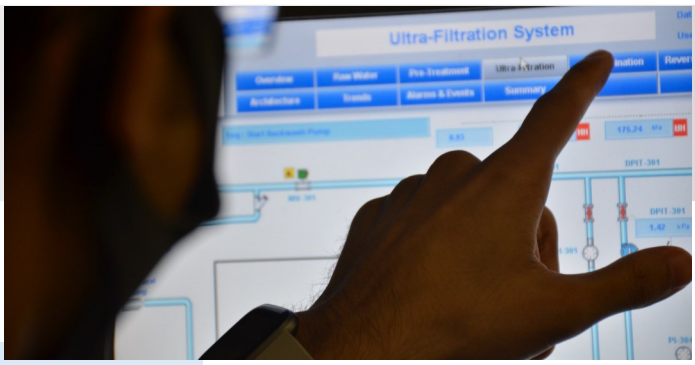
iTrust Times

A Quarterly Newsletter

Issue Highlights:



Jul — Sep 2020 | Volume 6 Issue 3

From Centre Director's Desk

MaCISSive Exercise and Success

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.

As we have now realised, COVID-19 has brought many unforeseen challenges to everyone. We in iTrust are no exception. One of the challenges the able iTrust staff and researchers faced, and met successfully, relates to our annual Critical Infrastructure Security Showdown (CISS) exercise. Sometime in early 2020 we asked: "Should we cancel CISS2020?" We discussed, and boldly decided against it. Fast forward a few months, countless hours of software development, infrastructure upgrades and testing, the iTrust team successfully completed its most sophisticated ever annual exercise named CISS2020-OL; the entire exercise was conducted online on an operational physical process. Below I share with you some statistics related to CISS2020-OL; additional information is in an article in this newsletter ably drafted by our editor Mark Goh.

The objective of CISS2020-OL remained unchanged, i.e., assess the effectiveness of the mechanisms available to defend critical infrastructure. "Insider threat-physical and cyber" was the threat model used. The attack target was SWaT: an operational 6-stage water treatment plant at iTrust. Remaining true to the threat model, all red and blue teams were given architectural and operational details of the target. A total of 84 attackers, grouped into 17 teams, launched attacks from their respective locations spread over 7 countries in North Ameica, Europe and Asia. Only the iTrust red team was considered "physical insider" and launched attacks from within the plant premises and directly from the SCADA workstation and the communications network. There were 10 defence teams whose detection mechanisms were being evaluated. To make the exercise realistic, no blue team member was allowed to disrupt the attacks; only their defence equipment was installed inside the plant premises.

The event lasted for 88 hours, spread over 9 days from July 27 to Aug 7, 2020. A total of 82 initial attacks and 2,657 updated attacks were launched. 97.7% of the attacks were on the IT infrastructure of SWaT while the remaining on its physical processes. The defence teams generated a total of 77,180 alerts. Interestingly, the rate

of ABFA (Alarms Before First Attack) was 51 alarms/ hour. There were 877 alerts generated/hour.

As you may imagine, a large amount of data - comprising 939GB of pcap data and 113MB of OT data spread over 18 files each with 63 features - has been collected and is under analysis. This data will be made public soon after the analysis is completed. I believe this trove of data would be welcome by researchers who wish to test their novel anomaly detection mechanisms.

Lastly, we wish to thank all those in MINDEF for their involvement in CISS2020-OL, in particular BG Percival Goh, BG Mark Tan, COL Edward Chen and LTC William Teo, who provided their immense support, without which the exercise would not have been successful.

Thank you for browsing through this newsletter.

Stay safe. Best wishes.
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

A Simulated Cyber War on Critical Infrastructure

When the world realised the full impact and spread of the then-poorly understood COVID-19 in Feb 2020, iTrust had just started conceptualising its fourth run of the Critical Infrastructure Security Showdown (CISS).

With the pandemic affecting global movement and eventually our own social lives, iTrust braced itself for CISS2020's existential question: to go ahead or not to?

