An iTrust Newsletter

Jul – Sep | Issue 6

iTrust Times

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Established in collaboration with MIT

From Centre Director's Desk

Participants at the Think-in session of the second Secure Cyber-Physical (SCy-Phy) Systems Week 2016

Dear Reader:

Greetings from iTrust, and welcome to this sixth issue of iTrust Times. In this special issue you will find a summary of various events during the Second Secure Cyber-Physical (SCy-Phy) Systems Week — an annual signature iTrust event.

I take this opportunity to express my sincere thanks to Prof Quek Tong Boon, the Singapore Ministry of Defence's outgoing Chief Defence Scientist (CDS), for his unfailing support to iTrust since its inception in Feb 2013. Prof Quek conceived the idea of iTrust and defined its operational semantics. Since my joining SUTD, and taking charge of iTrust, Prof Quek has been a guiding light and a strong supporter of our ideas and growth plans. I wish him all the best as he takes on his new role as the Advisor to the DSO National Laboratories.

I welcome our new CDS, Mr Quek Gim Pew. Mr Quek has indicated his strong support for iTrust. Thankfully he was able to find time from his busy schedule to open the SCy-Phy Systems Week with his remarks at the first event — the Think-in session. Over the coming years we hope to work closely with Mr Quek, and our sponsors at MINDEF, as iTrust expands and assumes an increasing role in protecting our critical national infrastructure.

I wish to thank all the SCy-Phy participants who came from afar to participate in and contribute to the Think-in session, and the discussants who helped make this session a learning experience for all. My sincere thanks to the organisers of the one-of-a-kind SWaT Security Showdown (S^3) event. Special thanks to SUTD Asst Profs

In This Issue

Martin Ochoa and Nils Tippenhauer for spending many days and nights in meticulously organising and conducting this event, and with the strong technical support from our laboratory engineers Kaung Myat Aung and Muhamed Zhaffi. Thanks to the iTrust staff who helped ensure the success of the entire SCy-Phy Systems Week with utmost dedication and precision!

iTrust's newest Water Distribution (WADI) testbed is now officially open! Thanks to Mr Teo Chin Hock, Deputy Chief Executive, Cyber Security Agency, for taking time off from his busy schedule to formally open the testbed. Thanks to Professor Kristin Wood, Co-Director of the SUTD-MIT International Design Centre, for funding the design and construction of WADI as a research facility.

I invite all readers to participate in the 18th IEEE High Assurance Systems Engineering (HASE) 2017 conference. iTrust is proud to have undertaken the responsibility of organising this important conference which, for the first time, is being held in Singapore! More details are in this newsletter.

I hope you will enjoy this special issue which, as always has been carefully edited by Mark Goh.

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

Left table (from bottom left): Dawn Tilbury (University of Michigan), Nils Tippenhauer (SUTD), Bruce McMillin, (Missouri University of Science and Technology), Deeph Chana (Imperial College London), Martin Ochoa (SUTD), Aditya Mathur (standing; SUTD), Jerry Khoo (National Research Foundation), Lorenzo Cavallaro (Royal Holloway, University of London), Quek Gim Pew (MINDEF), Chua Peng Huat (MINDEF), Abian Blome (Siemens AG), Indrakshi Ray (Colorado State University)
Right table (from bottom left): Daniel Trivellato (SecurityMatters), Tan Ee Sin (PUB), Luca Vigano (King's College London), Martin Dunn (SUTD), David Yau (SUTD), Saman Zonouz (Rutgers University), Mo Yilin (NTU), Yu Chien Siang (Quann Singapore), Quek Tong Boon (DSO National Laboratories), Marina Krotofil (Honeywell Cyber Security Lab), Eunsuk Kang (UC Berkeley), Alvaro Cardenas (UT Dallas)

SCy-Phy Systems Week 2016

SCy-Phy Systems Week 2016

Participants at Day 1 Think-in Session

The second Secure Cyber-Physical (SCy-Phy) Systems Week kicked off on 25 Jul 2016. This week-long event also featured the inaugural SWaT Security Showdown (S^3) – a hands-on security event on the Secure Water Treatment testbed (see the following article) – seminars and student outreach. This event was sponsored by the Ministry of Defence, Singapore.

Think-in Session (Day 1)

As in the previous year, Think-in was attended by a 100-strong audience comprising international cyber security professionals, local government agencies, industry and academia. After a brief welcome, Prof Aditya Mathur introduced the Guest of Honour Mr Quek Gim Pew, Chief Defence Scientist of the Ministry of Defence, Singapore.

Chief Defence Scientist Mr Quek Gim Pew making his opening remarks

Speaking at his Opening Remarks, Mr Quek summed up the objectives and agenda of SCy-Phy thus: To (a) create a platform for international and local security researchers and practitioners to present and share their latest research on the defence of Cyber Physical Systems (CPS); (b) offer participants a "live" and hands-on experience by delving into the architecture and defence mechanisms of the testbeds available in iTrust; and (c) introduce students to the tools and techniques of cyber security. While noting how the increased interconnectivity between the physical and cyber domain has led to greater efficiency and interactions in the way we live, work and play, Mr Quek also highlighted a number of high profile cyber security breaches as examples and reminders that we should continue to ensure that CPS remain dependent, safe, secure and efficient. To take it further, as cyber security is a global issue he encouraged interaction and collaboration within the international research community to tackle it together, with SCy-Phy Systems Week offering such an opportunity.

> **[The] diversity of participants [at SCy-Phy] promises a rich exchange of ideas and collaborations that can lead to a more holistic understanding of the cyber security space.**
>
> **Mr Quek Gim Pew, Chief Defence Scientist, MINDEF**

12 panellists from the US, Europe and Singapore were invited to speak at four sessions marked as: Threats, Defence, Models, and Safe and Secure Controls. A corresponding 12 representatives from local academia, government agencies and industry formed a panel of discussants to stimulate discussions.

