iTrust Times

A Quarterly Newsletter

Issue Highlights:

- Awards pg. 1
- Conferences & Seminar pg. 2
- Student project pg. 5
- NSoE PI Profiles pg. 6
- iTrust Year-end Statistics pg. 8

Oct — Dec 2019 | Volume 5 Issue 3

From Centre Director's Desk

Wrapping up 2019

Dear Reader:

Greetings from iTrust! I wish all our readers a Very Happy and Productive 2020.

As I write this, I reflect upon the growth of iTrust, its diversity, and the achievements of our researchers and staff. After an intense period of review, the National Satellite of Excellence (NSoE) has awarded 10 research projects totalling $7.3M. There is at least one PI among the awarded projects from each of the four institutes of higher learning in Singapore, namely, NUS, NTU, SMU, and SUTD. In addition the Advanced Data Sciences Center, managed by UIUC, also received one grant. Together, these projects will focus on the development and assessment of technologies for the automatic generation of anomaly detectors and command validators, attestation and assessment, incidence response and recovery, digital twinning, attack prevention, and novel approaches to the design of secure critical infrastructure.

Doctoral students are making significant contributions to iTrust. Congratulations to Daniele Antonioli, Hamid Reza Ghaeini, and Mujeeb Chuadhary for defending their doctoral theses. Technologies developed by these graduates include Daniele's and Nils Tippenhauer's mini-CPS toolkit, Hamid and Nils' intrusion detection system, and Mujeeb's process anomaly detection system using device and process noise fingerprinting.

In an existing NRF funded project, our researchers are close to completing a pilot implementation of technologies for anomaly detection, based on machine learning, in an operational city scale plant. When completed, this project will be the first where technologies developed in iTrust technology have entered a large scale operational plant. I hope to be able to say more about this project in the next issue of iTrust Times.

As many of you may know, Secure water Treatment (SWaT) is one of iTrust's four flagship testbeds. Data generated from SWaT is being used by hundreds of researchers from across the globe. The extensive use of SWaT since its inauguration in 2015 has led to significant degradation of some of its critical components including the RO filtration units, valves, and sensors. Interestingly, we now have data from SWaT when it was brand new in 2015, as well as more recently collected data when SWaT has significantly degraded in its performance. These two datasets offer machine learning researchers a unique opportunity to test their algorithms that aim at

predicting maintenance needs for critical infrastructure. Upgrade of SWaT has already begun. I hope that a refurbished SWaT, i.e., SWaT 2.0, will be available to researchers by the second quarter of 2020. Once ready, we plan to run the plant for a few days and collect fresh data that will be made public on iTrust website as before.

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

Awards

In recognition of Ivan's contributions to the cyber profession and community

On 8 Nov 19, iTrust Deputy Director for Cybersecurity Technologies Ivan Lee received the **Professional Award** at the Cybersecurity Awards (TCA) organised by the Association of Information Security Professionals (AiSP).

Figure 1: (L to R) Mr David Koh, Chief Executive, Cyber Security Agency of Singapore, Mr Heng Chee How, Senior Minister of State for Defence, Mr Ivan Lee and Mr Steven Wong, AiSP President

This award **recognises the significant achievements of cybersecurity professionals and their contributions to their profession and community**. Nominees also demonstrated how they have raised Singapore's standing in cybersecurity beyond Singapore by leveraging their cybersecurity expertise.

The full media release of the event can be accessed here: https://www.aisp.sg/document/media/20191108_MR-TCA2019.pdf

New R&D Project Awarded

Research Focus

OT data integrity

Honeywell has engaged iTrust in an R&D project that utilises blockchain technology to create a platform to **ensure data in operational technology (OT) systems are tamper proof**. The motivation for this project arises from the following problem statements:

- In the event of a cyber-attack, if the central log repository is down, responders are unable to trace the actions resulting in delayed investigations
- In the event of an insider attack, actions performed can be erased or altered and hence forensic investigation becomes more difficult.

This project will record important transactions in an OT system on the blockchain. Doing so helps create a **nonrepudiation audit trail**, which is especially important when operators issue commands for tracing and validating during a forensic investigation. Information such as command issue, time, operator name, source IP, destination IP and status of command could be hashed and stored in the blockchain. The blockchain's immutable property ensures that such **information cannot easily be tampered with unknowingly.**

Research Assistant Aung Maw will work with researchers from Honeywell's Industrial Cyber Security Center of Excellence to develop this platform.

