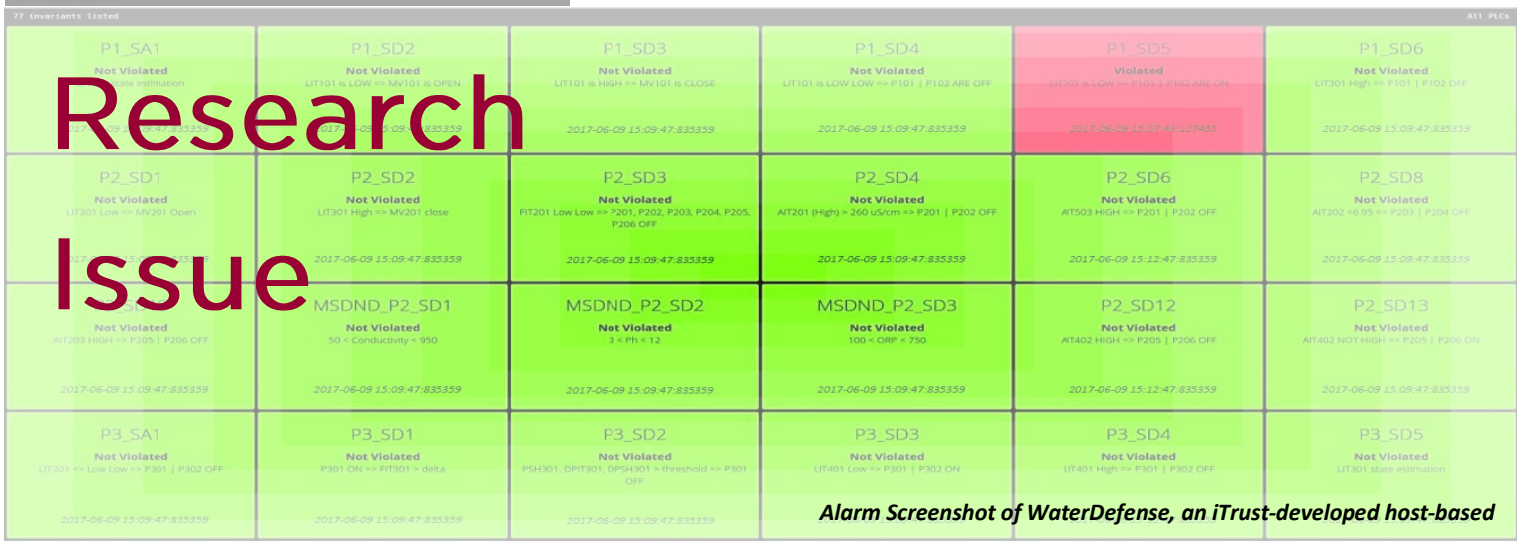
An iTrust Newsletter Oct - Dec 2017 | Issue 11

# iTrust Times

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

## From Centre Director's Desk




***Alarm Screenshot of WaterDefense, an iTrust-developed host-based***

# Research Issue

Dear Reader:

Greetings from iTrust!

Welcome to the 11th issue of iTrust Times! This issue offers a glimpse into iTrust research projects—new and ongoing, our ever expanding international collaborations, and what we do via well designed outreach programmes to realise our commitment to train Singaporeans in cyber security.

In April 2016 iTrust had signed an MoU with Netherlands-based TNO (Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek) for research collaboration. Soon after, iTrust and TNO collaborated on a joint proposal for testing blockchain implementations. This project has now been awarded by the National Research Foundation (NRF) jointly to iTrust and TNO and was launched in October 2017. Follow the link below to read a news article on TNO-iTrust collaboration: https://time.tno.nl/en/articles/blockchain-security-by-design-innovation-and-security-hand-in-hand/

iTrust's progress in using system design to create powerful attack detection mechanisms for Industrial Control Systems led Attila Cybertech to jointly propose a project with iTrust. This project, also funded by the NRF, will focus on using plant designs and machine learning to create high-accuracy and low-false alarm mechanisms for detection process anomalies in industrial plants. The tools developed in this project are aimed for direct use in securing large and complex Industrial Control Systems.

A number of visitors from Singapore and other countries continue to visit iTrust. iTrust staff and researchers have again showed their talents in designing and implementing training programmes in cyber security.

That's all for now folks! Thanks for browsing this newsletter!

Best wishes,

Aditya Mathur
Professor and Head of Information Systems Technology and Design Pillar, and
Centre Director, iTrust

**In This Issue**

# Research Focus

## New Projects

The National Research Foundation (NRF) held its second **National Cybersecurity R&D Grant Call** in Nov 2016, targeting submissions from the industry with research proposals that improve cyber tools and capabilities for the cybersecurity needs of Public Service and Singapore. iTrust and its industry collaborators responded to the grant call. Two projects were approved by NRF on 30 June 2017. Funding agencies for industry collaborators are EDB in "Testing for Blockchain Security by Design", and IMDA in "Advanced-Intelligent Anomaly Detection System".

### Testing for Blockchain Security by Design

*Industry collaborator: TNO South East Asia*
*Project PI and Co-PIs: Prof Aditya Mathur, Asst Profs Georgios Piliouras and Pawel Szalachowski*

BLOCKTEST

Blockchain technology is widely viewed as an emergent, breakthrough and disruptive technology. Spanning over two years, the project aims to achieve the objectives of (i) developing a security reference architecture for blockchain to identify components in the design that require security controls to be implemented; and (ii) creating capabilities and tools to enable testing for Security by Design of Blockchain. This two-year project also marks the first joint R&D project collaboration under the SUTD-TNO Memorandum of Understanding that was signed by both parties in April 2016.

