iTrust Times

A Quarterly Newsletter

Issue Highlights:

Apr —Jun 2024 | Volume 10 Issue 2

From Centre Director's Desk

Dear readers,

Greetings from iTrust!

First and foremost, I would like to extend my heartfelt gratitude to iTrust Cyber Tech Lead Francisco for his outstanding contributions over the past 8 years and wish him the best in his future endeavours.

At iTrust, we have been actively engaged in exploring maritime cybersecurity. During the Singapore Maritime Week (SMW) 2024, iTrust participated in two MoUs led by the Maritime and Port Authority of Singapore (MPA). The first MoU, with the partners from Estonia, aims to boost cybersecurity within the maritime sector. The other, with local collaborators, focuses on enhacing maritime cybersecurity capabilities and developing the talent pipeline in the cybersecurity domain. Once built, the MariOT testbed will play an important role in supporting the activities under these MoUs.

iTrust is committed to translating its cybersecurity research into impactful technologies for real-world applications. A new project funded by SUTD under the Research Translation Innovation Platform (RTIP) Funding scheme aims to develop AI-driven technology capable of accurately detecting and decoding network packets containing anomalous payloads.

Since 2020, iTrust has actively been involved in the NATO's cybersecurity exercises. In Locked Shields 2024 (LS2024), iTrust contributed an enhanced version of the GASP system, and provided green team support to the Blue Teams defending GASP systems against Red Team attacks. Through those exercises, iTrust demonstrated its strong capability in creating and managing the OT digital twins meeting the demands and requirements for the world's largest and most complex live-fire cyber defence exercise.

In April, iTrust organised the inaugural International Conference on the Design of Cyber-Secure Water Plants (DCS-Water '24) in Buford, Georgia, USA, in collaboration with The Water Tower. This conference brought together a diverse group of researchers and practitioners to present and discuss novel methods and tools for protecting water plants against cyberattacks. During the conference, iTrust launched the inaugural Critical Infrastructure Artificial Intelligence (CI.AI) Challenge 2024. This Challenge aims to develop AI-driven solutions capable of detecting and mitigating cyber threats within iTrust's Secure Water Treatment (SWaT) testbed.

Looking ahead, iTrust is honoured to serve as the main organiser of the 19th ACM Asia Conference on Computer and Communications Security (AsiaCCS'24), a leading cybersecurity conference to be held in Singapore on 1-5 July 2024. There will be a special tour to visit labs at iTrust and Future Communications R&D Programme at SUTD on 1 July. As the general chair, I eagerly anticipate welcoming a record number of participants from around the globe.

Jianying Zhou Centre Director, iTrust, SUTD
Professor of Cyber Security, ISTD Pillar, SUTD

CSA SINGAPORE

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust Centre for Research in Cyber Security

LS2024

Locked Shields 2024

By: Aanand R, Cybersecurity Technology Engineer, iTrust

I had the opportunity to participate in Exercise Locked Shields 2024 (LS24), representing both iTrust, and Singapore as part of the Green Team in Tallinn, Estonia in both the Partners Run on 6 and 7 March 2024, and in the Main Execution Run from 23 to 26 April 2024. LS24 was the 14th edition of the annual cyber defence exercise organised by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). The event is currently the largest, and most complex live–fire cyber defence exercise, and iTrust is a regular participant and contributor to the exercise. For LS24, iTrust contributed an enhanced version of its gas pipeline (GASP) cyber twin.

Fig 1.: Collaboration between iTrust and its sister-lab NCL during Main Execution Run of Locked Shields 2024. (From Left to Right) R Aanand CSTE, SEAH Choon Meng NCL Program Director, KANG Niklaus NCL Deputy Head of Technology, WONG NCL Felix Infrastructure Engineer

As part of the GT, our responsibilities included enhancing and modifying GASP as per exercise requirements throughout development cycles and ensuring its availability during Partners and Main Execution runs. We supported Blue Teams who were defending various systems against Red Team attacks and managed ticket requests submitted by Blue Teams whenever they faced issues.

