An iTrust Newsletter

Apr – Jun | Issue 5

iTrust Times

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT

From Centre Director's Desk

SUTD-TNO MOU signing ceremony with SUTD Provost Prof Chong Tow Chong (fourth from left) and Managing Director of Defence, Safety and Security, TNO Mr Henk Geveke (fifth from left) as signatories. Deputy Ambassador from Embassy of the Kingdom of the Netherlands, Mr Hans Akerboom (second from right), was also present at the ceremony

Dear Reader:

Greetings from iTrust, and welcome to this fifth issue of iTrust Times. I am happy to note that this is the first anniversary of our newsletter! Thank you, Mark!

National Research Foundation, ST Electronics, and SUTD have partnered to set up the ST Electronics-SUTD Cyber Security Laboratory. The Corp Lab will be directed by Professor Yuval Elovici with support from SUTD faculty. This significant research effort is aimed at creating usable technology directed at the design of secure IoT devices and complex Cyber Physical Systems.

Through the efforts of iTrust faculty and staff, SUTD and TNO recently signed an MoU for research cooperation. The MoU will facilitate creation of new joint projects in cyber security between iTrust and TNO, and university partners including TU Delft, TU Eindhoven, and TU Twente. This experience, coupled with the young and aspiring faculty in iTrust and our world class testbeds, promises an intellectually rich research partnership.

This partnership is already blossoming. iTrust, in collaboration with TNO, recently conducted two week-long workshops in Darknets and Crypto Currencies. Professor Pieter Hartel from TU Twente was the key organiser and conductor of these workshops. He was supported by TNO researchers Mark van Staalduinen, Rolf van Wegberg, and Esra van Beelen. The workshops were well received. The ever exciting Second SCy-Phy Systems Week is scheduled for the week of July 25 at iTrust. A unique feature of this week is the SWaT Security Showdown (S3), where selected international attack and defence teams engage in attacking and defending a 5-gallons/min, 6-stage water treatment plant. S3 will assist iTrust researchers in assessing their attack detection and control mechanisms.

As I always say, and mean, iTrust is a welcoming and friendly research centre. Let us know if you are interested in participating in this exciting journey towards highly resilient CPS.

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

In This Issue

SUTD-TNO MoU

Cyber attacks transcend geographical boundaries. An attacker can launch an attack from Country A using a command and control server physically located in Country B. The server in turn controls botnets located in several countries to simultaneously carry out the attack in Country C.

In light of such cyber risks and threats, research and innovation in cyber security and resilience received an international boost with a new collaboration between the SUTD and The Netherlands Organisation for Applied Scientific Research (TNO). The collaboration was formalised in a Memorandum of Understanding (MoU) signed between the two institutions on 31 Mar 2016.

Through this partnership, both parties look forward to strengthening current and future research initiatives as well as harnessing one another's research strengths in the different domains of cyber security, such as Cyber Physical Systems, the Internet of Things (IoT), Block Chain Security, Dark Web Training and Cybercrime. This will take the form of student, researcher and staff exchanges between the SUTD and TNO. Furthermore, this collaboration aims to enhance Singapore's and the Netherlands' knowledge and expertise in cyber physical system security.

(Left to right): Prof Aditya Mathur (iTrust Centre Director), Prof Chong Tow Chong (SUTD Provost), Mr Henk Geveke (TNO's Managing Director of Defence, Safety and Security) and Mrs Annemarie Zielstra (TNO's Director of Cyber Security and Resilience)

The three-year MoU was signed by SUTD's provost Professor Chong Tow Chong and TNO's Managing Director of Defence, Safety and Security, Mr Henk Geveke, and was witnessed by Deputy Ambassador from Embassy of the Kingdom of the Netherlands, Mr Hans Akerboom, SUTD's iTrust Centre Director, Professor Aditya Mathur and TNO's Director of Cyber Security and Resilience, Mrs Annemarie Zielstra.

SUTD's provost, Professor Chong Tow Chong, noted: "SUTD seeks to better the world through technology and design – a very appropriate mission for today as the world becomes more technologically advanced. However, due to the increasing dependency on technology, the accompanying rise in cyber attacks on critical infrastructures is inevitable. With the growing importance of cyber security, SUTD's collaboration with TNO is timely. The exchange of our students and researchers with TNO will greatly benefit us as it will allow us to share and learn best practices from one another as well as advance our knowledge in the area of cyber security and resilience."

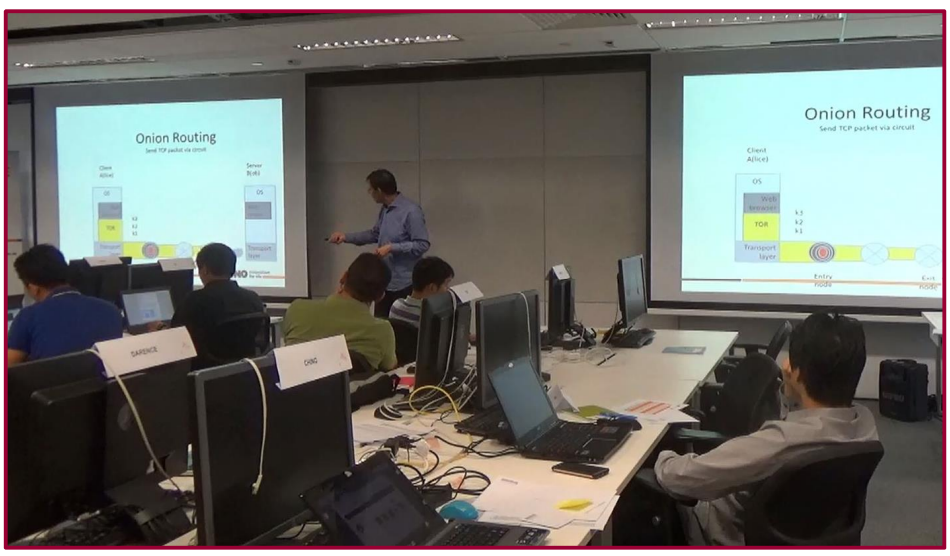
Managing Director of Defence, Safety and Security, Mr Henk Geveke, added: "At TNO, we welcome this collaboration with great pleasure. We look forward to sharing our scientific research on darknets, virtual currencies and underground markets internationally, and to continually strengthen the enforcement of cybercrime across the globe. Joining forces with SUTD and their testbed environment will allow TNO to experiment with criminal strategies in a controlled setting, which will enable us to study the design of cybercrime to a fuller extent."

