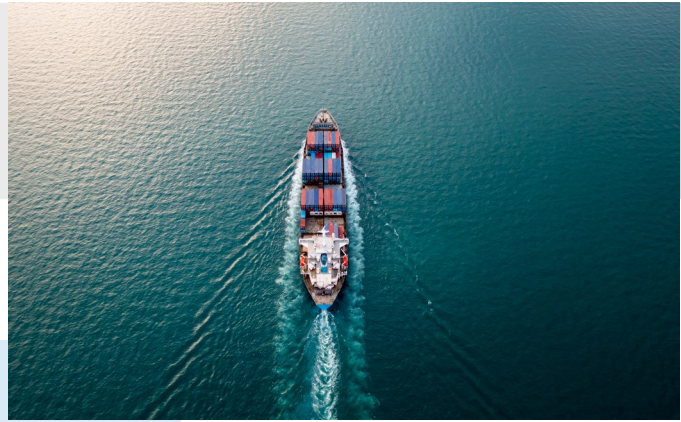


Issue Highlights:

- ◆ Visit to Maritime Companies *pg. 2*
- ◆ Roundtable Session with The Singapore Shipping Association *pg. 2*
- ◆ CSA-iTrust MSSD Scholarship Programme *pg. 3*
- ◆ Critical Infrastructure Security Showdown *pg. 3*
- ◆ Critical Infrastructure Defence Exercise *pg. 4*



Jul — Sep 2022 | Volume 8 Issue 3

Venturing High CISS

Dear Reader:

Greetings from iTrust! We are at the end of the third quarter of 2022 and iTrust is, as usual, buzzing with activities. As I compose this forward, the sixth Critical Infrastructure Security Showdown (CISS2022) is nearing its end. 10-teams from various countries

have launched attacks on three of iTrust's testbeds: namely, Electric Power (EPIC), water treatment (SWaT), and water distribution (WADI). This year is the first time that EPIC has been included as a potential target for the attackers. Several vendors and iTrust researchers are testing their anomaly detection mechanisms and systems. As in the past, a report summarising the attacks launched and performance of the various detectors, will be available to public in a few weeks following the event.

iTrust is making rapid progress towards establishing a one-of-a-kind research program in maritime security. This effort is being led by Professor Jianying Zhou and iTrust Assistant Director Mark Goh. Funds have been set aside by the Singapore Government to build a unique maritime shipboard OT testbed that will support research in maritime security. Progress in this area will be provided

in the next issue of the newsletter.

In addition to CISS, iTrust is working closely with MINDEF to organise Critical Infrastructure Cyber Defence Exercise (CIDeX). iTrust researchers Francisco Furtado, Jit Biswas, and Siddhant Shrivastava are working closely with MINDEF staff to prepare course material to familiarise the defenders participating in CIDeX. A composite red team will launch attacks on iTrust testbeds while the defender trainees defend the live operational plants.

iTrust is also proud to be awarded a scholarship programme by CSA to train the next generation of cyber professionals under the MSSD Programme. The scholarship programme is open for application and will run for 3 years.

That is all for now. Happy reading and best wishes to all readers of iTrust Times for a productive and happy 2022!

A handwritten signature in black ink, appearing to read 'Aditya Mathur'.

Aditya Mathur

Centre Director, iTrust, SUTD

Director, National Satellite of Excellence DeST-SCI

Professor Emeritus, Computer Science, Purdue University

Visit to Maritime Companies

Petit à petit, l'oiseau fait son nid

Little by little the bird makes its nest (French idiom). And so it is, the progress that iTrust is making towards maritime cybersecurity. At the invitation of the Singapore Maritime Institute (SMI), iTrust Co-centre Director Prof Jianying Zhou joined a delegation to visit CMA CGM

and Bureau Veritas at their respective offices in Marseille and Paris. CMA CGM is a French container transportation and shipping company and the world's third largest container shipping company while Bureau Veritas (BV) is a world leader in laboratory testing, inspection and certification services.

The visit was led by SMI's Executive Director Mr Tan Cheng Peng and the delegation also included representatives from the Institute of High Performance Computing (IHPC) and Singapore Institute of Technology (SIT); Prof Zhou was accompanied by iTrust Assistant Director Mark Goh and Cyber Tech Lead Francisco Furtado. The objective of the trip was to showcase iTrust, IHPC and SIT's capabilities and research thrusts in maritime R&D and find common grounds to collaborate with these leading maritime companies.

Since the conclusion of a 1-year study on cyber risk management in shipboard operational technology (OT) systems which led to a set of guidelines for cyber risk identification and mitigation, iTrust has been aggressively pursuing a new critical infrastructure



Figure 1: The IHL delegation led by SMI's Executive Director Mr Tan Cheng Peng (fifth from left) at CMA CGM's HQ in Marseille, with CMA CGM's Vice President, R&D Assets Ms Karine Desrues (fourth from right) (Photo credit: SMI)

domain. Encouraged by the positive feedback from the industry on the guidelines and using years of iTrust's experience and knowledge in protecting water and power infrastructure, Prof Zhou has submitted a proposal to the SMI to fund a new maritime OT (MariOT) testbed to augment cybersecurity research, training, exercise and education. The visits to CMA CGM and BV were to seek their inputs on the design of the testbed and how it could serve their cybersecurity needs and the entire maritime ecosystem.

