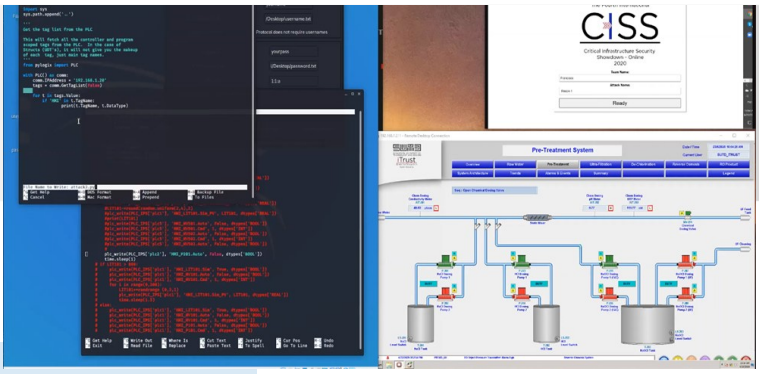
iTrust Times

A Quarterly Newsletter

Issue Highlights:



Apr — Jun 2020 | Volume 6 Issue 2

From Centre Director's Desk

Exercise CISS highest participation

Dear Reader:

Greetings from iTrust! From all in iTrust, we hope that you are able to productively manage the current COVID-19 situation and are staying healthy.

In iTrust, we have followed strictly the work-from-home and team-rotation guidelines. Despite a significant change in the way we are used to working, the COVID-19 could not daunt us. Soon after we realised the challenges we will be facing, we decided to move our annual signature event – the Critical Infrastructure Showdown – online and named it as CISS2020-OL. While this decision has led to a significant increase in the workload of our research and operational staff, they have worked hard to meet the challenge. Several new products have been designed, and existing products enhanced, to enable CISS2020-OL and are under intense testing before they are put to use. The international participation in CISS2020-OL promises to be at an all time high with participants from US, Europe, and Asia. More about CISS2020-OL are in this newsletter and at the iTrust website.

I take this opportunity to thank our industrial partner, Fortinet, for their technology contribution to iTrust (details in this newsletter). Their technology will assist in the conduct of CISS2020-OL.

The COVID-19 situation has disrupted universities in many ways; SUTD is no exception. iTrust has worked with SUTD to ensure that such disruptions do not impact the education of our students in any way. Towards this end, iTrust has offered internships to five of SUTD students. These interns have made notable contributions to the products that will be used during CISS2020-OL. More about these students can be found in this newsletter.

For those of you who have been waiting to get their hands on the CISS2019 report, the wait is over. The report is now avaliable at the iTrust web site. iTrust staff worked hard to produce this report that reveals the strengths and weaknesses of the technologies available commercially and in iTrust. Needless to mention, a lot more work is needed before process anomaly detectors for critical infrastructure are ready for rime-time, i.e. meet the requirements of ultra-high detection rate and ultra-low rate of false positives.

NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust
Centre for Research in Cyber Security

That's all for this edition of the newsletter! We will be back soon!

Best wishes,

Aditya Mathur
Centre Director, iTrust, Singapore University of Technology and Design
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

iTrust's signature annual cyber defence exercise is now fully online.

This fourth edition of the exercise, named CISS2020-OL, will be held during 27 July to 7 August. The exercise began in 2015 under the event named Secure Cyber-Physical (SCy-Phy) Systems Week. In 2019 it was renamed as Critical Infrastructure Security Showdown (CISS) to better reflect its purpose and domain. CISS2020-OL will be the first time the event is fully online, where all participants, i.e. the red and blue teams, will participate event online.

Objectives

CISS2020-OL aims to meet the following key objectives: (a) validate and assess the effectiveness of technologies developed by researchers associated with iTrust; (b) develop capabilities for defending critical infrastructure under emergency situations such as cyber-attacks; and (c) understand composite Tactics, Techniques and Procedures (TTPs) for enhanced Operation Security (OpSec). In addition, CISS2020-OL will enable red team members to understand approaches for compromising critical infrastructure and hence what protection mechanisms are necessary.