Advanced Course on Darknets and Virtual Currencies

The first fruitful collaboration between SUTD and TNO was the Advanced Course on Darknets and Virtual Currencies. Conducted over two five-day sessions in Apr 2016, the course was provided by iTrust in collaboration with TNO. It was led by Prof Pieter Hartel (University of Twente), with Dr Mark van Staalduinen (TNO's Senior Research

Scientist), Dr Rolf van Wegberg (TNO Researcher), and Ms Esra van Beelen (TNO Game Designer). The course objective was to help jump-start participants' capabilities in Darknet and Bitcoin related research and applications and keep them up-to-date on the latest technologies and research findings in this area.

A Dark Market is an online market trading goods andservices that may be illegal in some jurisdictions. Such markets (one of the most infamous is Silk Road) are typically located on an anonymity network – commonly known as Dark Web or Darknet – and accessed via the Tor browser, also known as "the onion browser". A virtual currency is defined by the European Central Bank as "a type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community." Of the virtual currencies in the market today, Bitcoin is by far the largest in market capitalisation and price.



Prof Pieter Hartel conducting one of the course sessions

The course covered a wide range of topics, from Anonymisation Networks, Criminal Business Models, Cryptocurrencies, Trading on Dark Web and Forensics. The course conductors used simple activities to explain concepts such as how the Tor browser worked. Dr Staalduinen demonstrated the effectiveness of wisdom of the crowd by asking participants to look into the different factors of how the masterminds behind Silk Road and Silk Road 2.0 were apprehended. A training game designed by Ms Beelen also provided participants with a simulated trading environment so they could learn how a Dark Market and its users operate and how to police such markets. Guest speaker Mr Roeland van Zeijst, a Digital Crime Officer at the INTERPOL Global Complex for Innovation, was also there to speak on the legal and law enforcement aspects surrounding such activities.

Opening of the ST Electronics-SUTD Cyber Security Laboratory

On 13 May 2016, Singapore Technologies Electronics Limited (ST Electronics) and SUTD announced the set-up of the ST Electronics-SUTD Cyber Security Laboratory. The joint laboratory was officially launched by Dr Yaacob Ibrahim, Minister for Communications and Information and Minister-in-charge of Cyber Security at the signing ceremony held at SUTD. The S$44.3m joint laboratory is supported by the National Research Foundation (NRF) under its Corporate Laboratory@University Scheme, and is the first corporate laboratory under this scheme to focus on cyber security.

Signing between ST Electronics' Deputy CEO & President, Defence Business Mr Lee Fook Sun (left) and SUTD Provost Prof Chong Tow Chong (right) and witnessed by Minister for Communications and Information and Minister-in-charge of Cyber Security Dr Yaacob Ibrahim

The laboratory aims to advance new frontiers in cyber security technologies and build next generation solutions and products to address today's and future cyber security challenges. As a research centre for cyber security it will leverage on ST Electronics' in-depth cyber security expertise and industry knowledge together with SUTD's academic know-how and multi-disciplinary effort in R&D. It will identify current and future cyber solutions required by the industry, develop cutting-edge technologies, provide proof of concepts and testbeds for the next generation of cyber security products and solutions.

The collaboration also aims to build indigenous capabilities in cyber security in Singapore by creating a platform for professors and students to conduct R&D, providing future career opportunities in this niche area of specialty, and increasing the cyber security talent pool and professionals required to support Singapore's Smart Nation Initiative.

“The ST Electronics-SUTD Cyber Security Laboratory brings together Singapore’s expert cyber security capabilities under one roof. We have a shared vision of accelerating the pace of development of innovative indigenous technologies that have cross-sector applications which address current as well as future cyber security challenges,” said Mr Lee Fook Sun, Deputy CEO & President, Defence Business of ST Engineering and President of ST Electronics.

“SUTD’s collaboration with ST Electronics comes at an opportune time, as cyber security challenges become increasingly sophisticated. The joint corporate laboratory will not only enable us to testbed diverse cyber attacks in ‘real world’ environments and design innovative cyber security solutions, but also provide relevant training that will boost Singapore’s pool of cyber security talents – a multi-pronged approach to boost our society’s cyber security capabilities through design, technology and education,” said Professor Thomas Magnanti, President, SUTD.

For a start, the main R&D areas of the joint laboratory will include three innovation areas:

- Cyber security big-data analytics;
- Trusted monitoring and mitigating techniques; and
- Detecting malicious and deceived insiders in an organisation.

