iTrust Times

A Quarterly Newsletter

Issue Highlights:

Jan—Mar 2021 | Volume 7 Issue 1

From Centre Director's Desk

Picking Up Where We Left Off

Dear Reader:

Greetings from iTrust!

On behalf of iTrust staff I wish you a happy and productive 2021!

Yet another unique year has passed that will be remembered as the year when the entire world fought against a deadly virus and, hopefully, won. Undeterred, our faculty, researchers, and staff exhibited continued their resolve to working hard. Thus we ensured iTrust remained focused in its mission towards research, education, and training in cybersecurity in the context of critical infrastructure. Below I have highlighted just a few of our achievements during the year.

Sometime in November 2020 we were delighted to learn that the digital twin for the SWaT testbed developed in iTrust has been selected as a special system for use in perhaps the world's largest cyber-exercise that involves over a thousand participants from about 30 countries. More on this exercise, scheduled in April 2021, will be made available in the next issue of this newsletter. In addition to its use in cyber exercises, the twin will be an important component in a graduate cyber-security course offered at SUTD and serve as a faithful companion of the SWaT testbed.

As you may be aware, iTrust has been organising the Critical Infrastructure Security Showdown (CISS) event since 2015 (though under a different name). CISS2020-OL was unique in that this was the first fully online event during which attacks were launched on the iTrust water treatment testbed (SWaT) while several blue teams from industry, academia, and the government deployed their defence tools. A consolidated report summarising the outcomes of the event is now available online. This 54-page report includes descriptions of the attacks launched, defence tools used, and the evaluation of commercial and academic tools for anomaly detection. Indeed, preparation of this report was a mammoth effort by a team of iTrust staff and researchers. I believe that researchers who focus on using methods from machine learning for anomaly detection will find valuable information in this report.

NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust
Centre for Research in Cyber Security

A lot more has happened in iTrust during 2020; some of the highlights are in this newsletter.

Once again, on behalf of all in iTrust, I wish you a Happy and Productive 2021!

Best wishes,

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

Research Focus

The Fourth International CISS Critical Infrastructure Security Showdown - Online 2020

After the exercise comes a cooling down period – the report is now available

Following the biggest event in iTrust's calendar, the technical report for last year's CISS2020-OL exercise is now **available on iTrust's website for download**. The report is made possible by iTrust Senior Research Assistant Francisco Furtado and Cyber Security Technology Engineer Beebi Siti Salimah Binte Liyakkathali working in collaboration with other researchers — Ken Chin, Thur You Fu and Yoga Kashenen s/o Yogaindran — in analysing the data and putting the report together.

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

Navigating maritime cyber security

By Senior Research Assistant Priyanga Rajaram

The maritime industry has showed an increasing trend in adopting ICT for enhanced monitoring, communication and connection capabilities, which can help improve productivity and reduce operational costs. With cyber threats on the rise, increased connectivity between and among ship-to-ship and ship-to-shore infrastructure also means that disastrous effects on one entity can cascade down to others. Hence it is crucial for the maritime industry to understand these cyber risks and how to mitigate them. To that end, the **Singapore Maritime Institute awarded iTrust on a research project titled "A Cyber Risk Management Study in Shipboard OT Systems."** The study's principal investigator is iTrust Co-Centre Director Prof Jianying Zhou. He is assisted by senior research assistants Priyanga Rajaram and Ruchitha Dumbala, with iTrust senior manager Mark Goh contributing as a subject matter expert.

To share the team's initial results, iTrust organised a webinar on 18 Dec 2020. The webinar started with a welcome remark by Dr Sanjay Kuttan, Executive Director, SMI. Prof Zhou then gave an introduction to the project and its objectives in meeting with the International Maritime Organisation's 2021 timeline on shipboard cybersecurity. Priyanga and Ruchitha presented the **major cyber risks associated with Communication systems, Propulsion, Machinery, Power Control Systems, Navigation systems, and Cargo Management systems.** The team then hosted a 20 minute Q&A session to take questions from the audience. iTrust is proud to share that the webinar had generated a lot of interest, with nearly **300 participants** from around the world and several follow up discussions on potential collaborations. The slides and video of the presentation can be downloaded from iTrust's website.

The next two webinars – mitigating plans for cyber risks identified and detailed guidelines – is scheduled for Apr 2021 and Aug 2021.

Powerhouse Workshop

Having partnered for seminars in previous sessions, iTrust and ADSC Illinois at Singapore Pte Ltd joined hands to co-organise a Workshop on Cybersecurity for OT Systems. The workshop will be held over two half-days, from 11 to 12 March 2021. **Topics include the use of machine learning, anomaly detectors and message authentication for Industrial Control Systems (ICS) Security to mitigation strategies for cyber attacks.** Specific ICS presented at the workshop include power and substation systems. The workshop is free of charge; interested participants can register here: https://www.illinois.adsc.com.sg/SecOT/

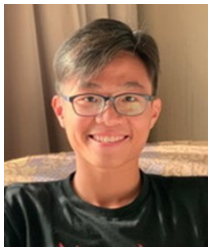
Internships

The 12 disciples of iTrust

The end of 2020 saw a flurry of requests for internship at iTrust

Four interns from Hwa Chong Institute and the Singapore Sports School began their internship with iTrust in Nov 2020. They were joined by six more in Dec 2020 and another two pre-matriculated SUTD undergraduates in Feb 2021. While safely distanced, the interns were able to work independently and also

with their supervisors to ensure their time with iTrust was meaningful and enriching. Their work is described below.