My involvement in LS24 allowed me to strengthen my skills and knowledge in development cycles and network automation. I was also exposed to the use of Rocket.Chat, MS Share Point, Cisco Anyconnect Secure Mobility VPN client, Arion Vault, the Filezilla Client, GitLab, Provedentia, and vCenter during the runs. My role in GT also meant I could learn from, collaborate, and network with representatives from the Digital Intelligence Service, ST Engineering, CSA, and our sister lab NCL, as well as organisations such as Aselsan, Fujitsu, TalTech who also made contributions to LS24.

MoU Signing

Maritime-related MOUs Signing at Singapore Maritime Week 2024

During the Singapore Maritime Week (SMW) 2024, the Maritime and Port Authority of Singapore (MPA) signed two memorandums of understanding (MoU) with SUTD. These MoUs, signed on 16 April 2024, in the presence of Senior Minister of State for Transport and Sustainability and the Environment Dr. Amy Khor, aim to enhance cybersecurity in the maritime sector through collaborative research, development, testing initiatives, and training programs.

Fig 2.: The Mou was signed by David Foo, Assistant Chief Executive (Operations Technology), MPA; Mr Roomet Leiger, Director, TalTech; Mr Silver Andre, Chief Executive Officer, Foundation CR14; Mr Tan Cheng Peng, Executive Director, SMI; and Prof Chua Chee Kai, Associate Provost, SUTD.

The first MoU was signed among MPA, Estonian organisations Tallinn University of Technology (TalTech) and Foundation CR14, the Singapore Maritime Institute (SMI), and SUTD. This MoU aims to boost cybersecurity within the maritime sector through collaborative research and development, testing initiatives, and training programs. Once built, SUTD's Maritime Testbed of Shipboard Operational Technology (MariOT) will be used to support simulations drills and exercises with industry partners.

Fig 3.: The MoU was signed by Mr Teo Eng Dih, Chief Executive, MPA; Ms Caroline Yang, President, SSA; Professor Chua Kee Chaing, President, SIT; and Professor Chong Tow Chong, President, SUTD.

The second MoU involved MPA, the Singapore Shipping Association (SSA), the Singapore Institute of Technology (SIT), and SUTD. This MoU focuses on enhancing cooperation and information exchange regarding cybersecurity among maritime entities. It also looks at developing maritime cybersecurity capabilities and reinforcing the talent pipeline in cybersecurity.

DCS-Water'24

DCS-Water'24—1st International Conference on the Design of Cyber-Secure Water Plants

The inaugural International Conference on the Design of Cyber-Secure Water Plants (DCS-Water '24) was a 2-day conference aimed at bringing together a diverse group of researchers and practitioners to present and discuss novel methods and tools for protecting water plants against cyberattacks. The conference was held in Buford, Georgia, USA and jointly organised by iTrust, Centre for Research in Cyber Security at the Singapore University of Technology and Design, and its international collaborator The Water Tower, a non-profit global water innovation hub for water and wastewater utilities, researchers, private companies, and water-related organizations to collaboratively solve critical, real-world water and environmental challenges.

The conference was evenly divided into four segments over two days: academic presentations, tools for training and R&D, industry perspective, and breakout session.

In the academic presentations, common topics amongst the presenters were the use of digital twins and physical testbeds, machine learning and datasets for a variety of use cases, including training, anomaly detection and decision making. Roman Malits (Technion Institute of Technology, Israel) and Tino Paulsen (Leuphana University, Germany) both used iTrust's Secure Water Treatment dataset (SWaT) for their machine learning models. Roman spoke about the use of distributed representations (SDRs) and a Hierarchical Temporal Memory unsupervised learning algorithm (HTM) to design a hierarchical online anomaly detection system for industrial cyber-physical systems. Tino's team adopted the variational autoencoders on Riemannian manifolds to improve anomaly detection rates. Another example of iTrust's dataset being used by researchers was Corwin Stanford's (Jackson State University, USA) team, who applied Long Short-Term Memory (LSTM) Recurrent Neural Networks (RNNs) on iTrust's Battle of the Attack Detection Algorithms (BATADAL) dataset for anomaly detection and lowering false positives in SCADA systems.