Traditionally, CISS, like many cyber exercises, has been an "onsite" exercise where red and blue teams gathered for a showdown. The problem statement was: How to organise one where the spirit of CISS is retained, but in a completely different realm?

In the article "Move fast and try not to break things" by The Economist (4th April 2020) the writer remarked how COVID-19 was driving innovation in public services: in the way things were done, new partnerships were formed and previously resisted and languishing ideas and reforms were dusted off and trialled.

Challenge accepted

Similarly, iTrust Centre Director Prof Aditya Mathur turned the pandemic on its head and saw it as an excellent opportunity to host CISS entirely online such that the red, blue and green teams and the observers can participate safely from wherever they are located, while remaining immersed in the "full experience." Doing so not only expanded CISS's reach to teams that might not have participated otherwise, it also spurred iTrust into upgrading its infrastructure, hence sprouting new technologies and tools and building new capabilities within the team. It was a beast of a challenge and a core team of 15 staff, researchers and students finally made it happen, and CISS2020-OL (online) transited from a concept to reality.

Let us play

This year's CISS is the largest yet, spreading over two weeks with **16 external red teams and 5 commercial blue teams** participating. The event brought participants from US, Europe, and Asia into a single location – the Secure Water Treatment (SWaT) testbed here at iTrust, Singapore University of Technology and Design (SUTD).

With digital connectivity, all manners of preparations and executions could be performed solely online through emails, video conferencing and virtual machines. Cognizant that this is the first time we were

Figure 1: A snapshot of participants in CISS

planning such an online event and on such a scale, the team worked hard to configure, troubleshoot and rehearse, so that participants could enjoy as technically beneficial and challenging an experience as possible, while not being short-changed by not being physically present at SWaT.

It is also this digital connectivity that is a bane for critical infrastructure owners and operators globally. Exposure to unknown threat actors and attack vectors creates risks and operational uncertainties and, in the worst case, even a nation's survival. Hence, **CISS2020-OL's objectives** are to (a) validate and assess the effectiveness of technologies developed by researchers and practitioners 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.

CISS2020-OL kicked off with an inaugural ceremony that was broadcast "live" via Zoom on 27 Jul 2020. Prof Aditya Mathur, Centre Director, iTrust and COL Edward Chen, Commander Cyber Defence Group, at Singapore Armed Forces, MINDEF welcomed participants to the event.

More is Less

Several new features were added to this year's exercise. Red teams were required to **share screens** from which their attacks were launched. This facilitated the judges and the red teams with (1) communication; (2) coordinating attacks; (3) understanding and logging the attacks; and (4) maintaining safe operation of SWaT. Doing so also reduced the need for judges to ask red teams to halt or repeat their attacks because, for example, the red teams proceeded with an attack without warning, as was the case in previous years.

Figure 2: A reminder that, while all is not normal, we still have to keep our critical infrastructure safe. COL Edward Chen (left) poses with Prof Mathur after their speeches at the inaugural ceremony.

Blue teams were given two options of **automatically logging and reporting the attacks** that their systems detected, which in turn enhanced efficiency and accuracy. The tools that made this possible were PEPPR – an OT data and alert aggregator, visualiser and player developed by iTrust Research Assistant Muhammad Syuqri Bin Johanna – and Alert Logger, developed by SUTD undergraduate Lau Yu Hui.

Other than blue team's detection logs, PEPPR also gathered time-stamped data from SWaT's historian and the **Attack Logger – which logs actions performed by red teams**, also developed by Yu Hui – and combined them into a single data-rich Excel file. This eliminated the Herculean task of having to extract data from different sources and then align them in chronological order, down to the seconds.

With more features added, a lot of manual work was reduced in data aggregation and analysis. This was also evident in how the following statistics could be generated just days after the exercise concluded on 7 Aug 2020, and which was shared by Prof Mathur at the Award Ceremony on 11 Aug 2020.