Session 1: Threats was represented by panellists Dr Deeph Chana (Imperial College London), Ms Marina Krotofil (Honeywell Industrial Cyber Security Lab), and Dr Bruce McMillin (Missouri University of Science and Technology).

In **"The Multifaceted Nature of Threats and Risks," Deeph Chana** observed that the ruling-out of non-obvious threat drivers and a lack of consideration of the interconnectivity of systems often led to a false sense of security. He outlined reasons why cyber security problems needed to be viewed and approached by the players – policy makers, technology innovators and academics – at a systems engineering level by considering a wide range of factors including political, societal, technical. In that, Deeph encouraged the building up of the "triple-helix" set of competencies, where people with practical experience and understanding of the academic, business and government could better make assessments of threats and risks in a multi-faceted and holistic manner.

Marina Krotofil's "Mind the Gap: What We Don't Know about CPS Threats Yet" reminded practitioners about the knowledge gaps that existed in cyber security and threats when designing, managing and operating CPS. She pointed out that there were times that an attacker did not need to perform a complex attack to achieve serious consequences, and cyber security professionals need to uncover and classify attacks that required a lot of knowledge and those that did not. Marina explained that many cyber attackers were still able to remain invisible because cyber security professionals did not yet have the monitoring visibility into the process control networks, forensic capabilities in the embedded systems, and know how attack indicators look like; it was through understanding these gaps that we could build and manage more secure CPS.

Bruce McMillin's "Unified Cyber-Physical Threat Detection" presentation laid out threats to CPS in the forms of cyber-enabled physical attacks, physically-enabled cyber attacks, or both. Agreeing with Deeph, he emphasised that when threat detection relied on treating the cyber and physical components as layers, the complex interactions that can occur were missed out. Bruce postulated that as threats were really a disruption of information flow, existing information flow models could be extended to unify both the cyber and physical aspects of a CPS and in that way, better perceive and mitigate those threats.

Top (left to right): Session 1 panellists Dr Deeph Chana (Imperial College), Ms Marina Krotofil (Honeywell Cyber Security Lab), Prof Bruce McMillin (Missouri University of Science and Technology). Bottom (left to right): Discussants Mr Leon Cheng (MINDEF), Dr Giedre Sabaliauskaite (SUTD), and Prof Yu Chien Siang (Quann Singapore)

Session 2: Defence was represented by panellists Assoc Prof Lorenzo Cavallaro (Royal Holloway, University of London), Mr Daniel Trivellato (SecurityMatters), Asst Prof Saman Zonouz (Rutgers University).

Lorenzo Cavallaro kicked off **Session 2: Defence** with his presentation on **"Misleading Metrics: On Evaluating Machine Learning for Malware with Confidence."** While machine learning (ML) was held as a promising technique to identify and classify malware threats, problems such as ML algorithms decay in real-world settings and concept drift continued to undermine ML's potential. Lorenzo introduced the framework of a conformal evaluator that his group developed and used to assess the quality of machine learning tasks, by introducing statistics (such as credibility and confidence) into the analysis. With this framework, he hoped to encourage more research in this area.

In his presentation on **"Aren't We Forgetting Someone?" Daniel Trivellato** emphasised the importance of ICS operators' requirements for solutions which were reliable, yet simple to understand and which required minimal effort to setup and operate. This was often overlooked when the focus was on boosting detection capabilities at the expense of usability. Daniel shared the direction taken by SecurityMatters – a company specialising in ICS monitoring and analysis – to address both needs

of advanced detection capabilities while achieving simplicity in its operations.

Saman Zonouz's "Proactive Cyber-Physical Intrusion Response" focused on smart grids as the CPS in question. His group observed two shortcomings in existing power systems platforms. Firstly, there was insufficient use of cybersecurity techniques in control devices, software for control systems and control centres for power systems. Secondly, while there was much analysis done on the physical and cyber aspects of the plant, ignoring the cyber-physical interdependencies meant there was disconnect in leveraging on the information. The challenges his group faced while mitigating these shortcomings in intrusion detection included how to effectively combine the cyber monitor alerts with the physical sensor measurements that were based on minimal trusted computer and sensing base (e.g., by encrypting the analogue signals at the data acquisition point before the signal reaches the analogue digital converter), even when some computers were compromised.

Top (left to right): Session 2 panellists Assoc Prof Lorenzo Cavallaro (Royal Holloway, University of London), Mr Daniel Trivellato (SecurityMatters), Asst Prof Saman Zonouz (Rutgers University). Bottom (left to right): Discussants Mr Lim Hwee Kwang (National Research Foundation), Dr Chen Binbin (Advanced Digital Sciences Center Singapore), Mr Ganesh Narayanan (Ernst & Young)

Session 3: Models was represented by panellists Dr Eunsuk Kang (UC Berkley), Prof Indrakshi Ray (Colorado State University), Prof Luca Viganò (King's College London).

With increasingly higher system complexity in modern CPS, the interaction between a malicious environment and system components has become even harder to predict. **Eunsuk Kang's** presentation on **"Architectural and Design Analysis for Secure Cyber-Physical Systems"** described how a combination of traditionally independent fields of safety engineering and computer security with software engineering and formal methods could be used to model and reason about the security of a CPS. His research revolved around leveraging on design-time analysis to generate potential attacks, assessing their impact on the system safety, and suggesting mechanisms for detecting and mitigating those attacks, with part of the work based on his stint at the Secure Water Treatment (SWaT) testbed at iTrust.