With the new laboratory, ST Electronics is able to bring both its cyber security expertise and in-depth domain knowledge in (a) design, development and commercialisation of advanced cyber security products; (b) design, build and operate Cyber Security Operations Centres with collected use cases and research data for testbeds; and (c) security solution integration and services.

SUTD will contribute its strong academic R&D and technology exploitation experiences and expertise in cyber security and CPS testbeds. The University has developed a rich research programme in applied cyber security with a strong focus on the design of secure and safe public infrastructure, and IoT. This is timely as Singapore moves towards becoming one of the world’s smartest cities. Through the intense collaboration between faculty and research staff, both SUTD and ST Electronics would stand to benefit from this vibrant research programme.

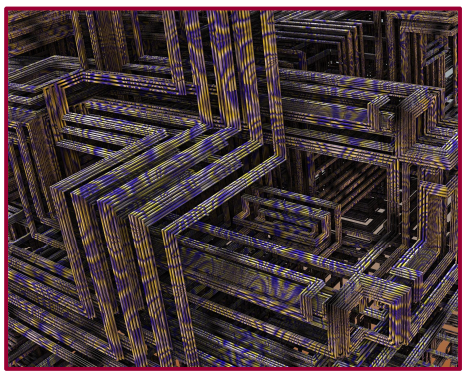
The joint laboratory is located at the new state-of-the-art SUTD campus at Changi, occupying 400 square metre of research and office space. At full-capacity, the lab will have around 60 cyber security researchers from SUTD and ST Electronics.

The Corporate Laboratory@University Scheme seeks to strengthen Singapore’s innovation system by encouraging public-private research and development collaboration between universities and companies. It also ensures that universities achieve impact by developing cutting edge solutions for problems faced by the industries. The collaboration creates employment opportunities and trains a pool of industry-ready research manpower for the industries.

Research Focus

New Research Projects

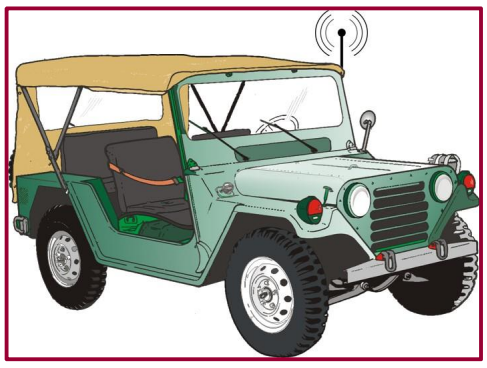
iTrust was awarded funding for two research projects, bringing the total number of projects in iTrust to eight since its inception in Feb 2013.



The first is **“Security by Design for Interconnected Critical Infrastructures”,** in collaboration with Imperial College London. The project aims to advance the state of the art in the design of secure interconnected public infrastructures such as power generation and water treatment plants. Its novelty is the application of security-by-design on interconnected public infrastructures.

Researchers will look into how best to model the system dependencies among components within an infrastructure and across several of them. They will also focus on impact analysis to determine the response of these systems to cyber attacks. To do that, an attack model – to model physical attacks as well as attacks on the PLC e.g. through malware injection – is required. With the system and attack models, the team will develop algorithms for conducting impact analysis at different levels. Finally, the methodology and the tools developed in this

project will be assessed for their effectiveness and practical utility through jointly designed experiments by both research centres and conducted on the power and water testbeds at iTrust.



The second is joint project with the Nanyang Technological University (NTU) that aims at developing novel approaches for assuring **security in autonomous vehicles (AVs)**. The project has four tasks, of which iTrust will focus on developing a modelling approach for aligning AV safety and security in compliance with international AV standards.

The research work is led by Dr Giedre Sabaliauskaite, and supported by two post-docs. The main research challenge the team will address is developing safe and secure autonomous vehicles, which will be able to withstand not only accidental failures, but also malicious cyber-attacks, while providing required functions and performance. This can be achieved only by integrating inter-related dimensions of autonomous vehicles, such as AV standards, functions, safety and security among others.

The team will develop a modelling approach for aligning AVs' safety and security, which integrates these dimensions at a single vehicle (system) as well as the multiple vehicle (system-of-systems) levels. Furthermore, to facilitate the use of modelling approach in practice, a supporting software toolkit will be developed. Finally, the research teams of iTrust and NTU will integrate their results and implement them on the NTU AV's platform.

Research Updates

Research & Security Innovation Lab for IoT

By Yuval Elovici

One of the project's first objectives is to design and build an automatic security testbed for IoT devices. The testbed, now fully operational (pictured), supports executing security tests such as penetration testing and detecting compromised IoTs that perform malicious activity within a specific context (e.g. time, location) or devices that are vulnerable to specific sensor signals. Simulators in the testbed will realistically simulate environmental conditions such as indoor and outdoor, static and dynamic environments, and mobile scenarios. The testbed realistically generates arbitrary real-time stimulations for sensors of the tested devices, including location signals and motion. Researchers can then perform data forensic analysis on data extracted from the tested devices.

One of the use cases identified for the project is Smart Wearables. Researchers will test a wearable IoT device's security against a set of security requirements and its behaviour in different user contexts, and thus determine if the device is compromised. By simulating environmental conditions (e.g. location, light, movement) in which the wearable operates, researchers can identify and detect possible context-based attacks that may be executed. Approaches to mitigate the threats posed by such devices can then follow.

