iTrust Times

A Quarterly Newsletter

Issue Highlights:

Jul — Sep 2024 | Volume 10 Issue 3

From Centre Director's Desk

Dear readers,

Greetings from iTrust!

I am delighted to share that the tender for design, construction and commissioning of the maritime testbed of shipboard OT (MariOT) systems has been awarded. ST Engineering Info-Security Pte Ltd will work with its partners to deliver an industrial-grade cyber-physical platform, combining essential shipboard operational technology systems with virtual simulation models. This will be an important milestone for iTrust to expand its capacity in securing critical infrastructure to the maritime sector. The MariOT tested will be used to support a variety of cybersecurity activities such as research, training, exercises and education. We are working closely with MPA and SMI in preparation for maritime cybersecurity exercises on the MariOT testbed.

iTrust has been organising Critical Infrastructure Security Showdown (CISS) since 2016, which is an OT-centric cybersecurity exercise using the OT testbeds hosted and operated by iTrust. CISS 2024 saw a record number of 55 red teams signing up this year. They were tasked to solve challenges related to critical infrastructure sectors in water, power and gas pipeline. A big congratulation to the top three red teams! Many thanks to the supporting partners and organising committee members.

A team of researchers, led by Assoc Prof Sudipta Chattopadhyay, gave a live demonstration of our 5G fuzzing and over-the-air exploitation tools in front of professional hackers, cybersecurity professionals and policy makers at this year's DEFCON. Congratulations to the team for developing a suite of practical and high-impact security testing tools.

iTrust was a main organiser of 19th ACM Asia Conference on Computer and Communications Security (AsiaCCS'24), a leading cybersecurity conference held in Singapore on 1-5 July 2024. As the steering committee chair of AsiaCCS and a general chair of AsiaCCS'24, I am pleased to witness the new record numbers of paper submissions and attendees from worldwide. A special tour was organised for the delegates to visit iTrust and Future Communications Connectivity Lab (FCCLab) in SUTD. They had the opportunity to know more about iTrust testbeds and OT cybersecurity. Thanks to our local organising committee and volunteers for their contributions to make the event a big success.

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

ACM AsiaCCS

ACM AsiaCCS 2024

The ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2024) has just wrapped up in Singapore, and it was a resounding success with a record-breaking number of participants! The conference brought together more than how many? subject experts in cybersecurity for a whirlwind of presentation and discussions of the latest research and advancements in the cybersecurity field.

Fig 1.: iTrust Cyber Tech Lead Siddhant Shrivastava giving an overview of iTrust to the visiting delegates

Fig 2.: iTrust Research Fellow Dr Yanlin Aung showcasing the IoT shielded room

iTrust was involved in the 1 July visit to SUTD where we showcased our various testbeds to the delegates. The delegates were brought to SWaT, WaDi, EPIC, and the IoT Shielded room during the tour. The delegates were also brought to SUTD Future Communications Connectivity Lab (FCCLab) for a tour as well.

This year's conference covered a wide range of hot topics — from secure machine learning to advanced threat detection and privacy-preserving technologies. Each keynote and research presentation offered a fresh look at the current challenges and potential solutions in cybersecurity.

Prof Jianying Zhou, Centre Director of iTrust, who was the co-General chair of the conference, also chaired the Cyber-Physical System Security (CPSS) Workshop

Fig 3.: FCCLab Deputy Director Prof Binbin Chen presenting an overview of the FCClab

Fig 4.: Ivan Christian (Research Assistant, iTrust) presenting on his paper.

on 2 July. At this workshop, Ivan Christian, Research Assistant from iTrust, had the opportunity to present his paper 'DRACE: A Framework for Evaluating Anomaly Detectors for Industrial Control Systems'.

Fig 5.: AsiaCCS 2024 Local Organising Committee with the volunteers from SUTD, NTU and SMU

If you missed any of the action or want to dive back into the discussions, feel free to visit the AsiaCCS 2024 website.

DEFCON

DEFCON 32

By: Associate Professor Sudipta Chattopadhyay

Our work on 5G fuzzing, specifically 5Ghoul was accepted for presentation in this year's DEFCON 32 demo labs at Las Vegas

Convention Center, Las Vegas, USA. For the unversed, DEFCON is a conference for "hackers" and has been held annually in Las Vegas since 1993. Being first-time attendees, we had a very enriching experience attending DEFCON 32.

Fig 6.: PhD Student Matheus Eduardo Garbelini (left) and Assoc Prof Sudipta Chattopadhyay (right) at DEFCON, proudly posing with their speaker badges

As part of our accepted demo lab presentation, we had the opportunity to show a physical demonstration of our 5G fuzzing and over-the-air exploitation tools to professional hackers, cybersecurity professionals, policy makers and so on. Notably, it was great to show, in front of a "hacker" audience, a live attack on a state-of-the-art 5G smartphone that results in manually rebooting the phone to restore any 5G connectivity.

Before the presentation, we were afraid that there won't be many audiences due to the nature of the research embodied in our tool. To our surprise, we were blessed with a full audience of around 70 persons and even had to repeat our presentation and demonstration for a second set of audience.

We received very positive feedback of our tool. A member of the audience focusing on RF security came forward to congratulate us, and shared that they were currently using our open source 5Ghoul tool for testing many 5G UEs in their settings. We also received encouraging feedback in extending our tools for 5G base station (gNB) testing and testing other 5G procedures.

