathur*

Water Defence is a cybersecurity platform specialised in **protecting water treatment plants from multi-point attacks**. The platform takes a comprehensive assessment of the components of the CPS, including sensors and actuators. State-dependent and -agnostic invariants are created and programmed. Since the code added to the different systems is ingrained into the respective cyclic control codes, potentially damaging anomalies can be detected whenever devices like sensors gather data.

### Argus

*Inventors: Aditya Mathur, Siddhant Shrivastava, Sridhar Adepur, Nils Tippenhauer, Kaung Myat Aung, and Giedre Sabaliauskaite*

Argus is a security system that defends CPS against cyber-

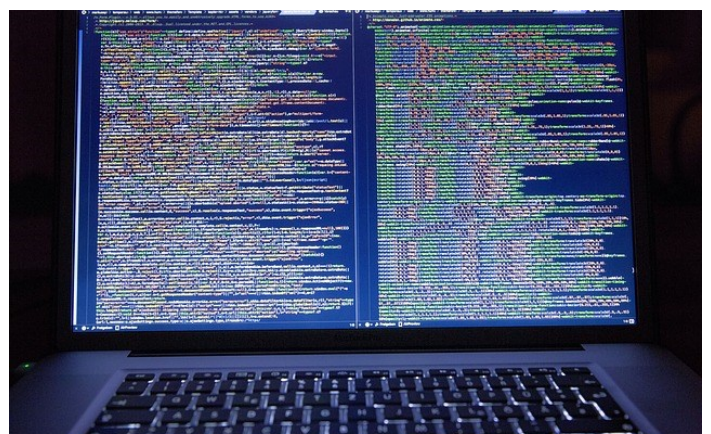
attacks. Argus – working orthogonally to existing intrusion prevention software – provides industrial control systems with a layered defence system that **recognises cyber attackers that have already gained unauthorised access into networked systems**. Cyber-attacks are monitored through a local intelligent checker that transmit state-related information about sensors and actuators to the global intelligent checker that ensures plant dynamics have not deviated from expected performance. If a deviation in dynamics is found, the global intelligent checker is able to detect, alarm, and pinpoint the source of the attack on the plant.

### Automated Identification of Unsecure Paths in Network Infrastructures

*Inventors: Jonathan Goh, Ivan Lee, Jing Hui Toh, and Sachidananda Vinay Mysore*

PathFinder is a reinforcement learning system employing a host of disciplines — network scanning, domain knowledge database, penetration testing, and machine learning algorithm — to **identify unsecured/vulnerable paths in network infrastructures**. PathFinder also finds applications in cyber security for the Internet of Things.

## Talks on Cyber Security



### Workshop on Ethical Hacking

*By Lauren Goh*

As part of iTrust’s continual outreach to increase awareness and interest in cyber security, a two day workshop on ethical hacking was organised during SUTD’s Independent Activity Period (IAP) on 18 and 19 Jan 2017.

The workshop - conducted at SUTD's Learning Environment for Experimental Technology (LEET) Lab - covered topics on **Networks Fundamentals, Introduction to Ethical Hacking, Machine Learning for Cyber Security and Reverse Engineering Malware** and was meant to equip the participants with a basic knowledge of the tools available to decipher and prevent cyber attacks. The trainers were Ivan Lee (Senior Associate Director, Cyber Security Technologies), and Research Assistants Toh Jing Hui and Francisco Furtado. They were aided by ISTD undergraduates Claudia Aw and Muhammad Syuqri.



