iTrust Times

A Quarterly Newsletter

Issue Highlights:

Jul—Dec 2021 | Volume 7 Issue 3

From Centre Director's Desk

Ye(a)r End with iTrust

Dear Reader:

Greetings from iTrust!

Yet another year is ready to end. Perhaps this year has been the most eventful for iTrust -- and all in a good way. In April, iTrust participated in the world's largest cybersecurity exercise, namely, Locked Shields 2021, organised by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). A digital twin, developed fully in iTrust, served as one of several target systems that were defended by blue teams from NATO member nations. In September, iTrust conducted its sixth annual Critical Infrastructure Security Showdown-Online (CISS2021-OL) in close partnership with Mindef. This event turned out to be largest iTrust has ever conducted. In the same month iTrust witnessed the signing of an MoU with Mindef that cements the long term R&D collaboration between the two organisations.

Professor Jianying Zhou and Mark Goh of iTrust are leading a new initiative to expand's iTrust scope in the design of safe and secure critical infrastructure to the maritime domain. In addition to obtaining a research grant in martitime cyber security, this duo is now working on the design of a realistic shipboard operational technology testbed to support research in maritime cyber security. This testbed, expected to be operational in 2024, is likely to be one-of-a kind and will complement the existing testbeds in iTrust.

iTrust has been fortunate to have some of the finest people as part of its admin and technical support staff. One such individual is Ivan Lee, our Depty Director of Cyber Technologies. After about 7+ years of dedicated service to iTrust, Ivan will be leaving to take up other challenging tasks. On behalf of all in iTrust, I wish Ivan the very best in his career. More on Ivan's contributions to iTrust can be found in an article in this newsletter.

Best wishes and regards to all readers of iTrust Times.

Aditya Mathur
Centre Director, iTrust, SUTD
Director, National Satellite of Excellence DeST-SCI
Professor Emeritus, Computer Science, Purdue University

NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust
Centre for Research in Cyber Security

Special Highlight

Fare Thee Well

Bye, bye Ivan, stay in touch!

By Prof Aditya Mathur, Centre Director, iTrust

I joined SUTD as the Head of the Information Systems Technology and Design (ISTD) pillar. Ivan had interviewed with me in September 2012 and joined the pillar in early 2013 as the ISTD Associate Program Director. Soon after joining ISTD Ivan came up to me and asked: "What will be my responsibilities?" My answer was, "Everything." Ivan was a bit taken aback but quickly composed himself, and with a bit of perceptible hesitance, said: "OK!"

Aditya: Your responsibilities are everything.
Ivan: Wait. What?

At ISTD, Ivan was involved in nearly all internal and external day-to-day administration of ISTD. Among the many tasks, Ivan assisted in: the creation of the Corporate Partners programme; hiring; managing IRB related matters; Project GREaT; ISTD budget; accreditation; collaterals for new ISTD programmes; and management of administration staff. Ivan advised me, and was with me in nearly all meetings I had with the potential funding agencies and collaborators. There wasn't any task where Ivan was not deeply involved. He helped design and operationalise LIPS: Laboratory for the Identification of Paths for Security. In 2014, Ivan conducted the first ethical hacking workshop for SUTD students. In the same vein, he helped launch the Passion@Live program aimed at arousing interest in Computer Science that was fast waning among high school graduates in Singapore. Ivan even assisted some of the ISTD instructors in conducting laboratory sessions for one of the courses. Ivan travelled abroad with ISTD faculty to recruit students for the newly established PhD programme.

iTrust was launched in 2012 with a grant from MINDEF. While SUTD was searching for a full time Centre Director for iTrust, the then Provost Professor Tow Chong asked me to serve as the acting Centre Director. Soon after iTrust was launched, in addition to working for ISTD, Ivan began assisting me in the intense planning to chart the shape and vision of iTrust. Propelled by his keen interest and knowledge in cyber security, and sensing that cyber security would become a dominant field in the near future, Ivan indicated his desire to move as a full-time employee of iTrust. I immediately agreed and in 2014 Ivan was appointed Associate Center Director.

