iTrust Times

A Quarterly Newsletter

Issue Highlights:

DeST-SCI

National Satellite of Excellence

Design Science and Technology for Secure Critical Infrastructure

Oct—Dec 2020 | Volume 6 Issue 4

From Centre Director's Desk

Wrapping Up A Year of Research

Dear Reader:

Greetings from iTrust!

In this issue we bring you highlights of a few selected research projects and the progress made by the corresponding research teams. Surprisingly, despite the many constraints imposed by COVID-19, the highlighted research projects, as well as several others, have maintained the expected rate of progress towards promised deliverables. Congratulations to all members of the research teams!

Datasets released by iTrust continue to be in high demand. At the time of penning this note, the datasets have been downloaded 2,810 times in response to a total of 1,029 requests emanating from 66 countries. While we are unable to track the publications resulting from the use of these datasets, we have come across a few that explicitly reference the datasets obtained from iTrust.

I am proud to announce the release of our most recent dataset collected during the international, fully online, cyber security exercise, CISS2020-OL. The data released is mostly unedited; names of red and blue teams as well as the response to attacks by the anomaly detectors, have been removed. A summary of the released dataset appears in this newsletter while additional details are available at the iTrust website. iTrust is continuing to analyse the performance of various anomaly detectors used during CISS2020-OL. We expect to release the outcome of this analysis in the first quarter of 2021.

We are truly thankful to all who use the iTrust datasets for the advancement of knowledge in the design of secure critical infrastructure. We will be happy to hear from you about any publication from your group that contains results obtained through the use of the datasets.

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

NATIONAL RESEARCH FOUNDATION
PRIME MINISTER'S OFFICE
SINGAPORE

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust
Centre for Research in Cyber Security

Research Focus

Research Updates

Scalable Hybrid Honeypot Infrastructure for IoT Threat Intelligence and Response

By Dr Yan Lin Aung, Research Fellow, iTrust

In the age of Industry 4.0, Internet of Things (IoT) will have profound impact on industries as more and more devices are connected to the Internet, collecting and processing data, and becoming smart. However, security aspects of IoT devices are often neglected, leading to large-scale attacks on IoT devices. In 2016, a malware called Mirai created a botnet that was capable of launching a major denial of service attack against one of the Internet's backbone: a domain name server that made major services such as Twitter and Facebook unreachable to most users. Variants of this threat have appeared regularly in Mirai's aftermath, with millions of devices still vulnerable to such attacks. Due to the heterogeneity of IoT devices and the massive numbers of devices, it is challenging to foresee new attack waves.

Researchers at iTrust have been working on a hybrid (low and high interaction) honeypot infrastructure, designed to scale to various kinds of devices, and to collect real-time data on attacks running in the wild (Figure 1). The current setup includes consumer IoT devices such as IP camera, printer, smart plug, smart bulb as well as industrial control systems and emulators. These devices are manifested on 29 public IP addresses in the wild using commercial and private VPN services. For scalability, the researchers adopted lightweight and small footprint containers to forward the network traffic to IoT devices and emulators hosted in the IoT testbed at SUTD.

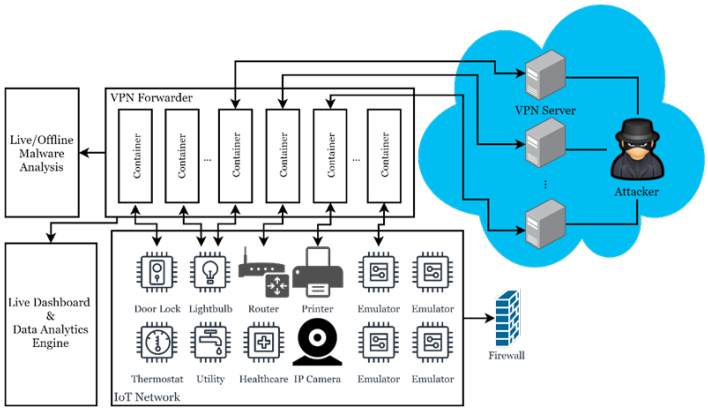

Figure 1: Scalable Hybrid Honeypot Infrastructure for IoT Threat Intelligence and Response