Fig 4.: iTrust Founding Centre Director Prof Aditya Mathur introducing Prof Richard DeMillo from Georgia Tech as the opening speaker

Digital twins and testbeds also featured heavily in the presentations. Sam Bryce (Fortiphyd Logic, USA) and Saranachon Iammongkol (Cybersecurity Technology Institute, Taiwan) both espoused the use of digital twins for raising awareness of OT security and providing realistic training and demonstration. Sam also spoke about leveraging on 3D graphic visualisations utilising WebGL to see the physical impacts of cyber-attacks on simulated water plant. From a testbed's perspective, Thomas Edgar (Pacific Northwest National Laboratory, USA) shared how his laboratory, in collaboration with Idaho National Laboratory, set up the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency's (CISA) Control Environment Laboratory Resource (CELR) to run threat hunting and incidence response training exercise for water systems. Nazmul Kabir Sikder (Virginia Tech, USA) showed how his team used both the digital twin and physical testbed (named the AI and Cyber for Water and Agriculture; ACWA) to validate AI- and data-driven technologies, by comparing the theoretical results with real-life results.

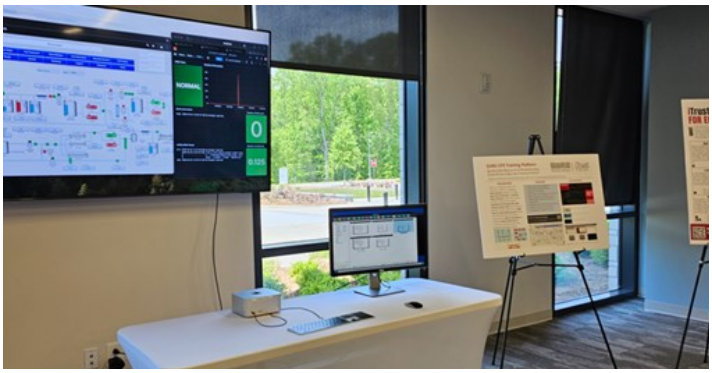

Fig 5.: iTrust's booth at DCS-Water '24 showcasing iTrust's technologies and professional training capabilities

About 50 cyber and water professionals from the academia, government and industry attended DCS-Water '24. Given the encouraging participation and feedback, the organising committee has decided to organise DCS-Water '25 in May 2025.

CI.AI Challenge 2024

CI.AI Challenge 2024: Advancing AI in Industrial Cybersecurity

The inaugural Critical Infrastructure Artificial Intelligence (CI.AI) Challenge 2024, organised by iTrust, is a pioneering challenge that brings together global talent to tackle cybersecurity challenges in industrial control systems (ICS).

The primary goal of this challenge is to develop AI-driven solutions capable of detecting and mitigating cyber threats within the Secure Water Treatment (SWaT) testbed, an industrial-grade testbed at iTrust that replicates water treatment plants. The challenge is open to researchers, engineers, data scientists, and professionals, and aims to create the most effective and innovative AI algorithms. The challenge is structured into two phases: the Historical Challenge and the Live Challenge.

In the Historical Challenge phase, participants received the dataset under SWaT's normal and attack scenarios. This dataset, comprising sensor and actuator readings captured over a continuous period of 72 hours, was divided into training and test data. The objective was for participants to develop algorithms that learn the normal behaviour of SWaT's physical processes using the training dataset and detect anomalies in the testing dataset, whilst attempting to achieve high detection rates with minimal false alarms. The top five models from the Historical Challenge will advance to the Live Challenge phase, from 3 Jul 2024 to 10 Jul 2024. Participants will be given VPN access to live data of SWaT, where they will have to detect real-time anomalies. This phase includes a baselining period and a final evaluation, during which physical manipulations and cyber-attacks will be conducted to test the accuracy and efficacy of the participants' algorithms. For more information on the types of attacks launched in both phases, please refer to the CI.AI website: https://itrust.sutd.edu.sg/ci-ai-challenge-2024/

The performance of the algorithms is assessed using three key metrics: Detection Rate, False Alarm Rate, and Target Identification Rate. To ensure a balanced evaluation of the algorithms developed, a weighted combination of the three key metrics is used to determine the overall metric. After the challenge has concluded, iTrust plans to prepare a jointly authored manuscript to share the findings and methodologies with the cyber security community.

