iTrust Times

A Quarterly Newsletter

Issue Highlights:

- Critical Infrastructure Security Showdown — pg. 2
- NSoE Projects — pg. 4
- Awards — pg. 8
- Visit by Senior Minister Teo — pg. 10
- iTrust-ADSC Seminars — pg. 11

Jul — Sep 2019 | Volume 5 Issue 2

From Centre Director's Desk

Forging Ahead

Dear Reader:

Greetings from iTrust! Welcome to the Volume 5 Issue 2 of the iTrust Newsletter!

The readers may recall that iTrust now has a fully operational National Satellite of Excellence (NSoE). A call for proposals, issued in April 2019, resulted in 24 submissions from six academic and research organisations in Singapore. The proposals were reviewed by a diverse team of evaluators and the recommendations presented to the Steering Committee. I am pleased to report that starting October 1, 2019, 10 new research projects will be launched in the following research areas: automation of anomaly detectors and command validators, incidence response, attestation and assessment, digital twinning for water and electric power systems, attack prevention, and novel approaches. Abstracts of all funded projects are available at the iTrust website. The subsequent issues of this newsletter will offer a glimpse into these projects.

Some of you may be aware of the technology evaluation exercises that iTrust has conducted since 2015. These exercises were conducted under the week-long event labelled Secure Cyber Physical (SCy-Phy) Systems Week. This year we renamed the exercises as the Critical Infrastructure Security Showdown (CISS). The objective of the exercises remains unchanged, which is to assess technologies targeted at defending critical infrastructure. CISS 2019 took place during the week of August 26, 2019. Seven attack teams and six defence teams participated in the event. The massive amounts of attack and defense data collected is currently under analysis and will be made public in the near future. This data will serve as a valuable addition to the existing testbed data available via the iTrust website and aid researchers in testing their machine learning algorithms.

iTrust continues to be in the national and international spotlight. Senior Minister Teo Chee Hean visited iTrust on June 30 and was given a glimpse of advanced technologies under development at iTrust. Congratulations to researchers Siddhant Shrivastava, Aung Maw for winning the blockchain hackathon, to Stefanos Leonardos and Georgios Piliouras for winning the best papar award at the 1st International Conference on Mathematical Research for Blockchain Economy (MARBLE), held in Santorini, Greece, and to Stefanos Leonardos, Daniel Reijsbergen and Georgios Piliouras for winning the best best paper award at the 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC).

National Research Foundation
Prime Minister's Office
Singapore

Singapore University of Technology and Design

iTrust
Centre for Research in Cyber Security

Congratulations to Ivan Lee on the successful launch of Tegasus in partnership with SGInnovate and ST Engineering. Initially Tegasus will offer the following two courses in the area of secure critical infrastructure: Cybersecurity Industrial Control Systems Engineer (CSIE) and Cybersecurity Industrial Control Systems Supervisor (CSIS).

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

CISS
Critical Infrastructure Security Showdown 2019

Good versus good

After a one year hiatus, CISS – dubbed S317 in 2017 and S3 in 2016 – returned in Aug 2019, bigger and better. This year's exercise saw participation from seven Red Teams and six Blue Teams in a joint effort towards the overarching goal of improving the robustness and resilience of critical infrastructure (CI.) Other than Singapore, the participants hailed from across Japan, South Korea to Italy, Estonia and the United States. Blue Teams deployed their defence mechanisms alongside iTrust's, bringing to a total of more than 10 mechanisms concurrently and passively sniffing out attacks launched by the Red Teams over four days.

Each Red Team was given four hours to perform reconnaissance and launch attacks, and their attacks were presided over by a panel of judges from the Cyber Security Agency (CSA), Ministry of Defence and PUB, Singapore's water agency, and iTrust. The Red Teams were scored against the attack objectives of whether they were able to manipulate physical processes and sensor data, and to what extent they could exert control over the plant. Bonus points were also awarded to unique attack vectors that Red Teams could successfully demonstrate.

Following four days of intense and closely fought exercise, NSHC Security (Singapore) topped the charts of the Red Teams and was declared the winner. CTF.SG (Singapore) and Politecnico di Milano (Italy) came in a close second and third place respectively. Throughout the exercise, iTrust collected a valuable trove of data from the attack platform – the Secure Water Treatment (SWaT) testbed – and the detection logs from the Blue Teams. This year also saw the introduction of the fruits of labour by iTrust Research Assistant Muhammad Syuqri Bin Johanna: PlantViz, an aggregator and graphical display of several iTrust's anomaly defence mechanisms, and an attack logger that captured all the attacks launched by the Red Teams. Together, they will serve as crucial datasets required by modelling and machine learning researchers to develop and strengthen defence mechanisms. The datasets, along with a post-exercise report, will be posted on the iTrust website in the coming months.