A unique and appealing feature of the badge provided by DEFCON 32 (Fig 7) was that it was made from a newly released Raspberry Pi RP2350 where we could play a game on it, along with tutorials to flash new firmware and customise the badge.

Overall, it was a great experience and an honor to speak at our first DEFCON. We thank iTrust and SUTD for supporting this research that leads to a practical, high-impact tool.

Fig 7.: Unique DEFCON badges

CISS 2024

CISS 2024

By: Andy Tay, Research Assistant, iTrust

This year's Critical Infrastructure Security Showdown (CISS): The Orthanc Obstacles introduced an exciting new competition format. In previous editions, the cyber exercise followed a two-phase format, with a 48-hour Capture the Flag (CTF) qualifying round followed by live cyber-attacks on iTrust testbeds.

Collaborating with the Digital Intelligence Service (DIS) and supported by iTrust's sister lab, the National Cybersecurity R&D Lab (NCL), iTrust developed the operational technology (OT) focused CTF challenges that included the use of its Secure Water Treatment System (SWaT) testbed and Gas Pipeline (GASP) cyber twin. Leveraging NCL's advanced computing resources and network infrastructure, iTrust was able to host more than 40 teams simultaneously for the 2-day CTF.

In addition to the new exercise modality, iTrust also welcomed new collaborators - Deutschlands Bester Hacker (DBH), IllusionIQ, and Illinois Advanced Research Center at Singapore (IARCS) – to CISS 2024, where they contributed to more than half of the 52 IT

and OT challenges, ranging from Modbus to PLC ladder logic, honeypots and a power grid digital twin. NCL also provided a team of engineers to support the CTF round the clock alongside iTrust's and IARCS' engineers and researchers.

After a neck and neck competition up to the final hours of the exercise, Team Sesame (Singapore) emerged as the champions, followed by Team UncleCY (Singapore) and Team KrautStike (Germany). Congratulations to the top three red teams, who will receive cash prizes of S$4,000, S$2,000 and S$1,000 respectively.

The annual CISS is funded by the Cyber Security Agency of Singapore.

Live Demo

Cyber-Physical Attacks Live Demo to MPA

By: Siddhant Shrivastava, Cyber Tech Lead, iTrust

The Maritime and Port Authority of Singapore (MPA) and members from the Singapore Maritime Officers' Union recently witnessed a live demo of cyber-physical attacks on critical infrastructure systems, using iTrust's Secure Water Treatment Testbed (SWaT) as the demo platform. The attendees were seated in the MPA Port Operations Control Centre (POCC) at PSA Vista and were guided through the demo by iTrust Research Associate Siddhant Shrivastava through an immersive Zoom session, where they could see live feeds of SWaT's HMI screen and CCTVs.

Fig 8.: MPA's Assistant Chief Executive (Operations) Mr David Foo (second from left) explaining the water poisoning attack to MPA board member Ms Mary Liew (left) and MPA's Chief Executive Mr Teo Eng Dih (second from right) (photo credit: MPA)

Supported by iTrust's cyber security technology engineers, MPA showed how cyber attacks could be launched remotely – directly from POCC – on the SWaT testbed. The first attack scenario involved launching an OT network-based attack on the raw water stage, causing flooding by opening the motorised valve. The second was an attack on the chemical treatment stage, by turning on the hydrochloric acid dosing pump to increase the acidity of the water even when it defied plant logic. These attacks were representative of recent real-world incidents, such as the Maroochy Shire sewage spill attack in Australia and the Florida Water Treatment plant poisoning attack in the USA, and highlighted the ease with which malicious attackers could compromise critical infrastructure when they discover vulnerabilities such as weak or unprotected remote access.

The live demonstration underscored to the attendees the importance of securing critical infrastructure systems, and emphasised the need for more secure systems to protect against such realistic threats.

MariOT Award

MariOT Award

iTrust has recently awarded to ST Engineering Info-Security Pte Ltd for the design, construction and commissioning of a Maritime Testbed of Shipboard OT (MariOT) Systems. Scheduled to be ready by March 2025, the MariOT testbed will be an industrial-grade cyber-physical model, combining essential shipboard operational technology systems with virtual simulation models. When operational, it is used to support a variety of cybersecurity activities such as research, training, exercises and education. Users of the MariOT testbed include faculty, research, staff, and students, as well as government agencies and local and international collaborators. The MariOT testbed is funded by the Singapore Maritime Institute under the Maritime Transformation Programme.

Internship

Reflections

By: Sebastian Tay, iTrust Intern, NUS student

My time in iTrust was an eye-opener to the field of Operational Technology and cybersecurity. The hands-on involvement in my project has allowed me to better understand the meaning of Operational Technology and the importance of it in the nation's security. the project has

allowed me to further identify numerous areas for improvement in a project and to readily pick up new technologies that can assist me.

Moreover, experiencing setbacks was something that I got to experience throughout my time here, from stagnated progress to having to rollback certain features. All these taught me the importance of taking a step back and coming back to tackle with a fresh perspective.

Fig 9.: From left to right: Jovan Tay, Sebastian Tay, Felix Chan, Tan Shi Yu (2nd row), and Sim Kian Seng, Sean Wang, Pan Zai

All in all, my time here in iTrust has indeed been enriching, giving me the opportunity to further improve my technical and soft skills which I am grateful for.

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

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 (NSoE)

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

iTrust

Centre for Research in Cyber Security

Scan to view previous issues

https://itrust.sutd.edu.sg

itrust@sutd.edu.sg

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