The outcome of the intensive and fruitful two-day discussions with CMA CGM and BV are four concrete areas that iTrust could work on in collaboration with each company. Thanks to SMI, iTrust is now, little by little, making inroads – or to misuse the word, “inwaterways” – into the maritime sector.



Fig 2: The BV team with SMI, IHPC, iTrust, SIT and representatives from the Maritime and Port Authority of Singapore (MPA) in Paris (photo credit: SMI)

Roundtable Session with The Singapore Shipping Association

Plans on iTrust's maritime testbed and cybersecurity risk management pain points faced by the shipping industry were shared during the roundtable session

On 22 Jul, iTrust hosted the Singapore Shipping Association's Cybersecurity Sub-committee members at SUTD to share the outcomes of a survey of its members on maritime and port pain points in cyber risk management and cyber drill requirements. The three-hour session also included a sharing by Prof Zhou on iTrust's plans to build a maritime testbed and a tour of iTrust's OT testbeds. Participants at the session included

those from MPA, SMI, shipping lines, ship management, maritime technology and oil and gas companies.



Fig 3: Prof Jianying Zhou (eight from left) with MPA, SMI and SSA members (photo credit: Chris Chung)



iTrust is proud to be selected by Cyber Security Agency of Singapore (CSA) as the anchor research centre to host the CSA-iTrust Master of Science in Security by Design Scholarship (CiMS) Programme.

The CiMS programme was announced by Mrs Josephine Teo, Minister for Communications and Information and Minister-in-charge of Smart Nation and Cybersecurity, at the Operational Technology Cybersecurity Expert Panel (OTCEP) Forum 2022.

The programme aims to grow and develop a pool of cybersecurity professionals in Singapore. CSA is funding 80 scholarships over 3 years to encourage STEM professionals to pursue the Master of Science in Security by Design (MSSD) at the Singapore University of Technology and Design. This scholarship is open to Singaporeans or Singapore Permanent Residents enrolled in the MSSD programme (part- and full-time). Successful applicants can expect to receive stipends during their candidature (for full-time students) and a full sponsorship for their tuition fees, along with other benefits. Please visit <https://itrust.sutd.edu.sg/capability-development/cims> for more information.



The Critical Infrastructure Security Showdown 2022 (CISS 2022) is iTrust's sixth international technology assessment cyber exercise. CISS 2022 is held entirely online and is sponsored by the National Research Foundation and the Ministry of Defence.

CISS2022 returns the following exciting additions:

- CTF-style challenges for Stage 1
- Electric Power and Intelligent Control (EPIC) testbed as additional attack surface
- 4 hours of pure OT platform for Red Teams

A record 28 Red Teams from the academia, industry and government sectors signed up for CISS 2022. As with the previous year, Stage 1 was organised to admit the top 10 Red Teams into the finals. This year, iTrust is proud to partner with the National Cybersecurity R&D Laboratories (NCL) at the National University of Singapore to organise a Star Wars-theme Stage 1. Spanning over 48 hours, Red Teams were tasked to solve various ICS-centric challenges. The top 10 Red Teams, in no order of merit, are: 404: APT Not Found; CISS The Day; COMCYBER FRA; GeForceTwo; Hired Goons; JPZS; RED ALERT; Team Italy; uncleCY; and White Caps.

In addition to CISS, the Ministry of Defence, Singapore (MINDEF) is also organising the Critical Infrastructure Defence Exercise (CIDeX) 2022.

CIDeX is an inclusive cyber exercise that gives Singapore's critical infrastructure (CI) operators and regulators a learning platform to appreciate and practice the defence of a CI. With a better insight into how a CI – comprising IT and OT networks – can suffer from cyber attacks and their adverse consequences, the CII teams can distil these lessons and tailor them to



augment their respective organisations' cyber response and protection strategies.

In 2021, the inaugural CIDeX was originally part of the two-week Critical Infrastructure Security Showdown cyber exercise. Having grown in scale, CIDeX 2022 returns this year as a standalone cyber exercise with the addition of another CI system to bring it to a total of three such systems. These systems will be attacked by a composite red team and defended by the CII blue teams.

Last year's inaugural CIDeX saw nearly 50 CI participants forming teams of 10 each. The CI sectors that were represented at CIDeX 2021 included water, power and telco. These sectors will return this year, along with two additional CI sectors – land transport and maritime. CIDeX 2022's modality is updated to having the five CI blue teams monitor and defend the CI systems concurrently over two days. This update brings new challenges to the CI blue teams, who have more systems to monitor over a longer period, as well as to the composite red team that is tasked to launch attacks against 50 CI guardians.

A comprehensive familiarisation programme will be conducted to equip the CII blue teams with the capability and confidence to navigate through the CI platform and utilise cyber tools to monitor the platform and respond to cyber attacks.

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_taykongnee

TAY Boon Kiat

Cyber Security Technology Engineer
boonkiat2_tay@sutd.edu.sg

National Satellite of Excellence

Jillian CHIN

Manager

Siti Nadhirah Shaik NASAIR Johar

Research Associate

Angie NG

Manager

angie_ng

General Enquiries

iTrust: itrust

NSoE: nsoe_destsci

CiMS: cims

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



<https://itrust.sutd.edu.sg>



itrust@sutd.edu.sg



Singapore University of Technology and Design | 8 Somapah Road, Building 2 Level 7, Singapore 487372