Where do I begin to enumerate all that Ivan has done to realise iTrust's vision of a world-class research center in cyber security for Critical Infrastructure? Soon after joining iTrust, Ivan began enhancing his skill sets in the design of secure Critical Infrastructure. He attended numerous certification courses to upskill himself. For example, in 2013 he was certified as Ethical Hacker, Security analyst, by the US DHS ICS-CERT ICS Cybersecurity (301).

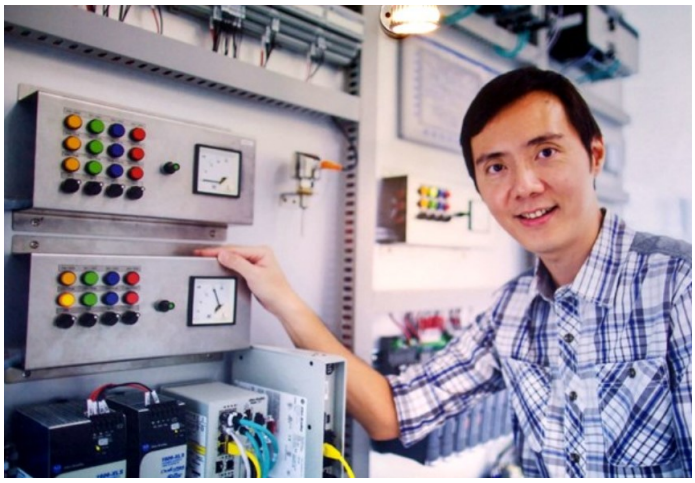
Ivan also travelled to the US to attend cyber security courses at one of the most advanced laboratories: the Idaho National Laboratory. His grounding in Computer Science at NUS, coupled with continuous acquisition of skills in computer networks and cyber security, made him an outstanding contributor to iTrust.

Perhaps the most challenging task for iTrust was to create realistic and fully operational physical testbeds that would enable researchers to test and demonstrate their technologies towards the design of safe and secure Critical Infrastructure. To do so required sourcing for designers and builders, working closely with internal stakeholders and consulting various Singapore government agencies for design validation. This is

where Ivan excelled. He worked with me over the years to establish four world-class testbeds that today are widely considered to be the crown jewel for researchers across the globe.

In 2012, iTrust was a nascent cyber security center in the sea of similar centers across the world focusing on information and cyber security. One of my goals was to make iTrust known, locally and globally. This was achieved by international cyber events such as the Secure Cyber-Physical (SCy-Phy) Systems week and the Critical Infrastructure Security Showdown (CISS) exercises, where Ivan played a key role in their organisation and execution. Among Ivan's many contributions in this area is Zycron—a hybrid system that offers a simulated environment for training and cyber exercises. Ivan has effectively interfaced Zycron with the SWaT testbed that made it possible to offer members of red and blue teams a realistic environment for training in defending critical infrastructure against cyberattacks.