Phases

The event consists of the following phases:

- Phase I [May 4 - 29, 2020]
  Participant selection (red & blue teams)
- Phase II [June 22 - July 3, 2020]
  Participant familiarisation (red & blue teams)
- Phase III [July 6 - 16, 2020]
  Target system selection (red teams)
- Phase IV [July 27 - Aug 7, 2020]
  CyberFire (red & blue teams, observers)
- Phase V [Q3 – Q4, 2020]
  Data analysis and reporting

Participants

All red and blue teams will be offered an online tour of the Secure Water Treatment (SWaT) testbed – one of the target systems – and have their questions answered. In addition, they will also be provided:

- information on SWaT, the digital twin, digital twin player, and various anomaly detection and plant safety technologies that will be deployed during the exercise;
- a Frequently Answered Questions (FAQs) (provided separately); and
- access to past data collected from SWaT since 2015, including data collected during CISS 2019.

When required, blue teams can carry out hardware installations on SWaT prior to the event. However, during the event, the blue team shall ensure that:

- The installations do not interfere with the regular plant operation and existing iTrust technologies;
- It will make its own arrangements for the data generated by its hardware to be piped to their computers outside of the SWaT during the exercise; There shall be no efforts made to prevent, halt or thwart any attacks launched by the red teams.

Target system selection

Target system selection is the first component of the exercise where red teams are tasked to access the target systems available for attacks. Target systems consist of SWaT and variations of its digital twin.

Figure 1 below captures the interactions among the participants and the target systems.

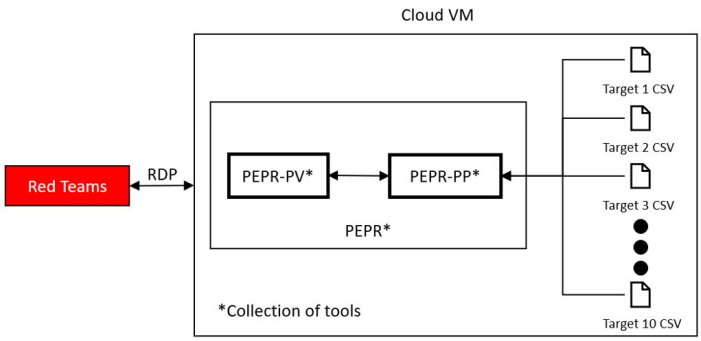


Figure 1: Interactions between red team and CISS2020-OL system and tools during target selection phase

Each target system will be kept live during this phase. Red teams will be provided unique URLs to connect to each target system. Data generated by each target system, including OT data captured by the historian and the pcap files, will be piped online and can be viewed through PlantDecode and PlantViz [OT]. All target systems will offer identical, or near identical, user interface.

Each red team will then be asked to make known their target system selection to iTrust; they will then be informed if their selected target system is SWaT or one of its digital twin variant. This selected target system shall be the one in which they will launch their attacks during the next phase: the CyberFire exercise. Bonus points will be awarded to the red teams who are able to correctly select the physical SWaT testbed instead of its digital twin. A red team that selects the digital twin will be granted up to 0.5-CFM (2 hours) to attack SWaT after it has completed launching attacks on the digital twin that it selected, if it so wishes. Note that this 0.5-CFM is included in its allotted 1 CFM slot.

CyberFire activities

The CyberFire activities will be spread over 16 CyberFire modules (CFM) in 2 weeks. Each CFM slot is 4 hours and is scheduled from 9am to 1pm and from 2pm to 6pm, GMT+8, with a one hour break in between for system reset. At the time of this writing, 11 red teams and 3 blue teams have confirmed their participation.

