iTrust Times

A Quarterly Newsletter

Issue Highlights:

Jan—Mar 2024 | Volume 10 Issue 1

From Centre Director's Desk

Dear readers,

Greetings from iTrust!

2024 has started with a bang right off the block, and some these activities are highlighted in this issue of iTrust Times.

We have seen a trend of IT-OT convergence which connects IT systems to their OT counterparts. As national laboratories specialising respectively in OT and IT security, iTrust and NCL have established a close partnership in providing an integrated IT-OT platform to support the national cyber exercises in protection of critical infrastructure. More collaborations between iTrust and NCL are in the works, including joint professional training, student engagement and cyber exercises.

Maritime is a new sector of critical infrastructure that iTrust has started to explore. After we released the guidelines for cyber risk management in shipboard OT systems for classic ships in Jan 2022, we further investigated the cyber risks in autonomous ships and released the new guidelines for cyber risk management in autonomous shipping in Jan 2024. Both guidelines can be downloaded from iTrust website. As autonomous ships are still at the early stage for commercial operations, we hope the new guidelines will seed discussions for safe and secure operation of autonomous ships. We also keeping abreast with autonomous ship technology advancements and in close contact with our stakeholders and partners to refine the guidelines as needed.

iTrust researchers have made significant progress in the R&D of 5G security. Led by Associate Prof Sudipta Chattopadhyay, his team has developed a powerful tool 5Ghoul and discovered a number of vulnerabilities present in the firmware implementation of 5G mobile network modems from major chipset vendors Qualcomm and MediaTek. The team also developed a tool U-Fuzz for autonomic security testing of IoT devices. Those tools have a good potential for commercialization.

iTrust continues to offer unique education and training programs to nurture future talents in cybersecurity. We not only provide the internship opportunities to university students, but also host the intern students from local secondary schools. Besides the CiMS scholarship program managed by iTrust and open to MSSD students in SUTD, we are also in discussion with SUTD Academy to provide cybersecurity courses for professional education, by leveraging our world-class OT testbeds.

iTrust is the main organiser of ACM AsiaCCS'24, a leading cybersecurity conference to be held in Singapore on 1-5 July 2024. The preliminary programme has been released. We will organise a special tour to visit iTrust and FCP at SUTD on 1 July. More details will be available at the conference website.

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

A Tale of Two Sisters: NCL & iTrust

By: Mark Goh, Assistant Director, iTrust

In its simplest form, an IT-OT convergence connects IT systems to their OT counterparts, thereby allowing them to communicate and transmit data to each other. Even as both IT and OT departments exist within an organisation, there is still a gap to be bridged so that they can work in concert to protect the organisation's assets.

As national laboratories specialising respectively in IT and OT security, the National Cybersecurity R&D Lab (NCL) at the National University of Singapore and iTrust, Centre for Research in Cyber Security at the Singapore University of Technology and Design, have in recent years fostered a tighter bond. As sister laboratories receiving guidance from the same Governance Board, the partnership and conjoining of both laboratories' platforms was a natural transition, and I've had the pleasure of witnessing this transition taking place in 2022 in several forms.