Towards Practical Attestation Solutions for Countering Advanced Attacks to Industrial Control Systems

By Assoc Prof Binbin Chen, Pillar of Information Systems Technology and Design, SUTD

Most Industrial Control Systems (ICS) today have limited ability to attest the integrity of the software running on their devices. Malware implanted on a device in an ICS could pose a significant security risk to its operations. While there are research solutions for attesting software integrity of devices, applying those solutions to securing a real-world ICS environment presents several challenges. Motivated by this gap, this project aims to design practical solutions that can attest the software integrity in a real-world ICS environment.

The project team, consisting of researchers from SUTD, Singapore Management University (SMU), Advanced Digital Sciences Center (ADSC) and University of Illinois at Urbana Champaign (UIUC), is developing solutions that can work under various real-world constraints - including the lack of hardware security modules in legacy devices, difficulty of upgrading software images on existing devices, and the various complex operational scenarios - while achieving the highest assurance against various advanced attacks (e.g., those stealthy attacks that try to mimic normal operational sequences.)

Towards this goal, one approach that the team is actively pursuing is to construct a non-invasive attestation exoskeleton setup that can carry out real-time behaviour attestation of programmable logic controllers (PLC) in an ICS. The proposed exoskeleton design requires minimum change to an existing ICS' setup, and will not interfere with the normal operations of the ICS. Some challenges the team must overcome include: (1) automating the construction of the exoskeleton based on given authenticate PLC logic; (2) supporting multiple ICS protocols, including the MMS and Modbus protocols and; (3) detecting various types of advanced attacks in real time.

The team has tested the exoskeleton prototype based on the setup of the Electric Power and Intelligent Control (EPIC) testbed at iTrust (Figure 2 next page) and demonstrated promising initial results.

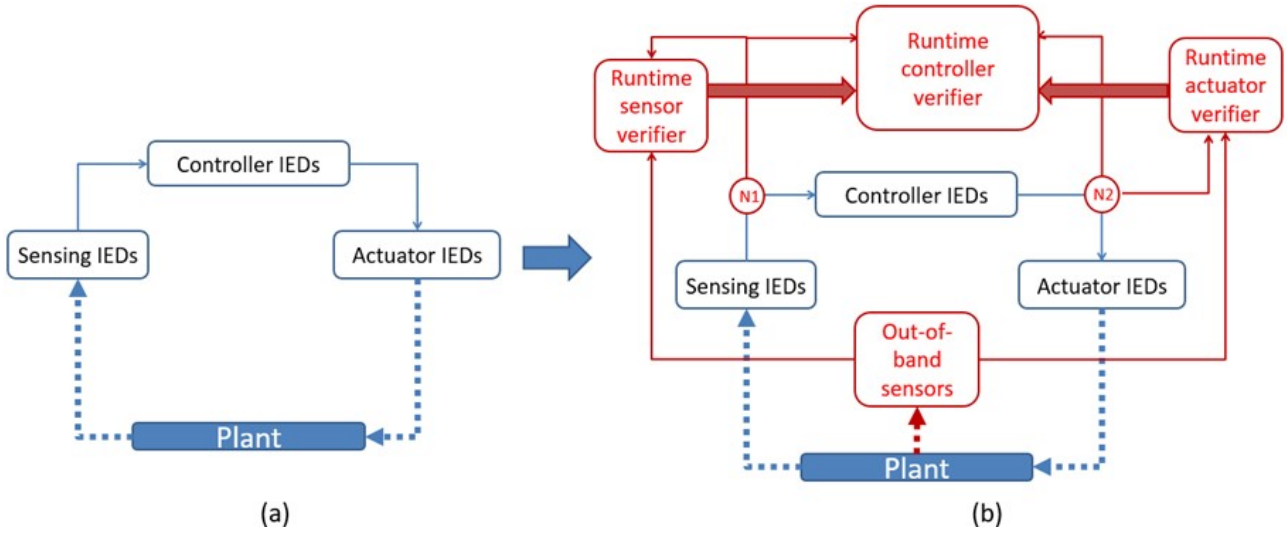

Figure 2: Attesting the integrity of an Industrial Control System (ICS) using a non-invasive exoskeleton-based approach.