Conferences

Securing Critical Infrastructures

By PhD student Sridhar Adepu

At "Resilience Week 2019" San Antonio, Texas, Sridhar presented a student paper titled **"Attack Modeling, Anomaly Detection and Avoidance in Cyber-Physical Systems."** The paper describes proposed attack models that capture both physical and cyber-attacks

and unify a number of existing attack models into a common framework useful for researchers in the experimental assessment of attack detection techniques.

At another conference – 34th IEEE/ACM International Conference on Automated Software Engineering 2019 – Sridhar presented a paper **"Challenges in Secure Engineering of Critical Infrastructure (CI) Systems".** The paper characterises major challenges in securing CI based on iTrust researchers' experience working with realistic testbeds and proposes a set of future research directions in developing tools and methods for **secure engineering of CI systems.** In particular, securing CI will involve activities throughout an entire system lifecycle (from design to deployment and maintenance), and this paper proposes ways in which software engineering methods (e.g., requirements analysis, modeling, verification, and usability) can play an important role in the development of secure CI.

Protecting CI from a controls perspective

By postdoctoral researcher Dr Mohammadreza Chamanbaz

The adoption of event-triggered control strategies in Networked Control Systems (NCSs) can drastically reduce communication resources within the feedback loop. However, the nature of such a strategy is that any new information is exchanged only when the stability criterion is violated. But because a DoS attack can affect the availability of the interconnecting network it has the potential to seriously hinder the underlying physical processes and overall operations of an NCS.

In light of the above, Dr Chamanbaz's paper, **"Robust Stabilization of Resource Limited Networked Control Systems Under Denial-of-Service Attack,"** presented at the 58th IEEE Conference on Decision and Control, proposes to develop new event-triggering control strategies that are capable of ensuring the stability of the closed loop system subjected to DoS attacks characterised by their frequency and duration, while accounting for uncertainty of the NCS model. Specifically, the paper proposes an attack-resilient event-based robust control algorithm for discrete-time uncertain systems.

The primary goal of the work is to **analyse the effect of DoS attacks on a discrete-time uncertain network controlled system, and characterise the relationship between frequency and duration of the attack signal and closed-loop stability.** The Input-to-State Stability (ISS) theory is applied to derive the transmission rule and on/off periods of DoS attack signal.

While in most attack detectors whereby the control and attack detection designs are carried out independently - the controller is designed first and, subsequently, the detection mechanism is formulated - Dr Chamanbaz's second paper, **"A Physics-Based Attack Detection Technique in Cyber-Physical Systems: A Model Predictive Control Co-Design Approach"** proposes co-designing these two critical components and a joint control and attack detection mechanism using elements from model predictive control (MPC).

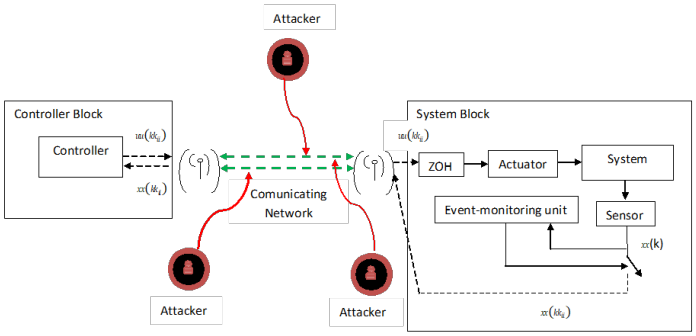

Figure 2: Block diagram of proposed control technique under DoS attack

His research team augmented the standard MPC problem with an additional constraint, restricting the future state/output trajectory to remain within some time-invariant neighborhood of a carefully designed reference trajectory. This involves the predicted states and inputs over the prediction horizon. The first component of the control vector is applied to the plant and the predicted outputs are used to construct the future reference trajectory. The reference trajectory at time k is the Nth component of the predicted trajectory provided as the minimiser of the MPC problem at time k-N, where N is the prediction horizon. The difference between actual real-time output and the reference output trajectory is stored in a residual time-series. The residual is used in a non-parametric cumulative sum (CUSUM) anomaly detector to decide on the presence of attack in control signal or measurement output (Fig. 3 next page.)