Recognising the complexities in and interaction of cyber, physical, and even human components in a CPS, and each with its own set of constraints, **Indrakshi Ray** presentation on **"Specification and Analysis of Cyber-Physical Systems"** focused on some of the challenges of modelling and analysing CPSs. Similar to Eunsuk's presentation, Indrakshi proposed a hybrid approach to CPS modelling wherein the specification team (computer scientists using formal methods) work with the prototype team (consisting of engineers using simulators) during the requirement and design phases of a CPS. She also proposed some ideas about how to design and verify such systems to ensure their functional and non-functional properties.

Top (left to right): Session 3 panellists Dr Eunsuk Kang (UC Berkley), Prof Indrakshi Ray (Colorado State University), Prof Luca Viganò (King's College London). Bottom (left to right): Discussants Dr Zhou Jianying (Institute for Infocomm Research), Dr Jonathan Goh (SUTD), Dr Khurum Junejo (SUTD)

Expanding Indrakshi's thoughts on the human component in CPS and Deeph's views on a multi-stakeholder approach, **Luca Viganò** in his presentation on **"Formalising and Reasoning about Socio-Technical Security"** argued that a resolution to CPS security would only be found by treating it as a true socio-technical problem rather than a technical one. In that, practitioners must understand how the two components of a system, the technical and the social, could better cooperate, and consider the system as a socio-technical system. Luca then introduced a socio-technical design principle encompassing the concepts of "Beautiful Security" and "Invisible Security", in which it contributes to a positive user experience and reduces user intervention and hence reducing human error.

Session 4: Safe & Secure Controls was represented by panellists Asst Prof Alvaro Cardenas (UT Dallas), Asst Prof Mo Yilin (NTU), and Prof Dawn Tilbury (University of Michigan).

In **"Performance of Control Systems under Undetected Attacks," Alvaro Cardenas** focused on attacks which manipulated the sensor or control signals of Industrial Control Systems (ICS) that can be tuned by the attacker to cause a continuous spectrum in damages while remaining undetected. Attackers do so by following closely the expected behaviour of the system while injecting just enough false information at each time step to achieve their goals in manipulating the system. In his work, Alvaro reported that other than having good anomaly detectors, control algorithms could also mitigate the impact of undetected attacks. He analysed the performance of control systems to such types of attacks in a variety of control systems, including those designed with differential privacy guarantees.

Mo Yilin discussed the problem of information fusion in his presentation on **"Secure Information Fusion in Cyber-Physical Systems."** In a CPS where some sensors were assumed to be malicious, instead of reducing uncertainty through a combination of information, the malicious sensors reported a fusion of real and false data. While detecting the presence of malicious sensors was relatively easy, the difficulty was in knowing exactly which set of sensors was under attack (and thus to isolate them). Other modes of attacks (replay attack and false data injection attack), and intrusion detection (residue based detector) and isolation techniques (compressive sensing) were also explored.

Dawn Tilbury selected discrete-parts manufacturing control systems as the CPS for discussion in her presentation on **"Safe and Secure Controls: Key Issues and Challenges."** She highlighted some of the potential vulnerabilities (backdoors, internet connectivity etc.) and possible attack surfaces (false data injection on a sensor, DoS attack on network etc.), as well as the challenges in understanding, classifying and distinguishing between faults, errors and cyber attacks. In Dawn's research programme, the vision for tomorrow's manufacturing control systems is one in which there is a cyber-physical control plane with a global view of the system, with models of the different components to compare between simulated and actual results to detect anomalies that could point to a possible cyber attack.

Top (left to right): Session 4 panellists Asst Prof Alvaro Cardenas (UT Dallas) Asst Prof Yilin Mo (NTU), Prof Dawn Tilbury (University of Michigan). Bottom (left to right): Discussants Mr Tan Ee Sin (PUB), Mr Abian Manuel Blome (Siemens AG), Asst Prof Martin Ochoa (SUTD)

The Think-in session was then closed with a summary of discussions by Prof Aditya Mathur and Mr Lim Soon Chia, Cyber Security's Director of Technology.

SWaT Security Showdown (Day 2 & 3)

The two-day SWaT Security Showdown (S^3) was one of the highlights of the SCy-Phy Systems Week. Using the Secure Water Treatment (SWaT) testbed as the

"front line," attack and defence teams faced off to demonstrate their respective capabilities in a hands-on cyber security event conducted in the context of a modern and operational Industrial Control System (ICS). 12 local and international teams from academia (including SUTD) and companies, were invited to participate in this one-of-a-kind event.

Objectives

The objective of the S^3 was three-fold: (a) showcase the extensive range of capabilities of the SWaT testbed (testing, demonstration, experimentation, research) to local and international guests, and offer them hands-on experience; (b) showcase the research conducted at iTrust, and in particular the detection engines (used against cyber attacks) developed; and (c) verify the efficacy of our countermeasures with respect to unknown cyber attacks, since attacks not detected will challenge researchers to think of new defence techniques and attacker models.

By inviting six attack teams of security experts, such an exercise would help SUTD researchers to evaluate their research outcomes in a practical and highly competitive environment. Participants would also increase their technical skills by solving interesting challenges in a realistic setting. As all participants will share their work (e.g., methodology, reports and findings from the event) with iTrust, researchers will be able to strengthen their defence models and design a more secure CPS.

"The S^3 is a one-of-a-kind event not seen anywhere else in the world as it provides a realistic testbed to carry out such security exercises. In organising such an event, we are exposed to a wide range of attacks and defence systems, which will help us design more robust and secure CPS.

S^3 co-organiser Asst Prof Nils Tippenhauer, SUTD"

The six attack teams were from Applied Risk, Ernst and Young (EY), Lancaster University, National University of Singapore (NUS), Siemens AG, and University of Illinois Urbana-Champaign-Advanced Digital Sciences Center (UIUC-ADSC).