LEarning from Network and Process data to secure Water Distribution Systems

By Assoc Prof Stefano Galelli, Pillar of Engineering Systems and Design, SUTD

The overarching goal of this project is to design and implement analytics to improve the cyber- physical security of water distribution systems (WDS). To meet this goal, the project addresses three specific problems: (1) Overcoming the lack of network and process data describing water distribution systems undergoing cyber -physical attacks; (2) Improving the accuracy of attack detection algorithms by harnessing the information contained in both network and process data; and (3) Facilitating and automating timely attack responses.

Digital twinning forms the backbone of our project: with a digital twin, we can simulate both network and process data of WDS undergoing cyber-physical attacks, and therefore design detection algorithm and real-time response mechanisms. For this reason, our efforts have mostly focused on the development of the digital twinning approach.

This approach builds on the interaction between a process-based numerical model (EPANET/ WNTR) and a network emulation platform (MiniCPS). The former simulates the hydraulic processes of a water distribution system, while the latter is a Python library that extends the network emulation tool Mininet to provide support for industrial network protocols. As illustrated in Figure 3, the integration between the two models relies on an Sqlite database: as the simulation progresses, the database allows to exchange information between physical and cyber layer (and vice versa).

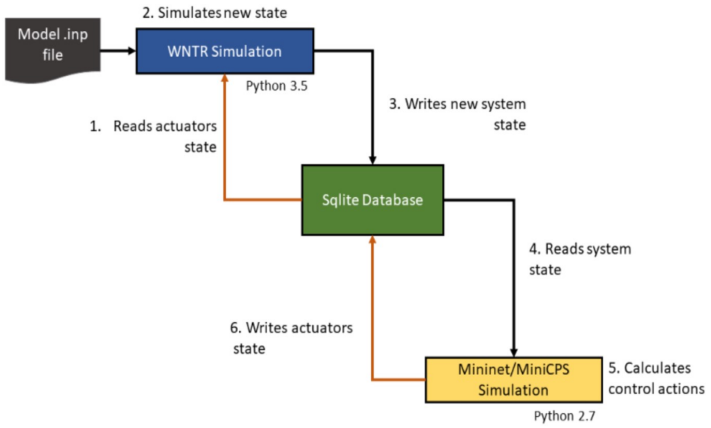

Figure 3: Architecture of the digital twin

Automated Framework for Generating Cyber-physical Range for Smart Grid

By Dr Daisuke Mashima, Senior Research Scientist, Advanced Digital Sciences Center Illinois at Singapore Pte Ltd

Cyber-physical range is a sandboxed, virtual environment that emulates high-fidelity behaviour of cyber-physical systems such as smart power grid. Portable, configurable cyber-physical range is desired not only by research communities (e.g., cybersecurity and AI) but also by system operators. We aim at designing modelling language, called smart grid modelling language (SG-ML), that describes the cyber range in smart grid context, and then developing the toolchain for instantiating the system according to the SG-ML.

In the first year of the project, we started with prototyping of the smart grid cyber range (Figure 4) to derive required information to configure the cyber range. The prototype implementation was designed based on the architecture of a modernised substation, having experimentation of emerging attack vectors in mind. Our paper "False Data Injection Cyber Range of Modernized Substation System" elaborating the prototype of the smart substation cyber range was presented at the IEEE SmartGridComm 2020 in November. We are also pleased to announce that the intern student who led the implementation won the Outstanding Undergraduate Researcher Prize from the National University of Singapore. The implementation has been further enhanced to support IEC 61850 standard, which is employed in iTrust's Electric Power and Intelligent Control (EPIC) testbed. The components of the cyber range will be made publicly available to contribute to the research community in the relevant area.