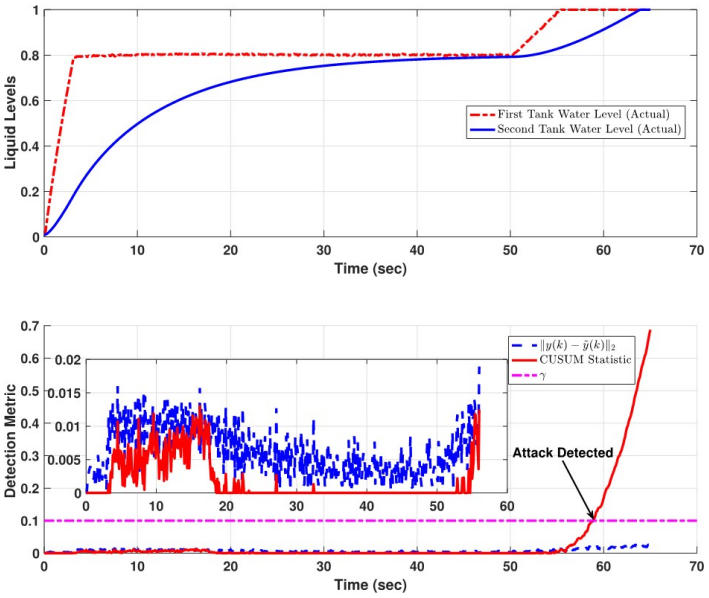

Figure 3: A coupled tank system where the reading from the level sensor reporting liquid level in top tank is compromised starting from t=50 sec. The top figure shows the actual level of both tanks. The bottom figure shows the residual as well as CUSUM statistic.

How datasets play a role in cybersecurity research and education

By Principal Research Scientist Robert Kooij

Dr Kooij presented a paper titled **"Using Datasets from Industrial Control Systems for Cyber Security Research and Education"** at the 14th International Conference on Critical Information Infrastructures Security (CRITIS 2019), which was held in Linköping, Sweden, from September 23 to 25, 2019.

The paper is a joint work with Delft University of Technology (DUT) and argues that the **availability of high-quality benchmark datasets is an important prerequisite for cyber security research and education.** The paper presents two studies on the use of the six datasets from the domain of Industrial Control Systems (ICS), that are made publicly available by iTrust. The first study uses the SWaT dataset, which led to a novel and explainable anomaly detection method called TABOR (Timed Automata and Bayesian netwORks), which has been shown to lead to a better detection performance than methods based upon Deep Neural Networks and Support Vector Machines. Fig. 4 depicts the Timed Automaton constructed for the level sensor in Stage 1 of SWaT, LIT101.

The second study conducted in the context of education made use of iTrust's BATADAL (water distribution network) dataset in a graduate course on cyber data analytics, taught at TU Delft. Research outcomes and the success of the course indicate an appreciation in the research community and positive learning experience in education.

Figure 4: Timed automaton learned from LIT101 in SWaT

Finding attacks on CI using smart fuzzing

By postdoctoral research Dr Christopher Poskitt

Suppose a new defence mechanism has been installed for SWaT or some other examples of CI. The typical way of assessing the mechanism is by subjecting it to attacks or attack data, and observing how effective it is at detecting them. For systems such as SWaT, attack benchmarks can be used for this purpose. But in general, realistic attacks for testing defences are not readily available, and up to now, typically require a large manual effort to put together.

Dr Poskitt's paper, **"Learning-Guided Network Fuzzing for Cyber Physical Systems,"** presented at the 34th IEEE/ACM International Conference on Automated Software Engineering 2019, introduces "smart fuzzing", an **automated, machine learning guided technique for systematically finding test suites of network attacks on CI**, without requiring any knowledge of the system's control programs or physical processes (other than the unsafe ranges of sensor readings). This technique uses predictive machine learning models and metaheuristic search algorithms (e.g. genetic algorithms) to guide the fuzzing of actuators so as to drive the system into different unsafe states (Fig 5 next page). Dr Poskitt's team implemented smart fuzzing on SWaT and WADI testbeds, and was able to **automatically derive attacks that drove them into 27 different unsafe states** involving water flow, pressure, tank levels, and consumer supply. Six of the unsafe states are not covered by the attacks in the existing SWaT dataset and benchmark.