Attack platform

For added realism, all red teams must attack SWaT by

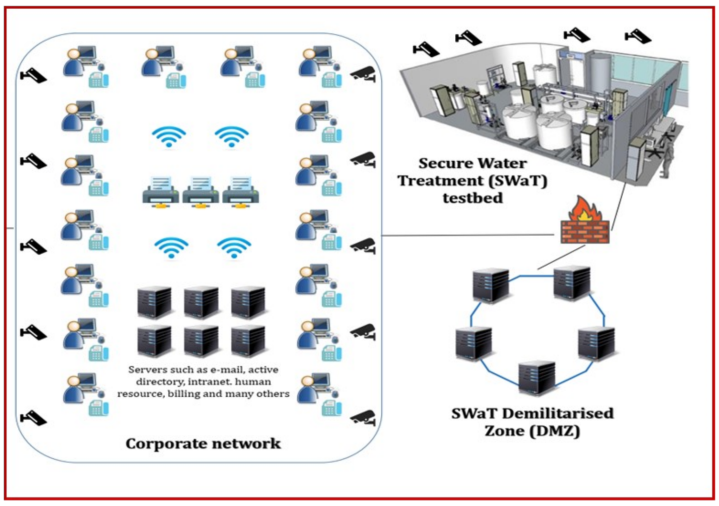


Fig 2: High-level Architecture of ZyCron Cyber City

first entering the network via the ZyCron Cyber City (ZCC); they will land in ZCC's corporate network through a VPN connection. ZCC (Figure 2) is a full-fledged virtual organisation comprising of Information Technology (e.g., e-mail server, file server, printer server, CCTV, honeypot and intranet) and Operational Technology (processes in SWaT). To make these entities "alive," various types of network traffic are also crafted and included in ZCC. As an IT environment ZCC is not set up with best practices i.e., it is intentionally built with minimum security features and contains vulnerabilities for red teams to explore and exploit. Note there is no internet access within the ZCC.

Launching attacks

Active stage: During a CFM the assigned red team will be asked to demonstrate its attacks and achieve the pre-determined goals. At this time, the red team is considered "active" and will have online access to its pre-selected target system via a VPN connection. The CFM duration includes, but is not limited to: reconnaissance, designing and launching attacks, interactions with judges and taking breaks.

Hunting stage: Active teams will be able to design attacks on the target system and launch them remotely using the Attack Designer/Launcher (see Figure 1). This tool is only applicable to SWaT and is meant to facilitate better understanding of the operational technology environment when under attack. The red team will need to "hunt" for its pre-selected target system (in Phase III) before it can begin to launch attacks. As all red teams must enter SWaT via the ZCC to launch attacks, failure to do so and to identify the

pre-selected target system will lead to a lower score.

Attack launch stage: Prior to launch, the active red team must do the following throughout its CFM:

a. Share with iTrust the "live" screen of the computer that is used to launch the attack via an online communication tool (e.g. Skype);

b. Allow iTrust to video record the screen; and

c. Inform judges (1) the intention of the attack; (2) the targeted component(s); and (3) the launch procedure.

Only one attack can be launched on either SWaT or the digital twin variant, but not both at the same time. The duration of an attack will be determined in real time by iTrust's cyber security technology engineers stationed physically at SWaT. Attacks that take a long time, e.g., 30 minutes, to have a noticeable impact on the plant will likely be halted by the judges before the impact is visible.

Attack monitoring

Blue teams and the active red teams will be able to view in real time the state of each state variable in the target system. Any anomaly resulting from the attack, or otherwise (i.e., a false alarm), and reported by one or more iTrust detectors, will be visible only to the organisers, observers and judges and not to the red or blue teams.

Scoring of red teams

The performance of each red team will be assessed in real time by a team of judges consisting of cyber security experts and engineers working in the critical infrastructure domain. All teams that successfully complete the exercise will be given a certificate of participation. Judges during the event will score each team based on criteria such as complexity of the attacks launched and success of the attack in resulting in an anomaly in at least one of the plant state variables. **Top three red teams will receive cash awards of S$2,000, S$1,000 and S$500 respectively.**

Attack detection by blue teams

It is important for blue teams to note that CISS2020-OL is being conducted to simulate attacks on a live city-scale plant. Hence, it is assumed that the security systems deployed by each blue team are operational throughout the exercise except when the target system, i.e., SWaT or the digital twin, is not running or is being reset.