The research team posing in front of the IoT testbed (left to right): Kandasamy Murugandadam (IoT lab engineer), Suman Sankar Bhunia (RA), Vinay Sachidananda (RF), Priscilla Pang (Project Manager), Nils Tippenhauer (Co-PI, SUTD), Yuval Elovici (iTrust Research Director and PI), Shachar Siboni (PhD Student, BGU), Asaf Shabtai (Collaborator, BGU), Chandra Sekar (RA), Toh Jing Hui (RA), Mohannad Alhanahnah (RA) and joined by Ivan Lee (SAD, CST) and Aditya Mathur (iTrust Centre Director)

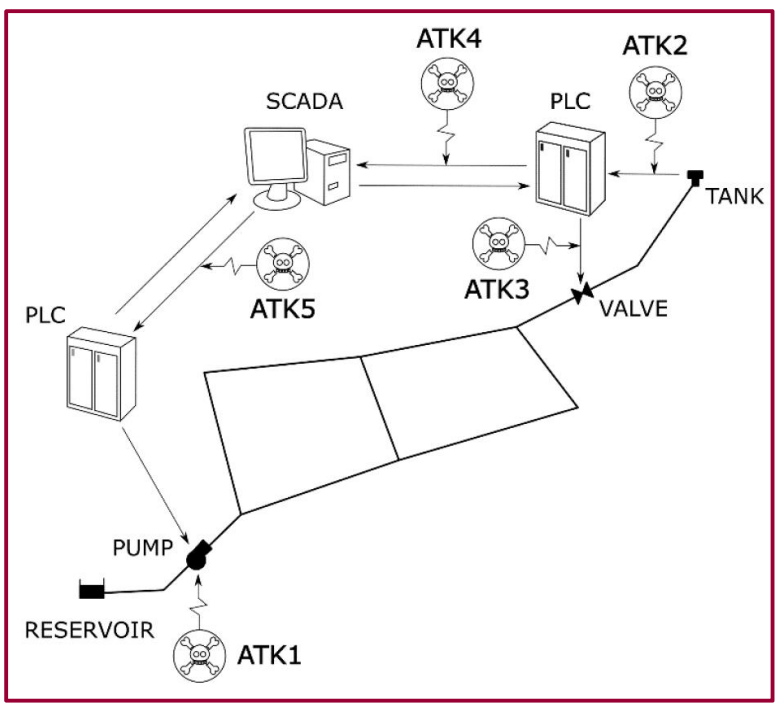
Our researchers are also working an IoT scanner system and an IoT honeypot. In the IoT scanner system, we will set up a platform to passively monitor wireless communications such as those using IEEE 802.11 WLAN, and aggregate data of communicating parties. Data collected is then filtered, analysed, and stored. To discover new attack vectors and evaluate the resilience of IoT devices to cyber attacks, we are building an IoT honeypot that poses itself as a vulnerability in places where the attackers are

looking. One such honeypot is the IP camera. Initial work includes gathering information on various attack models and vulnerabilities, and performing traffic monitoring and analysis. Expect interesting findings and results in the next six months!

Advancing Security of Public Infrastructure using Resilience and Economics

By Jonathan Goh

This project has entered into second year of research. With a (nearly) full team of researchers, work is intensively underway. Our work on attack detection and layered defence are presented in this update. We are currently developing numerical modelling environments that simulate the dynamics of a Water Distribution System, and effects of cyber-physical attacks on it, using a combination of a novel MATLAB-based toolbox, EPANET and C-TOWN network. In this work, several attack scenarios and models were looked into.



Examples of possible cyber-physical attacks to a WDS

Attack Detection

In attack detection, we adopted standard Kalman filters to estimate the state of the physical processes while minimising the effect of noise. Using this estimation, we evaluated existing attack-detection techniques such as bad-data detection algorithm and CUSUM. In the upcoming months, we will evaluate strengths and weaknesses of these techniques for different classes of cyber-attacks, physical processes with more complex dynamics (non-linear), and possible network-induced imperfections (e.g. delays). On the same note, another group had surveyed existing literature on intrusion detection systems (IDS) for CPS, a portion of which utilises machine learning (ML). The group formulated attacks on the SWaT testbed and evaluated the attack detection capabilities of nine well known supervised ML classifiers. More than 20,000 readings from all stage-1 sensors and actuators were collected. Four classifiers were able to detect a majority or all of the attacks. These encouraging results were published in the Cyber-Physical System Security Workshop 2016.

Layered Defence

This portion of the project involves the development of a design methodology for hardened intelligent checker (IC) and observer devices. The IC checker module comprises two elements: an IC sensor to measure parameters and a design logic that compares the parameter values to predefined constraints. Inconsistencies may indicate abnormal CPS operation. Initial work focused on developing a prototype local IC (LIC) to protect one of the tanks in SWaT and prevent it from overflowing (and thus defending it against an attack). Future work will extend to other components of the testbed, such as reverse osmosis and ultrafiltration systems.

Cyber Physical System Protection

By Aditya Mathur

The research team is on schedule in meeting the project milestones and also started exploring alternative approaches to complement what was originally proposed.

We had further developed CPSVerif – a self-contained software toolkit capable of performing systematic analysis on CPS – to support modelling of discrete control logic, continuous physical reactions, as well as systematic exploration of behaviours of such hybrid systems.