Research Focus

DeST-SCI

iTrust's first grant call in critical infrastructure security

The National Satellite of Excellence (NSoE) in Design Science and Technology for Secure Critical Infrastructure (DeST-SCI), managed by iTrust, announced its inaugural grant call on 3 Apr 19 to solicit research proposals on design science and technologies for the creation and enhancement of critical infrastructure. The grant call was opened to academic and research institutions and public agencies.

At the close of the grant call in Jun 19, iTrust received 24 proposals. After several rounds of reviews and clarifications by an evaluation committee, 10 projects, totalling $7.35M have been approved.

The awarded projects are:

1. A Two-track Approach to CPS Reconnaissance: Causal-graphs and Axiomatic Design
Assoc Prof Arlindo Silva, SUTD

2. Automated Framework for Generating Cyber Physical Range for Smart Grid
Dr Daisuke Mashima, ADSC

3. Automated Incident Response and Recovery in ICS
Prof Zhou Jianying, SUTD

4. Design and Reinforcement Security on Smart Grids Against Cyber-physical Attack
Assoc Prof Yuen Chau, SUTD

5. Digital Twinning of Secure Water Treatment Facilities
Assoc Prof Law Wing Keung, Adrian, NTU

6. Enhancing Dynamic Analysis of Firmware in IoT Infrastructures via Component Functionality Inference
Assoc Prof Liang Zhenkai, NUS

7. FBI - Featherlight Blockchain for IoT
Asst Prof Dinh Tien Tuan Anh, SUTD

8. LEarning from Network and Process data to secure Water Distribution Systems (LENP-WDS)
Asst Prof Stefano Galelli, SUTD

9. Scalable Hybrid Honeypot Infrastructure for IoT Threat Intelligence and Response
Prof Zhou Jianying, SUTD

10. Towards Practical Attestation Solutions for Countering Advanced Attacks to Industrial Control Systems
Assoc Prof Binbin Chen, SUTD

Awards

iTrust continues to chalk up awards around the globe

National Blockchain Challenge 2019

Blockbuster of A Technology

iTrust Research Assistants **Aung Maw and Siddhant Shrivastava** participated in the National Blockchain Challenge 2019 that took place from 14 to 16 June 2019 at the Lifelong Learning Institute, Singapore. The event was sponsored by SkillsFuture SG, Our Singapore Fund, Lifelong Learning Institute, Amazon Web Services, and supported by top blockchain companies. 67 people participated in the Challenge and six teams reached the finals.

Siddhant and Aung delivered a technical pitch for their Blockchain solution, which they called "Blockbusters." Blockbusters uses the principles of decentralisation, immutability, and data replication to **solve the problem of data tampering in Critical Infrastructures** arising from a cyber attack. In the event that data is manipulated, Aung and Siddhant demonstrated Blockbuster could also **recover lost data.**

The judges, comprising a panel of representatives from Business Angel Network (BANSEA), Kleros, IOST and GovTech, awarded iTrust the **overall first prize and the vertical prize in the Cybersecurity category.**

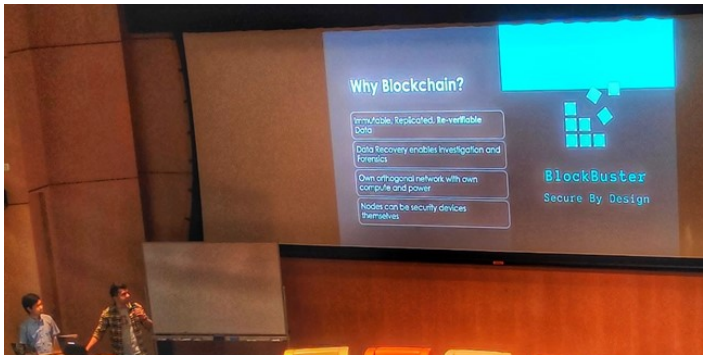

Figure 1: Aung Maw (left) and Siddhant (right) presenting their technology

An NRF-funded project "Testing for Blockchain Security by Design" took home two best paper awards in May 2019