### Advanced-Intelligent Anomaly Detection System

Industry collaborator: Attila Cybertech Pte Ltd
*Project PI: Prof Aditya Mathur*

This project aims to improve the security of cyber-physical systems (CPS) by employing data analytics to derive physical constraints that detect anomalous behaviour in largescale CPS. Over two years, the team will develop methods to continuously access data from multiple sources of a cyber-physical system and develop a machine learning system for anomaly detection. The detection solution developed will be validated in a testbed at SUTD, and likely then deployed in selected plants across Singapore.

A third project, under a **seed grant call by the Singapore Cybersecurity Consortium** to spur the commercialisation of cybersecurity technologies, was also awarded.

### Identification of IoT devices behind NAT while ensuring the preservation of data privacy

*Industry collaborator: Custodio Technologies Pte Ltd*
*Project PI: Prof Yuval Elovici*

This 1-year project aims to develop a method to passively map out Internet of Things (IoT) devices in users' premises while preserving privacy. This will help build a security layer between IoT devices and telecommunications infrastructure to monitor and detect potentially malicious traffic.

## Project Updates

### Autonomous Vehicle Security

*By Giedre Sabaliauskaite, Project Investigator*

Ensuring the safety of autonomous vehicles (AVs), i.e. reducing the number of traffic crashes to prevent injuries and save lives, is a top priority in AV development. The team is investigating relationships between vehicle safety and security, and developing a modelling approach for integrating AV security and safety in compliance with international standards.

This research takes into consideration several international standards: SAE J3016, which describes main terms for AVs; ISO 26262 – road vehicle functional safety standard; SAE J3061 – vehicle cybersecurity guidebook; and NHTSA Automated Driving Systems 2.0 – A Vision for Safety, which proposes an approach for automated vehicle technology safety, among others.

At the heart of the proposed safety and security alignment

approach lies the Six-Step Model (Figure 1), that incorporates six dimensions (hierarchies) of the AVs, namely, (1) functions, (2) structure (components), (3) safety failures, (4) security attack, (5) safety countermeasures, and (6) security countermeasures. The model allows analysis of inter-dependencies across these dimensions, and thus enables comprehensive evaluation of AV safety and security, using AV functions and structure as a knowledge base for understanding the effect of failures and attacks on the vehicle performance.

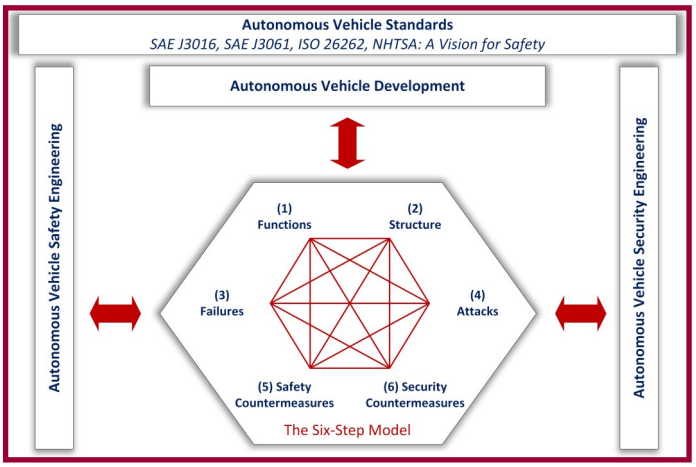



***Figure 1: The Six-Step Model used in integrating AV security and safety in compliance with international standards***

The project team is in the first year of this 3-year project, and is developing an approach at the level of a single-vehicle. Starting next year, it will expand the approach to multi-vehicle level that includes vehicle-to-vehicle communications. Already, the initial results of this work have been accepted for publication in two international conferences: the Second International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2017) in October 2017, and the Future of Information and Communication Conference (FICC 2018) in April 2018.

## Research & Security Innovation Lab for IoT

*By Priscilla Pang, Project Manager*

In the second year of IoT research, the team has made the following progress.

### IoT Scanner

The IoTScanner is aimed at identifying and characterising IoT devices by analysing encrypted MAC layer traffic by passively sniffing them from its vicinity. The framework for such a device type classifier is shown in Fig. 3.

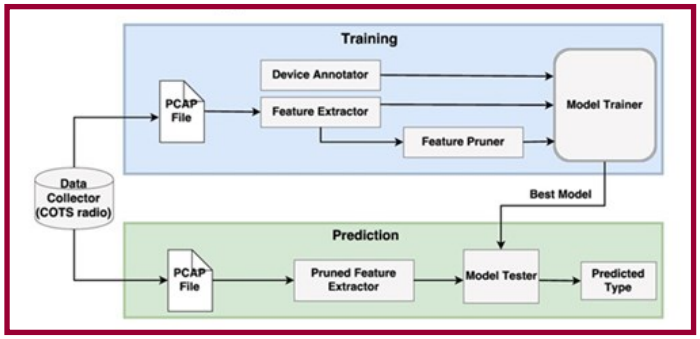



***Figure 3: IoTScanner – Framework for Device Type Classifier***

The team has worked in two directions: First, discovering network structures with (directional) links with an overall traffic statistics and displaying them in a dynamic graphical view. Second, classifying the IoT devices types, (e.g. cameras, smartphones, and smart speakers) based on their MAC layer traffic patterns regardless of their manufacturers and firmware versions.