Some of the S^3 organisers and participants gathering for a group shot at SWaT testbed at the end of the two day event

Online challenge

Prior to the S^3 event, participants were invited to take part in an online challenge to familiarise with SWaT and typical attacks. These challenges covered five categories:

- PLC: Dedicated access to the SWaT PLC for 48 hours
- Forensics: Forensics exercises on real SWaT traffic captures
- miniCPS: Interaction with a network and physical process simulation of SWaT
- Trivia: Testing participants' knowledge on SWaT
- Miscellaneous: Warm-up challenges related to CPS security

The points obtained by the teams were then added to the teams' points obtained on the actual S^3 event.

<u>Actual event</u>

On the actual day of the event, each attack team was given three hours to carry out the challenge in the following manner:

- Decide on which pre-defined goals (set out by S^3 judges) that the team wished to achieve. These goals were categorised into Physical Process Goals (by gaining control over physical actuators and processes) and Sensor Data Goals (by demonstrating control over sensor readings of different components);
- Decide on an attacker profile the team wished to adopt;
- Inform these goals and profile to the S^3 judges, on which the teams would be assessed and awarded their score; and
- Carry out these pre-defined goals.

Meanwhile, the defence teams had pre-installed their defence systems prior to the event to passively and closely monitor the plant behaviour for anomalies during the attacks. While the challenge was to demonstrate that their systems could detect as many attacks as possible, for the purpose of this challenge, their systems would allow the attacks to go through even if a breach was detected.

Results

After two days of intense activity, the **NUS GreyHats** team was declared as the overall winner based on the combined performance in both phases (online and actual) of the competition, while the team from **UIUC-ADSC** won the live challenge at the SWaT site. All attacks launched by the six attack teams were detected almost immediately by the defence mechanisms installed in SWaT.

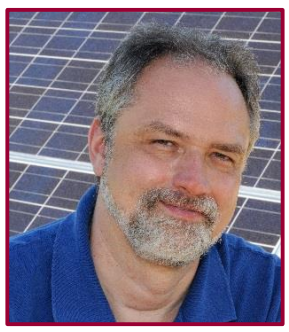
> **This is the first time we are participating in a cyber physical event, particularly on cyber defence. Other than hardening our virtual defences, we cannot overlook the physical aspects of security such as installations of hardware backdoors. Our advice to organisations is: You don't own what you can't defend, and ignorance is a hacker's greatest weapon.**
>
> **Overall winner, NUS GreyHats**

Mr Lim Soon Chia, Director of Technology at the Cyber Security Agency of Singapore (CSA), who was at the event, said:
“Cyber threat is a clear and present risk, and increasingly so for Industrial Control Systems (ICS). The S3 event brings cyber security alive and into action. For the first time, cyber defenders are pitted against attackers in a realistic ICS water plant setup. This reveals the vulnerabilities and risks that ICSs are subjected to, and highlights the importance of security by design, and the need to be prepared and ready against cyber security threats.”

As part of iTrust’s mandate to share and transfer knowledge back to society, a report of the work done by the participants will be compiled and made available on iTrust’s website (www.itrust.sutd.edu.sg) at a later date.

Invited Talks (Day 4 & 5)

Concluding SCy-Phy Systems Week were technical talks by four invited speakers over two days. iTrust regularly organise these seminar talks and invite cyber security professionals to share their expertise. These talks are open to the public to attend.



Bruce McMillin spoke about the interpretation of formal information flow properties and interference within the context of a CPS blending both physical and cyber information flow properties across multiple security domains, in which an electric smart grid was used as an example.

Saman Zonouz's presentation focused on past and potential future threats against critical infrastructures and embedded devices, and discussed the challenges in design, implementation, and analysis of security solutions to protect CPS. He also shared novel classes of working systems that his group had developed to overcome these challenges.

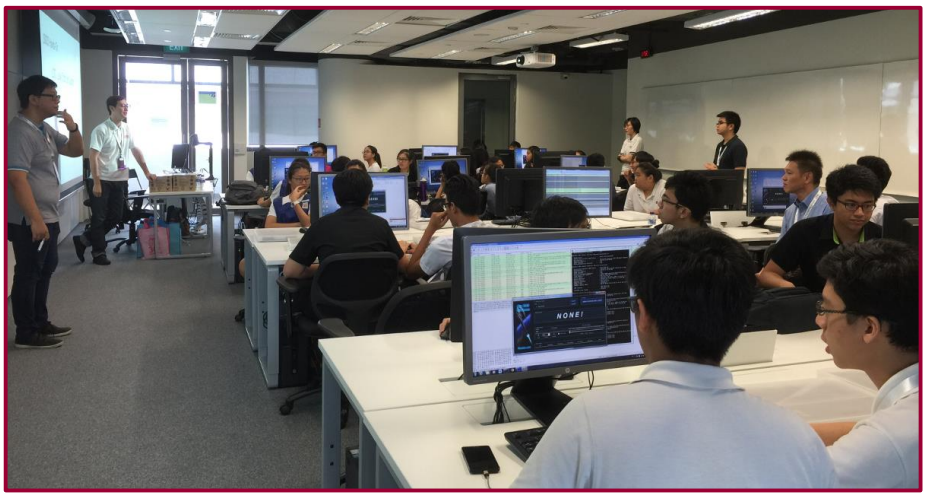
Luca Viganò introduced a novel and declarative way to specify privacy goals, called "alpha-beta privacy", where alpha represented the intentionally released information and beta the actual cryptographic ("technical") messages the intruder could see. "Alpha-beta privacy" then meant that intruder would not be able to derive any "non-technical" statement from beta that he cannot derive from alpha already.