In the first paper, iTrust postdoctoral researchers Dr Stefanos Leonardos, Dr Daniel Petrus Reijsbergen and SUTD Asst Prof Georgios Piliouras (ESD pillar) devised a new algorithm for **added security in Proof of Stake (POS) Blockchain protocols.** Their work won the Best Paper Award at the IEEE International Conference on Blockchain and Cryptocurrency (ICBC 2019). POS Blockchain protocols rely on voting mechanisms to reach consensus on the current state of data, but are vulnerable to faults when validators accidentally or maliciously withhold their votes. The team studied weighted voting in these protocols and designed an algorithm to enhance their security. The research paper also discussed potential issues and limitations of weighted voting in trustless, decentralised networks and related the results to the design of current PoS protocols. Congratulations!

The second paper, "Oceanic Games: Centralization Risks and Incentives in Blockchain Mining" won the Best

Paper Award in the 1st International Conference on Mathematical Research for Blockchain Economy (MARBLE). This paper was co-authored by Dr Stefanos Leonardos and Asst Prof Georgios Piliouras in collaboration with Nikos Leonardos from the National and Kapodistrian University of Athens. The paper utilises the theory of Oceanic Games, originally developed by the 2012 Nobel Laureate in Economic Sciences, Loyd S. Shapley, to **unveil the instability of decentralised blockchain mining.** The theory models the interaction between "big" mining pools and "oceanic" or individually insignificant miners and can be proven useful in the broader context of blockchain governance and long-term sustainability.

Events

iTrust-ADSC Seminars

The Impact of Network Modelling on Feasibility Results for Consensus

Jonathan Katz, a professor of computer science at the University of Maryland, and director of the Maryland Cybersecurity Center, presented the effect of different network models on the feasibility of various tasks related to consensus. He highlighted the assumptions about the power of adaptive adversaries in distributed protocols, noting that while in one model adaptively secure broadcast is impossible when more than half the parties may be corrupted, in another model adaptive security is possible for any number of corruptions. He also discussed the synchronous and asynchronous communication models for network communication and argued that neither provides a perfect model for real-world traffic.

Prof Katz then introduced a new "hybrid" protocol for consensus that is resilient to some fraction of corruptions when the network is synchronous and remains secure (though for a lower threshold of corruptions) even when the network is asynchronous.

Attack Trees with SAND: From Generating Security Test Cases to Extending with Defences

Attack defense trees are used to show the interactions between potential attacks on a system and the system

defences. In this talk, Dr Hoang Nga Nguyen first presented how to use attack trees to generate security test cases to provide a systematic security evaluation. This is done by transforming attack trees into equivalent formal representations where the generation of test cases can be done by model checking. Dr Hoang then presented an extension of attack defence trees with sequential composition, which allows for the description of attacks that are performed as a sequence of steps.

Dr Nguyen summarised the main contributions of his group's work: a formal representation of attack defence trees with sequential conjunction, a demonstration that this representation is equivalent to a process-algebraic one, and an algorithm for identifying the existence of attacks. Dr Hoang Nga Nguyen is a Research Fellow in Cybersecurity and Cyber-Physical Systems at Coventry University, and was a visiting researcher at iTrust for a week in Aug 2019.

Hacking Robots: Lessons Learned, Current Research and New Perspectives

Industrial robots are complex cyber-physical systems used in critical installations, and which entail almost every possible risk, from safety to economical damage. During the past two years, there have been numerous efforts at hacking (and securing) these robots.

In his talk Assoc Prof Stefano Zanero shared the main results from his group's research: a complete attacker and threat model for industrial robots; robot-specific cyberattacks that violate the fundamental "laws of robotics"; and an assessment of robot deployments and their protection.

He also reviewed the current research on the security of robot programming languages and at our future perspectives, including hardware and architectural ideas to improve robot resilience to penetration. Assoc Prof Zanero is an Associate Professor with the Department of Electronic, Information and Bioengineering at the Politecnico di Milano.

Visits

The number of visitors to iTrust has surpassed 1,000 since its inception in 2013

Senior Minister and Coordinating Minister for National Security, Mr Teo Chee Hean, visited SUTD's ST Engineering Electronics-SUTD (STEE-SUTD) Cyber Security Laboratory and iTrust on 24 June and witnessed the centres' contribution to Singapore's cyberspace security.