Participation

To date we have 14 confirmed red teams from Finland, France, Korea, Netherlands, Poland and Singapore, and 5 commercial blue teams.

CISS
Critical Infrastructure Security Showdown 2019

The **technical report for last year's CISS exercise is now available** on iTrust's website for download. Special thanks to iTrust researchers — Senior Research Assistant Francisco Furtado, Research Scientist Dr Nandha Kumar Kandasamy and Research Assistant Beebi Siti Salimah Binte Liyakkathali — for their analysis of the data and putting the report together.

Fortinet's Contributions to Cybersecurity

Fortinet contributes its Secure Ethernet Switches and FortiGate Firewall technology to iTrust

Industrial partnership and collaborations have always been a key to iTrust's constant effort to produce innovative and translatable technologies that is meaningful to the industry. One such partnership is with Fortinet, a global leader in IT cybersecurity. Patrice Perche, Senior Executive Vice President, Worldwide Sales & Support, Peerapong Jongvibool, Regional Director, SEA & HK, and Yue Chin Beng, Regional Sales Director, Operational Technology/Critical Infrastructure of Asia Pacific, visited iTrust on 11 December and was given a tour of its testbeds and capabilities.

iTrust wishes to thank Fortinet's generosity in contributing its Secure Ethernet Switches and FortiGate Firewall technologies to foster partnership in the

cybersecurity space. Cyber Security Technology Engineer Ian Teo will be working closely with Fortinet to utilise their technology to upgrade the capabilities of iTrust's testbeds.

Fig 3: Fortinet's Patrice Perche (leftmost) and Peerapong Jongvibool (rightmost) with iTrust's Dr Nandha Kandasamy(second from right) and Desmond Wan at EPIC testbed

Visiting researcher

Using process and network data to detect cyber-attacks in industrial control systems

By visiting researcher Gabriele Puce

Gabriele Puce, who is pursuing his Master's Degree in Computer Science and Engineering at Politecnico di Milano, did a research stint at iTrust from Oct 2019 to Feb 2020, under the supervision of Assoc. Prof. Stefano Galelli.

The goal of his research is to **improve the performance of algorithms used to detect the presence of cyber-attacks in urban water infrastructures.** Specifically, this was achieved by developing an intrusion detection system (IDS) that fuses information on physical processes (e.g., water flow, levels) and the state of the monitoring and control network. The rationale is that the joint use of these data could help improve both detection accuracy and localisation of cyber-physical attacks. For example, process data on the water level of a tank could indicate we if there was an anomalous event; looking at the same data while analysing the information exchanged in the monitoring and control network could help explain the nature of such anomaly.

Since data on water systems undergoing cyber-attacks are limited, Gabriele and Stefano began their research by developing a digital twin for water distribution systems; that is, a numerical model that simulates both process of network data. The digital twin (Figure 4) relies on two main components: Mini-CPS for the cyber layer and EPANET for the process layer. The third component is an Sqlite database that allows the two models to exchange information during the simulation.

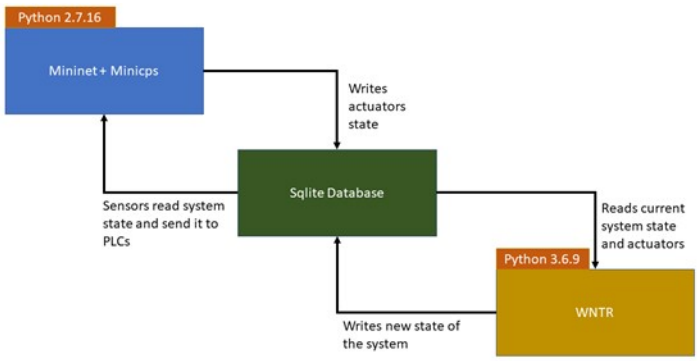


Fig 4. Graphical representation of the digital twin

With the digital twin at hand, Gabriele and Stefano simulated a wide array of normal operating conditions, as well as cyber-attacks aimed to disrupt the system's physical processes. So far, they have been working primarily with Man in the Middle attacks and DoS attacks. This ongoing work focuses on the IDS, and for which they are using unsupervised machine learning algorithms.