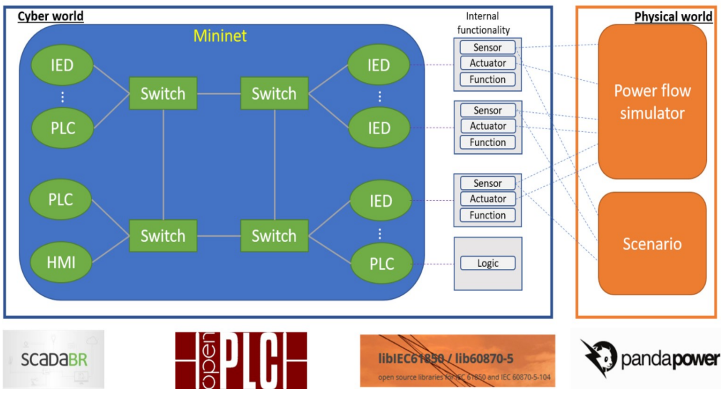

Figure 4: Prototype Architecture of IEC 61850-compliant Smart Substation Cyber Range Using Open-source Software

Based on the findings through the prototyping, we drafted SG-ML schema, which is defined in XML format. The SG-ML draft schema takes advantage of existing, standardised configuration/modelling framework, in particular IEC 61850 Substation Configuration Language. Since such information is already available for system operators, utilising it for cyber range modelling is expected to facilitate the task. The team is currently working on the implementation of toolchain for automated generation of the cyber range, while expanding the scope of SG-ML modelling to support larger-scale systems.

FBI – Featherlight Blockchain for IoT

By Dr Daniel Petrus Reijsbergen, Research Fellow, iTrust

Blockchain technology allows cryptocurrencies such as Bitcoin to maintain a shared ledger of transactions even when some of its participants behave maliciously. However, the inherent features of blockchains – such as immutability and decentralisation - are also attractive to use in contexts beyond cryptocurrencies. For example, a consortium of utility companies can use a blockchain to create a tamper-resistant log of meter readings and firmware updates (Figure 5.) The development of such a blockchain framework is the goal of this project.

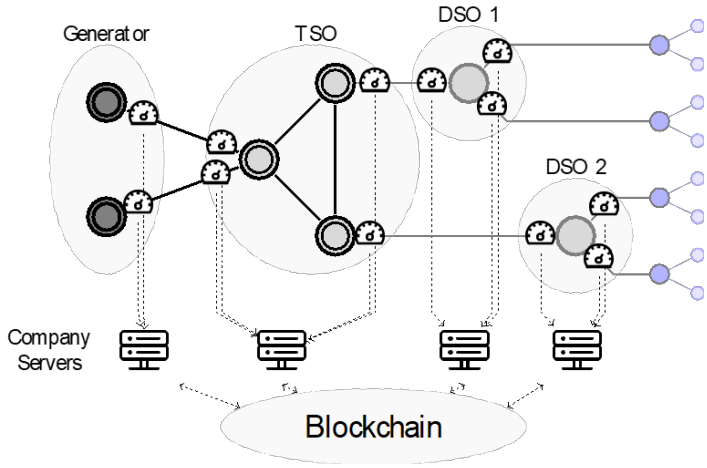

Figure 5: Smart grid with four companies (one generator, one transmission system operator, and two distribution system

As part of this project, we have developed techniques that mitigate the scalability and efficiency challenges that are common in blockchains. As a first contribution, we have explored the potential to speed up blockchains though multithreading by analysing historical data from seven prominent blockchain platforms. One important finding is that in real-world systems such as Ethereum, transaction execution can be sped up by as much as six times. As a second contribution, we propose a data sharing framework in which utility companies are rewarded for sharing meaningful data. To determine whether the data uploaded by companies to the blockchain is accurate, we perform on-the-fly anomaly detection. This requires efficient processing of matrix multiplications, and we present experimental results that show how this can be achieved. Finally, to secure meter reading integrity we propose a scalable two-layer framework. In this framework, a large collection of low-level blockchains store measurement hashes, and a high-level blockchain controls write access to the low-level blockchains. We

have tested this system using a testbed that includes both smart meters and a network of Raspberry Pis. These experiments show that our framework is able to support realistically-sized systems.