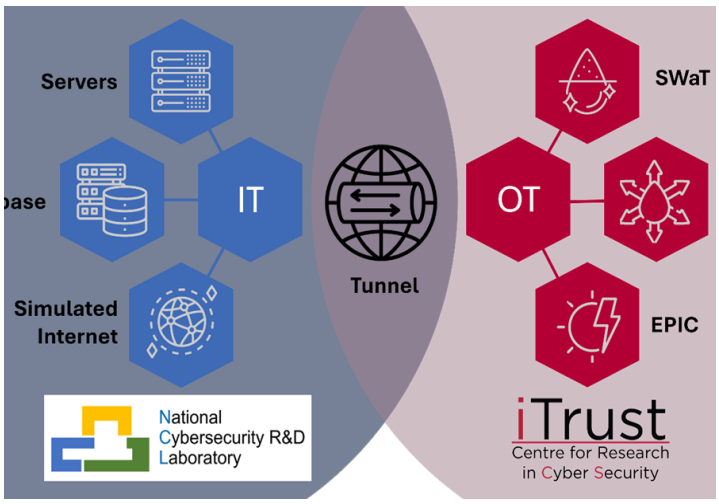

Fig 1.: Connection of IT and OT platforms between NCL and iTrust

Hosting Digital Twins

iTrust has developed digital twins that replicate its water treatment testbed, for professional training and education, among other use cases. Depending on the modes in which the digital twins operate, they can impose a heavy resource requirement. The first NCL-iTrust partnership was to lean on NCL's powerful servers to host iTrust's digital twins, so that multiple copies of them could be available simultaneously for students to access and operate them for their research and education. Other than students from SUTD's Master of Science in Security by Design, PhD students from the University of Bristol were among the users of the digital twin hosted by NCL..

Critical Infrastructure Security Showdown (CISS)

CISS is an annual red teaming cyber exercise organised by iTrust and the Ministry of Defence and is held in two stages: Stage 1 and Finals. In Stage 1, red teams are tasked with meeting a host of OT challenges in a CTF format over a 48-hour period, with the top 10 teams admitted to the Finals. With numerous experiences of hosting CTF under its belt, NCL helpfully hosted the entire Stage 1, dedicating not just hardware resources but also manpower to continuously monitor the network throughout the 48-hour period, including responding to queries raised by red teams.

Critical Infrastructure Defence Exercise (CIDeX)

NCL and iTrust partnered together to support the inaugural CIDeX that was organised by the Digital and Intelligence Service (DIS). At CIDeX, NCL's IT platform ingested process data and network packets generated from the operation of iTrust's OT testbeds – the Secure Water Treatment (SWaT), Water Distribution (WaDi) and Electric Power and Intelligent Control (EPIC). The process data and network packets were then used for process visualisation and monitoring during the cyber exercise.

In the past 2 years, NCL's professional team of experts, led by Principal Investigators Assoc Profs Chang Ee-Chien and Liang Zhenkai and Program Director Mr Seah Choon Meng, has provided exceptional support to iTrust in its activities. The merger has helped form a tighter knit between both laboratories, and the spirit of collaboration has been one of the key highlights for me in 2022 and 2023. With both laboratories having their funding renewed by the Cyber Security Agency of Singapore (CSA), I look forward to many more joint activities with NCL in the coming years.

This article first appeared in NCL Newsletter 2024 Volume 7.

Maritime Sector Updates

Guidelines for Cyber Risk Management in Autonomous Shipping

By: Li Meixuan, Research Assistant, iTrust

iTrust published a new Guidelines for Cyber Risk Management in Autonomous Shipping on 18 Jan 2024. This follows its first publication of cyber risk management for shipboard OT systems in Feb 2022. The new guideline aims to provide guidance

and mitigation measures to the broad maritime industry on OT risks associated with the Maritime Autonomous Surface Ship (MAAS) as the technology for automation becomes more mature.

At the recent International Conference on Applied Cryptography and Network Security (ACNS2024) in Abu Dhabi, UAE, iTrust Research Assistant, Ms Li Meixuan had the opportunity of presenting insights in developing the autonomous shipping guidelines. She highlighted the research questions and future work that could make a difference in the future of autonomous shipping cybersecurity.

Fig 2.: iTrust Research Assistant, Li Meixuan presenting on the Guidelines for Cyber Risk Management in Autonomous Shipping at ACNS2024.

Drawing upon diverse range of expertise, iTrust actively sought inputs from various industry partners, ensuring that the guidelines reflect a holistic understanding of the cyber risks associated with MASS operations. The guidelines begin with a retrospective glance at the evolution of MASS projects. Along the way, a myriad of technological advancements has nudged the field of MASS forward. By analysing the insights from guidelines issued by various shipping organisations, Meixuan and the team distilled perspectives on best practices and industry standards governing autonomous ship operations. While MASS is arguably still at a nascent stage especially in regards to commercial operations, Meixuan and the team, with their previous experience in shipboard OT cyber risk assessment, was able to put together an initial advisory on MASS cyber risk assessment, ready to be refined and adopted as MASS technology, regulation and acceptance mature.