Through this challenge, participants develop advanced AI algorithms that can identify and analysing cyber threats in real-time, thus enhancing the robustness of Operational Technology (OT) and ICS environments. The challenge then leads to the creation of predictive and reactive AI systems that effectively detect and respond to unusual behaviour or potential threats. Intelligent systems are designed not only to detect threats but also to propose and implement strategies to mitigate these risks, hence ensuring the integrity and security of critical infrastructure. From the innovative solutions developed, participants contribute to the body of knowledge in cybersecurity and help to establish new benchmarks and best practices for AI applications in OT and ICS.

Future developments may include a new edition of the CI.AI Challenge, which will integrate information technology (IT) data to evaluate and enhance the effectiveness of solutions in detecting both IT- and OT-based attacks. This will further foster collaboration and innovation in the field of industrial cybersecurity.

RTIP Award

Deep Learning-Based Early Intrusion Detection System to Mitigate Process Anomalies in Industrial Control Systems

iTrust was awarded a project to enhance the security of Industrial Control Systems (ICS) through the use of deep learning-based early intrusion detection system. Over a one-year timeframe, the team, led by iTrust Research Fellow Dr Gauthama Raman, will develop AI-driven technology capable of precisely detecting and decoding network packets containing anomalous payloads that impact the behaviour of Programmable Logic Controllers (PLCs), resulting in process anomalies. This capability plays a crucial role in facilitating anomaly detection at the IT-OT level, thus safeguarding the operations of ICS without any disruption.

The team's methodology is designed to undergo rigorous testing on iTrust's testbeds, which include SWaT, WaDi, and EPIC, before potential deployment in industrial settings with the support of iTrust's translation partners. Dr Raman received a funding of $155K by SUTD under the Research Translation Innovation Platform (RTIP) Funding scheme to pursue the development.

CiMS Writing Competition

In March 2024, the CSA-iTrust Master of Science in Security by Design Scholarship programme conducted a writing competition and received three excellent writeups from its scholars. They were asked to share the reasons behind their application to the scholarship and how the scholarship has benefitted them.

Three themes were common among their responses: Firstly, they recognised the trend of the " swift convergence of Information Technology and Operational Technology, especially in critical infrastructures." Secondly, though the CiMS scholarship, they were able to tap into the MSSD programme's unique focus on "integrating cybersecurity principles into the design phase," allowing them "access to invaluable resources, and… engage in specialised coursework and practical experiences." Thirdly, the CiMs scholarship " opened doors to networking opportunities…enabling me to connect with like-minded professionals," and also "alleviates the burden of tuition fees, enabling students to focus on their studies without compromising other extracurricular activities."

Three winning submissions were given a corporate photoshoot. Congratulations to Alvin Ting, Krishnan Parthipan and Lee Si Hao!

About the CiMS: The 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). Applications are opened to Singaporeans and PRs who have enrolled in the MSSD Programme, and are available annually till end-Jul. More details can be found here: https://itrust.sutd.edu.sg/capability-development/cims/

Visits

iTrust SUTD Centre Director Jianying Zhou and Assistant Director Mark Goh hosted Lithuania's Vice -Minister of the Economy and Innovation Erika Kuročkina, Dr. Sigute Stankeviciute and their colleagues at iTrust on 31 May 2024.

Fig 6.: Mark Goh (left) and Prof Jianying Zhou (second from left) engaging with Dr Sigute Stankeviciute, Head of ManuFuture Lab, Innovation Agency Lithuania (seated, in white), and Ms Erika Kurockina, Lithuania's Vice-Minister of Economy and Innovation

They discussed the various use cases of digital twins for city planning and cyber security, and shared iTrust's experience in organising and supporting international and local cyber exercises, especially its engagement with NATO. The visit also allowed the Lithuanian counterparts to see the collective and collaborative efforts that Singapore puts into ensuring a safe, secure and resilient cyber space.

A Toast to Francisco!