This development led to CPSVerif evolving into two different software toolkits - TAuth and HyChecker. TAuth supports modelling of security-critical components of CPS (e.g. security protocols) while HyChecker models and analyses more complicated CPS. TAuth has been applied to several timed protocols (e.g. Kerberos), and we found a new attack in Kerberos V using TAuth. In upcoming work, we plan to check if there are security protocols in SWaT which they can analyse using TAuth. Extending TAuth to support synthesising more kinds of

parameters (other than time) is also in the works. In HyChecker, they built a model of the SWaT system using the actual control programme in the PLCs in the system as well as a model of the physical environment (e.g. the water flow).

We developed a second toolkit, MiniCPS, which combines a set of tools for real-time high-fidelity emulation of network traffic with CPS component simulation scripts, and a simple API to interface with real-time physical-layer simulations. MiniCPS is used to model the communications and control aspects of SWaT, thereby allowing researchers to experiment with different network topologies, and test SDN-related prototypes.

Finally, we also designed physical layer transmission schemes that ensure confidentiality and minimise information leakage to illegal receivers during data transmission. Two network architectures were considered and evaluated: single-hop network and two-hop network, with promising results.

iTrust Infrastructure

Water Distribution (WADI) Testbed

iTrust proudly presents its second testbed, WADI, which is an extension to the first testbed, SWaT. Completed in May 2016, WADI – comprising two elevated reservoir tanks, six consumer tanks, two raw water tanks and a return tank with a combined flowrate of 10 US gallons per minute – simulates and completes the water supply network by taking in a portion of SWaT's permeate for storage and distribution.

The availability of WADI is timely, as traditional SCADA systems used in water distribution systems to control and monitor processes are vulnerable to cyber intrusions and attacks. Indeed, an undetected malicious attack to a water distribution system (e.g. injection of high dosage of chemicals) could lead to potentially fatal consequences for consumers.

In WADI, we consciously opted for a different PLC brand from SWaT, so that our researchers can verify

The Water Distribution (WADI) testbed

our defence models on different PLC brands. Exposing our defence models to a variety of PLC brands helps us determine how robust our models are.

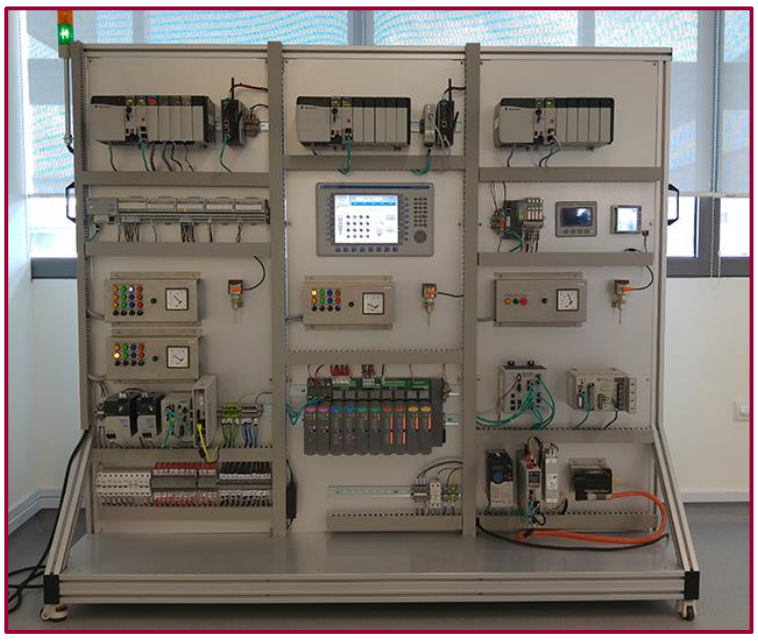
In addition to attacks and defences being carried out on the PLCs and networks, WADI has the capabilities to simulate the effects of physical attacks such as water leakage and malicious chemical injections. Unlike a water treatment system plant which is typically contained in a secured location, a distribution system comprises numerous pipelines spanning across a large area. This highly increases the risk of physical attacks on a distribution network. Together with SWaT, WADI provides opportunities for researchers to work on a full spectrum of possible cyber and physical attacks on a water treatment and distribution plant.

Training Skids

At iTrust, emphasis is placed on applied research. At the same time, we want to ensure that our infrastructure caters to training. Besides the testbeds, which are geared towards intensive research by faculty, researchers and external collaborators, iTrust has a suite of training skids (pictured next page) that serve as suitable platforms for students to tinker around and hone their skills before upgrading to the actual testbeds.

These training skids emulate SWaT, and are a realistic and safe training ground for students in the cyber-security related courses at SUTD. As with WADI, the four training skids run on different and widely used PLC brands (National Instrument, Rockwell, Schneider Electric and Siemens) to provide a wider base for learning and training. The available PLC programming software supplements the training, too.

In line with iTrust's mandate of knowledge transfer, the skids will also be available to local government and private agencies for staff training.



A training skid installed with Rockwell PLC

Events

SCy-Phy Systems Week 2016

SUTD will host its second SCy-Phy Systems Week from July 25 to 29. Organised by iTrust, this is an annual event that brings together research expertise from the cyber security community to deliberate on focused areas and challenges in cyber security. Last year's inaugural SCy-Phy Systems Week attracted about 200 participants over a week of events.