IoT Sector Updates

5Ghoul & U-Fuzz Research

The objective of IoT sector in the second phase of the National Satellite of Excellence in Design Science and Technology for Secure Critical Infrastructure (NSoE-DeST-SCI) programme is to address the growing attack surfaces of IoT systems, with two focus areas: (1) developing technologies to discover new attack surfaces in IoT devices, and (2) developing detection and mitigation techniques to protect IoT devices from zero-day attacks. In a recent meeting, IoT sector lead Associate Prof Sudipta Chattopadhyay presented his team's research and discoveries on 5Ghoul and U-Fuzz. 5Ghoul is a described as "a family of implementation-level 5G vulnerabilities", or a collection of CVEs (Common Vulnerabilities and Exposures) present in the firmware implementation of 5G mobile network modems from major chipset vendors Qualcomm and MediaTek. Using wireless fuzzing, the team discovered 14 vulnerabilities n the chipsets, of which 12 were new. Of the 10 vulnerabilities that affected 5G modems from Qualcomm and MediaTek, six had a high severity rating. For their discoveries, they were awarded US$36,000 by Qualcomm and MediaTek, and featured in Channel News Asia in Dec 2023. Technical information on 5Ghoul can be accessed at https://5ghoul.com/

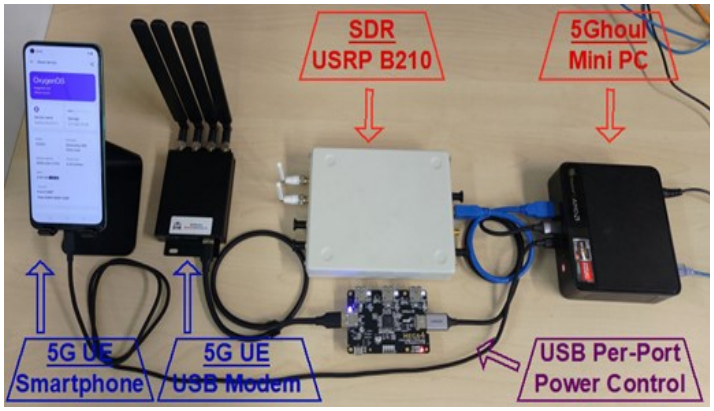

Fig 3.: Hardware Setup for 5Ghoul PoC testing and fuzzer evaluation

U-Fuzz is a framework to systematically discover and replicate security vulnerabilities on arbitrary wired and wireless IoT protocol (e.g., CoAP, Zigbee, 5G NR) implementations. U-Fuzz offers possibility to automatically construct the protocol state machine with only a few packet traces of normal (i.e., benign) communication. Thus, IoT device manufacturers can use U-Fuzz almost out-of-the-box for security testing, irrespective of the protocols they use for IoT devices. Using the framework, the team uncovered 11 new vulnerabilities across 5G NR, Zigbee,

CoAP. For their discoveries, they were awarded US$4,500 by MediaTek. Technical information of U-Fuzz can be accessed at: https://github.com/asset-group/U-Fuzz.