Figure 2: SM Teo at iTrust's Internet of Things testbed

The visit was hosted by SUTD President Prof Chong Tow Chong, ST Chief Digital Officer and Chief Technology Officer Mr Harris Chan and iTrust Centre Director Prof Aditya Mathur. Mr Teo's visit included research work presentations and interactive demonstrations on how cyber-threats can be prevented, detected, and thwarted.

SUTD's Office of Research organised the annual **Fostering Industrial Research Success Together (FIRST) Industry Workshop** on 24 July. The Workshop provides a platform to foster collaborative research success by developing and deepening industry-academia ties. The Workshop brings together relevant high-level stakeholders from industry, academia and the Government while showcasing relevant SUTD graduate-level research capabilities. Programme highlights included a keynote address by Prof Eugene Fitzgerald (CEO of SMART, MIT's Research Enterprise in Singapore), industry booth and research showcase by SUTD's graduate students and researchers, as well as a tour of SUTD's research centres, including iTrust's testbeds.

Virtualisation and visualisation @ visitation

On 12 Sep, 10 engineers and management staff from PUB - Singapore's water agency - visited the iTrust **virtual reality (VR)-based security and operations technology designed for water systems**, called VVateR. The demonstration of VVateR was led by research assistant Siddhant Shrivastava, who conceptualised the project in mid-2018. The student assistants involved in the demo were Filbert Cia and Tan Joon Kang. Research assistant Muhammad Syuqri, who developed the PlantViz technology demonstrated how it could **work with VVateR to provide with graph-based visualisations of anomaly detection mechanisms.**

Figure 3: Aditya explaining VVateR and PlantViz while research assistants Siddhant (far right) and Syquri (third from right) looked on

VVateR was originally modelled after SWaT testbed. With the help of the students operating the VR headset Siddhant explained its benefits and concomitant parts and how it aids in the security and training in critical infrastructure. For example, when VVateR is connected to an operational plant it enables operators to **visualise simulated cyber attacks and their adverse effects.** The ability of VVater to include the **operation of the plant in a unified Human-Machine Interface** was demonstrated. Other benefits include asset management, security by design, remote teleoperation, and visual reconnaissance for post-incident analysis.

Visiting Students

Two highly motivated students self-funded their research stints at iTrust

Wenjie Dong, an undergraduate from East China University of Science and Technology started his two

month research stint with iTrust in Jul 19. He assisted postdoctoral research Dr Gauthama Raman on developing an anomaly detection mechanism (ADM) – dubbed **the Auto-Encoder Detector (AED)** – against cyber-attacks. Previously developed detection mechanisms in iTrust include the Distributed Attack Detector (DAD) and Multilayer Perceptron Detector (MLP). Some of the research questions that they addressed are:

- Is a deep understanding of the CI plant design to approach anomaly detection required when using data-centric methods?
- How can the behaviour of CI components be modelled by Auto-Encoders?
- How effective is AED in detecting process anomalies resulting from cyber-attacks on a CI, when compared with existing ADMs like DAD and MLP?

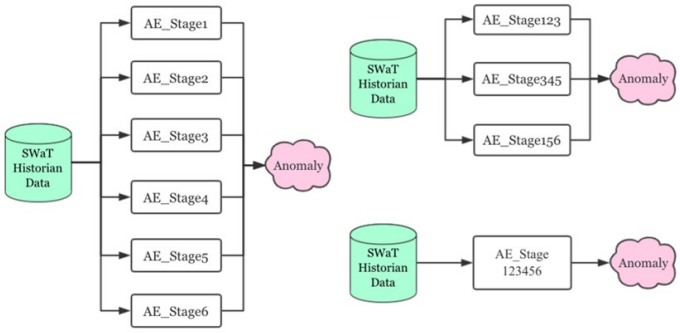

Figure 4: AED Strategy in Detecting Anomalies

AED is a well-designed group of Auto-Encoder models that are a special form of **feed forward neural network with multiple fully connected hidden layers.** As shown in Figure 4, AED is divided into 10 models (white boxes), catering to different combination of stages in SWaT, and work in tandem to raise attack alarms. Data from sensors and actuators, collected during normal operation for several days, is fed into Auto-Encoders for training. During the model fine-tuning process, such concepts as window-size, rate-of-change and Theil'U loss function are introduced to improve prediction performance and minimise false alarm rate.