Marina Krotofil addressed the topics of data processing, end-to-end data flow configuration requirements and explained the risks derived from external threats and internal errors. She shared a novel attack vector on ICS, and a conceptual tool which aided in the discovery of the attack surface at the early stage of risk assessment.

Outreach: IoT Playground – Securing the Internet of Things (Day 4 & 5)

By Toh Jing Hui

As part of the SCy-Phy Week, iTrust organised an outreach workshop for students from secondary schools, institutes of technical education, junior colleges, polytechnics and SUTD to introduce them to some of the common security loopholes – and the associated privacy issues – in the Internet of Things (IoT) devices. To allow for more students to sign up, the workshop was conducted on two days, and was attended by 86 students from seven schools – a very encouraging response.



Jinghui (left) at of the sessions at the IoT Playground workshop

The IoT introductory workshop was conducted by Toh Jing Hui, a Research Assistant in iTrust, who provided the students with a foundational understanding of networking, security, and ethical hacking, as well as in what ways IoT could potentially affect them and why security of such devices were important. This included concrete examples of how an attacker could crack into and perform data leakage attacks on IoT devices such as an activity tracker and IP camera. Mitigation techniques and best practices to minimise oneself against these threats were also discussed.

The second half of the workshop was a hands-on session in Wireshark (to observe and make sense of wireless traffic), performing a DoS attack, brute forcing an encryption key, and hacking an IP camera. Summarising the workshop, Jing Hui discussed the factors to consider when designing an IoT device to ensure that it would not be easily compromised. Jing Hui was also assisted by SUTD students Claudia Aw and Muhammad Syuqri during the hands-on session.

> **I enjoyed knowing more about hacking and the inter connectivity between systems. It was also fascinating to get to try out the coding and analysing the systems.**
>
> **A student at the IoT Playground workshop**

Events

Water Distribution (WADI) Testbed Opening Ceremony

The WADI testbed was officially launched by the Deputy Chief Executive of Cyber Security Agency (CSA) Mr Teo Chin Hock on 26 Jul 2016. In his welcome remarks, Prof Kristin Wood, Co-director of the SUTD-MIT International Design Centre (IDC) said that IDC was proud to be the sponsor of the testbed, and stressed the importance of testbeds in validating research work and being in line with IDC's mission of

Jinghui being assisted by SUTD students Syuqri (left) and Claudia (right; both standing) during the IP Camera hands on session

Asst Prof Stefano Galelli explains the WADI testbed to Mr Teo Hock Chin (second from right) and Prof Kristin Wood (right)

using design to address key societal challenges, in this case, cyber security of CPS.

WADI was completed in May 2016 and comes equipped with two elevated reservoir tanks, six consumer tanks, two raw water tanks and a return tank to simulate a water distribution network. It takes in a portion of SWaT's permeate for storage and distribution and has a combined flowrate of 10 US gallons per minute, or about 2.3 m^3 per hour.

18th IEEE International Symposium on High Assurance Systems Engineering

IEEE Advancing Technology for Humanity

IEEE computer society

iTrust Centre for Research in Cyber Security

Increasingly complex and interdependent systems require careful design to ensure continued operation in the presence of component failures, natural disasters, software/hardware vulnerabilities, and latent software errors. Such systems span broad range of applicability. Devices such as pacemakers and insulin pumps, aim at better life for individuals, while large public infrastructure such a smart power grid, rapid public transport, and water treatment and distribution, impact the daily lives of a mass of people. Often such systems are interdependent in complex ways implying that flaws in the design of one may affect the behaviour of a system-of-systems.

A key question then becomes "What design innovation is needed to bring about systems whose operation in accordance with functional and non-functional requirements is assured with a very high probability?" The theme for **HASE 2017 is "High Assurance through Design Innovation"** and will focus on this and related questions and answers which are of paramount importance to engineers who design and build interdependent complex systems that impact individuals, entire cities and even nations.

Call for Papers

Researchers and practitioners are invited to submit original work, not previously published, to HASE 2017. All submissions must be written in English and formatted according to the IEEE formatting guidelines for conference papers.

All papers must be submitted through the EasyChair, in PDF format. Page limits for papers under different tracks are given below. All submissions will be reviewed by at least three members of the Technical Programme Committee. Please visit http://itrust.sutd.edu.sg/hase2017/ for more information.

The final HASE 2017 technical programme will be divided into the following tracks:

Track A: Theoretical foundations of assurance (8 pages)

Contributions under this track will focus on formal methods that aid in modelling and validating new and existing designs of complex systems.

Track B: The practice of assurance (4 pages)

Contributions under this track will focus on methods that have been applied in the design of high assurance systems, or have been tested in realistic testbeds.

Track C: Tools (4 pages)

Contributions under this track will focus on new or existing tools and their effectiveness in creating high assurance designs.

Track D: Ideas under trial (2 pages)

Short papers under this track will focus on new ideas that fall under design innovation. Such ideas might not have undergone a rigorous test but are worthy of discussion.

Papers that cut across Tracks A, B, and C are welcome.

Track E: Student Session (2 pages)

This track will feature research presentations by undergraduate and graduate students. Papers under this category must have a student as the first author who is enrolled full time at a recognised university. Student authors will be asked to provide a letter from the university confirming their full time enrolment.

Limited travel support is available for students with accepted papers under this session to partially cover the air fare and hotel costs.

For **submission guidelines**, please visit http://itrust.sutd.edu.sg/hase2017/

Important dates (GMT+8)
Submission deadline: 12 September 2016 @ 11:59 PM
Acceptance notification: 10 October 2016
Camera-ready submission: 7 November 2016 @ 11:59 PM
Contact: hase2017@sutd.edu.sg

CommunicAsia 2016

iTrust's Research Director **Prof Yuval Elovici** was invited to speak at the session "Enterprise Cybersecurity: Securing for Sustainable Growth" in CommunicAsia on 2 Jun 2016.