Student interns

iTrust accepted summer internships for five students to assist us with CISS2020-OL. Here is a summary of their research objectives and tasks.

"Super decider"

By student intern Madhumitha Balaji

In water treatment and distribution plants, sensors and actuators measure and detect physical and chemical parameters e.g., the level of water in a tank, pressure in pipes and pH. Logic controllers in the plants use these data to perform pre-programmed tasks, for example, turning on a pump when water

levels drop below a pre-set minimum. To protect the plants from cyber attacks and ensure they are functioning properly, it is important to detect these attacks and respond accordingly. The problem with detection of attacks is decision fusion – multiple detectors report the behaviour as an attack or normal operation. **Plant operators have to decide whether the plant is under attack (or a plant malfunction) from multiple data sources reporting the same event.** Madhumitha is working under the supervision of Research Assistant Siddhant Shrivastava on a Super Detector that makes a **more reliable decision** based on the reports of other attack detectors using machine learning. To do so, she will be employing ensemble techniques and stacking algorithms. In addition, the output of the Super Detector not only depends on reports of other detectors but also on the status of the plant itself i.e., sensor and actuator values, enabling it to make a more informed decision. She targets the Super Detector to be deployed in CISS2020-OL to better assist the iTrust blue team in detecting the attacks launched by the red teams.

Baby brother

By student intern Lim Yang Zhi

Yang Zhi is assisting iTrust Centre Director Prof Aditya Mathur on a Digital Twin of Secure Water Treatment (SWaT) and distributing it across several virtual machines. The Digital Twin is used to **provide evaluation of anomaly detection algorithms and plant protection algorithms.** This will allow personnel working on such detection and protection algorithms to improve on their algorithms, providing a better layer of security for the plant without having to run their algorithms on the plant itself. As the Digital Twin is a separate architecture from SWaT, it can act as a second SWaT for red teams to attempt to attack during CISS2020-OL.

Yang Zhi is also working on tools to capture incoming and outgoing packets within the Digital Twin. Apart from capturing data that is sent between controllers and the SCADA in the Digital Twin, which can be analysed by a plant operator, the tools can also be used to alter packet data. Hence, the tools can be used to **train personnel in cybersecurity on various exploits and attacks and to test the effectiveness of detection and protection algorithms** in the event of a cyber security attack. The tools are an added arsenal of attack vectors which red teams can adopt during CISS2020-OL to launch attacks on the Digital Twin.

Tell me all about it

By student intern Lau Yu Hui

Yu Hui is assisting iTrust Senior Manager Mark Goh in capturing and streamlining red and blue teams' actions during CISS2020-OL. To that end, she is tasked with improving the Attack Logger's functionalities and GUI. The Attack Logger, developed by Research Assistant Muhammad Syuqri Bin and first deployed during CISS 2019, allows organisers to **document red teams' actions during each step of their attacks**, including the type of attack, its target in SWaT, its nature, as well as the time at which the attack was launched and ended. As the Attack Logger will eventually be integrated with PlantViz – an aggregator and visualiser of several detectors' detections developed by iTrust – these documented information can then be analysed alongside plant status and detectors' data to determine the detectors' efficacies in detecting attacks. The Attack Logger is thus an **important tool for CISS2020-OL organisers for tracking, documentation and analysis.**

Yu Hui is also developing a new tool – Alert Logger – for blue teams to easily **report their detections as they occur.** The premise lies in a blue team's system being deployed in an operational plant, and which raises an alert to the operator when it detects an attack. During CISS2020-OL, a similar set up will also be in place, and with blue teams having access to their systems, they can use the Alert Logger to log a time-stamped alert and report their logs to iTrust for analysis. Future work includes integrating Alert Logger with PlantViz to aid with analysis of blue teams' detections.