*Francisco Furtado (standing) assisting a student at the workshop*

The first day built up the participants' fundamental knowledge needed to dive deeper into the field of ethical hacking. Starting with the basics of understanding number systems, network types and network layers, they advanced into the interpretation of IP addresses and the construction of legitimate networks, set up with shared routers and default gateways. There were also hands on



**As a whole, the workshop was an eye-opening experience to learn more about Ethical Hacking. The sharing was done in a concise and adequate manner, and a great part of the workshop is the hands on learning experience, which helped to ingrain the concepts I learnt and make the workshop fun.**

**Workshop participant**

sessions using software tools — such as the Cisco Packet Tracer — installed in LEET Lab's workstations, to simulate the construction and testing of the participants' own networks. The trainers also covered the five hacking phases of Reconnaissance, Scanning, Gaining Access, Maintaining Access and Clearing



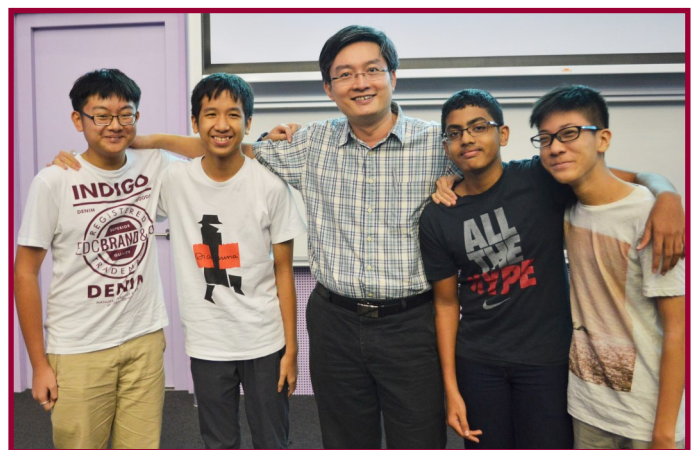
Tracks, as well as a cyber attacker's strategies based on the

preparatory findings on the vulnerabilities of the host.

On the second day, using specialised tools installed on the Virtual Machines on their laptops, the participants put on the hat of a malware analyst to witness how malwares worked. In particular, the OllyDbg software — an x86 debugger that emphasises binary code analysis — helped participants to identify the execution steps of the malware even though the code was encrypted. About 50 students attended the workshop. The slides of the workshop can be downloaded from iTrust's website.

## **Defence Scientists Programme (YDSP) Science and Technology Camp**

On 23 Nov 2016, iTrust hosted a group of 83 students from various secondary schools as part of the bi-annual Young Defence Scientists Programme (YDSP) Science and Technology Camp. YDSP, an initiative by Defence Science and Technology Agency (DSTA) and DSO National Laboratories, aims to generate greater interest in defence science and technology among students. The camp theme was "Cyber-Security" where the students were exposed to topics in computing such as Python, Networking Equipment, Encryption, HTTPS and SSL during the five day camp.



*Boon Kai with some of the budding young defence scientists*

As part of the camp, the students were provided an opportunity to visit iTrust to gain insights into Cyber-Security. The visit started with Neo Boon Kai, Manager (Cyber Security) from DSTA who shared today's cyber landscape and case studies of recent cyberattacks.

Following that, Toh Jing Hui, Research Assistant at iTrust, presented some examples of cyber vulnerabilities present in our daily lives and the implications of such threats to society, companies and individual.

## Cyber Security Awareness Day

A week later, iTrust Research Assistant Toh Jing Hui was invited by Mr Wong Tuck Wah, Section Head, Cyber & Network Security at ITE College East to give a talk at its inaugural Cyber Security Awareness Day (CSAD). Jing Hui had conducted cyber security workshops in 2015 and 2016 which were attended by some of ITE College East's students and his talk is an extension of the collaboration between iTrust and ITE College East. Jing Hui's presentation and video demonstrations focused on **security challenges in IoT devices as well as the additive manufacturing industry**. Mr Huynh Thien Tam from Kroll, and Dr Magda Chelly from Responsible Cyber Pte Ltd, were also among the speakers at CSAD. The talk was attended by about 100 ITE students and staff.