In his presentation **"Insider Threat: Challenges and Potential Solutions",** he spoke on the challenges in detecting threats within an organisation, as an insider's behaviour may be very similar to the behaviour of a non-insider user. This difficulty is compounded by the fact that detection mechanisms may create many false positives that may require costly investigation. The advent of smart devices now means that an insider may leak information without leaving forensic evidence such as through the use of a smartphone's camera to capture confidential information. On a more serious level, an insider could even perform an advanced persistent threat (APT) using stolen credentials of a legitimate user.

Prof Elovici at CommunicAsia 2016

Prevention and Detection

To overcome such threats, Prof Elovici and his team carried out research work on prevention and detection methods. To prevent unintentional leakage of information (either through a removable storage device, email client or cloud service), his teamed worked on **adding a benign Detectable Malware Signature (DMS)** to sensitive files. When such files are brought out of the organisation, common antivirus and firewall software will notify the user that the document has been quarantined or deleted. In email clients and cloud services, the user would not be able to send or upload the file.

To thwart insiders who deliberately aim to bring sensitive files out of the organisation, honeytokens (a fabricated data item that may indicate the presence of malicious activity in a computer system) are deployed. They are termed honeytokens as they are considered to be more attractive than typical data items, and thus attract an insider to use it without authorisation. Prof Elovici's team developed the **HoneyGen** - a novel method to automatically generate honeytokens that are similar to real data.

Challenges

Prof Elovici sees the need to develop innovative technologies for insider detection based on data collected by the organisation. Given that the data varies across different sectors, he opined that these technologies may need to be adapted to each specific domain. In the course of developing them, the main challenges that researchers might face include coping with the insider's ability to perform data misuse without leaving forensic evidence and achieving high true positive and low false negative.

Asia ACM Conference on Computer and Communications Security (CCS)

Two iTrust's researchers presented at the Asia CCS, Xi'an, China, in May 2016. **Dr Jonathan Goh** presented the workshop paper entitled **"Behaviour-Based Attack Detection and Classification in Cyber Physical Systems Using Machine Learning".** He gave a summary of various behaviour-based machine learning (ML) approaches for the intrusion detection through the use of SWaT using supervised learning techniques. The methods described not only detected the occurrence of a cyber-attack at the physical process layer, but also identifies the specific type of the attack. In **"Distributed Detection of Single-Stage Multipoint Cyber Attacks in a Water Treatment**

Plant" Sridhar Adepu shared that, using the flow properties of water from one stage to the other, a neighbouring controller was found effective in detecting single stage multi-point (SSMP) attacks on a CPS. The method was based on physical invariants derived for each stage of the CPS from its design. Further, distributing the attack detection code among various controllers added to the scalability of the proposed approach.

ICT Systems Security and Privacy Protection (IFIP SEC) 2016

Sridhar Adepu also presented at the IFIP SEC in Ghent, Belgium in Apr 2016. **"Using Process Invariants to Detect Cyber Attacks On A Water Treatment System"** was an experimental investigation to assess the effectiveness of process invariants in detecting cyber attacks on Industrial Control Systems (ICS). The impact of power failure was also studied. Results of this work pointed out challenges in implementing invariant based attack detection in an operational ICS.

World Readiness Programme Symposium

In May 2016, iTrust was invited by CHIJ St Nicholas Girls' School (CHIJ SNGS) for the second year running to present on cyber security at the Joint Integrated Programme (IP) World Readiness Programme (WRP) Symposium for about 500 Secondary One Joint IP students from Catholic High School, CHIJ SNGS and Singapore Chinese Girls' School. The WRP prepares Joint IP students with the knowledge and skills to become well-informed and responsible global citizens.

Given last year's rousing reception, Ivan Lee, iTrust's Senior Associate Director for Cyber Security Technologies, was approached by the Joint IP to speak on **cyber security and cyber crime**. The first part of Ivan's talk focused on the impact of cyber security on individuals, organisations and society, and the next generation of cyber crimes and the 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 intercept print jobs, a robot for reconnaissance, a 3D printer's outputs being sabotaged, and a vacuum cleaner to carry out security sweeps. At a cyber physical system level, a live demonstration of an attack on the Secure Water Treatment (SWaT) testbed was also shown. Unsurprisingly, the interactive demonstrations drew many students to participate in them and understand the issues discussed first hand.

Ivan interacting with students during his talk

Jing Hui demonstrating the drone's reconnaissance capabilities to a hall full of students

Moving on from interactive demonstrations to critical thinking, Ivan's second part of the talk focused on cyber crime. He introduced the nature of trans-boundary cyber crime and the various actors responsible, from individual (script kiddies) to organisations (criminal syndicates) and nations (state sponsored). Ivan also saw it important to raise awareness of an evolving menace – ransomware – through an encryption demonstration and reminded the students to be extra careful when receiving and opening emails of unknown origins.

Ivan, with the help of iTrust's laboratory engineer Muhamed Zhaffi and Research Assistant Toh Jing Hui, facilitated a debate among the students on security versus privacy, using the FBI vs Apple case as the platform for the debate. This provided the students the opportunity to consider the challenges faced by both parties, and ensured a lively and entertaining debate to conclude the symposium.

iTrust has come up with an informative and engaging programme that not only raises awareness of the need for cyber security – which is increasingly becoming a critical area of expertise – among our youths, but also enables students to think about related issues from different perspectives through discussion and debate.

