iTrust Times

A Quarterly Newsletter

Issue Highlights:

Oct—Dec 2022 | Volume 8 Issue 4

From Centre Director's Desk

SEA OF ACTIVITIES

Dear Reader:

Greetings from iTrust!

Happy New Year to all friends of iTrust! I am as excited about iTrust in 2023 as ever. In 2023, I foresee at least the following new activities. First, a one-of-a-kind testbed for research, education, and training in maritime security. Second, the start of Phase II of the National Satellite of Excellence (NSoE). And third, further strengthening of our partnerships with NATO CCDCOE. I will not be surprised if more new activities pop up during 2023.

Under the leadership of Professor Jianying Zhou and Assistant Director Mark Goh, there is notable progress towards the design and construction of the maritime testbed. iTrust has already been awarded a grant of SGD4.7M that would go towards the construction of this testbed. Professor Jianying and Mark have been traveling to various European countries and have established an enviable network of collaborators in the area of maritime security.

NSoE Phase I will conclude on March 31, 2023; Phase II is expected to begin on April 1, 2023. Phase II will focus on research as well as significant technology development. The entire Phase II proposal was written in collaboration with key critical infrastructure stakeholders in Singapore. Thus, the outcome from the R&D tasks included in the proposal is expected to be of value and use to these stakeholders. The proposal also includes funds to move the technology developed in iTrust to high(er) TRL for pilot and potential deployment at the stakeholders' sites.

CCDCOE has asked iTrust to contribute to Locked Shields 2023 (LS23) in a variety of ways. Do stay in touch for upcoming issues of the iTrust Times to find out more about iTrust's proud contributions to the world's largest live-fire cyber exercise.

That is all for now. Happy reading and best wishes to all readers of iTrust Times for a productive and happy 2023!

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

Key Events

iTrust's sixth international Critical Infrastructure Security Showdown 2022 (CISS2022), co-organised with the Ministry of Defence, Singapore, continues to evolve with new and exciting features and attract ever higher numbers of top red teams from around the world.

A record 28 red teams from Asia-Pac, Europe and North America signed up for CISS this year, with a notable number of them having specific expertise in OT security and pentesting capabilities. In partnership with the National Cybersecurity R&D Lab (NCL), an OT-centric Stage 1 was crafted to admit the top 10 performing red teams into the final stage. Stage 1 was run over 48 hours in July and comprised a variety of time-sensitive CTF challenges that the red teams had to meet.

Fig 1: iTrust Cyber Tech Lead Francisco interacting with the red teams

In addition to the new Stage 1 format, CISS 2022 also introduced iTrust's Electric Power and Intelligent Control (EPIC) testbed into the exercise platform. With this addition, red teams could test their skills on three different OT infrastructures. After 40 hours of attacks, the judges determined the top three red teams based on their ability to achieve preset challenges and also the uniqueness of their attacks. These red teams are: GeForceTwo (Australia), and CISS The Day and uncleCY (Singapore; joint second). Congratulations!

Fig 2: Organisers, judges and student helpers at CISS 2022. (Left to right, back row) Reuben Chng, Delaney Ng, Matthias Yeo, William Teo, Mark Goh, Nicolas Soh. (Left to right, front row) Andy Tay, Siddhant Shrivastava, Muhammad Ramadan Mohamad Saifuddin, Gregory Chong

The inaugural Critical Infrastructure Defence Exercise (CIDeX) 2022 is the largest OT hands-on-keyboard

Critical Infrastructure defence exercise. It provided a platform for Singapore's cyber defenders to train together the defence of Critical Information Infrastructure (CII).

With a better insight into how the CII - comprising IT and OT networks - can suffer from cyber attacks and their adverse consequences, the blue teams could distil these lessons and tailor them to augment their respective organisations' cyber defence and protection strategies.

Prior to CIDeX, the SAF's Cyber Test and Evaluation Centre (CyTEC) conducted a comprehensive 3-day pre-exercise training programme to equip the blue teams with the capability and confidence to navigate through the CII platform and utilise appropriate cyber tools to monitor the platform and respond to the cyber attacks.

Over 50 cyber defenders from 17 organisations representing five critical sectors — energy, water, telecommunication, land transport and maritime — combined to form five blue teams to monitor and defend the CII systems over two days. A white team coordinated with a composite red team to launch a series of live simulated cyber attacks on these systems, while the five blue teams worked in concert to detect and respond against the attacks.