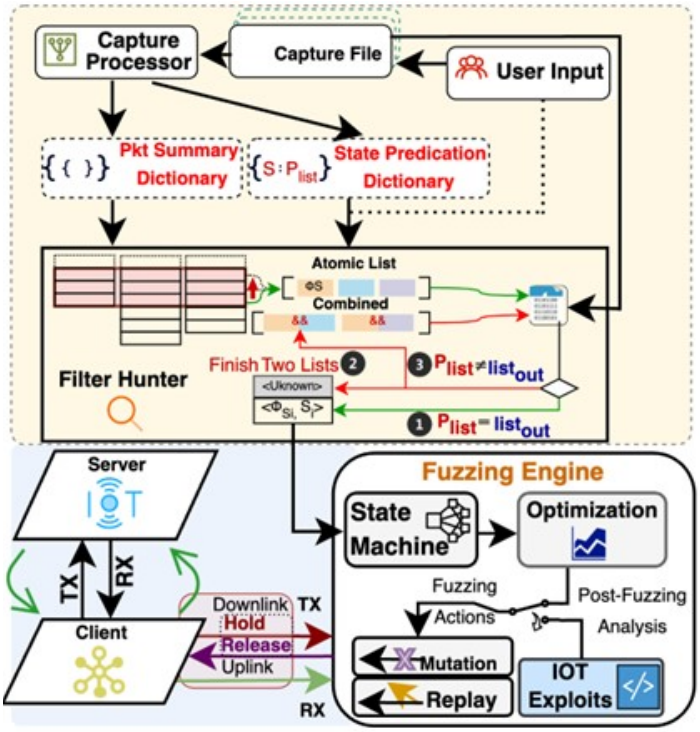

Fig 4.: U-Fuzz framework

Collaboration

Python Programming Course at Yusof Ishak Secondary School

By: Andy Tay, Research Assistant, iTrust

In line with iTrust's dedication to nurturing future talents in cyber security, iTrust conducted two courses for students in Jan and Mar 2024.

On 17 Jan, Andy conducted a fundamental cyber security course during SUTD's Independent Activity Period (IAP). This period offers students the flexibility to organise and participate in various courses and activities of their interests. The course is designed to introduce fundamental IT and OT security principles and cyber security awareness to the participants. The topics included social engineering, social media security, and the tactics, techniques, and procedures (TTP) used by cyber attackers. About 30 SUTD staff, researchers and students attended the course.

iTrust was approached by Yusof Ishak Secondary School (YISS) to provide a 4-day Python programming course for about 20 Secondary 2 students in March. The programme is specifically tailored for beginners with no prior programming experience.

Fig 5.: Andy Tay (standing) guiding YISS students during the Python Programming Course

The first three days featured hands-on activities aimed at building programming fundamentals and encouraging algorithmic thinking. On the fourth day, students collaborated in groups to showcase games they had developed, utilising the knowledge acquired from the initial three days. With some guidance from Andy and Keenan, one of the more advance students also developed DirBuster, a cybersecurity tool to uncover hidden web directories on a website.

Fig 6.: Future cyber warriors with iTrust trainers Andy Tay (front row, first from right) and Keenan Hong (standing, first from right)

Awards

Spectra Secondary School Awards Day

iTrust was presented with the 'Friends of Spectra' Award on 8 Mar 2024. The award was in appreciation of iTrust's partnership with Spectra Secondary School for supporting its Industrial Experiential Programme (IEP) for the past 3 years.

Fig 7.: iTrust Assistant Andy Tay receiving the award on behalf of iTrust at the award ceremony

A total of 18 students have been attached to iTrust for 3 weeks as interns since 2021. Their internship focuses on skill acquisition and applied knowledge, where they undergo a basic theoretical understanding of cyber security and also given a chance to put learning into practice by engaging in hands-on quality assurance testing for iTrust's technologies.

Visits

Visit by Raffles Institution

By: Andy Tay, Research Assistant, iTrust

On 1 Feb 2024, iTrust welcomed 20 teachers from Raffles Institution as part of their visit to SUTD to learn about its curriculum and pedagogical innovation. The teachers were given a tour of iTrust's testbeds by Andy who explained how the testbeds serve as a platform for conducting applied research and facilitating training and education in the safety and security of critical infrastructure.