Mr Loh Chih Hui, Vice-Principal (Academic), CHIJ SNGS

Visitors

Acting Minister for Education Mr Ong Ye Kung visited iTrust's testbeds on 20 May 2016. Accompanied by SUTD President Prof Tom Magnati and Provost Prof Chong Tow Chong, he was given a tour of the Secure Water Treatment (SWaT) and Water Distribution (WADI) testbeds by Asst Profs Stefano Galelli and Nils Tippenhauer. Asst Prof Martin Ochoa was also on hand to give an introduction iTrust's IoT projects.

COO and President of **Rohde & Schwarz Asia** Mr Peter Riedel visited iTrust on 24 May 2016. He was given an introduction and tour around SWaT and IoT testbeds by Ivan Lee to understand the how iTrust's research into cyber security defence models can help detect and thwart potential cyber threats to critical infrastructure and smart devices. This was followed by a visit from **DST Group Australia** a week later.

Siddhant Shrivastava was a **visiting researcher** from the Birla Institute of Technology and Science (BITS) Pilani who completed his six-month stint with iTrust in June 2016.

Siddhant was supervised by Prof Aditya Mathur and collaborated closely with Research Assistant Sridhar Adepu on designing a Layered Defence for CPS, which was first presented as a poster at the Singapore Cybersecurity Conference (SG-CRC) in Jan 2016.

The idea of orthgonally defending a CPS using a parallel pervasive monitoring mechanism ("Argus") was tested on the SWaT testbed. The findings proved that a wide array of attacks (even insidious insider attacks) could be detected by Argus, results of which will be published in IEEE Internet Computing. Whilst at iTrust, he even mentored a student from Nanyang Polytechnic to create a web interface for 'Argus'.

Siddhant also got the opportunity to analyse the BlackEnergy malware that was attributed to the Ukraine blackouts in 2015, and drafted a corresponding report on "Malware for Cyber-Physical Attacks".

Siddhant's stint at iTrust enabled him to receive a student scholarship to attend BlackHat Asia 2016.

Profiles

Arlindo Silva

Arlindo has a PhD in Mechanical Engineering and 25 years of teaching and research experience. He started his career at the Dept. of Mechanical Engineering, University of Lisbon (UL), Portugal, where he taught Materials, Design and other Engineering related topics at all levels of higher education before moving to Singapore in 2015.

He has written three books and co-edited another two, published over 100 articles in journals, conferences and book chapters, and filed over 50 patents with his students on innovative designs. His current research interests rest on engineering design, product development, creativity, materials selection methodologies, cost modelling and management of uncertainty in design. He received the MIT-Portugal Education Innovation Award in 2009 and was a Professor of Excellence at UL in 2011, 2012 and 2014. He was also a Senior Materials Education consultant at

Granta Design Ltd, Cambridge, UK, and is an active member of PDMA, ASEE, DS and SPEE.

He is currently an Associate Professor with the Singapore University of Technology and Design, Engineering Product Development Pillar, where he teaches Introduction to Design, and the SUTD-MIT International Design Centre, where he co-leads the Experimental Design Thrust.

Yuen Chau

Dr Chau Yuen received the BEng and PhD degree from Nanyang Technological University (NTU), Singapore, in 2000 and 2004 respectively. 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 twice the recipient of Hewlett Packard Prize.

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 to 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 Associate Editor for IEEE Transactions on Vehicular Technology, and awarded as Top Associate Editor from 2009 – 2015. He has filed five patents and published over 300 research papers at international journals or conferences.

Jemin Lee

Dr Jemin Lee, the principal investigator (PI) for the research project “Network Engineering Techniques for Wireless Security” has returned to her native South Korea.

In her time with iTrust, she developed physical layer security techniques for cellular networks and smart grid networks, and also proposed new security frameworks for emerging networks such as IoT and Fog networks. While leading the project in iTrust, she submitted more than 20 papers to top journals and conferences. For her contribution to wireless communication and security, she also received IEEE ComSoc Outstanding Young Researcher Award in 2014.

Jemin is now an Asst Prof with the Daegu Gyeongbuk Institute of Science and Technology (DGIST). We wish her all the best in her career! Asst Prof Tony Quek, from SUTD’s Information Systems Technology and Design (ISTD) pillar, has agreed to take over the reins as PI for the project.

Jemin Lee (right) with iTrust Research Director Prof Yuval Elovici

Publications

Network Engineering Techniques for Wireless Security

1. C. Cheng, J. Lee, T. Jiang, and T. Takagi, “Security analysis and improvements on two homomorphic authentication schemes for network coding,” IEEE Transactions on Information Forensics and Security, vol. 11, no. 5, pp. 993-1002, May 2016
2. C. D. T. Thai, J. Lee, and T. Q. S. Quek, “Secret group key generation in physical layer for mesh topology” in Proc. IEEE Global Commun. Conf., San Diego, CA, Dec. 2015, pp. 1-6
3. C. D. T. Thai, J. Lee, and T. Q. S. Quek, “Physical-layer secret key generation with colluding untrusted relays,” IEEE Transactions on Wireless Communications, vol. 15, no. 2, pp. 1517-1530, Feb. 2016
4. C. D. T. Thai, J. Lee, C. Cheng, and T. Q. S. Quek, “Physical-