A Two-track Approach to CPS Reconnaissance: Causal-graphs and Axiomatic Design

By Assoc Prof Arlindo Silva, Pillar of Engineering Product Development, SUTD

In this project, rather than focusing on the security challenges posed by existing cyber-physical systems (CPSs) in critical infrastructure, we aim to reduce the possibility of those challenges arising in the first place, by developing and evaluating novel approaches to support the process of designing a CPS. Ultimately, we aim for systematic approaches that lead to more robust CPS designs, in which conceptual flaws have been eliminated long before the system is built. Furthermore, we aim to trace relations and conditions identified in the design through to invariant properties of the implemented system, and to use these in monitoring the system for anomalous behaviours (e.g. due to attacks).

In particular, we will develop two novel and complementary approaches in the context of CPS design. First, we will investigate axiomatic design theory, in which the functional requirements of the CPS are related to a set of design parameters, and systematically analysed using matrix methods. Second, we will investigate design graphs, in which causal relations and dependencies are modelled, and used to analytically identify different clusters of CPS components, as well as 'weaker' nodes of the system that could be targeted by an attacker. Finally, we will combine the approaches by deriving invariants for the implemented CPS based on the conditions and relations identified in the design stage.

These two approaches have been applied to SWaT with success (100% detection of attacks) and we are now applying the same procedure to WADI and hope to have results soon. The third step will be to investigate whether the same procedure can be applied to cascading effects across two testbeds, Secure Water Treatment (SWaT) and Water Distribution (WADI).

Cyber-Physical Attacks in Transmission Systems Using Digital Twin

By Assoc Prof So Ping Lam, Nanyang Technological University

Modern power grids are considered as critical infrastructures, which typically include critical physical devices and complex communication architecture. The security requirements are the key concerns in power grids. To ensure security in power grids, there are three key security requirements, such as confidentiality, integrity, and availability (CIA). While the modern power grid is expected to enhance the efficiency, economic, and energy distribution, cyber, physical, and cyber-physical security are the major concerns to compromise the CIA triad. Particularly, insecure communications and physically unprotected entry points pave the path for the adversaries. Specifically, nowadays, the modern power grid is facing the threats of both cyber and physical attacks. Sometimes, they may happen simultaneously in the new form called cyber-physical attacks which combine the physical topology attacks and the cyber topology attacks as shown in Figure 6.

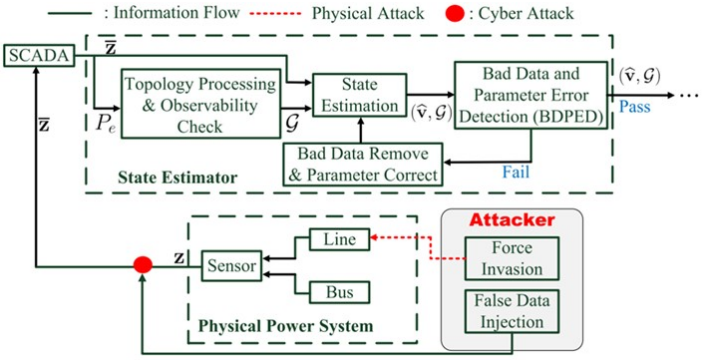

Figure 6: A cyber-physical attack on the transmission line [1]

Digital Twinning of Secure Treatment Facilities

By Di Tang, Research Associate, Nanyang Technological University

The objective of this project is to develop a digital twin for the detection of potential cyber-attacks by comparing real-time data (e.g., value of sensors and status of actuators) with predictions of the corresponding components using machine learning (ML) algorithms. This project is based on the Secure Water Treatment (SWaT) testbed facility at iTrust. The digital

twin is implemented on the Thingworx platform (from the collaborator CAD-IT Pte Ltd) as follows:

A mashup consisting of the six PLCs of the SWaT testbed has been established which together show the value/status of the main components of the system. Thingworx connects with the SWaT testbed to collect real-time data from the Supervisory Control and Data Acquisition (SCADA) station and stores the value streams. These data are used to train the ML algorithms (under development) to provide the predictions. Basic operational logics are imitated through translating the logics from RSLogix 5000 to JavaScript on Thingworx. The value/status predictions on primary components are expected to be achieved by running the JavaScript programs (under development).