CIDeX 2022's platform had three OT testbeds

Fig 4: A total of 55 cyber defenders from 17 organisations participated in CIDeX 2022

contributed by iTrust — the Secure Water Treatment (SWaT), Water Distribution (WaDi) and Electric Power and Intelligent Control (EPIC) OT testbeds, integrated with an Enterprise IT network of VMs hosted within the National Cybersecurity R&D Laboratories (NCL) at the National University of Singapore (NUS). It was also the first time that iTrust partnered with the NCL by connecting our respective OT and IT platforms. As "sister" research centres reporting to the same Governance Board, this was a natural partnership encouraged and supported by the Governance Board.

Fig 5: Blue teams putting their training to good use as they worked together to defend the CI platforms

Technical partners for CIDeX included ST Engineering, which provided technical leadership in the design, setup, and preparation of the entire exercise environment, as well as Keysight Technologies, which provided numerous hardware to support the exercise.

Research Focus

Maritime Cybersecurity

iTrust ventures into the maritime domain to keep cyber attacks at bay

A new and exciting journey awaits, now that iTrust SUTD, led by Prof Jianying Zhou, has been awarded $4.77M funding by Singapore Maritime Institute (SMI) for iTrust to design and build a maritime testbed of shipboard operational technology systems (MariOT). Major shipboard OT systems to be included in MariOT are navigation, communication, propulsion and cargo management, with a host of features to ensure that it is future-proof, flexible, configurable and also

Fig 6: MariOT testbed Letter of Award signing ceremony at SMI Forum, witnessed by (left to right, standing) Mr Wong Weng Sun, SMI Chairman, Mr Chee Hong Tat, Senior Minister of State for Transport and Prof Chua Chee Kai, SUTD Associate Provost for Research, with (left to right, seated) Mr Tan Cheng Peng, SMI Executive Director and Prof Aditya Mathur, iTrust Centre Director

compatible with navigation simulator available at the Centre of Excellence in Maritime Safety (CEMS) in Singapore Polytechnic. The award was announced at

the SMI Forum 2022 on 11 Oct 2022.

The support received from Maritime and Port Authority of Singapore (MPA), Singapore Maritime Institute (SMI), American Bureau of Shipping (ABS) and CEMS has been instrumental in helping Prof Zhou and his team to get the proposal approved. iTrust can now look forward to MariOT being a high-fidelity platform to help the maritime industry increase its cybersecurity posture through R&D, education, cyber drills and technology testing. The MariOT testbed is expected to be completed in Q4 of 2023 and will be iTrust's fourth industrial-scale OT testbed for cybersecurity activities. Following the award of the MariOT testbed project, iTrust Co-centre Director and maritime sector lead Prof Jianying Zhou and Assistant Director Mark Goh embarked on a study trip to three countries with a strong maritime heritage during Oct and Nov 2022. The trip was to engage with maritime cybersecurity organisations for concrete research and industrial collaboration, and to better understand the maritime research cybersecurity landscape and advancements in these nations.

A host of visits were lined up in Finland. This included meetings with Wärtsilä, a global leader in innovative technologies and lifecycle solutions for the marine and energy markets, Aalto University and VTT Technical Research Centre of Finland, the largest research and technology company and research centre conducting applied research in Finland. We also had virtual meetings with Turku University and Jyväskylä Security

Figure 7: Visit to Wärtsilä's premises (left to right): Kim Eklund, Director, Cyber as a Service, Piia Karjalainen, Head of Maritime Affairs, Matti Suominen, Cyber Security Lead, Marine Power, Prof Zhou and Mark (Photo credit: Piia Karjalainen)

Figure 8: Visit to VTT's premises (left to right): Nikolaos Papakonstantinou (Research Team Leader, Applied Cybersecurity) and Petri Puhakainen (Cyber Security Lead), Prof Zhou and Mark

Figure 9: Visit to Aalto University's premises (left to right): Mark, Dr Victor Bolbot, postdoc researcher, Asst Prof Osiris A. Valdez Banda, Marine Risks, Safety & Systems Engineering and Prof Zhou

Technology (JYVSECTEC), a company that provides information and cyber security solutions through R&D, training and exercises. Discussions with Aalto and Turku University, VTT and JYVSECTEC revolved around understanding each others' capabilities and interest in maritime cybersecurity, and find ways to collaborate in joint projects and research exchanges, cyber exercises and interconnecting platforms for cyber exercises. Intense discussions with Wärtsilä over two days led to concrete ways in which both parties could work on common topics of interest, including R&D using the MariOT testbed, technology validation of security products and contributions to a second version of iTrust's publication in cyber risk management of shipboard OT systems.