Anusha Kumaresan is pursuing her Masters in Electrical and Electronics Engineering at National Institute of Technology, Puducherry. She is on a 6 month research attachment with iTrust from Jul 19, under the supervision of Principal Research Scientist Dr Robert Kooij and Research Scientist Dr Nandha Kumar Kandasamy. Her work focuses on **enhancing the security of smart inverters.**

With the increasing demand for clean energy, several energy utilities are increasing renewable energy sources (RES) in their generation portfolio. RESs are generally distributed and require improved and efficient distributed controllers to stabilise the grid. To accommodate high penetration scenarios of the intermittent RESs without impacting power quality or reliability, smart inverters are being employed. High penetration of RESs can create voltage fluctuations and frequency variations. Two major smart functionalities that can address high RES penetration include dynamic Volt/VAR control for voltage fluctuations and active power control/curtailment for frequency regulation.

Smart inverters require a platform for the coordinated operation in distribution feeders and the utility grid, and Distributed Energy Resource Management System (DERMS) is one such platform. Control of geographically distributed smart inverters will result in increased cyber threats on the grid and hence enhancing the security of smart inverters is essential.

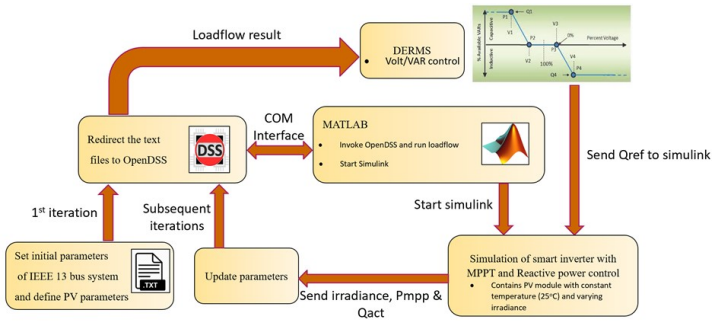

Figure 5: Data flow between different processes to implement controllable smart inverter in a distribution system

As a first step, Anusha set up a co-simulation environment to realise DERMS functionalities in a distribution grid with smart inverters. OpenDSS platform was used to implement a standard distribution feeder — the IEEE 13 node system. A model of smart inverter with active power curtailment and Volt/VAR control functions was implemented in MATLAB-Simulink. The data flow for the co-simulation is as shown in Figure 5. Future work aims to enhance the security of smart inverters at the actuator level.

Conferences

By Francisco Furtado and Beebi Siti Salimah binte Liyakkathali

The Kaspersky Industrial Cybersecurity Conference (KICSCon) 2019 was held from 18 to 20 Sep in Sochi, Russia. This is the 7th edition of the international conference. This year's focus was to 'discuss new trends in industrial cybersecurity, a current threat landscape and a necessary move from cybersecurity to the concept and embodiment of cyber-immunity.' The conference was attended by international industrial experts from Brazil, Germany, Israel, Russia, Spain and the USA. iTrust was invited back by Kaspersky to present its research work, and was represented by Research Assistants Francisco and Salimah. In 2018, Dr Riccardo Taormina (now an Assistant Prof in TU Delft) had presented on iTrust's behalf.

The first day of the conference was lined up with presentations from international cybersecurity experts. Dale Peterson, CEO at Digital Bond in USA, spoke on developing ICS Security Products with the future in mind where products can no longer provide passive-only solutions. Patrick Miller, Managing Partner of Archer International at USA, spoke on how to approach ICS Security from a risk management perspective as well as effectively communicate with executives and board members to get support for the necessary ICS security. Eugene Kaspersky, Kaspersky's CEO , spoke on moving from Cybersecurity, where endpoint devices are protected, to Cyberimmunity, where all the systems are secured by design.

On the second day of the conference Yan Sukhikh, Head of Information Security in Schneider Electric (Russia) presented on the safety of critical information infrastructure. Stephen Gerling, a Security Evangelist at ROSEN Technology & Research Center GmbH discussed the current likelihoods of manipulating the GPS systems, the threats and possible solutions. Francisco and Salimah presented and shared their research work titled **"Validating Defence Mechanisms of the Cyber-physical System via Attack Tool."** Noting the increase in the number of defence mechanisms for CPS, they stressed the importance of validating defence mechanisms for their completeness and robustness. To that end

Figure 6: Francisco (left) and Salimah (right) presenting their work at KICS

they introduced the motivation underlying iTrust's organising of the CISS Exercise and also shared the attack tool, which they developed, and mutation operators to aid in this validation. This was followed by a video demonstration of their attack tool on SWaT.