Farewell Francisco!

By Aditya Mathur, iTrust Founding Centre Director

A student, a colleague, and a friend - that is what Francisco has been to me. It was sometime in 2013 when I met Francisco for the first time. He was a student in my freshman Python class. With an ever-present smile, Francisco had a unique presence. He seated himself on my left towards the end of the classroom. The Python class utilised SUTD's flagship active learning for content delivery. I would spend a few minutes lecturing and then ask the students to solve a problem. As programming is tough especially to those who have not been exposed to it, support instructors were also present in the classroom. Despite that, Francisco made himself available to help other students as he already knew how to program.

I believe I had asked Francisco to join iTrust soon after he graduated from SUTD with a degree in Computer Science. He did so in October 2016, joining iTrust as a research assistant in Project ASPIRE, funded by the National Research Foundation (NRF). Over the next two years, Francisco made numerous contributions to the project. He organised the SWaT Security Showdown 2017, conducted a cyber awareness outreach programme for over 200 secondary school students, developed an MITM attack launch tool named A6-L1, among other achievements.

Between 2019 and 2023 iTrust saw a significant surge in R&D activities. All three OT testbeds - SWaT, WaDi and EPIC - were fully functional and in use by researchers from all IHLs in Singapore. The renamed Critical Infrastructure Security Showdown (CISS) became a major international event thanks to COVID. Most notably, and significantly benefiting to MINDEF and iTrust, was Singapore's entry into NATO's coveted cyber exercise, Locked Shields. The workload increased significantly, and iTrust needed someone who could oversee technical activities in all testbeds, interface with MINDEF and NATO, as well as guide researchers when needed. It is in the management of all these activities that Francisco was

promoted to Cyber Tech Lead, and where he excelled. In this role, Francisco worked marvellously well with MINDEF and NATO nations in smooth deployment and operation of the digital twins developed in iTrust. Francisco also played a key role in supporting MINDEF's flagship cyber-security event – the Critical Infrastructure Defence Exercise (CIDeX.) Most recently, Francisco spent time at The Water Tower in Buford, Georgia, where he worked with me in an ongoing pilot exercise in a large-scale wastewater treatment facility.

Francisco is technically gifted and highly proficient. His excellent academic background, coupled with rich work experience in iTrust, places him in the category of highly sought after individual in the domain of critical infrastructure security. Francisco has made numerous friends in iTrust, and how can he not, with a personality full of humility and an ever-present smile? On behalf all in iTrust, I thank Francisco for his outstanding service. On behalf of iTrust, we wish him, and his wife Natalie, the very best their careers!

New Hire

Joel Ng joins iTrust as a cybersecurity technology engineer. He graduated with a Bachelor of Engineering in Computer Science and Design (CSD) in 2024 from the Singapore University of Technology with a specialisation in Cybersecurity. Joel's wide variety of interest includes scuba diving, gaming and cooking.

iTrust Matters

General Enquiries

iTrust: *itrust*

NSoE: *nsoe_destsci*

CiMS: *cims*

Email addresses end with the domain ***@sutd.edu.sg***

Management

Prof. Jianying ZHOU

Centre Director, iTrust, Singapore University of Technology and Design

Professor, Information Systems Technology and Design (ISTD), Singapore University of Technology and Design

jianying_zhou

Prof. Aditya P MATHUR

Founding Centre Director, iTrust, Singapore University of Technology and Design

Director, National Satellite of Excellence, DeST-SCI

Professor Emeritus, Computer Science, Purdue University

aditya_mathur

Mark GOH

Assistant Director, iTrust

mark_goh

Scan to view previous issues

iTrust Laboratories

Andrew TAY

Research Senior Technologist

andrew_taykongngee

Aanand R

Cyber Security Technology Engineer

Aanand_r

Joel NG

Cyber Security Technology Engineer

Joel_ng

National Satellite of Excellence

Jillian CHIN

Manager

jillian_chin

Angie NG

Manager

angie_ng

Siti Nadhirah Shaik NASAIR

Snr Research Associate

siti_nadhirah

Vanessa LEE

Deputy Manager

vanessa_lee