The IoTScanner can sniff packets from WiFi, Bluetooth Low Energy, and Zigbee enabled devices and form the network structures. It has built up a machine learning based system to discover IoT device types in known and unknown environments. A provisional patent has been filed for the IoTScanner system.

### IoT Security Analysis Testbed

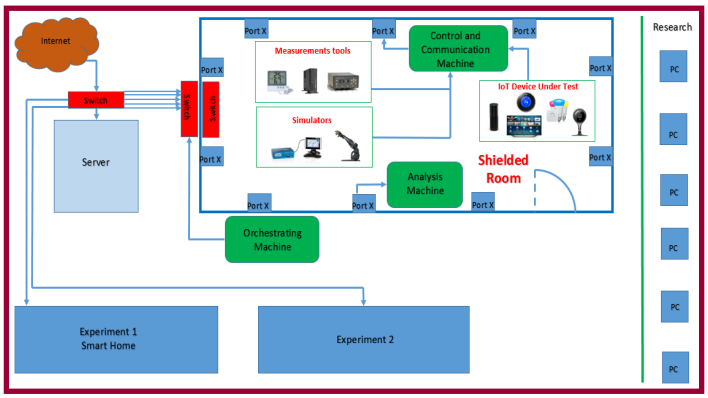



***Figure 4: Physical design of the IoT Security Analysis Testbed***

The IoT testbed (Figure 4 above) has been extended with

new tests and capabilities. It is now capable of evaluating the resilience of IoT devices under testing against DoS attacks and performing static analysis of the firmware. Develop-ment of a privacy valuation capability is ongoing. The team has also worked on various fuzzing techniques for finding unknown vulnerabilities in IoT under test.

## Conference Presentations

**Asst Prof Roland Bouffanais** and iTrust postdoc researcher **Dr Carlos Murguia** presented at the **20th World Congress of the International Federation of Automatic Control**, in Toulouse, France in July 2017.

**Roland's group** looked at the problem of a network of processors aiming at cooperatively solving linear programming problems subject to uncertainty, arising from sensor data, which are noisy and spoofable under some forms of attacks. In their theoretical framework, each node only knows a common cost function and its local uncertain constraint set. **"Randomised Constraints Consensus for Distributed Robust Linear Programming"** proposes a randomised, distributed algorithm working under time-varying, asynchronous, and directed communication topology.

The algorithm is based on a local computation and communication paradigm, which makes its application range extremely wide especially with future architectures, which tend to be more decentralised by design. At each communication round, nodes perform two updates: (i) a verification in which they check—in a randomised setup—the robust feasibility (and hence optimality) of the candidate point; and (ii) an optimisation step in which they exchange their candidate bases (minimal sets of active constraints) with neighbours and locally solve an optimisation problem whose constraint set includes a sampled constraint violating the candidate optimal point (if it exists), agent's current basis, and the collection of neighbour's basis.

The researchers showed that if a processor successfully performs the verification step for a sufficient number of communication rounds, it can stop the algorithm since consensus has been reached (Figure 5). The common solution is—with high confidence—feasible (and hence optimal) for the entire set of uncertainties except a subset having arbitrary small probability measure. They also demonstrated the effectiveness of the proposed distributed algorithm on a multi-core platform in which the nodes communicate asynchronously. This work has far-reaching implications for a wide range of decentralised networked control systems, in particular for CPS security.

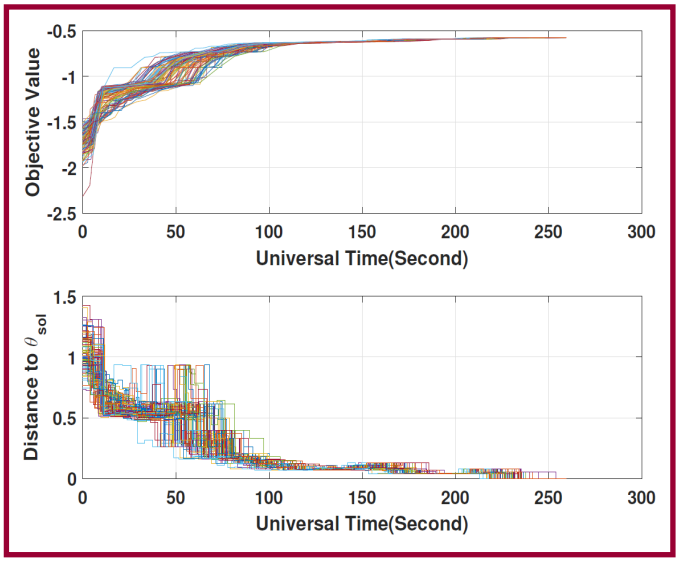



***Figure 5: The objective value and the distance of candidate solutions from the solution $\theta_{sol}$ along the distributed algorithm execution for a problem instance corresponding to a network with 100 nodes, with each node subjected to 100 constraints***

**Carlos Murguia's** research aims to address the problem of characterising the impact of sensor attacks on physical processes modelled by Linear Time-Invariant (LTI) stochastic difference equations when fault detection techniques are deployed for attack detection. The complete fault detection scheme comprises the estimator (to suggest a fault or an attack when the difference between measurements and the estimation is larger than expected), and a change detection procedure (to decide whether the estimator and the system are sufficiently different to declare the presence of faults/attacks). Carlos' group uses dynamic observers as estimators and the chi-squared procedure for change detection.