Cyber Security? Game on!

By Kohlmann Lee

I started learning Python from scratch and researched on cyber security data breaches and common malwares. My supervisor, Research Assistant Siddhant Shrivastava introduced me to the augmented/virtual reality (AR/VR)and **gaming designing aspect of cyber security** and explained how iTrust uses VR to represent SWaT so that researchers can conduct simulated attack and defence. The tools I used throughout the internship were Unity and Visual Studios, which were essential to game development as they serve as a platform to create games. After creating a simple game, I was then tasked to convert it to a VR game to be displayed on the Oculus Quest, with the added functions of setting up a multiplayer networking system and writing scripts for the collaborative touch to be initiated.

Throughout my internship there were many things that I did not understand and which made me very frustrated at times while performing certain tasks. However, it was precisely because of such circumstances that I learnt to be more proactive and enthusiastic in questioning and researching. As **shared by Professor Aditya "If you don't ask questions you will never learn",** and I truly agree. My internship at SUTD iTrust was certainly an eye-opener and a truly enriching experience.

CryPythongraphy

By Ross Lee

In my first four weeks of internship, my supervisor, Research Assistant Francisco Furtado tasked me to learn the basics of Python. To entrench my learning, I was given two tasks using Python. In the last two weeks, Francisco provided me with learning materials for basic cryptography. I understood different methods of encryption, such as Caesar Cipher and Transposition

Cipher, and also learnt how to decrypt text files using the brute force technique.

During this 1.5 months with iTrust, I've learnt a lot on programming with Francisco's help. With no prior knowledge in programming there were times when it was frustrating to see that my code didn't work as planned. Nonetheless, it was **fulfilling to see that I was able to understand the fundamentals of programming** and write out simple lines of code to carry out small tasks.

Speaking the Same Language

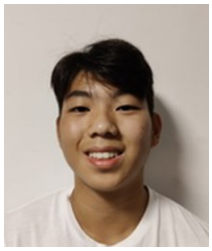
By Jonas Lim

I met iTrust Research Scientist Dr Nandha Kandasamy at the power testbed, EPIC, for our first meeting. I was first tasked to learn the basics of Python as a lead up to **publish and subscribe messages**, which I used in power grids as a way to establish communication between multiple devices. My other assignments include writing a program to determine the total power consumed in kWh for billing purposes, adding a counter to calculate the total energy value and publish the feed and discharge energy. My final assignment was to develop a GUI to show all these different variables.

My internship at SUTD was nothing short of fulfilling. During my internship, I learnt how to be independent and how to think out of the box. **I realised how similar Python was to the language we speak**, as long as we give commands loud and clear, things will happen how we want them to happen. This makes it all the more important to be systematic when giving commands and being clear about what you want and how to get there.

Player 2 has Entered The Game

By Yu Qin



After learning about the SWaT testbed and various attack vectors and tools that hackers can utilise to launch attacks on a critical infrastructure, my supervisor, Research Assistant Siddhant Shrivastava assigned me and my fellow intern Kohlmann a task to create **our own games in Unity.** The next step was to try to recreate our game on unity to make it compatible with the Oculus Quest VR headset. Despite not being able to complete the VR version of the game, the learning process was extremely fulfilling. We were given the challenging task of implementing **multi-player collaboration** in the same game.

Unlike in a school setting, there was much less step-by-step guidance in the internship and I had to search around for learning material independently. Much of what I found through the internet equipped me with skills to navigate the Web more smoothly to find what I needed. I feel that this skill would aid me in the future in research papers, projects, and many other areas of my life.

Machine Learning: Yay or Nay?

By Dillon Cheong

With the importance of securing critical infrastructures, there has not been a conclusive solution to monitor the different systems based on their behaviour. I was tasked to assist Dr Gauthama by researching different machine learning algorithms and test their performance with a Secure Water Treatment Plant (SWaT). Using both static and live data, we are **testing the machine learning algorithms and determining the performance of the algorithm** by calculating the accuracy of the predictions for a normal data set and the recall score of the individual attacks. The accuracy score is determined by the number of false positives we find from the predictions, while a recall score of the individual attacks will give the number of true positives we received. Besides testing the difference in performance of specific machine learning algorithms and comparing them, we will be able to answer questions such as which techniques are better for machine learning algorithms to monitor SWaT.