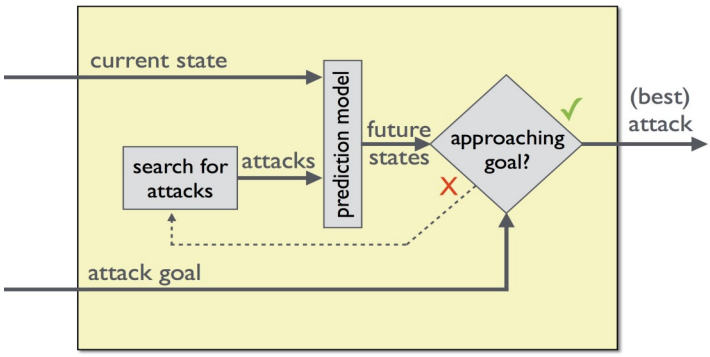

Figure 5: Finding attacks on critical infrastructure with smart fuzzer

His team also used the tool to assess the effectiveness of an iTrust-developed detection system for SWaT, finding two attacks that were not detected by its checks, thus highlighting a potential weakness that could be exploited in certain conditions. Finally, the tool was deployed successfully in the Critical Infrastructure Security Showdown (CISS) held in Aug 2019.

iTrust-NSoE Seminar

Scalable, Smart and Highly-interactive IoT Honeypot

As the number of commercial IoT devices grows, so do cyberattacks that target and exploit their vulnerabilities. Given that some of the attack vectors used in the wild against IoT devices might be novel, or not well understood, it is important to have up-to-date threat intelligence regarding the devices to be able to coordinate rapid remediation steps on devices not yet attacked.

In this talk Dr Martín Ochoa, who was previously a Co-PI in Project ReSILIoT (Research & Security Innovation Lab for IoT), reviewed the project's efforts to design, build and maintain a scalable and highly interactive IoT Honeypot at iTrust. He presented the results of this effort, and the insights gained on data collected in the wild over several months. Some challenges the team faced in order to improve the scope of the devices covered by the IoT Honeypot (a research track under the project), scalability, and the ability to analyse and share the data collected, were also highlighted. These challenges are now the subject of a study of a recently launched NSoE project, **Scalable Hybrid Honeypot Infrastructure for IoT Threat Intelligence and Response**, in which Dr Ochoa serves as a visiting expert.

Dr Ochoa is the Head of Research of the Total Fraud Protection division at Cyxtera Technologies in Bogotá, Colombia.

iTrust Student Project

How effective is Security Awareness Training?

It is a well-known fact around 90% of all cyberattacks start with a phishing email. To defend against such attacks, many organisations use Security Awareness Training as a means to reduce the employees' susceptibility to phishing attacks. The anticipated outcome of such training is a reduction of the so-called Click-Through-Rate (CTR). At the policing level, the Interpol Global Complex for Innovation (IGCI) ran a BECareful campaign in Oct 2019 to raise awareness of social engineering scam in the business community.

In response to such threats, Principal Research Scientist Robert Kooij, aided by SUTD undergrad student Lam Ying Sheng, embarked on a project **"Impact of Security Awareness Training on the Economic Losses due to Phishing".** They presented their findings to IGCI on 2 Dec 2019 in two parts.

The first part reported the outcome of an embedded phishing training conducted on around 20,000 participants. Using the data collected, they developed a model to **predict the employees' CTR as a function of the persuasiveness of the phishing email**, and whether or not the employee received the Security Awareness Training. In the second part they determined the **impact of the Security Awareness Training in terms of economic indicators**, by using an economic model that quantifies economic risks due to phishing. As the model can predict the anticipated profit for the cybercriminal, Robert and Ying Sheng were able to quantify the decrease in profitability for the cybercriminal as a result of the employee's Security Awareness Training. Fig. 6 (next page) shows the impact and frequency of Security Awareness Training on the conditional profit for the cybercriminal. It is clear that the impact of weekly training is much higher than of only a one-time training session (or none at all). The IGCI showed interest in the model and would explore another session where they can give realistic inputs for the model parameters.