Carlos' work on **"Reachable Sets of Hidden CPS Sensor Attacks: Analysis and Synthesis Tools"** is a set of mathematical tools for quantifying and minimising the impact of sensor attacks on the process dynamics. To capture these attacks (where, when, and how), Carlos modelled the attacks as additive perturbations affecting sensors measurements and propagated to the system dynamics through output-based controllers. To quantify the effect of attacks, Carlos proposed using the reachable sets of attacks as a measure of impact.

Hidden attacks, defined as attacks that are able to maintain the alarm rate of the detector equivalent to its attack-free false alarm rate, can be characterised as hidden reachable sets in a system. For a given process dynamics, control structure, and attack detection procedure, the group derived ellipsoidal bounds on the hidden reachable sets using Linear Matrix Inequalities (LMIs). It also provided synthesis tools (as a form of mitigation measure) for minimising the bounds of hidden reachable sets by properly redesigning controllers and detectors (Figure 6).

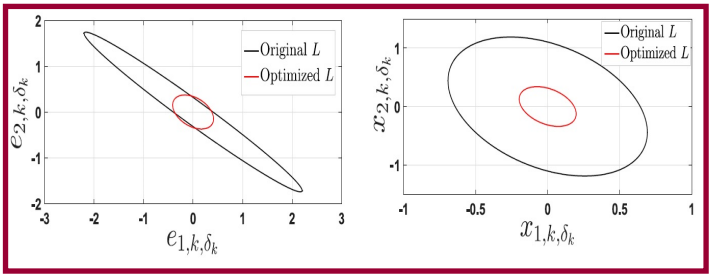



***Figure 6: The improvements in the hidden reachable set ellipsoid bounds $\mathcal{E}_e$ (left) and $\mathcal{E}_x$ (right) through application of synthesis tools to design the optimal observer gain***

Two papers, by iTrust Research Assistant **Rizwan Qadeer** and postdoc researcher **Ragav Sridharan**, were presented at the **European Symposium on Research in Computer Security (ESORICS)** in Oslo, Norway in September 2017.

**"Multistage Downstream Attack Detection in a Cyber Physical System"** presented a detection scheme for attacks on a CPS, by leveraging on the connectivity of a multistage process to detect attacks downstream from the point of attack (Figure 7). The methods form a control

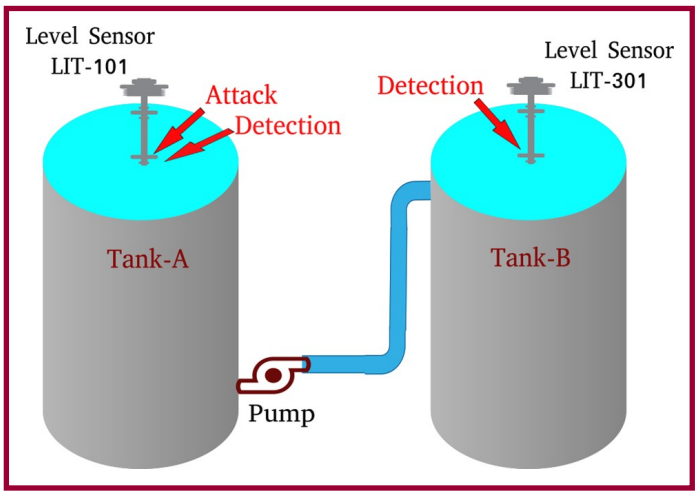



***Figure 7: Leveraging the connectivity of two stages (Tanks A & B) for a multistage attack detection scheme***

theoretic approach to CPS security by characterising SWaT with a mathematical model, obtaining a residual (error) signal from sensor measurements and sensor measurement estimates, and then using Cumulative Sum (CUSUM) and Bad-Data detection methods to detect the presence of a sensor attack. In particular, the attacks are designed to not raise alarms on the detectors in the same stage where the attack takes place, requiring detection to take place on a separate part of the system.

Building on the hypothesis that encrypted linked layer traffic from similar devices (e.g. IP cameras) will have rather similar characteristics irrespective of their manufacturers, and that they will differ from other types of devices (e.g. smart watches), the paper **"Link-Layer Device Type Classification on Encrypted Wireless Traffic with COTS Radios"** presented a framework called PrEDeC (Privacy Evasive Device Classifier). Use of PrEDeC enables an attacker to violate user privacy by using the encrypted link-layer radio traffic to detect device types in a targeted

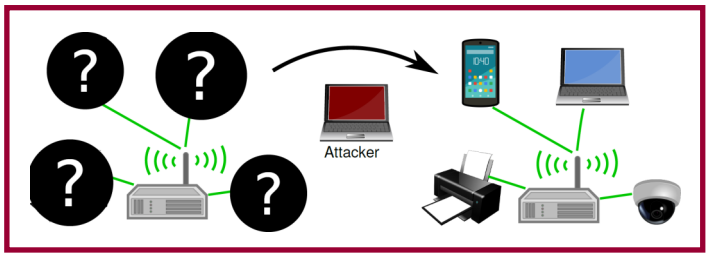



***Figure 8: Attacker passively identifying neighbouring device types via wireless traffic sniffed using COTS radio and pre-trained classifier***

environment (see Figure 8 on previous page). The researchers experimented with 22 IoT devices and classified them into 10 classes based on 76 hours of wireless traffic. While 850 features were extracted for each of the devices present in the traffic for classification via machine learning, the researchers observed that whittling it down to 49 features produced a similar accuracy but with better efficiency. Future work could involve developing defence mechanisms to mitigate such privacy threats.