Break me if you can

By student intern Ng Jo-shen

As part of preparations for CISS2020 -OL, Jo-shen is assisting iTrust Deputy Director Ivan Lee with setting up of virtual machines within Zycron Cyber City (ZCC). He is tasked with researching **vulnerabilities in operating systems and software in order to create exploitable systems**. This also involves testing of such exploits to judge their exploiting difficulty and how obvious they are to red teams.

The objective is to **create realistic and exploitable systems** to pose a challenge to the red teams and test their capabilities. At the same time it affords iTrust a **glimpse into real-world attack vectors** deployed by red teams on IT systems.

I'm watching you

By student intern Tan Li Yuan

Li Yuan is assisting Research Assistant Siddhant Shrivastava on PlantAR. This task focuses on utilising and making use of **augmented reality's (AR) functionalities to visualise SWaT.** Beyond social media, AR is also adopted by online businesses to market and sell their goods, through creating realistic previews of their goods and assisting customers in making informed decisions. Thus, PlantAR's objective is to enable users to have immersive user experience while visualising SWaT, **without the need for them to be physically on site.**

This is an important feature as plant operators have to closely monitor their plants from the control room. However, in the case of an off-site operation, or if the plant is located far away, operators may not have immediate access to the control room and plant at all times, thus posing risks and challenges in monitoring the plant especially during a cyber-attack. PlantAR offers a promising solution to **literally bridge this geographical gap and aid operators in monitoring the plant** from wherever they are.

Awards

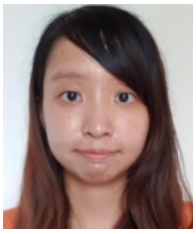
Best Paper Award

A paper entitled "Challenges in Machine Learning based approaches for Real-Time Anomaly Detection in Industrial Control Systems," co-authored by **Dr Chuadhry Mujeeb Ahmed, Dr Gauthama Raman Mani Iyer Ramani and Prof Aditya Mathur** received the best paper award at the 6th ACM Cyber-Physical System Security Workshop (CPSS 2020). Congratulations!

Profiles

HOR Miao Yun

Research Senior Officer



Miao Yun is pursuing a part-time degree in Business from the Singapore University of Social Sciences, intake of 2020. Prior to that, she came from a business background and had been working in MNCs. She has experience in marketing, supporting different projects

Miao Yun has been playing musical instruments for many years. She was in the school band and participated enthusiastically in various band performances and dinner events. She had also participated in the Singapore Youth Festival (SYF) central judging competition. She likes to pick up new activities and has gone for hiking and snorkeling expeditions overseas.

LinkedIn

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

Ivan LEE
Deputy Director, Cyber Security Technologies
ivan_lee

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

National Satellite of Excellence

HOR Miao Yun
Research Senior
Officer
miaoyun_hor

Siti Nadhirah Shaik NASAIR Johar
Research Associate
siti_nadhirah

Angie NG
Manager
angie_ng

Priscilla PANG
Manager
priscilla_pang

General Enquiries
nsoe_destsci

iTrust Laboratories

Mark GOH
Senior Manager
Editor, iTrust Times
mark_goh

Beebi Siti Salimah Binte LIYAKKATHANI
Cyber Security
Technology Engineer
liyakkathali

Ian TEO
Cyber Security Technology Engineer
ian_teo

iTrust
Centre for Research in Cyber Security

https://itrust.sutd.edu.sg
itrust@sutd.edu.sg
Singapore University of Technology and Design | 8 Somapah Road, Building 2 Level 7, Singapore 487372