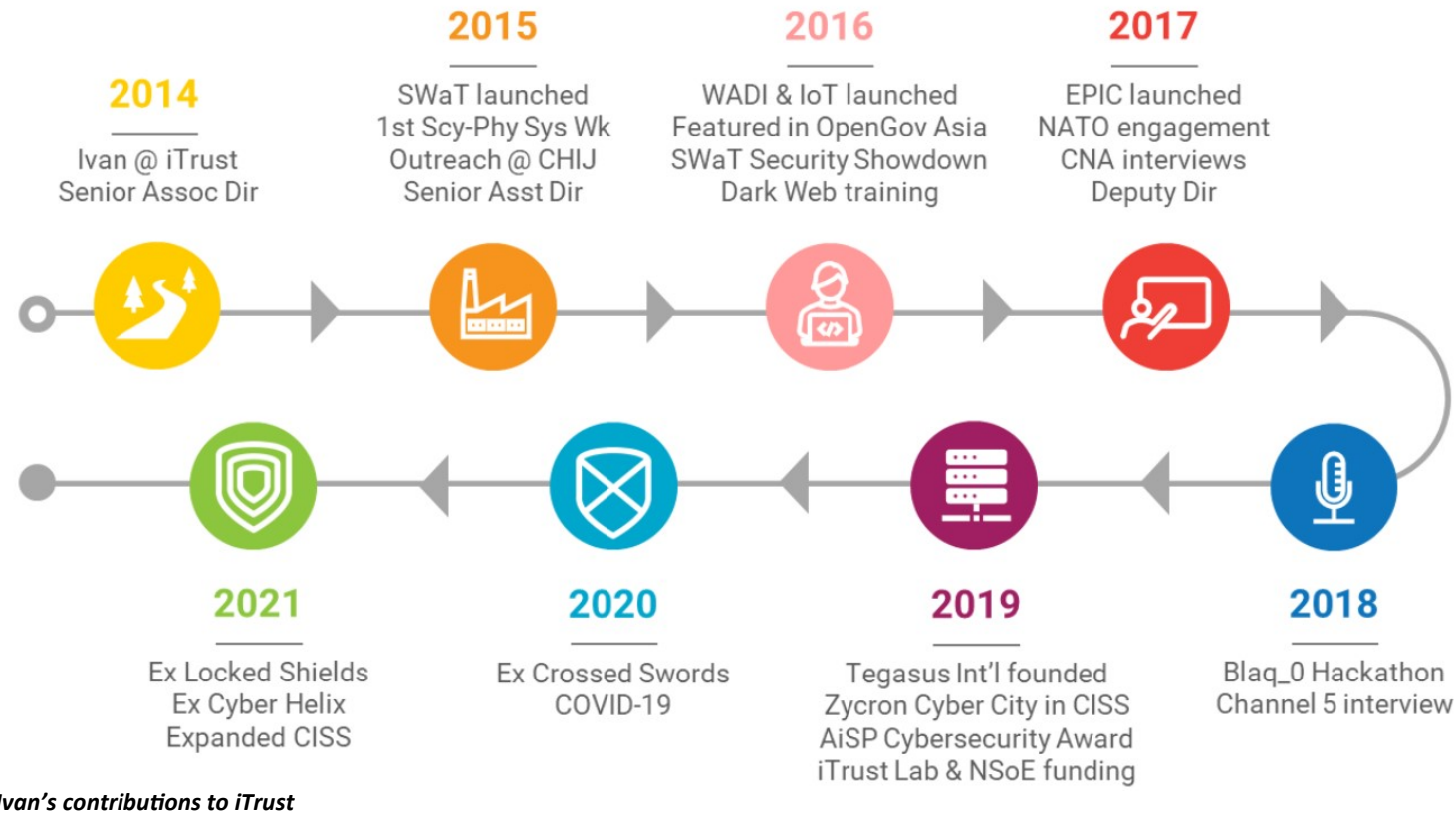
Ivan also played an important role in Singapore's involvement in NATO's cyber-security exercises conducted by CCDCOE in Estonia. Starting in 2018, Ivan assisted me in strategising our collaboration with CCDCOE and MINDEF to ensure that iTrust is a recognised contributing partner in the NATO exercises,



In Ivan, iTrust

namely Crossed Swords and Locked Shields. Ivan travelled to Tallin and Riga with other iTrust members to ensure that our technologies were used without any hiccups. Ivan's contributions, coupled with the many achievements of iTrust in R&D over the years, paved the way for Mindef to sign an MoU with SUTD in September 2021 to deepen this partnership.

I have been able to list only a fraction of what Ivan has accomplished for iTrust, SUTD, and Singapore during his approximately 8+ years with us. Ivan will surely be missed in iTrust. On behalf of all in iTrust, I wish Ivan — a brilliant administrator, dedicated individual, highly energetic and often bursting with humor — the very best for his career.



Ivan's contributions to iTrust

New Dawn

iTrust's signature annual cyber exercise saw more than 150 cybersecurity professionals from 30 organisations participated as White, Green, Red and Blue teams.

If CISS2020-OL (Critical Infrastructure Security Showdown 2020 - Online) was the dawn of iTrust's new modality of organising an international cyber exercise on a fully integrated online platform, then this year's would be described as a bright new morning. The prospects look promising. Building on the solid foundation from last year's development of new tools to support the entire exercise, this year focused on making the foundations more robust and inserting new exercise (pun intended) equipment in the park. It would, however, be a mistake to conclude that the park is merely a digital sandbox.