Together with Prof Mathur at the Award Ceremony,

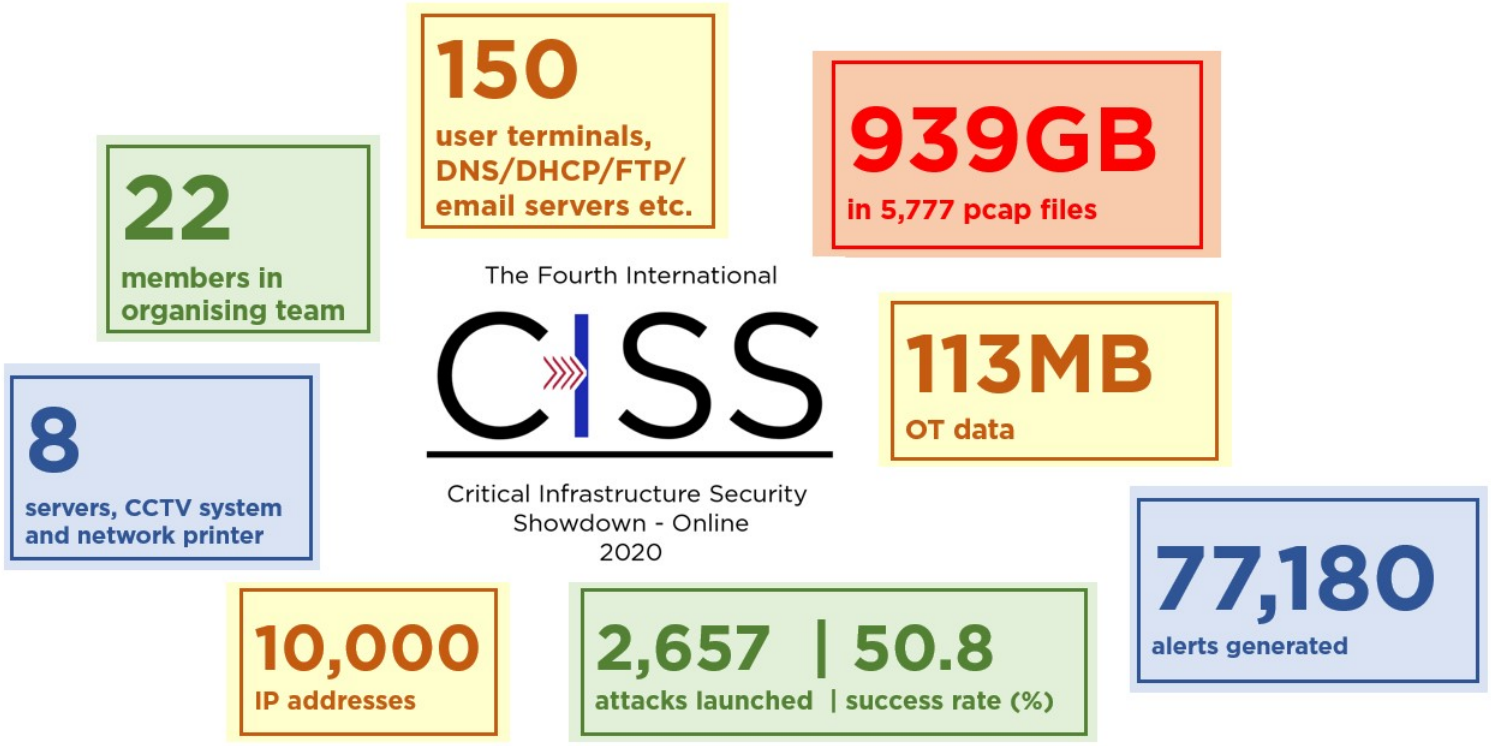


Figure 3: What we put in, and what we got out of, CISS2020-OL

which was also broadcast "live" from iTrust, was COL Edward Chen, who did honours of announcing the top three performing red teams of CISS2020-OL. They are: **Kopitiam (1st place; Singapore), KPMG (2nd; Singapore) and JYVSECTEC (3rd; Finland). Congratulations!**

The iTrust team has already begun the process of sifting through and analysing the massive amount of data for post-event reporting. Readers can expect the report to be published by the end of 2020. Data collected during the event will be made publicly available after any necessary anonymisation. Thank you everyone for your support and interest in iTrust's signature event; we look forward to your continued participation next year. See you at CISS2021!