PhD student Gayathri Sugumar presented a paper titled **"Assessment of a Method for Detecting Process Anomalies Using Digital-Twinning"** at the 15th European Dependable Computing Conference in Naples, Italy. In her work, she explored methods for detecting process anomalies resulting from cyber-attacks on critical infrastructure. While noting that the results of an assessment on a testbed may be more authentic than those carried out using simulation alone, the former is fraught with challenges such as the time required to set up and launch attacks thus limiting the variety and number of attacks launched as compared with simulations. To overcome such limitations while maintaining the reliability of the outcome of the assessment, an approach based on **timed automata models of a critical infrastructure** was investigated.

The investigation involved the development of a digital twin for SWaT. A design-centric anomaly detection method, as well as an attack launcher, were integrated with the model and experiments were performed. The outcome of this investigation revealed the value of the proposed approach in rapid assessment of a design-centric anomaly detection method.

A modeling approach, and a case study, were used to assess the effectiveness of anomaly detection in a simulation environment. The entire methodology that begins

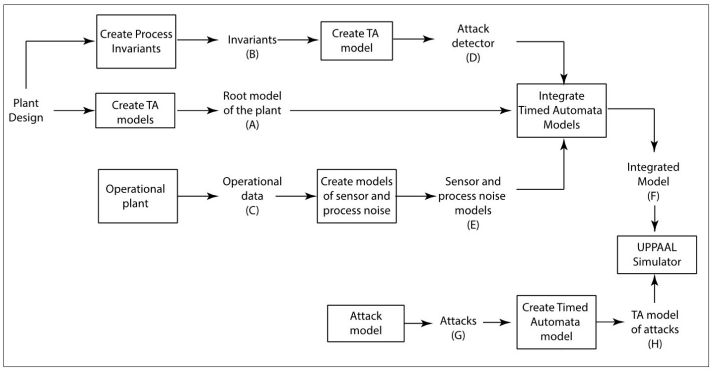

Figure 7: Steps in modeling and validation for assessing the effectiveness of an invariant-based anomaly detection mechanism using process simulation

with the design of a critical infrastructure (CI) and ends in the evaluation of an anomaly detector, is illustrated in Figure 7. As shown, the method leads to the creation of eight intermediate models comprising a root model of CI and model of sensor and process noise. This is followed by creating a model of anomaly detector and attack. The intermediate models are integrated in the UPPAAL simulator to assess the effectiveness of the anomaly detector.

iTrust Matters

Feel free to reach out to us to explore research collaborations, testbed usage and training and testing services.

Management

Ivan LEE
Deputy Director, Cyber Security Technologies
ivan_lee@sutd.edu.sg

Prof. Aditya P MATHUR
Centre Director, iTrust
Director, National Satellite of Excellence, DeST-SCI
Professor Emeritus, Computer Science, Purdue University
aditya_mathur@sutd.edu.sg

Prof. Jianying ZHOU
Co-Centre Director, iTrust
Professor, Information Systems Technology and Design
jianying_zhou@sutd.edu.sg

National Satellite of Excellence

Angie NG
Manager
angie_ng@sutd.edu.sg

Priscilla PANG
Manager
priscilla_pang@sutd.edu.sg

General Enquiries
nsoe_destsci@sutd.edu.sg

iTrust Laboratories

Mark GOH
Senior Manager
mark_goh@sutd.edu.sg

Desmond WAN
Senior Technologist (Water)
desmond_wan@sutd.edu.sg

iTrust is looking for interested individuals to fill the following positions:

1) Laboratory Specialist (Power)
2) Associate/ Senior Officer (Project Management)

For detailed job description and requirements, please visit https://itrust.sutd.edu.sg/join-us/administration-positions

In the previous issue's article titled "Attack Tool for Validating Defence Mechanisms" we stated that the A6-L0 attack tool was developed by Research Assistant Salimah. The statement should instead be: "The A6-L0 attack tool was developed by then-ISTD faculty member Asst. Prof Nils Tippenhauer and his research team. It was subsequently enhanced by Salimah." We are sorry for the error.

iTrust
Centre for Research in Cyber Security