Figure 1: Red Week: Judges in session

The physical operational technology (OT) testbeds – the Secure Water Treatment (SWaT) and, introduced to this year's exercise, the Water Distribution (WADI) – were very much in play this year, as with previous CISS iterations. Nothing beats knowing that an attack caused a physical impact on the plant, be it a pump gone awry or the tank overflooding (testbed engineers on standby with mops and buckets can testify to that.) And, ubiquitous to a modern critical infrastructure (CI) setup, the testbeds were integrated with a fully operational corporate IT environment – complete with email server, worldwide web, intranet etc. - functioning under a fictitious company, Zycron Pte Ltd. Intrusion Detection Systems (IDS) were also added to network as an added challenge to the Red Teams. A walk in the park, it was not.

Other than the physical testbeds, the size of the park was literally doubled by a parallel universe of sorts: CISS2021-OL also saw the **introduction of the SWaT and WADI digital twins** – digital representations of the testbeds that behave and react as the testbeds would. Yet another addition was the set up of a "Blue Week," where CI regulators and operators banded together to defend the park against a composite Red Team. With all these exciting features, what, then, was needed were players in the park (Squid Game, anyone?).

With the immense support and technical expertise from the Singapore's Ministry of Defence (Mindef) and Cyber Security Agency (CSA), this year saw **13 Red Teams, 6 Blue Team vendors and 12 CI operators and regulators** signing up for CISS2021-OL. The first week featured the traditional "Red Week" where international Red Teams barraged through a list of attack objectives in their attempt to claim the top prize of S$4,000. During the inaugural "Blue Week" on the second week, CI operators and regulators were trained to monitor and defend a plant network against a composite Red Team trying to outfox them in their backyard. A post-event report detailing the exercise will be posted on iTrust's website in early 2022.

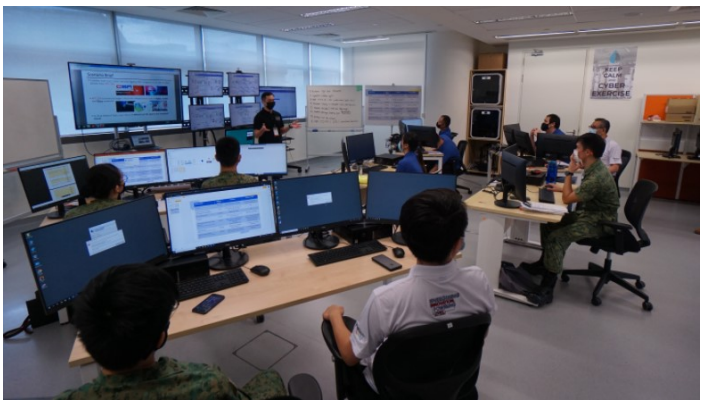


Figure 2: Blue Week participants defending the OT network

iTrust Webinar: A Cyber Risk Management Study in Shipboard OT Systems

By Senior Research Assistant Priyanga Rajaram

The third of a series of webinars on shipboard cyber risks

Ships are becoming increasingly reliant on digital technologies for their day-to-day operations, such as navigation, communication, propulsion, power management and cargo management. With the emerging threat landscapes in the maritime sector, weak security could result in ship damage, loss of lives and reputational and economic loss for the company that might take years to recover. Hence, adopting an effective cyber risk management approach will help to safeguard ships, crew and the cargo from emerging and existing cyber threats.

To this end, the Singapore Maritime Institute funded iTrust a research study titled "A Cyber Risk Management Study in Shipboard OT Systems." At the first webinar on 18 Dec 2020, the team shared its initial findings on the cyber risks identified in shipboard OT systems. A second webinar on 01 Apr 2021 reviewed existing guidelines and presented mitigation measures to manage the risks identified earlier.

After the second webinar, the team started working towards designing a **cyber risk assessment approach to assess the severity and likelihood of the risks**. Following that, the team then came up with a checklist based on a tiered security model to help shipowners ensure that the most crucial security controls can first be addressed. The team framed the checklist in a way that is easy to implement, while considering the balance of risks versus costs. The purpose of this approach is to help shipowners assess the cyber hygiene of their vessels and also implement effective risk mitigation measures with the help of checklist. On 27 Aug 2021, the team conducted a third webinar titled "A Cyber Risk Management Study in Shipboard OT Systems Part III: Cyber Risk Assessment and Checklist" to exhibit their results from this part of the study. A sample checklist can be seen in the Figure 3 below. The team then hosted a 30-minute Q&A session to take questions from the audience. Similar to the first and second webinars, the third one also generated significant interest, with nearly 200 participants globally.