Like Singapore, the maritime and shipping industry is one of Norway's most important industries. Even before the trip, Prof Zhou has had a years-long working

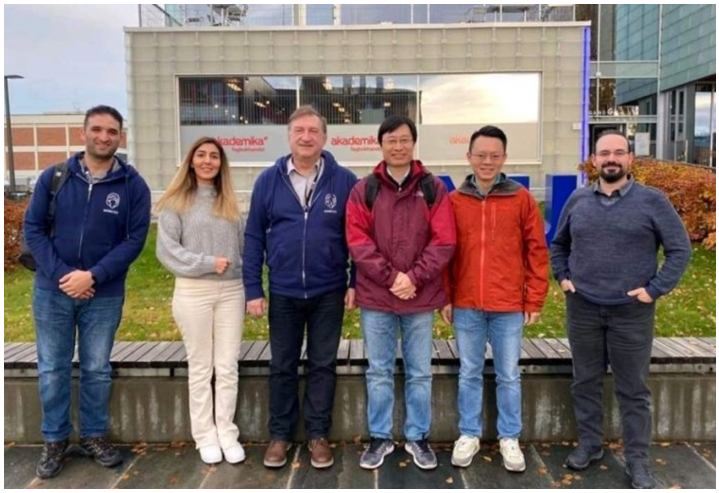

Figure 10: Visit to NTNU's premises (left to right): PhD students Ahmed Amro and Aida Akbarzadeh, Prof Sokratis Katsikas, Director, NORCICS, Prof Zhou, Mark & Aybars Oruc, PhD student

relationship with Prof Sokratis Katsikas, the Director of the Norwegian Center for Cybersecurity in Critical Sectors (NORCICS) at the Gjovik campus of Norwegian University of Science and Technology (NTNU). Prof Katsikas' team of PhD students arranged for a one-day discussion to share their impressive list of research in maritime cybersecurity and also showcased the centre's Norwegian Cyber Range. The team was delighted to learn that iTrust's testbeds and SWaT digital twin are

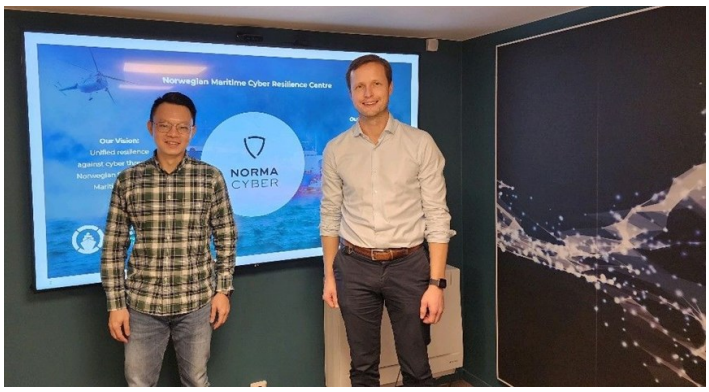

Figure 11: Visit to NORMA Cyber's premises: Mark (left) with Lars Benjamin Vold, NORMA Cyber's Managing Director

accessible remotely to support their research. The team is also keen to participate in iTrust's annual signature cyber exercise CISS and conversely for Singapore to participate in the European Cyber Security Challenge (ECSC). Joint research and training curriculum were also proposed.

The visit to NTNU, Gjovik was followed by one to the Norwegian Maritime Cyber Resilience Centre (NORMA Cyber) in Oslo the next day, courtesy of introduction by Aybars Oruc. We were hosted by NORMA Cyber's Managing Director, Lars Benjamin Vold who shared how the centre delivers centralised cyber security services to more than 80 Norwegian shipowners and other entities within the Norwegian maritime sector. It is also interested to utilise the MariOT testbed for enhanced technology validation of IDS for shipboard operations.