At the invitation of REDCON Security Advisors, a local cyber security company, iTrust Centre Director Prof **Aditya Mathur** presented at the first **Cyber-Physical Security Symposium (CP2S)** on 4 October 2017. The event, in conjunction with Safety & Security Asia 2017 Expo, was held at Marina Bay Sands. Aditya's presentation **"Challenges in Designing Secure Critical Infrastructure"** summarised iTrust's research progress in exploring approaches based on plant dynamics and machine learning

for detecting coordinated cyber-physical attacks on critical infrastructure (Figure 9). Research problems that stand in the way of realising the dream of a highly resilient critical infrastructure were also highlighted.


***Figure 9: Screenshot of web GUI of an attack detection system based on invariants***

Aditya also presented at the **Public Sector CIO Convex 2017** on 6 October 2017. His presentation **"Can AI Secure Critical Infrastructure?"** explored the use of AI in the design of secure critical infrastructure, in conjunction with a physic-based approach (Figure 10). In light of increasing cyber attacks on critical infrastructure he discussed how AI might be a viable solution for rapid detection and prevention of cyber attacks, and how security can be designed into a system before it is built.

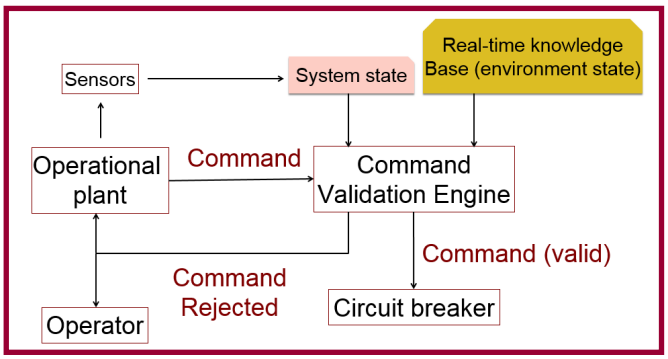
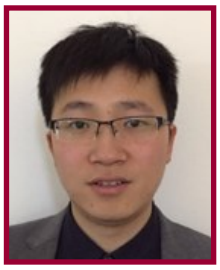



***Figure 10: Incorporating AI into the design of critical infrastructure***

## Visiting Researchers

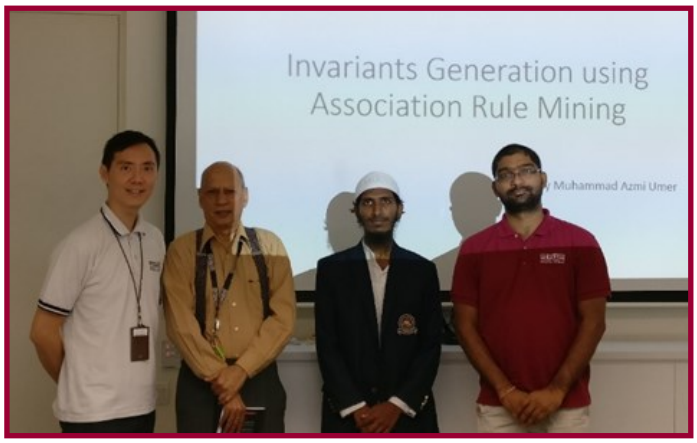
Amidst the hum of computer servers are the occasionally furious hacking sounds on keyboards and lively discussions among a United Nations-esque clique of researchers. At iTrust, we continue to attract a host of research talents from around the globe, and the past few months had been particularly active. Between May to September this year, 11 students passed through the research halls of iTrust. They hail from Erasmus University Rotterdam, Imperial College London, Karachi Institute of Economics and Technology (KIET) and Missouri University of Science and Technology.



***Dr Cheng Feng***

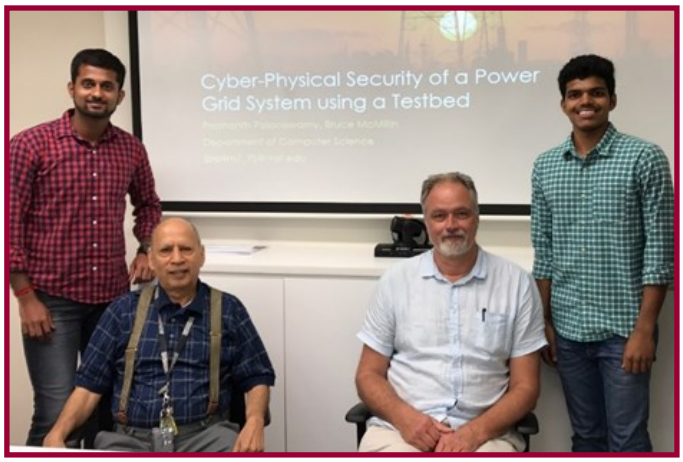
Prior to his visit to iTrust in June, **Dr Cheng Feng (Imperial College London)** had been collaborating with iTrust postdoc Dr Venkat Reddy in the NRF-funded project "Security by Design for Interconnected Critical Infrastructures." As invariant rules are manually written by system engineers during the design phase of an ICS, they can be limited and error-prone. Many invariants also remain undiscovered especially for those that are distributed across several subsystems. Whilst at iTrust, Cheng worked with Venkat to use **machine learning techniques to automatically learn these invariants** from operational data logs to be used as checkers for anomaly detection in ICS.