The team received positive feedback from the audience, and one of the attendees, Mr. Himadri

OT sub-system(s)	*Cyber risk checklist*	*Mitigation checklist*	*Security tier*
Satellite Communication System (SATCOM)	❑ Phishing email attempt	❒ **T1-13** Antivirus software is installed. ❒ **T1-14** Files and email attachments downloaded from emails are scanned with antivirus software before opening it. ❒ **T1-15** Crew awareness is established on the following: o The crew can distinguish phishing emails from the real ones o The crew is aware that emails from unknown sources should be viewed carefully, and suspicious emails should not be opened o The crew is aware that they must not click on unknown links ❒ **T1-16** Email security is implemented – For example, S/MIME (Secure Multipurpose Internet *Mail* Extension) can be implemented to encrypt the email and ensure authenticity & integrity of the email.	1

Figure 3: Sample checklist to evaluate and mitigate cyber risks for shipboard OT systems

Shikhar Ghosh, Senior Manager, MSI ship management, invited the team to present at an internal webinar for the members at MSI ship management, as they were interested in gaining more awareness on maritime cybersecurity. MSI is an established international ship management company with a fleet of tankers, bulk carriers, container ships and specialist offshore vessels. Prof Jianying Zhou, the study's Principal Investigator, and Senior Research Assistant Priyanga Rajaram gave an overview of the study to MSI on 22 Sep 2021. During the Q&A, the attendees were particularly keen on mitigation strategies for managing cyber risks.

The slides and video of all three webinars can be downloaded from iTrust's website. A last and final webinar is scheduled for Jan 2022 to summarise the study's finding.

Mindef, SUTD join hands to build defences against cyber attacks

Straits Times, 17 Sep 2021, Mindef, SUTD join hands to build defences against cyber attacks

With the growing threat of cyber attacks on critical infrastructure, the Ministry of Defence (Mindef) is seeking to tighten its defences by further training its experts and studying the methods employed by hackers.

It is doing so through a partnership with the Singapore University of Technology and Design (SUTD) to strengthen collaboration in several areas, including research and technology, threat modelling and training, Mindef said yesterday.

A memorandum of understanding on **operational technology security for critical infrastructure** was signed by defence cyber chief Brigadier-General (BG) Mark Tan and SUTD Associate Provost for Research and International Relations Professor Yeo Kiat Seng.

The signing took place at the university on the sidelines of a two-week cyber-security exercise co-organised by the Singapore Armed Forces (SAF) and SUTD, called the Critical Infrastructure Security Showdown.

Mindef said that recent cyber attacks on critical

Figure 4: BG Tan (left) and Prof Yeo signing the MoU

infrastructure, such as fuel pipelines and power distribution systems, are "stark reminders of the increasingly sophisticated cyber threats that countries face".

"The MOU underscores Mindef's and the Singapore Armed Forces' commitment to build up cyber-security expertise and capabilities against potential operational technology cyber threats."

Operational technology (OT) systems include computer systems designed to be deployed in critical infrastructure, such as power, water, manufacturing and similar industries.

Such infrastructure overseas has been hit by hackers recently. Colonial Pipeline, which supplies about 45 per cent of fuel used on the east coast of the United States, was hit by a ransomware attack in May.

That same month, a cyber attack on Brazilian food giant JBS forced the closure of all its beef plants in the US.

OT infrastructure and enhancements have been used in projects such as energy-efficient buildings and the Republic of Singapore Air Force's Smart Airbase, said Mindef.

The agreement is expected to cement collaboration between Mindef/SAF and the SUTD iTrust Centre for Research in Cyber Security in several areas.

The iTrust centre will allow Mindef to **test cyber-**

defence measures and better understand vulnerabilities in OT systems. The centre will provide training and training infrastructure, and cyber exercises will be conducted.

Both parties will also analyse emerging OT attacks and study the tactics, techniques and procedures employed by attackers.