The final port of call of the study trip was to the University of Plymouth and University of Bristol. The University of Plymouth houses the Cyber-SHIP Lab for maritime cybersecurity research and is co-located with the university's existing maritime facilities, including a training simulator and lab. With its experience and facilities in maritime cybersecurity research, the University of Plymouth is a natural partner that iTrust seeks to collaborate with, including participation in CISS, joint proposals and staff/researcher exchanges. Our visit was hosted by Prof Kevin Jones, Executive

Figure 12: Visit to University of Plymouth's training simulator (from left to right): Prof Kevin Jones, Executive Dean for Science and Engineering and Principal Investigator for the Cyber-SHIP Lab Project, Mark, Prof Zhou & Dr Adan Lopez-Santander

Dean for Science and Engineering and PI for Cyber-SHIP Lab, Dr Kimberly Tam, Academic Lead at Cyber-SHIP Lab, Chloe Rowland, Project and Knowledge Exchange Manager at Cyber-SHIP Lab and Steve Rice, Marine-i Project Manager.

We were also delighted to visit the University of Bristol, where we were hosted by Prof Awais Rashid, Head, Bristol Cyber Security Group and his team of lecturers and researchers, including SUTD's PhD graduate and ex-iTrust researcher Dr Sridhar Adepu. Prof Rashid was also a visiting professor to iTrust on two separate occasions. A common topic of interest was

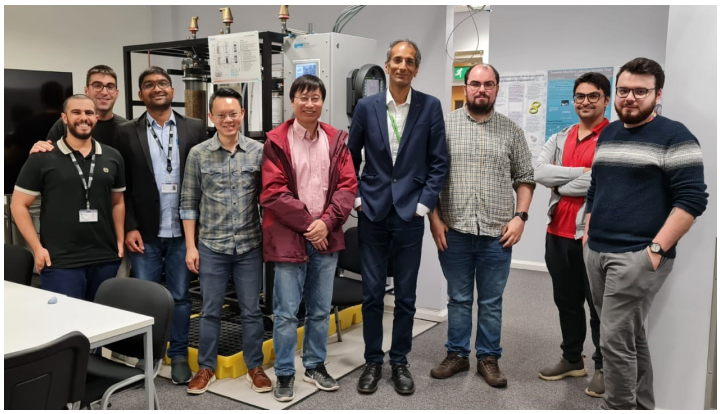

Figure 13: Prof Zhou and Mark with Prof Awais Rashid (fourth from right) and his team at Bristol Cyber Security Group

the security of cyber-physical infrastructures, supported by the group's wide array of testbed infrastructure, including ICS training boxes, federated architecture and physical industrial control hardware to control multiple physical and virtual processes.

Partnerships

iTrust signs a Memorandum of Understanding with ClassNK to work on maritime cybersecurity

iTrust and Japanese classification society ClassNK - Nippon Kaiji Kyokai inked a Memorandum of Understanding on 18 Oct 2022 to collaborate across three important maritime cyber security areas: R&D, risk management and training. A ship classification society is a non-governmental organisation that establishes and maintains technical standards for the construction and operation of ships and offshore structures.

Figure 14: Prof Aditya Mathur (left) with Capt Naoki Saito, General Manager and Head of Cyber Security, ClassNK

Following the MoU signing, in Dec 2022, iTrust and ClassNK discussed concrete plans to expand the scope of iTrust's publication in cyber risk management of shipboard OT systems, such as the inclusion of autonomous shipping. This then led to a wider network of collaborators to include those from Aalto University and Wärtsilä. A webinar will be held to discuss this topic and invite ideas and contributions from the audience.

iTrust partners with SUTD Academy to provide specialised OT cybersecurity training for professionals

By Calvin Chen, Deputy Manager, SUTD Academy

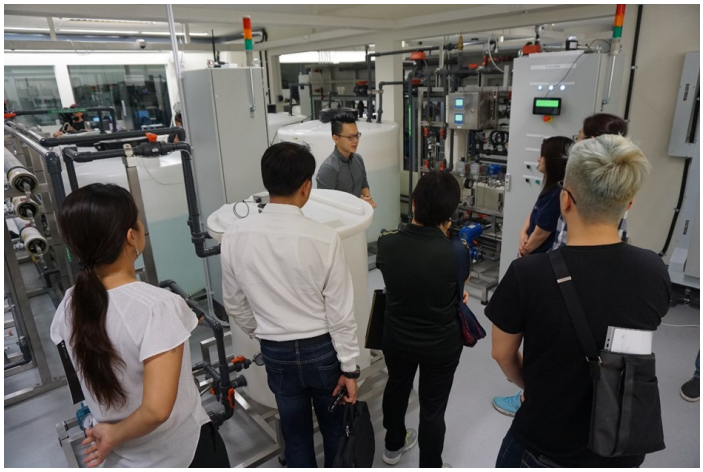

Figure 15: Participants having a tour of the water treatment (SWaT) and water distribution (WADI) testbeds at iTrust. This allows the participants to familiarise with the testbeds that will be used during live decision-making exercises