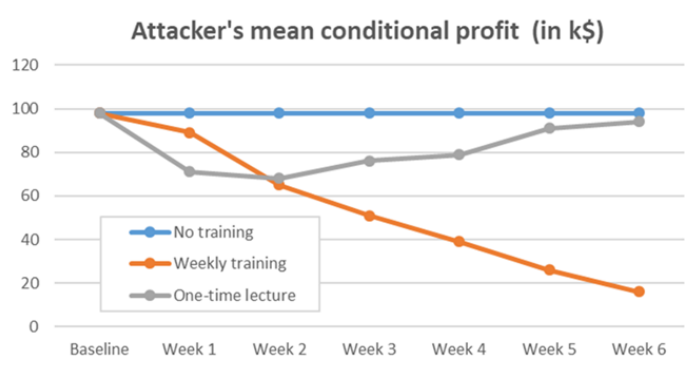

Figure 6: Impact of Security Awareness Training on the conditional profit of phishing attacks

Profiles

In the last issue we reported the newly awarded projects from iTrust's inaugural call for proposals under its National Satellite of Excellence office. The profiles of SUTD Principal Investigators are highlighted here.

Assoc Prof Binbin CHEN

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

Binbin Chen is an Associate Professor at SUTD since July 2019. Prior to joining SUTD, Binbin was a Principal Research Scientist at Advanced Digital Sciences Center (ADSC), University of Illinois. He received his PhD from the NUS and Bachelor from Peking University, in Computer Science. His current research interests include wireless networking, distributed systems, and cyber security for critical infrastructures. His research has received several awards, including the Best Paper Award in ACM SIGCOMM conference 2010 for the work on Error Estimating Coding. His research has been funded by National Research Foundation (NRF), Energy Market Authority (EMA), Agency for Science, Technology and Research (A*STAR), Building & Construction Authority (BCA), and the Singapore Cybersecurity Consortium.

Asst Prof Tien Tuan Anh DINH

Project: FBI - Featherlight Blockchain for IoT

Tien Tuan Anh Dlinh's research lies at the intersection of distributed systems, databases and security. He is interested in building and applying security primitives, either based on cryptography or trusted hardware, to improve both security and performance of large-scale systems. He obtained his PhD in computer science from University of Birmingham in 2010, in applying formal methods to verify security properties of P2P systems. His latest interest is centered around blockchains.

Asst Prof Stefano GALELLI

Project: LEarning from Network and Process data to secure Water Distribution Systems (LENP-WDS)

Dr. Stefano Galelli graduated in Environmental and Land Planning Engineering at Politecnico di Milano in 2007 and received a Ph.D. in Information and Communication Technology from the same university in early 2011. Before joining SUTD as an Assistant Professor, Dr. Galelli spent two years as Post-Doctoral Research Fellow at the Singapore-Delft Water Alliance (National University of Singapore), where he led the Hydro-informatics research group. Dr. Galelli serves in various research communities—AGU, EGU, ASCE and iEMSs—as a reviewer and convener, and sits on the editorial board of Environmental Modelling & Software and the Journal of Water Resources Planning and Management. For this service, he received the Outstanding Reviewer Award from Environmental Modelling & Software (2011), the Journal of Water Resources Planning and Management (2015) and the Best Associate Editor Award for the Journal of Water Resources Planning and Management (2018.) At SUTD, Dr. Galelli leads the Resilient Water Systems Group, which develops algorithms and tools for the optimal operation of large-scale water resources systems. For his contribution to research, Dr. Galelli was awarded the Early Career Research Excellence Award (2014) by the international Environmental Modelling & Software society and the SUTD Excellence in Research Award (2017.)

Assoc Prof Arlindo SILVA

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

Arlindo has a PhD in Mechanical Engineering and more than 25 years of teaching and research experience. His current research interests rest on engineering

design, product development, creativity, materials selection methodologies, additive manufacturing in composite structures, cost modelling and management of uncertainty in design. He has published over a hundred and twenty papers in journals, conferences and book chapters, has more than 50 patents and authored/co-edited five books in engineering related topics. He received the MIT-Portugal Education Innovation Award in 2009 and was a Professor of Excellence at the University of Lisbon in 2009, and 2013 to 2015, before joining SUTD as an Associate Professor with the Engineering Product Development Pillar. He was also a Senior Materials Education consultant at Granta Design Ltd, Cambridge, UK, and is an active member of PDMA, ASEE, ASME, ASTM International, INCOSE, DS and SPEE. He is the current National Additive Manufacturing Innovation Cluster Hub Director at SUTD, liaising Singaporean companies with SUTD's expertise in Additive Manufacturing and Composites Technologies through the Digital Manufacturing and Design Center. He teaches Introduction to Design, and develops his research between the SUTD-MIT International Design Center, where he co-leads the Experimental Design Thrust, and DManD. He is also the Program Director for the new Master of Engineering in Innovation by Design at SUTD and a member of the Executive Committee of the Design Business Chamber Singapore.