Similar to last year, three key events are planned during this week. A Think-in event is scheduled for July 25 where researchers and practicing engineers from academia and the industry will discuss issues in securing large public infrastructure such as that for power and water. Select participants will be invited to the SWaT Security Showdown (S3) session at the Secure Water Testbed (SWaT) – a first – in which they will attempt to attack the system whilst going undetected. On Jul 28 and 29, there will be outreach workshops on cyber security for students. Several invited talks during these two days are also planned. A snapshot of the week's events are as follows:

July 25: Think-in Session
July 26: SWaT Security Showdown I
July 27: SWaT Security Showdown II
July 28: Outreach I, Invited Talks 1 & 2
July 29: Outreach II, Invited Talks 3 & 4

The programme details are being worked out; do visit iTrust's website at itrust.sutd.edu.sg for updates.

iTrust Seminar Series

Professor Dieter Gollmann was invited as a speaker under the iTrust Seminar Series at SUTD on 17 Mar 2016. His topic was "Cyber-Physical Systems Security" in which he posited that while cyber physical systems (CPS) are characterised by an IT infrastructure controlling the physical components, security measures need to go beyond protecting the IT infrastructure alone. By examining the security limitations security that traditional IT security platforms provide, he also suggested what additional pre-emptive measures could be put in place to enhance CPS security. One such way is verifying the inputs from sensor readings by performing plausibility checks. Such checks compare and relate the readings of an individual sensor with those of other sensors to flag out implausible readings as suspicious.

Prof Gollman heads the Institute for Security in Distributed Applications and is a Professor at the Technische Universität Hamburg-Harburg. He has contributed to national and European projects in the areas of dependable communications and computing. He has been acting as a consultant for HP Laboratories (Bristol). He has been serving on the program committees of the major European conferences on computer security (ESORICS), and cryptography (EUROCRYPT) as well as other international conferences in these areas.

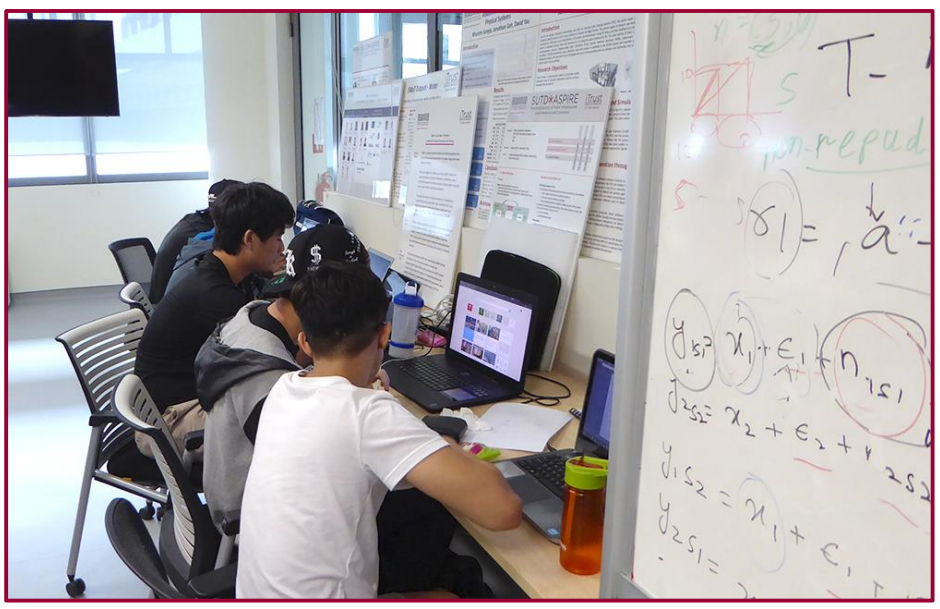
Outreach

University Immersion Programme

A group of bright young students from Nanyang Polytechnic (NYP) was attached to iTrust for five weeks. The students, currently pursuing their Dipolma in Information Technology/Security, gamely signed up for this attachment during their term break, under NYP's university immersion programme. This

programme exposes its top performing students to an R&D environment where they can get to work closely with the universities' professors and researchers. The objective is for its students to gain valuable experiences through R&D activities and supplement and elevate their technical knowledge. In iTrust, they were also able to help tackle real world problems through applied research using the SWaT testbed.

The five students – Shuan Chua, Clive Goh, Nur Ramadhan Bin Jumali, James Lee and Tan Kwok How – were assigned to three projects: Intelligent Checker, Security by Design, and Data Acquisition. In the first two weeks, the students poured over literature and familiarised themselves with SWaT testbed, so that they could formulate the problem statement and propose solutions. Next, they also quickly picked up the Python programming language which would become useful in their research. The students were tutored and supervised by iTrust's laboratory engineers Kaung Myat Aung and Muhamed Zhaffi, research assistant Sridha Adepu, SUTD student researcher William Koh and exchange student Siddhant Shrivastava, from the Birla Institute of Technology and Science (BTIS) Pilani.



The NYP student researchers working on their respective projects

Ramadhan's work focused on designing and developing a **web interface for the Secure Water Treatment (SWaT) testbed's Intelligent Checker**. The web interface serves as a user-friendly configuration platform for the laboratory engineer to define constraints (e.g., maximum and minimum water level) and monitor the testbed in real-time. Security features such as password login and login and system logs were added to the interface. These were done with the aid of several programming languages, including Python, HTML, and Javascript, and software such as Flask and Adobe Dreamweaver.

Clive and James worked together on the **Security by Design** project. Their task was to figure out which security measures should be embedded into the design of a CPS right from the start. Flow and time invariants were considered. By considering using invariants – being parameters dictated by the laws of physics – it would ensure that anomalies or breaches in the system could be detected and verified. They then compared theoretical (calculated) and experimental time (taken to fill a tank) and flowrate, and postulated a reasonable deviation (in time/volume) beyond which a CPS could be suspected of being compromised.