To further improve the prediction accuracy, new ML algorithms with probabilistic assessment shall also be developed in the future for sensors/actuators that are difficult to predict precisely according to operational logic alone. The algorithms shall be written in Python and connected to Thingworx using Flask.

Design and Reinforcement Security on Smart Grids Against Cyber-physical Attack

By Assoc Prof Yuen Chau, Pillar of Engineering Product Development, SUTD

Complex cyber-physical systems (CCPSs) are present in national critical infrastructures, the smart grid being a well-known representative of CCPS. However, the heterogeneous, diverse, and complex nature of smart grids introduces a new level of security vulnerabilities compared to traditional CCPSs, which makes the smart grid an attractive target for cyber attackers. Catastrophic impacts on smart grids call for an urgent need to improve their security against anomalies and malicious attacks. In general, security improvements in smart grid field focus on (1) prevention; (2) protection; (3) detection and; (4) control mechanisms.

To deal with these four topics, the motivation of this project is to develop a new security reinforcement process (Figure 7) with defence-in-depth concepts in which the security reinforcement process could further be categorised into three phases: (1) Design; (2) Monitoring, and; (3) Operation. The security reinforcement process has the capability of identifying the potential vulnerabilities, threats and impacts from the cyber-physical perspective, and developing comprehensive detection, mitigation and control approaches against cyber-physical attacks. To that end, the objective of this project is to integrate security reinforcement process, from designing to monitoring and operation phases with novel technologies to ensure the smart grid has the characteristics of security, reliability, and resiliency.

To do so, firstly, security vulnerabilities of the evaluated system are analysed in the design phase. Then, a robust abnormal detection framework is developed using fused information from IT and OT systems in the monitoring phase. In operation phase, a secure and robust optimal control mechanism is studied with fully distributed characteristics that ensures high levels of security and robustness. The security reinforcement process differs from the existing security solutions in that it has the general and functional frameworks/mechanisms that range from prevention/ protection at infrastructures interconnection levels e.g., communication and operation infrastructures, all the way to the control systems' functional characteristics that are designed to maintain smart grid under safety and stable operation in the face of various incidents such as malicious cyber-physical attacks.

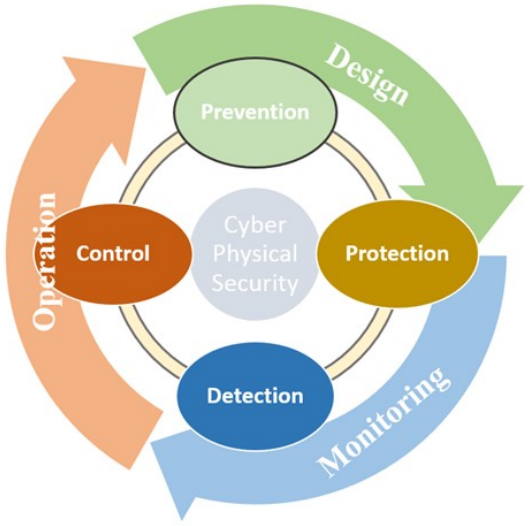

Figure 7: Concept of cyber-physical security reinforcement

[1] H. M. Chung, W. T. Li, C. Yuen, W. H. Chung, Y. Zhang, and C. K. Wen, "Local cyber-physical attack for masking line outage and topology attack in smart grid," IEEE Transactions on Smart Grid, vol. 10, no. 4, pp. 4577-4588, July 2019.

Datasets

CISS2020-OL

By Prof Aditya Mathur, Centre Director, iTrust

Keeping true to its goal of designing secure critical infrastructure, on 1 Dec 2020 iTrust has released a new dataset collected as part of an international cyber-security exercise. This exercise, named Critical Infrastructure Security Showdown 2020-OnLine (CISS2020-OL), was conducted during July 27 - Aug 7, 2020 at iTrust. Red teams from seven countries launched attacks on the iTrust Secure Water Treatment (SWaT) testbed. Details of this event are available in Volume 6 Issue 3 of the newsletter and also at the iTrust website.