Joint scholarships may be awarded to selected personnel under the Command, Control, Communications and Computers Expert vocation for undergraduate and postgraduate studies to develop deep expertise, said Mindef.

The vocation was introduced in 2019 to develop a highly skilled cyber force to guard defence systems and networks.

BG Tan said: "Mindef/SAF recognises the importance of working with key partners like SUTD to keep pace with the latest developments in cyber-security research and technology."

Professor Yeo said the iTrust centre's state-of-the-art critical infrastructure test beds enable complex simulations of cyber attacks and the development of defences.

"Under the MOU, we will also help to conduct research and groom the next generation of cyber experts who can help defend our nation's critical infrastructure."

Figure 5 (Left to right): Mr David Koh, CEO (CSA), Mr Gaurav Keerthi, Deputy CEO (CSA), Mr Heng Swee Keat, Deputy Prime Minister, Mr Beh Kian Teik, Deputy CEO (NRF), and Professor Chong Tow Chong, SUTD President

Figure 6 (Left to right): Mr David Ong, CEO (Attila Cybertech), Mr Gui Swee Hee, Director of Engineering at Attila Cybertech, Mr Heng Swee Keat, Deputy Prime Minister, Francisco Furtado, Senior Assistant Researcher (iTrust) and Professor Aditya Mathur, Centre Director (iTrust)

Visits

What does foiling a cyber-attack look like?

DPM Mr Heng Swee Keat visits iTrust to find out

Deputy Prime Minister, Coordinating Minister for Economic Policies, and Chairman of the National Research Foundation Singapore (NRF), Mr Heng Sweet Keat, viewed a **live demonstration of iTrust's PlantProtect thwarting a cyber-attack** on a water treatment testbed. He also observed Attila Cybertech's ADPICS Commander, an AI-powered Anomaly Detection system for Operational Technology (OT) that protects OT assets against cybersecurity threats.

As centre of research for cybersecurity, iTrust hosts several world-class testbeds and training skids designed to replicate large-scale cyber physical systems. Its researchers are also employing machine learning techniques to detect anomalous behaviours in critical infrastructures.

iTrust Internship

"What do you like most about your internship?" To this question posed by iTrust Centre Director Prof Aditya Mathur, the four student interns' unanimous answer was: "Attacking SWaT!" **Spectra Secondary School** students Amos Chan, Muhammad Rusyaidi, Febain Cruz Tan and Avina Yik interned with iTrust to explore their curiousity in cybersecurity during their school holidays. In just three weeks, they managed to **learn Python programming and launch cyber attacks on SWaT**, under the guidance of their supervisors Mavis Ang, Ivan Christian and

Siddhant Shrivastava.

Figure 7: (left, front to back) Avina Yik, Muhammad Rusyaidi, Amos Chan, Febain Cruz Tan and Ivan Christian (right, front to back) Prof Aditya Mathur, Siddhant Shrivastava

iTrust Matters

LinkedIn

Management

Prof. Aditya P MATHUR
Centre Director, iTrust
Director, National Satellite of Excellence, DeST-SCI
Professor Emeritus, Computer Science, Purdue University
aditya_mathur

Prof. Jianying ZHOU
Co-Centre Director, iTrust
Professor, Information Systems Technology and Design
jianying_zhou

Ivan LEE
Deputy Director, Cyber Security Technologies
ivan_lee

iTrust Laboratories

Mavis ANG
Cyber Security Technology Engineer
siewting_ang@sutd.edu.sg

Mark GOH
Senior Manager
Editor, iTrust Times
mark_goh

Andrew TAY
Cyber Security Technology Engineer
andrew_taykongngee

TAY Boon Kiat
Cyber Security Technology Engineer

General Enquiries
itrust

National Satellite of Excellence

HOR Miao Yun
Research Senior Officer
miaoyun_hor

Priscilla PANG
Manager
priscilla_pang

General Enquiries
nsoe_destsci

Siti Nadhirah Shaik NASAIR Johar
Research Associate
siti_nadhirah

Angie NG
Manager
angie_ng

iTrust
Centre for Research in Cyber Security

https://itrust.sutd.edu.sg
itrust@sutd.edu.sg
Singapore University of Technology and Design | 8 Somapah Road, Building 2 Level 7, Singapore 487372