Red team tools: Badder and better

By Goh Yee Kit

I am tasked to assist iTrust Deputy Director Ivan Lee with developing tools and techniques for the iTrust red team in order to enhance their arsenal of

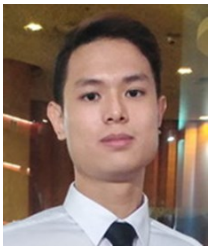
tools for them to be used in launching attacks during future CISS exercises. These tools will be used to test the detection mechanisms and to test the blue team's ability to detect the attacks. My main tasks are mutating payloads so that they would not be detected by anti-virus software and also to develop a C2 solution for full control. Thereafter I will move on to try and evade IDS/IPS systems with my attacks.

Learning a Second Language
By Adrian Heng

The SWaT testbed uses Allen-Bradley's ControlLogix Controllers and communicates over Ethernet/IP, where it utilises the Common Industrial Protocol (CIP) for its upper layers. I have been assigned the work of implementing the communication protocol into SWaT's replica, the digital twin.

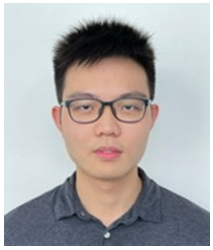
So far, I have experimented with CPPPO's Ethernet/IP Controller Communications Simulator and am learning how it is done in Python, **so that the Ethernet/IP can be used by the digital twin.** I have also used Pylogix – which works with the simulator - for reading and writing tag values. In the coming months, I aim to have a working skeleton for the communication and add it to the current working code of the digital twin.

Body Double: SWaT Digital Twin
By Nicholas Png



To ensure that our nation's critical infrastructure are secured, research and development is required to delve into the intricacies of ensuring their robustness. I was blessed with the opportunity to take part in **virtualising the physical SWaT testbed** with Professor Aditya Mathur and his team. The virtual SWaT is designed to be a close replica of its physical counterpart, allowing researchers to study the OT aspects at their own discretion. My main task is to **deploy the virtualised SWaT into different machines and assist in setting up the communication protocols.** This setup closely mimics the physical counterpart, where the physical components and hardware are independent.

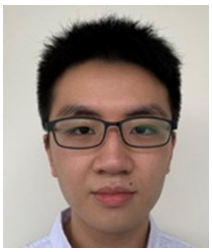
Within these few months, I was able to learn the different protocols being used in the industry and strengthen my knowledge in OT. I hope to be able to contribute more to the coming future and continue learning.



Virtual Power
By Ryan Qiu

I have been assigned to the Electric Power and Intelligent Control (EPIC) testbed to **develop a virtual substation with two incomers and bus coupler**. I started by developing the circuitry using a Simulink, and subsequently the IEDs, PLCs and the SCADA system. Currently, EPIC only has one protocol but we aim to add more industry standard protocols to it in the future. I was not familiar with many of the tools being used when developing the virtualisation and had to either self-source or consult my supervisor, iTrust Research Scientist Dr Nandha Kandasamy. It has been an enjoyable learning process and I look forward to gaining more knowledge and experience in this field.

Communicating Attacks
By Shao Hong Sze



Over the past 3 months in iTrust, I have been exposed to numerous aspects of operational technology. I am deep diving into using OPC UA (Open Platform Communications United Architecture), a protocol recommended as the communication layer within the "Industry 4.0" movement. In addition, using my newfound knowledge of OPC UA, I am working on **writing attack scripts that will be used in future international cyber exercises.**

Benjamin Lim (left) and Jian Qing Tan are pre-matriculated undergraduate students at SUTD. Even before starting their term at SUTD they sought internship with iTrust to gain some experience. Being new to cybersecurity,

for a start, they spent their first month building up foundations in Python, networking, communication protocols and machine learning. These skills will come in handy in the coming months when they assist their supervisors in the ongoing development of SWaT digital twin.

Visits

SUTD President Prof Chong Tow Chong hosted a visit by **Permanent Secretary (Defence Development), MINDEF, Mr Joseph Leong** to SUTD on 16 Feb 2021. Mr Leong was accompanied by several others from DSO National Laboratories, the Defence Science and Technology Agency, MINDEF and the Singapore Armed Forces. Mr Leong's visit included a briefing and demonstrations on SUTD's research, especially in the areas of artificial intelligence, robotics, autonomous technologies, and cyber security.

iTrust Matters

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

Ivan LEE
Deputy Director, Cyber Security Technologies
ivan_lee

National Satellite of Excellence

HOR Miao Yun
Research Senior Officer
miaoyun_hor

Siti Nadhirah Shaik NASAIR Johar
Research Associate
siti_nadhirah

General Enquiries
nsoe_destsci

Angie NG
Manager
angie_ng

Priscilla PANG
Manager
priscilla_pang

iTrust Laboratories

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

Mark GOH
Senior Manager
Editor, iTrust Times
mark_goh

Beebi Siti Salimah Binte LIYAKKATHANI
Cyber Security Technology Engineer
Liyakkathali

Andrew TAY
Cyber Security Technology Engineer
andrew_taykongngee

General Enquiries
itrust

iTrust
Centre for Research in Cyber Security