**Muhammad Azmi Umer**, a PhD student from **Karachi Institute of Economics and Technology**, was with iTrust from 19 June 2017 to 30 Aug 2017. He was tasked to carry out research on process anomaly detection in CPS through the use of machine learning techniques. In particular, Azmi used **Association Rule Mining** – a rule-based machine learning method to uncover relationships between seemingly unrelated data in databases – to generate invariants from a seven-day dataset (invariants are rules that govern that physical and chemical behaviour of the process within a plant.) These invariants, that hold true during a plant's operation, then formed the basis on which process anomaly detection techniques can be developed. Through Azmi's work, a paper – Integrating design and data centric approaches to generate invariants for distributed attack detection – co-authored with SUTD's Aditya Mathur and Sridhar Adepu and Khurum Junejo (KIET) was subsequently submitted for publication.




***(Left to right): Ivan Lee (Senior Associate Director, iTrust), Aditya Mathur (Centre Director, iTrust), Muhammad Azmi Umer and Sridhar Adepu (SUTD PhD student)***

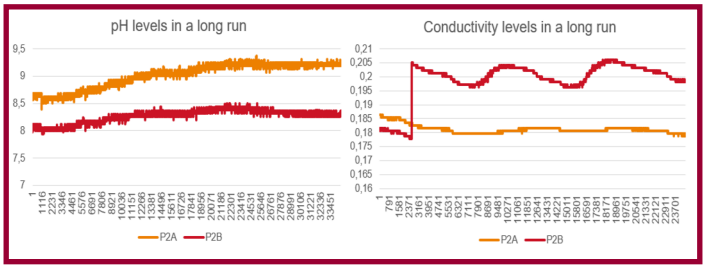
**Prashanth Palaniswamy** and **Sai Sidharth Patlolla**, graduate students of Prof Bruce McMillin – an iTrust collaborator – at **Missouri University of Science and Technology**, sought out research learning opportunities at iTrust. During their time here from June to August, Prashanth and Sai carried out a **Multiple Security Domain Nondeducibility (MSDND)** analysis on the Secure Water Treatment (SWaT) and Electric Power and Intelligent Control (EPIC) testbeds, respectively. They used the MSDND approach developed at Missouri S&T, as a model to determine information flow among multiple domains, such as those in a CPS. If two (or more) security domains are determined to be MSDND-positive (i.e. there is uncertainty as to whether information in one domain is true or false) then the domains are not secure. In applying MSDND on the testbeds, they could then determine which points are vulnerable to cyber attacks and how attacks can be detected and prevented.




***(Left to right): Prashanth Palaniswamy, Bruce Mcmillin and Sai Sidharth Patlolla with Aditya Mathur***

**Casper de Winter's (Erasmus University Rotterdam)** research focused on sensor placement in water distribution networks, and to quantify the effect of unreliable sensors on the probability of detecting a water contamination. Casper started with the assumption that sensors are not perfect, in part due to sensor degradation, measurement/communication errors, and cyber attacks. He performed several experiments on the Water Distribution (WADI) testbed at iTrust to test out this assumption.

**Comparing performance of sensors:** Two sensors P2A and P2B, located in close proximity, measured four water parameters: conductivity, turbidity, pH and oxidation reduction potential (ORP). Experiment runs showed that the time series of the pH (see Figure 11 next page, left) and ORP were highly correlated, but not for conductivity (see Figure 11 next page, right) and turbidity, with multiple inexplicable jumps in readings detected. There were also several missing values in the data.




***Comparison between sensors P2A's and P2B's performance in measuring pH (left) and conductivity (right) levels in WADI***

**Comparing sensor performance using standard solutions:** The performance of four sensors were also evaluated by standard solutions (used for sensor calibration) for these same four parameters. From the sixteen measurements (four sensors times four parameters), six were well off within two months, faster than the prescribed calibration frequency of 3 to 6 months. This rapid drifting showed that the sensors (and thus sensor values) were not always reliable.

The above two observations offer the evidence of imperfect sensors with the implication that a potential water contamination might escape detection.

***Casper (far right) with (from left) Ivan, Aditya and iTrust postdoctoral researcher Venkat Reddy***

iTrust also grooms local students in cyber security to help close the cyber human resource gap. In the past, polytechnic and post-junior college students had interned at iTrust. From April to September this year, four students from the **Institute of Technical Education College East** did their industrial attachment at iTrust. The students – **Alstin Lau, Soo Wei Lun, Abdul Razak, and Hein Htet San** – are pursuing their Higher National ITE Certificate (Higher Nitec) in Cyber and Network Security, and hoped to gain relevant industrial experience during these six months.