SUTD Academy, the Continuing Education and Training (CET) arm of SUTD, offers a comprehensive array of programmes to help organisations meet their reskilling goals, and equip individuals with the skills and competencies to develop a competitive advantage in today's knowledge-intensive and technology-driven economy.

A key signature training programme from SUTD Academy is its Design Innovation workshop whereby participants are introduced to innovation and creative problem-solving methods with the problem statement coming from the organisations of the participants. The other key training programmes offered are Cybersecurity, Data Science and Digital HR courses. They can be offered as short courses, or stackable individual modules that can lead to a graduate certificate or ModularMaster Certificate.

Figure 16: Participants having a hands on session using the training skid available at SWaT testbed

SUTD Academy partners iTrust to develop CET training, providing the Operational Technology (OT) platform for hands-on Cybersecurity training to professionals. These training programmes tap on the technical expertise and research knowledge from iTrust to package it as a CET course. Participants will be introduced to Cyber threats and methods to protect against cyber-attacks in the context of critical infrastructure, and they will be trained in decision-making skills under extreme cyber threats. A key aspect of the training is the use of digital twin simulation for virtual training.

Scholarships & Internships

iTrust's contribution to cybersecurity talent pipeline

The CSA-iTrust Master of Science in Security by Design Scholarship (CiMS) Programme aims to grow and develop a pool of cybersecurity professionals in Singapore. This programme is funded by the Cyber Security Agency of Singapore (CSA).

Since its launch in July 2022, iTrust has awarded eight scholarships to students pursuing the Master of Science in Security by Design (MSSD) at SUTD. The scholarship covers tuition fees and the usage of iTrust testbeds to further their research interests. Full time students are also given a laptop and a monthly stipend of $3,600. Top students can also look forward to a cash award if they maintain excellent academic results as well as opportunities for overseas exchanges.

For more infomation on the CiMS, visit: https://itrust.sutd.edu.sg/capability-development/cims/

Spectra returns

By Andy Tay, Research Assistant, iTrust

In November 2022, we concluded our second run of the 3-week basic cyber security course specially designed for secondary school students. In the first week, we provide the Spectra Secondary School students with an appreciation and understanding of the Confidentiality, Integrity and Availability (CIA) triad and how it is designed to guide policies for information security within an organisation. Basic Python programming was also included in the first week of the course to lay the foundations for PLC programming.

In the 2nd week, using the Secure Water Treatment (SWaT) testbed as a teaching tool, the students were introduced to cyber physical systems and basic plant operation. By understanding the 6-stage processes of SWaT, the students could learn how to launch attacks, see the impacts of those attacks and detect anomalies arising from those attacks.

In the final week, the students presented their assigned topics such as CIA Triad, Social Engineering and Cryptography, and shared what they learnt in during the internship. In a short space of 3 weeks, the students were also able to work on and present a Python-based mini project based assigned by their trainers.

Fig 17: Spectra Secondary School students with iTrust trainers Ivan Christian and Andy Tay (second and third from left)

iTrust is now on LinkedIn — connect with us! Feel free to reach out to us to explore research

collaborations, testbed usage and training and testing services. Email addresses end with the domain @*sutd.edu.sg*

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

Francisco FURTADO
Cyber Tech Lead, iTrust
francisco_dos

Mark GOH
Assistant Director, iTrust
Editor, iTrust Times
mark_goh

iTrust Laboratories

Andrew TAY
Cyber Security Technology Engineer
andrew_taykongngee

TAY Boon Kiat
Cyber Security Technology Engineer
boonkiat2_tay@sutd.edu.sg

National Satellite of Excellence

Jillian CHIN
Manager
jillian_chin

Siti Nadhirah Shaik NASAIR Johar
Research Associate
siti_nadhirah

Angie NG
Manager
angie_ng

General Enquiries

iTrust: *itrust*
NSoE: *nsoe_destsci*
CiMS: *cims*
Email addresses end with the domain @*sutd.edu.sg*