In **Data Acquisition**, Shaun and Kwok How worked on developing a Python script that was capable of acquiring data using OpenOPC, an open sourced software interface that allows a user to communicate with industrial standard OPC (OLE (Object Linking and Embedding) for Process Control) server and retrieve data. The OpenOPC script was then combined with existing data acquisition scripts to provide multi-layer data acquisition capabilities. Doing so provides redundancies for data collection in the event of a cyber attack on one of the layers, as well as data verification by comparing data collected across different layers.

iTrust would like to thank NYP, the teacher-in-charge, Mr Pang Nai Kiat and the students for contributing to our research work. Through this attachment, we hope that they have gained valuable experience and an insight into research work. We wish them the best in their studies and future endeavours!

NYP student researchers (left to right): Clive Goh, Tan Kwok How, Shaun Chua, James Lee and Nur Ramadhan Bin Jumali

Profiles

Roland Bouffanais

Asst Prof. Roland Bouffanais graduated from Ecole Polytechnique Federale de Lausanne (EPFL) in 2007 and then moved to MIT as a Postdoctoral Fellow & Associate in 2008. In 2011, he joined the Faculty of the Singapore University of Technology and Design, established in collaboration with MIT.

Dr Bouffanais' research focuses on the analysis of complex systems made of living or artificial agents and of biologically-inspired engineering problems. More specifically, some of his current research projects are concerned with control of swarm robotics systems, collective behaviours and the secure dynamic control of cyber physical systems. To these ends, Dr Bouffanais is building on his expertise in theoretical and computational science as attested by several awards he has received in the past years, including the prestigious IBM Research Prize in Computational Sciences.

Duan Lingjie

Lingjie Duan is an Assistant Professor in the Engineering Systems and Design Pillar at Singapore University of Technology and Design. He received Ph.D. degree in Information Engineering from The Chinese University of Hong Kong in 2012.

In 2011, he was a visiting scholar in the Department of Electrical Engineering and Computer Sciences at University of California at Berkeley. Lingjie has been actively working and contributing to the interdisciplinary research field combining telecommunication networks and microeconomics. He has used optimisation theory and game theory extensively as both modelling languages and solution tools to study the cooperative or competitive interplay among various parties in communications and networking.

Lingjie received the 10th IEEE ComSoc Asia-Pacific Outstanding Young Researcher Award in 2015. He was also the Finalist of Hong Kong Young Scientist Award 2014 under Engineering Science track. He has many highly-cited top engineering and business publications, and his works on network economics attract attention from academia and industry.

He is in the Editorial Boards of both IEEE Communications Surveys and Tutorials (COMST) and IEEE Transactions on Vehicular Technology from 2016. He also serves as the Program Co-Chair of IEEE INFOCOM'2014 GCCCN Workshop, ICCS'2014 special session on Economic Theory and Communication Networks, the Wireless Communication Systems Symposium of IEEE ICCC 2015, the GCNC Symposium of IEEE ICNC 2016, and IEEE INFOCOM'2016 GSNC Workshop. He also serves as a lead guest editor of Mobile Information Systems journal and a technical program committee (TPC) member of many leading conferences in communications and networking (e.g., ACM MobiHoc, IEEE SECON, ICC, WCNC).

Publications

Advancing Security of Public Infrastructure using Resilience and Economics

1. Introducing Cyber Security at the Design Stage of Public Infrastructures: A Procedure and Case Study Adepu S. and Mathur A., *2nd Asia Pacific Conference on Complex Systems Design and Management*
2. An Investigation into the Response of a Water Treatment System to Cyber Attacks, Adepu S. and Mathur A., *The 17th IEEE International Symposium on High Assurance Systems Engineering (HASE)*
3. Detecting Multi-Point Attacks in a Water Treatment System Using Intermittent Control Actions, Adepu S. and Mathur A., *Singapore Cyber Security R&D Conference 2016*
4. Data Driven Physical Modelling for Intrusion Detection in Cyber Physical Systems , Junejo K. N. and Yau D., *Singapore Cyber Security R&D Conference 2016*

5. Simulation of Cyber-Physical Attacks on Water Distribution Systems with EPANET, Taormina R., Galelli S., Tippenhauer N. O., Salomons E., Ostfeld A., *Singapore Cyber Security R&D Conference 2016*

6. An Agent-based Framework for Simulating and Analysing Attacks on CPS, Adepu S. and Mathur A., *15th International Conference on Algorithms and Architectures for Parallel Processing*

7. Using Process Invariants to Detect Cyber Attacks on a Water Treatment System, Adepu S. and Mathur A., *ICT Systems Security and Privacy Protection 2016*

8. Generalized attacker and attack models for Cyber Physical Systems, Adepu S. and Mathur A., *The 40th IEEE Computer Society International Conference on Computers, Software & Applications*

9. Attack Detection and Classification in Cyber Physical Systems Using A Machine Learning Approach, Junejo K. N., Goh J., Yau D., *2nd ACM Cyber-Physical System Security Workshop*

10. Assessing the effect of cyber-physical attacks on water distribution systems, Taormina R., Galelli S., Tippenhauer N. O., Ostfeld A., *World Environmental & Water Resources Congress*

11. Distributed Detection of Single-Stage Multipoint Cyber Attacks in a Water Treatment Plan, Adepu S. and Mathur A., *Asia CCS 2016*