Even without any background in computer programming, the students impressed their supervisors by learning to code in Python for their assignments. On top of Python, Razak and Htet San got their feet wet with InfluxDB and messaging protocols MQTT and ZeroMQ to **extract and store data of application and system parameters** (such as CPU and RAM usage). By obtaining a baseline of these parameters and setting thresholds, they could **monitor and detect anomalies that occur during data collection** such as unusually high traffic. Alstin and Wei Lun worked on an online portal where an IoT device owner could **upload the device's captured network traffic via cloud for security analysis.** To do that, they also had to familiarise themselves with Web Server Gateway Interface (WSGI) and GUnicorn. The files would then be analysed backend for detecting anomalies using machine learning (this portion of the work was managed by IoT post-doc researchers).

***ITE College East students (with third from left) Alstin Lau, Soo Wei Lun, Abdul Razak, and Hein Htet San, with (from left) Ivan, ITE teacher-on-charge Cheong Kit Hong, and (far right) iTrust senior specialist Kaung Myat Aung***

## iTrust Seminar Series

Three experts, Prof Ian Hayes (University of Queensland), Dr Yuan-Fang Li (Monash University), and Debdeep Mukhopadhyay (IIT-Kharagpur), gave seminar talks in

September and October.

*Ian Hayes*

In **"Synchronous Concurrent Refinement Algebra and Fairness"** Ian discussed a synchronous refinement algebra that his group developed to support reasoning about concurrent programs in a rely/guarantee style. The algebra is based on a general refinement algebra, into which are embedded sub-algebras of instantaneous tests and primitive atomic steps. The synchronous parallel operator executes by synchronising one atomic step at a time. The use of synchronous operators affords a straightforward encoding of fairness assumptions on the interaction of a process with its environment. This would allow the fair execution of a single process, fair termination and fair parallel.

*Yuan-Fang Li*

Multi-core processors have become the dominant computing platform in recent years. In the concurrency by default programming paradigm, permission-based dependencies have been investigated as an alternative approach to enabling automated parallelisation and avoiding errors that may arise when concurrency constructs are manually added, a common practice in mainstream languages such as Java. However, significant annotation overhead is required for such languages, thus diminishing their effectiveness. In his talk **"Extract Access Permissions from Java Programs"**, Yuan-Fang discussed his ongoing work on automatically extracting implicit dependencies from a sequential Java program in the form of emph{access permission rights}, by performing modular (inter-procedural) static analysis of the source program. This would in turn free programmers from the specification overhead that implicit concurrent approaches pose, hence facilitating the wider adoption of the concurrency by default paradigm.

With the advent of Internet of Things (IoT) the need and challenges of security have increased manifold. From the miniature devices, that are often resource constrained, to the pervasive omni-present cloud, all avenues for a potential attack need to be mitigated. In **"Break One Link and the Whole Chain Falls Apart!: Embedding Security in Things to Cloud"** Debdeep discussed the research activities at the Secured Embedded Architecture Laboratory (SEAL) in this direction, starting from physical security of the "things" in an IoT framework to developing dedicated cryptographic techniques for delegating data in the cloud. He also discussed on Key Aggregate Cryptosystems (KAC), which provides an efficient solution to allow users to decrypt multiple classes of data using a single key of constant size that can be broadcast to multiple users. SEAL attempts to develop parallel hardware architectures for such access mechanisms, and extend it to handle functionalities, like search in a controlled manner, over encrypted data generated by billions of devices in the IoT.

*Debdeep Mukhopadhyay*

## Outreach

**"Education is not the filling of a pail but the lighting of a fire."**

**William Butler Yeats, Irish poet and Nobel Prize winner in Literature**

Insofar that iTrust's outreach activities to schools is to raise awareness of and educate the next generation of leaders in cyber security, it is also about igniting their passion in this field. iTrust's focus on applied research also means that its outreach workshops go beyond a top-down transfer of knowledge and ideas, fusing them with hands-on activities and demonstrations to cement the learning process.

## Innova Junior College

iTrust was invited to **Innova Junior College's (IJC) Young**

**Tech Maker Fest 2017.** The Fest is an initiative to develop digital innovation literacies among youths with the aim of nurturing the next generation of technopreneurs.

iTrust ran a 3-hour introductory workshop on cybersecurity for students aged 15 to 18. To start off everyone on the same page, research officers Francisco **Furtado and Lauren Goh** walked through the fundamentals of networking and how a computer transmits data across the Internet and intranet, and how attackers can exploit vulnerabilities to their benefit. Common attacks favoured by cyber attackers were discussed: denial of service (DOS), password cracking, and disrupting Wi-Fi networks.

***IJC students learning to secure Singapore's future***

While participants got to try their hands in performing some of these attacks, Francisco and Lauren were quick to point out they were working in an experimental and controlled environment, and impressed upon the students the ethics of hacking.

The second half of the workshop focused on security and protection against cyber attacks, at an individual and systems level. The tools of encryption and hashing were introduced as methods that individuals could use to strengthen their protection against identity thefts. Differences between encryption (message security) and hashing (message integrity) were also explained. Next, Francisco and Lauren introduced iTrust's testbeds to showcase the work researchers were doing to secure and build resilience into Singapore's critical infrastructure.

## CHIJ St Nicholas' Girls School

*By Francisco Furtado*

On 25 August 2017, iTrust was invited to speak, for the third year running, on cybersecurity at **the Joint Integrated Programme (IP) World Readiness Programme (WRP) Symposium**. This Symposium was organised by CHIJ St Nicholas Girls' School (CHIJ SNGS) for about 150 Secondary One Joint IP students from **CHIJ SNGS, Catholic High School, and Singapore Chinese Girls' School**. The WRP prepares Joint IP students with the knowledge and skills to become well-informed and responsible global citizens.