A Cyber Risk Management Study in Shipboard OT Systems

First maritime project awarded to iTrust

iTrust has been awarded a funding support by the Singapore Maritime Institute for a one-year project (Sep 2020 to Sep 2021) on **"A Cyber Risk Management Study in Shipboard Operational Technology (OT) Systems."**

The maritime industry has showed an increasing trend in adopting more ICT for enhanced monitoring, communication and connection capabilities, which can significantly improve the productivity and reduce the operational costs. On the other hand, maritime infrastructure faces an evolving array of cyber threats. Increased connectivity between and among ship-to-ship and ship-to-shore infrastructure also mean that they cannot be treated as single entities, and that disastrous effects on one entity can cascade down to others. It is therefore crucial for the maritime industry to understand the associated cyber risks associated and develop the necessary cybersecurity technologies to protect their assets.

In response, the International Maritime Organisation (IMO)—a United Nations specialised agency with responsibility for the safety and security of shipping—called for **cyber risks to be identified and addressed in audits from 1 Jan 2020.**

Thus, this project aims for a cyber risk management study in shipboard OT systems, and provide an amalgamated "best practices" for maritime authorities and shipping lines in regards to cyber risk management of shipboard OT systems. The OT systems under consideration in this project are: **(1) navigation; (2) propulsion; (3) communications; and (4) cargo management.**

Figure 4: One of the OT systems being studied is the ship's navigation system

The Project Investigator is iTrust Co-Centre Director Prof Jianying Zhou. He will be supported by iTrust Senior Manager Mark Goh who will provide his domain knowledge in the maritime industry, and two research assistants doing the ground work of the study.

Visits

Visits by BG Percival Goh and BG Mark Tan

Benefactors of the CISS2020-OL Exercise

In a space of one month iTrust hosted visits by two Brigadier-Generals (BG) from the Ministry of Defence, Singapore. Both BGs' support were instrumental in the success of CISS2020-OL, by **contributing manpower to help co-organise the exercise and offer their cyber expertise to iTrust.**

After an introduction to iTrust by Centre Director Prof Aditya Mathur, BG Percival Goh, Comdr SAF C4 Comd / SAF Chief Information Officer (17 July) and BG Mark Tan, Defence Cyber Chief, (7 August) visited iTrust's testbeds to better understand how our research work translated to and are validated in the real world.

Figure 5: iTrust Deputy Director Ivan Lee (centre) hosts BG Percival Goh (right) and COL Edward Chen (left) at the IoT testbed

As BG Tan's visit coincided with CISS2020-OL, he also witnessed a red team launching its attacks on the SWaT testbed. As a token of appreciation, BG Tan and COL Chen presented commemorative coins to Associate Provost (Research and International Relations) Prof Yeo Kiat Seng and Prof Aditya Mathur.

Figure 6: (clockwise, from top left) BG Tan and COL Chen presents the token to Prof Mathur, BG Tan presents the token to Prof Yeo, and Prof Mathur explains a red team's attacks to BG Tan

Awards

Congratulations to our Centre Director!

iTrust Centre Director Prof Aditya Mathur, a Birla Institute of Technology and Science, Pilani (BITS Pilani) alumni, was awarded the **BITS Pilani Distinguished Alumnus Award.** The award recognises and honours alumni who have brought laurels to their alma mater by making significant and outstanding contributions to their profession. The award was instituted in 2011 and has been given each year ever since. Visit https://www.bitsaa.org/page/bits-pilani-distinguished-alumnus-awards for more information.

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*

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

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

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

General Enquiries
itrust

iTrust
Centre for Research in Cyber Security