12. Robust Network Synchronization of Time-Delayed Coupled Systems, Murguia C., Ruths J., Nijmeijer H., *6th IFAC International Workshop on Periodic Control Systems*

Cyber Physical System Protection

1. Generalised attacker and attack models for Cyber Physical Systems, Adepu S. and Mathur A., *IEEE Computer Society International Conference on Computers, Software & Applications (COMPSAC 2016)*

2. SWaT: Secure Water Treatment Testbed for Research and Training in the Design of Industrial Control Systems, Mathur A. and Tippenhauer N. O., *IEEE Computer Society International Conference on Computers, Software & Applications (COMPSAC 2016)*

3. Model Based Security Analysis of a Water Treatment System, Adepu S. and Mathur A., Jackson D. and Kang E., *2nd International Workshop on Software Engineering for Smart Cyber-Physical Systems (SEsCPS'16)*

4. Attacking Fieldbus Communications in ICS: Applications to the SWaT Testbed, Urbina D., Giraldo J. and Cardenas A., Tippenhauer N. O., *Singapore Cyber Security R&D Conference (SG-CRC 2016)*

5. Detecting Multi-Point Attacks in a Water Treatment System Using Intermittent Control Actions, Adepu S. and Mathur A., *Singapore Cyber Security R&D Conference (SG-CRC 2016)*

6. Symbolic Analysis of an Electric Vehicle Charging Protocol, Li L., Pang J., Liu Y., Sun J., Dong J. S., *ICECCS 2014: 11-18*

7. A Hybrid Model of Connectors in Cyber-Physical Systems, Chen X., Sun J., Sun M., *ICFEM 2014: 59-74*

8. Optimizing Selection of Competing Features via Feedback-Directed Evolutionary Algorithms, Tan T. H., Sun J., Xue Y., Chen M., Dong J. S., Liu Y., *International Symposium on Software Testing and Analysis (ISSTA 2015)*

9. False Data Injection Attacks with Local Topology Information against Linear State Estimation, Sun Y., Li W., Song W., Yuen C., *IEEE PES Innovative Smart Grid Technologies 2015 Asian Conference (IEEE ISGT-Asia 2015)*

10. Weakly secure MDS codes for simple multiple access networks, Dau S. H., Song W., Yuen C., *IEEE International Symposium on Information Theory (IEEE ISIT 2015)*

11. Secure Erasure Codes with Partial Decodability, Dau S. H., Song W., Yuen C., *IEEE International Conference on Communications (ICC2015)*

12. On Block Security of Regenerating Codes at the MBR Point for Distributed Storage Systems, Dau S. H., Song W., Yuen C., *IEEE International Symposium on Information Theory (IEEE ISIT 2014)*

13. On Simple Multiple Access Networks, Dau S. H., Song W., Yuen C., *IEEE Journal on Selected Topics in Communications, Nov 2014*

14. On the Existence of MDS Codes Over Small Fields With Constrained Generator Matrices, Yuen C., *IEEE International Symposium on Information Theory (IEEE ISIT 2014)*

15. On the Secrecy Outage Capacity of Physical Layer Security in Large-Scale MIMO Relaying Systems with Imperfect CSI, Chen X., Lei L., Zhang H., Yuen C., *IEEE International Conference on Communications (IEEE ICC 2014)*

16. Achievable Ergodic Secrecy Rate for MIMO SWIPT Wiretap Channels, Yuen C., *IEEE International Conference on Communications (IEEE ICC 2015)*

Administration and Research Openings

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

1) **Administrative position:**
    a. Assistant laboratory engineer (iTrust office)
    b. Administrative executive (ST Electronics-SUTD Cyber Security Laboratory)
    c. Laboratory technician (ST Electronics-SUTD Cyber Security Laboratory)
2) **Post-doctorate** in the following projects:
    a. Autonomous Vehicle Security
    b. Research & Security Innovation Lab for IoT
    c. ST Electronics-SUTD Cyber Security Laboratory
3) **Research Assistant** in the following projects:
    a. Advancing Security of Public Infrastructure using Resilience and Economics (one opening)
    b. ST Electronics-SUTD Cyber Security Laboratory

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

Readership Survey

We hope you enjoy reading iTrust Times. Please take a short survey via Google form (no sign-in required): http://goo.gl/forms/EKxl4L30Db.

iTrust Contact

To explore research collaborations and outreach activities, feel free to contact iTrust staff listed below.

Mr Kaung Myat AUNG
Laboratory Engineer (Water)
kaungmyat_aung@sutd.edu.sg

Prof. Yuval ELOVICI
Research Director
yuval_elovici@sutd.edu.sg

Dr Jonathan GOH
Research Scientist
jonathan_goh@sutd.edu.sg

Mr Mark GOH
Manager
mark_goh@sutd.edu.sg

Mr Ivan LEE
Senior Associate Director, Cyber Security Technologies
ivan_lee@sutd.edu.sg

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

MUHAMED Zhaffi Bin Mohamed Ibrahim
Laboratory Engineer (Power)
zhaffi_ibrahim@sutd.edu.sg

Kandasamy MURUGANANDAM
Laboratory Engineer (IoT)
Kandasamy_m@sutd.edu.sg

Ms Angie NG
Deputy Manager
angie_ng@sutd.edu.sg

Ms Priscilla PANG
Manager
priscilla_pang@sutd.edu.sg

Mr TAN Yong Sheng
Technical Officer
yongsheng_tan@sutd.edu.sg

iTrust
Center for Research in Cyber Security

itrust.sutd.edu.sg