## Visits

SUTD welcomed a group of delegates from the **National Taiwan University (NTU)** on 5 Dec 2016, who were keen to find out more on SUTD's approach to design and innovation as well as to explore on potential collaborations. The delegation comprised Dr. Tei-Wei Kuo, Executive VP of NTU and CEO of D-School@NTU, Dr. Kuo-Hsian Su, Dean of College of Social Sciences, ED of D-School@NTU, Dr. Sheng-Lin Chang, Chair of Graduate Institute of Building and Planning, Director of Humanity and Society of D-School@NTU, and Dr. Kuei-Yuan Chan, Associate Professor of Mechanical Engineering, Director of Academic Affairs of D-School@NTU. iTrust hosted a group of delegates from the **HASE 2017 symposium** on 14 Jan 2017, as well as those from the **Global Young Scientists Summit 2017** on 18 Jan 2017, to showcase iTrust's cybersecurity facilities.

Key stakeholders from the Singapore government were

also kept apprised of iTrust's research progress. The deputy CE of **DSO National Laboratories** Mr William Lau visited iTrust and Temasek Laboratories@SUTD on 20 Jan 2017 to better understand the centres' capabilities and foster better and closer collaborations. **PUB's** engineers also visited iTrust on 1 Feb 2017 to assess iTrust's technology readiness.

## iTrust Activities

All work and no play a dull boy Jack maketh. iTrust and the ST Electronics-SUTD Cyber Security Laboratory organised a friendly soccer match between The Eagles and The Falcons on 5 Jan 2017. The teams comprised a motley mix of staff, researchers, students and even the lab directors! The closely-matched game ended 2-1 in favour of The Eagles.



*Happy faces after a good workout*

To welcome the new year, a lunch gathering for iTrust staff and researchers was also organised, in which iTrust Centre Director Aditya Mathur thanked everyone for their hard work and contributions in 2016.



*Even happier faces when there is food*

## Research Openings

iTrust is looking for qualified individuals to fill the following positions:

- 1) **Research Scientist** in the following project:
  - a. Advancing Security of Public Infrastructure using Resilience and Economics
- 1) **Post-doctorate/Research Fellow** in the following projects:
  - a. Advancing Security of Public Infrastructure using Resilience and Economics
  - b. Autonomous Vehicle Security
  - c. Research & Security Innovation Lab for IoT
- 2) **Research Assistant** in the following projects:
  - a. Advancing Security of Public Infrastructure using Resilience and Economics
  - b. Autonomous Vehicle Security
  - c. Research & Security Innovation Lab for IoT

For detailed job description and requirements, please visit <http://tinyurl.com/jh6uxlw>.

## Readership Survey

We hope you enjoy reading iTrust Times. Please take a short survey via Google form (no sign-in required): <http://goo.gl/forms/EKxl4L30Db>.

## iTrust Contact Information

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

### Mr Kaung Myat AUNG

Senior Specialist (Water)

[kaungmyat\\_aung@sutd.edu.sg](mailto:kaungmyat_aung@sutd.edu.sg)

### Prof. Yuval ELOVICI

iTrust Research Director

[yuval\\_elovici@sutd.edu.sg](mailto:yuval_elovici@sutd.edu.sg)

### Mr Mark GOH

Manager

[mark\\_goh@sutd.edu.sg](mailto:mark_goh@sutd.edu.sg)

### Mr Ivan LEE

Senior Associate Director, Cyber Security Technologies

[ivan\\_lee@sutd.edu.sg](mailto:ivan_lee@sutd.edu.sg)

### Prof. Aditya P MATHUR

Professor & Head of Pillar, ISTD Pillar

iTrust Centre Director

[aditya\\_mathur@sutd.edu.sg](mailto:aditya_mathur@sutd.edu.sg)

### MUHAMED Zhaffi Bin Mohamed Ibrahim

Specialist (Power)

[zhaffi\\_ibrahim@sutd.edu.sg](mailto:zhaffi_ibrahim@sutd.edu.sg)

### Kandasamy MURUGANANDAM

Specialist (IoT)

[Kandasamy\\_m@sutd.edu.sg](mailto:Kandasamy_m@sutd.edu.sg)

### Ms Angie NG

Deputy Manager

[angie\\_ng@sutd.edu.sg](mailto:angie_ng@sutd.edu.sg)

### Ms Priscilla PANG

Manager

[priscilla\\_pang@sutd.edu.sg](mailto:priscilla_pang@sutd.edu.sg)