This year, Ivan Lee, iTrust's Deputy Director for Cyber Security Technologies, led the Symposium to foster awareness of cybercrime and cybersecurity. Together with the help of Research Officers Lauren Goh and Francisco Furtado, Ivan's talk focused on the impact of cybersecurity on individuals, organisations and society, and the next generation of cybercrimes and the ongoing efforts to keep these attacks at bay.

To bring home the message of how real these threats were, Ivan's team of researchers demonstrated the use of a drone to conduct reconnaissance of wireless network devices, the freezing of IP cameras used for monitoring, and a 3D-printed drone. At a malware level, a live demonstration of a ransomware, programmed by Aaron Tan, a recent 'A' Level graduate, was shown. The interactive demonstrations meant that many students could participate and understand the issues discussed first hand.

The second part of the talk focused on the nature of social engineering and the social elements of trust, greed, fear and ignorance that allow humans to fall victim to such attacks as phishing and ransomware. Ivan raised the importance of being vigilant in revealing sensitive

information such as passwords even to so-called 'trusted' service providers.

The Symposium ended with a debate on Net Neutrality. Ivan facilitated a lively conversation among the students on an open versus a throttled Internet, pitting one half of the hall as Internet Service Providers (ISPs) against the other half of Internet giants (Google, Apple, etc) case. The students gave very interesting viewpoints by considering the challenges and motives of both parties, such as economic gains versus social good.

*Ivan (center) picking the minds of the next generation of leaders at a debate*

## Ministry of Education

Recognising the important role that educators play in shaping the minds of the future, iTrust also organised an introductory session on 27 July to a group of 12 Social Studies teachers, as cyber security forms a part of their syllabus. Topics ranged from ransomware to encryption and social engineering. The teachers were also given a tour of iTrust testbeds to understand the work done behind the scenes to keep our society safe.

*MOE teachers with trainers (back row, third from left) Research Officers Lauren Goh and Francisco Furtado*

## Visits

As the Chief of the Technology Branch at the **NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE), Mr Raimo Peterson** is naturally drawn to cutting edge technologies in cyber defence. He was invited to visit iTrust by the Ministry of Defence (MINDEF), Singapore, and along with MINDEF on 28 August, was joined by a delegation from DSO National Laboratories (DSO) and the Defence Science and Technology Agency (DSTA).

*(In foreground) iTrust Research Director Prof Yuval Elovici explaining iTrust's IoT research to NATO CCD COE Mr Raimo Peterson*

A month later, the NRF invited **Dr. Douglas Maughan** to visit iTrust. Douglas is the division director of the Cyber Security Division in the Homeland Security Advanced Research Projects Agency (HSARPA) within the Science and Technology Directorate (S&T) of the **US Department of Homeland Security (DHS).** Douglas is no stranger to iTrust, having visited iTrust in May 2016. Centre Director Prof Aditya Mathur welcomed Douglas with updates on research projects, and a demonstration of a variety of attack detection techniques that iTrust had developed. He was also given a tour of the Electric Power & Intelligent Control testbed (which at the time of his last visit was still in construction).

iTrust also hosted PUB Chairman Mr Chiang Chie Foo on 24 October. Being a close collaborator of iTrust, it was timely to update PUB on iTrust's research efforts—attack models

and defence mechanisms – and how these could translate into potentially useful technologies for PUB's plants. To illustrate this, Mr Chiang was shown several attack and detection demonstrations.

***iTrust Centre Director Prof Aditya Mathur explaining the attack and detection demonstration to PUB Chairman Mr Chiang Chie Foo (first from left)***

# iTrust Matters

## Research Openings

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

1) **Post-doctorate/Research Fellow** in the following projects:
   a. Advancing Security of Public Infrastructure using Resilience and Economics
   b. Advanced-Intelligent Anomaly Detection System
   c. BCS-T: Testing for Block Chain Security by Design
   d. Research & Security Innovation Lab for IoT
2) **Research Assistant** in the following projects:
   a. Advancing Security of Public Infrastructure using Resilience and Economics
   b. Advanced-Intelligent Anomaly Detection System
   c. Research & Security Innovation Lab for IoT

For detailed job description and requirements, please visit http://tinyurl.com/jh6uxlw.

## iTrust Contact Information

Please feel free to contact the relevant iTrust staff listed below to explore research collaborations and outreach activities:


**Mr Kaung Myat AUNG,** *Senior Specialist (Water)*
kaungmyat_aung@sutd.edu.sg

**Prof. Yuval ELOVICI,** *iTrust Research Director*
yuval_elovici@sutd.edu.sg

**Mr Mark GOH,** *Manager, iTrust*
mark_goh@sutd.edu.sg

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

**Prof. Aditya P MATHUR,** *Professor & Head of Pillar, ISTD Pillar & iTrust Centre Director*
aditya_mathur@sutd.edu.sg

**MUHAMED Zhaffi Bin Mohamed Ibrahim,** *Specialist (Power)*
zhaffi_ibrahim@sutd.edu.sg

**Ms Angie NG**
*Deputy Manager, iTrust*
angie_ng@sutd.edu.sg

**Ms Priscilla PANG**
*Manager, iTrust*
priscilla_pang@sutd.edu.sg

**Prof. Jianying Zhou,** *Professor & iTrust Associate Centre Director*
jianying_zhou@sutd.edu.sg