Fig 8.: Group photo of Teachers from Raffles Institution

Internship

Reflections

By: Mohamed Rian Shahrin and Koo Jun Sheng , Temasek Polytechnic interns

During their internship at iTrust from 26 June 2023 to 16 Feb 2024, Rian and Jun Sheng were mentored by Francisco, iTrust's Cyber Tech Lead. Both interns were involved in the recent Critical Infrastructure Security Showdown (CISS) 2023, as well as the Critical Infrastructure Defence Exercise (CIDeX) 2023. Rian took the initiative to produce an informative infographic outlining the impact of the "Industroyer" malware on OT systems and summarised the intricacies of MITRE Caldera for automated adversary emulation. The infographic (Fig 10) details real-world Tactic, Technique, Procedures (TTPs) affecting critical infrastructures. Rian also contributed to the implementation of CALDERA™, an adversary emulation platform harmonised with the MITRE ATT&CK™ framework, which significantly enriched iTrust's toolkit; an addition to iTrust set of tools for adversary emulation .

Jun Sheng participated in the CISS 2023' stage 1 Capture the Flag (CTF) as a non-competitive participant, enhancing his practical cybersecurity skills and gaining valuable insights into information gathering, Wireshark, and operational technology. In CISS finals, he took on the role of a Tech Writer, overseeing tasks such as checking connectivity and cloning of Virtual Machines (VMs) and creating batch script files on Windows for automation. Jun Sheng also documented notable tools and attacks employed by red teams during their engagements. With his knowledge and insights, Jun Sheng created an infographic poster focusing on industrial control system specific malware like PIPEDREAM (Fig 11).

On their final day of their internship, Rian and Junsheng presented their project, "Automation of Red Team Emulation", in which their lecturers were also invited. In their presentation, Rian and Junsheng showcased their collaborative effort in crafting an ENIP plugin for MITRE Caldera, tailored for application in SWaT. Both interns developed the Mitre Caldera Operational Technology (OT) Plugin for the ENIP protocol, where they designed the ENIP payload in Python for the Caldera Agent, compiled Python payload files into single-file executables, and documented specific capabilities related to SWaT.

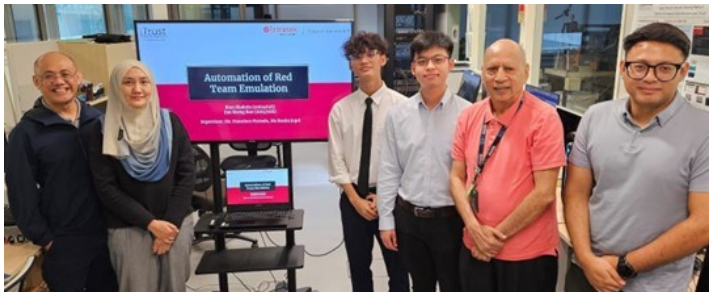

Fig 9.: Interns Rian and Jun Sheng (centre) accompanied by their Senior Lecturers from Temasek Polytechnic, Diploma of Cybersecurity and Digital Forensic (from left Mr Shaun Tan, Ms Rosita Jupri), and their mentors from iTrust (from right Francisco Furtado and Prof Aditya Mathur)