5. layer secret key generation with untrusted relays" in Proc. IEEE Global Commun. Conf., Workshop on Trusted Communications with Physical Layer Security, Austin, TX, Dec. 2014, pp. 1–6
6. F. Wang, X. Yuan, J. Lee, and T. Q. S. Quek, "Wireless MIMO switching with trusted and untrusted relays: degrees of freedom perspective," in Proc. IEEE Int. Conf. Commun., London, UK, Jun. 2015, pp. 1-6 J. Lee and T. Q. S. Quek, "Device-to-device communication in wireless mobile social networks," in Proc. IEEE Semiannual Veh. Technol. Conf., Seoul, Korea, May 2014
7. J. Lee, J. Ryu, C. D. T. Thai, J. Wang, F. Wang, and T. Q. S. Quek, "Friends or foes – the design of confidential cooperative communication with untrustworthy relay," IEEE Commun. Mag.
8. J. Ryu, J. Lee, and T. Q. S. Quek, "Confidential cooperative communication with trust degree of potential eavesdroppers," IEEE Transactions on Wireless Communications
9. J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Secure communication via jamming in massive MIMO Rician channels" in Proc. IEEE Global Commun. Conf., Workshop on Massive MIMO: From theory to practice, Austin, TX, Dec. 2014, pp. 1–6
10. J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," IEEE Trans. Wireless Commun., vol. 14, no. 12, pp. 6854-6868, Dec. 2015
11. Jong Yeol Ryu, Jemin Lee, and Tony Q. S. Quek, "Trust degree based beamforming for MISO cooperative communication system," IEEE Communications Letters, vol. 19, no. 11, Nov. 2015
12. L. Q. Duy, T. Q. S. Quek, and J. Lee, "A game theoretic model for enabling honeypots in IoT networks," in Proc. IEEE Int. Conf. Commun. (ICC), Kuala Lumper, Malaysia, May 2016
13. P. Mohapatra, N. Pappas, J. Lee, T. Q. S. Quek, and V. Angelakis, "Stability region of 2-user full-duplex broadcast channel with secrecy constraint," in Proc. IEEE Int. Conf. Commun. (ICC), Kuala Lumper, Malaysia, May 2016
14. R. Hsu, J. Lee, and T. Q. S. Quek, "Reliable and Privacy Preserving Secure D2D Communication in LTE-A,? in Proc. ACM Int. Conf. on Security and Privacy in Wireless and Mobile Networks, New York, NY, Jun. 2015
15. R.-H. Hsu, J. Lee, T. Q. S. Quek, and J.-C. Chen, "GRAAD: Group anonymous and accountable D2D communication in mobile networks," IEEE/ACM Transactions on Networking
16. R.-H. Hsu, J. Lee, T. Q. S. Quek, and J.-C. Chen, "ReSIoT: Reconfigurable security for IoT," IEEE Wireless Communications
17. S.-Y. Chang, J. Lee, and Y.-C. Hu, "Noah: Keyed noise flooding for wireless confidentiality," in Proc. ACM Symposium on QoS and Security for Wireless and Mobile Networks (Q2SWinet), Cancun, Mexico, Nov. 2015, pp. 141- 148

Advancing Security of Public Infrastructure using Resilience and Economics

1. Jawaid F., and Junejo K. N., "Predicting Daily Mean Solar Power Using Machine Learning Regression Techniques," accepted in 6th International conference on Innovative Computing Technology (INTECH) 2016, Ireland
2. Zuberi F. A., Khatri S., and Junejo K. N., "Dynamic Gesture Recognition using Machine Learning Techniques and Factors Affecting its Accuracy," accepted in 6th international conference on Innovative Computing Technology (INTECH) 2016, Ireland
3. Muhammad W., Mushtaq M., Khan M. Y., and Junejo K. N., "Comparative Study of Supervised and Unsupervised Machine Learning Approaches for Sentiment Analysis of Product Reviews," accepted in 6th international conference on Innovative Computing Technology (INTECH) 2016, Ireland
4. Nguyen H. H., Tan R., Yau D. K. Y,, "Collaborative Demand-Response Load Management with Safety Assurance in Smart Grids," ACM Transactions on Cyber-Physical Systems
5. Goh J., Adepu S., Junejo K. N., and Mathur A., "A Dataset to Support Research in the Design of Secure Water Treatment Systems," The 11th International Conference on Critical Information Infrastructures Security
6. Adepu S., and Mathur A., "An Experimental Investigation into Detecting Cyber Attacks on a Water Treatment System Using Process Invariants," 7th International Conference on Cyber-Physical Systems (ICCPS)
7. Adepu S., Shrivastava S., and Mathur A., "Argus An Orthogonal Defense Framework," IEEE computing magazine, Cyber Physical Security and Privacy Joint Special issue with IEEE intelligent Systems
8. Murguia C. and Ruths J. "Characterization of a CUSUM Model-Based Sensor Attack Detector," IEEE 55th Conference on Decision and Control
9. Komareji M., Shang Y., Chamambaz M., Bouffanais R., "Consensus in networked multiagent systems under communication constraints, time-delays and dynamically changing topologies," IEEE Transactions on Control of Network Systems
10. Rocchetto M. and Tippenhauer N. O., "CPDY: Extending the Dolev-Yao Attacker with Physical-Layer Interactions," ICFEM 2016
11. Murguia C. and Ruths J. "CUSUM and x2 Attack Detection of Compromised Sensors," Multi-conference on Systems and Control 2016
12. Rocchetto M. and Tippenhauer N. O., "Extending the Dolev Yao Attacker with Physical Layer Interactions," Computer Security Foundation 2016
13. Ahmed C. M., Adepu S., Mathur A., "Limitations of State Estimation Based Cyber Attack Detection Schemes in Industrial Control Systems," Smart City Security and Privacy Workshop (SCSP-W) CPS Week 2016
14. Rocchetto M. and Tippenhauer N. O., "On Attacker Models and Profiles for Cyber-Physical Systems," ESORICS 2016 (European Symposium on Research in Computer Science)
15. Rocchetto M. and Tippenhauer N. O., "On Attacker Models for Cyber-Physical Systems,"Singapore Cyber Security R&D Conference 2016

iTrust Matters

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. 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 the relevant 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
iTrust 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

Ms TAO Yuxuan
Manager, ST Electronics-SUTD Cyber Security Lab
yuxuan_tao@sutd.edu.sg

iTrust
Center for Research in Cyber Security

itrust.sutd.edu.sg