The time-stamped dataset released, containing one row every second, consists of two sets of Excel files. One set of files is labelled "Target-x" and the other as "CISS2020_OL-y." There are three target files and 18 CISS_OL files. Each Target file contains approximately one hour of data collected while running SWaT under normal operating conditions. Each CISS_OL file contains data collected during approximately a 4-hour run during which a red team launched attacks on SWaT.

Each Target data file contains 82 columns where each column corresponds to one state variable of SWaT. Each CISS2020_OL data file contains 97 columns. In addition to the SWaT state, as in Target files, the dataset contains attack information. Specifically, the following information is available: attack launch (AL), attack update (AU), attack target, attack type (IT, OT, or both), attack intent, attack mode, attack outcome (Success, Fail), attacker ID (anonymised), attack ID, and attack sub-ID. While not all columns in the two sets of files contain data that might be relevant to the researchers, most do.

The dataset released is available to all interested researchers and can be requested via iTrust's website. Our sincere hope that this new dataset will assist researchers using machine learning in building effective models for anomaly detection and procedures for the ensuing incidence response. It may be noted that the data released now corresponds to SWaT that has been in operation since 2015. The newly released data, when compared with that released in 2015, and again in 2019, is likely to be of value to those interested in investigating sensor drift and recommending maintenance schedules for valves and pumps in a water treatment plant.

Dataset for Scalable VPN-forwarded Honeypots

By Dr Yan Lin Aung, Research Fellow, iTrust

Recent large-scale attacks exploiting IoT devices have raised significant security concerns for the stakeholders involved. The efficacy of setting up honeypots to survey the threat landscape and for early detection of threats to IoT devices is evident. Until recently, few implementations of honeypots have emerged with the goal of better understanding vulnerabilities, threats and large-scale attacks targeting IoT devices. However, the availability of dataset collected by these IoT honeypots in conjunction with analysis and insights on the dataset to advance research on IoT security has been scarce.

Researchers at iTrust have worked on high-interaction honeypots incorporating real IoT devices. The honeypots are manifested on 40 public IP addresses in the wild while forwarding the traffic to 11 real IoT devices. Their work was published in the 9th ACM Conference on Data and Application Security and Privacy (CODASPY '19). To foster further research on IoT security, our researchers are now sharing the dataset with the research community. The dataset corresponds to 136GB of network traffic data collected by the honeypots in the wild for 18 months, from 2017 to 2018. Using Zeek tool, the dataset is generated in JSON format from 258,871 PCAP files resulting in more than 81.5 million logs. Public IP addresses of the honeypots present in the logs are partially anonymised to protect their identities.

Details of the dataset and threat intelligence insights - extracted using an open-source threat-hunting and security monitoring platform - are provided in their upcoming paper to be presented in Sixth Annual Industrial Control System Security (ICSS) Workshop. Researchers who are interested in downloading the dataset can make a request at iTrust's website: https://itrust.sutd.edu.sg/itrust-labs_datasets/

Wrapping Up 2020

As we wrap up the year, we would like to share with our readers the reach and impact of iTrust's work:

Figure 8: Dataset requests by the numbers

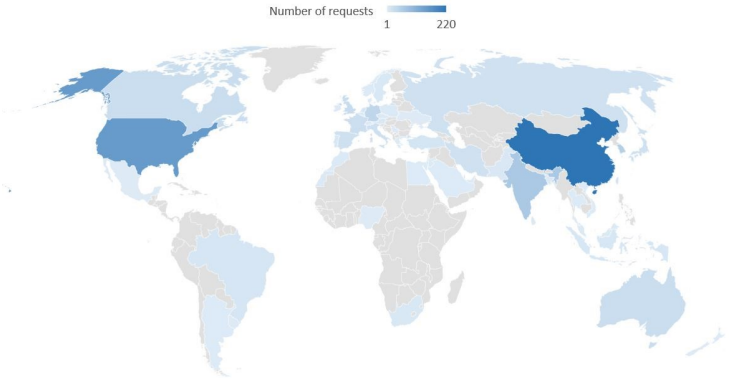

Figure 9: Dataset requests by regions

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

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 LI-YAKKATHANI
Cyber Security Technology Engineer
liyakkathali

General Enquiries
itrust

iTrust
Centre for Research in Cyber Security