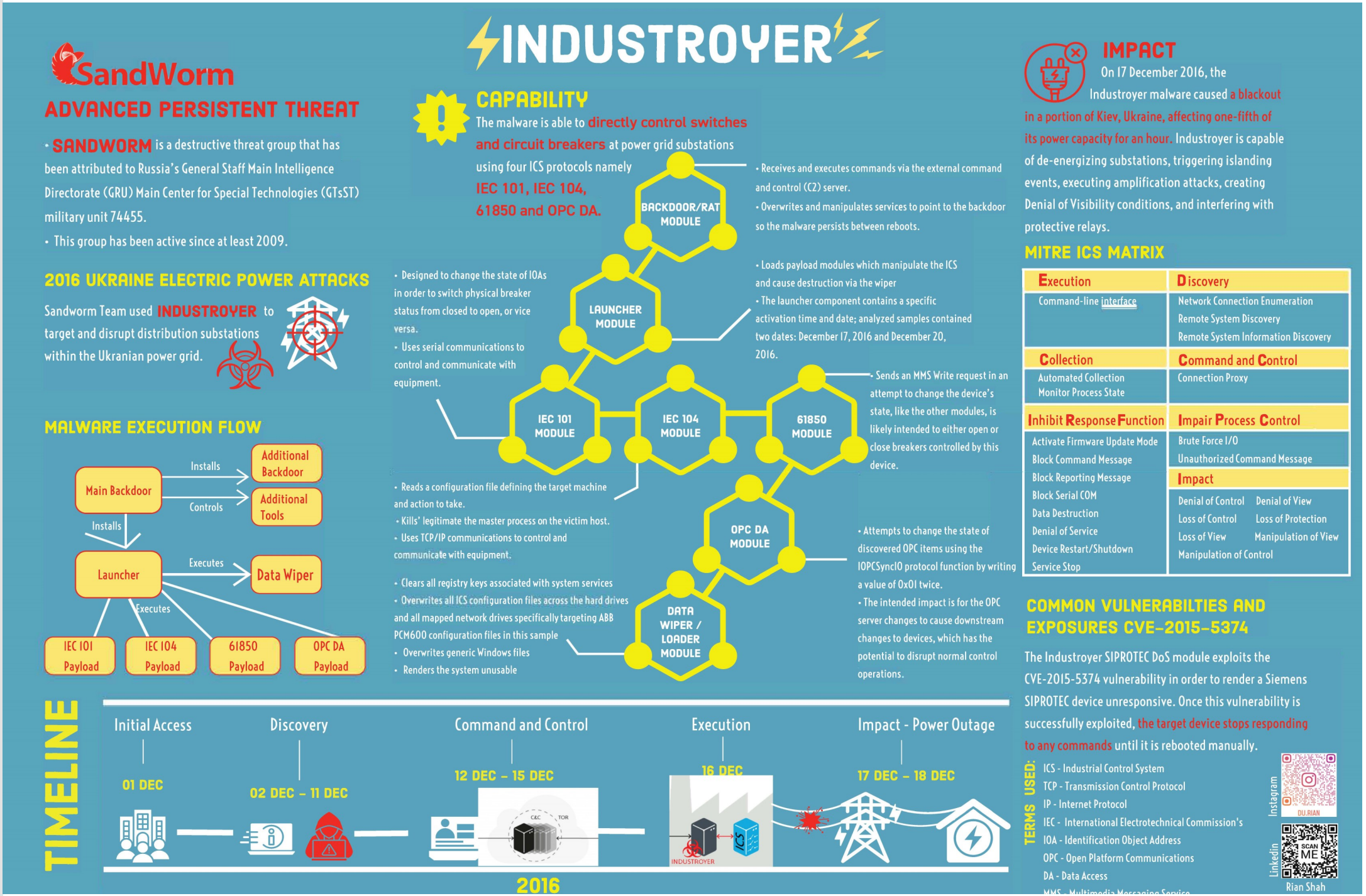

Fig 10.: Industroyer infographic created by Rian

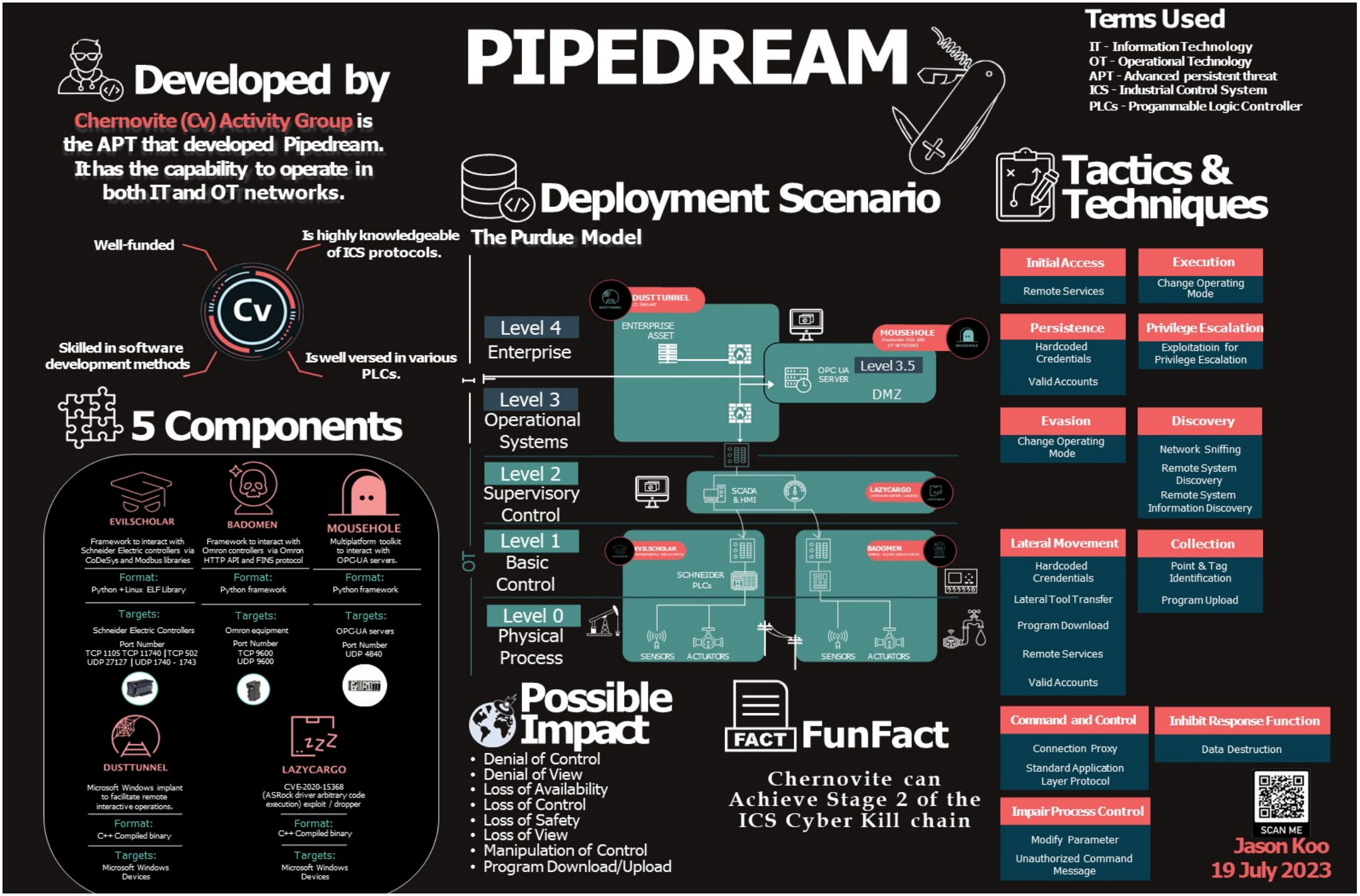

Fig 11.: Pipedream infographic created by Junsheng

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

Francisco FURTADO
Cyber Tech Lead, iTrust
francisco_dos

Mark GOH
Assistant Director, iTrust
mark_goh

iTrust Laboratories

Aanand R
Cyber Security Technology Engineer
Aanand_r

Andrew TAY
Research Senior Technologist
andrew_taykongngee

National Satellite of Excellence

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

Scan to view previous issues

iTrust Matters

Upcoming Events

Design of Cyber-Secure Water Plants (DCS-Water'24)

Conference Date: 23—24 April 2024

The 1st International Conference on the Design of Cyber-Secure Water Plants (DCS-Water'24) is a 2-day event aimed at bringing together a diverse group of researchers and practitioners to present and discuss novel methods and tools for protecting water plants against cyberattacks.

Register here:

ACM ASIA Conference on Computer and Communications Security (ACM ASIACCS 2024)

Conference Date: 1—5 July 2024

Building on the success of ACM Conference on Computer and Communications Security (CCS), the ACM Special Interest Group on Security, Audit, and Control (SIGSAC) formally established the annual ACM Asia Conference on Computer and Communications Security (ASIACCS).

Register here:

General Enquiries

iTrust: *itrust*

NSoE: *nsoe_destsci*

CiMS: *cims*

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