Assoc Prof Chau YUEN

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

Dr Yuen received his BEng (2000) and PhD degree (2004) from NTU. He is the recipient of Lee Kuan Yew Gold Medal, Institution of Electrical Engineers Book Prize, Institute of Engineering of Singapore Gold Medal, Merck Sharp & Dohme Gold Medal and Hewlett Packard Prize (twice).

Dr Yuen was a Post Doc Fellow in Lucent Technologies Bell Labs, Murray Hill during 2005. He was a Visiting Assistant Professor of Hong Kong Polytechnic University in 2008. During the period of 2006 - 2010, he worked at the Institute for Infocomm Research (I2R, Singapore) as a Senior Research Engineer, where he was involved in an industrial project on developing an 802.11n Wireless LAN system, and participated actively in 3Gpp Long Term Evolution (LTE) and LTE-Advanced (LTE-A) standardization. He joined the Singapore University of Technology and Design as an assistant professor from June 2010, and received IEEE Asia-Pacific Outstanding Young Researcher Award on 2012.

Dr Yuen serves as an Editor for IEEE Transactions on Communications and IEEE Transactions on Vehicular Technology, and was awarded the Top Associate Editor (2009 – 2012). He has filed 5 patents and published over 150 research papers at international journals or conferences.

Prof Jianying ZHOU

Projects: (1) Automated Incident Response and Recovery in ICS; (2) Scalable Hybrid Honeypot Infrastructure for IoT Threat Intelligence and Response

Prof. Jianying Zhou received PhD in Information Security from Royal Holloway, University of London. Before joining SUTD, he was a principal scientist and the head of Infocomm Security Department at the Institute for Infocomm Research, A*STAR. He has also worked at the headquarters of Oracle as a security consultant.

Prof. Zhou's research interests are in applied cryptography and network security, cyber-physical system security, mobile and wireless security. He has published 200+ referred papers at international conferences and journals with 8000+ citations, and received ESORICS'15 best paper award. He has 2 technologies being standardized in ISO/IEC 29192-4 and ISO/IEC 20009-4, respectively.

Prof. Zhou is a co-founder and steering committee co-chair of International Conference on Applied Cryptography and Network Security (ACNS). He is also steering committee chair of ACM AsiaCCS, and steering committee member of Asiacrypt. He has served 200+ times in international cyber security conference committees (ACM CCS & AsiaCCS, IEEE CSF, ESORICS, RAID, ACNS, Asiacrypt, FC, PKC etc.) as general chair, program chair, and PC member. He has

also been in the editorial board of top cyber security journals including IEEE Security & Privacy, IEEE TDSC, IEEE TIFS, Computers & Security.

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

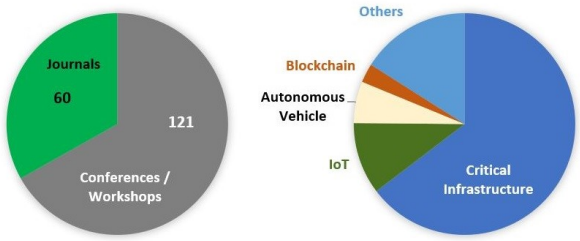

Figure 7: iTrust publications in international journals, conferences & workshops

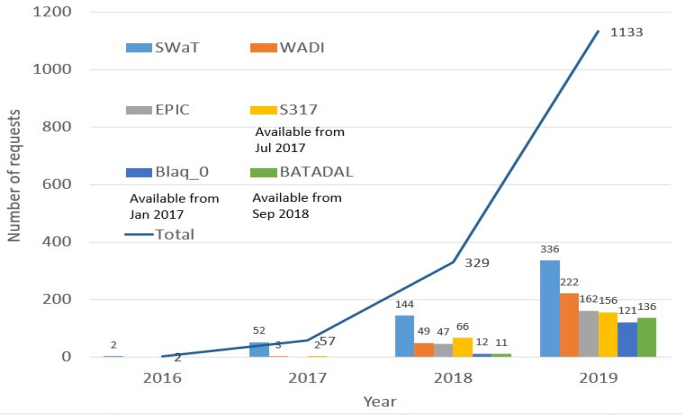

Figure 8: Datasets generated from iTrust testbeds and requested by researchers from around the globe

Figure 9: Visitors to iTrust testbeds (2015 - 2019)

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
Centre for Research in Cyber Security