An iTrust Newsletter Jul - Sep 2017 | Issue 10

iTrust Times

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

From Centre Director's Desk

Participants at Day 1 & 2 of Think-in Session at the 3rd Secure Cyber-Physical (SCy-Phy) Systems Week 2017

Dear Reader:

Greetings from iTrust!

Welcome to the 10th issue of iTrust Times. This issue offers you a glimpse into several events that took place during summer. iTrust organised the third annual Secure Cyber Physical Systems (SCy-Phy) week. Once again, this event was well attended. I sincerely thank Rear Admiral Harris Chan for opening the week with his remarks at the start of the Think-in session. This was followed by an excellent keynote talk by Neil Hershfield from the U.S. Department of Homeland Security. Thank you Neil for taking time off from your regular duties and flying all the way to Singapore to deliver your keynote.

This year's SUTD Security Showdown (S3-17) – a highlight of the SCy-Phy Week – was planned carefully by a large group of faculty and staff led by Professor Nils Tippenhauer. Five teams from four countries participated in the competition. Data collected during S3-17 is currently under analysis. A detailed report will be available at the iTrust website.

The first phase of iTrust comes to an end in February 2018. iTrust faculty and staff participated in a half-day brainstorming session to discuss research focus in iTrust Phase II. Government representatives from CSA, GovTech, MINDEF, NRF, EMA, and IMDA, as well as several from industry, participated in this session. We expect iTrust II to aggressively forge ahead in its quest to create methods and tools to design highly resilient Critical Infrastructure as well as CPS such as maritime and land transport infrastructure.

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

Best wishes,

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

In This Issue

- Secure Cyber-Physical (SCy-Phy) Systems Week 2017
- SUTD-TU Delft workshop
- Launch of Electric Power & Intelligent Control testbed
- iTrust brainstorming session

Events

"If you have an apple and I have an apple and we exchange these apples then you and I will still each have one apple. But if you have an idea and I have an idea and we exchange these ideas, then each of us will have two ideas," said George Bernard Shaw, an Irish playwright.

Such exchanges were aplenty at the third instalment of the **Secure Cyber-Physical (SCy-Phy) Systems Week,** which ran from 5 to 9 June, and featured 14 panellists from the U.S., Europe, Asia and Singapore, including Mr Neil Hershfield, from ICS-CERT at the U.S. Department of Homeland Security, as the keynote speaker. Since the first run of SCy-Phy in 2015, iTrust has invited 35 local and international cyber security professionals from government agencies, academia and industry as panellists during the Think-in sessions. This year, iTrust's signature event is supported by the **Ministry of Defence (MINDEF)** along with the **SUTD-MIT International Design Centre (IDC)**.

Even as Think-in was extended to two days this year, there was no shortage of topics to discuss, speakers to invite, and opportunities for deep and intense discussions. Seven sessions were designed, up from four from the previous years: Threats, Interconnected Systems, Models, Defences, Translating Research to Industry, an IDC Micro-Design Experience and Lightning Talks on iTrust Research Projects. In total, more than 130 attendees participated in the various sessions.

In his opening address, **Rear Admiral Harris Chan,** Future Systems and Technology Architect, MINDEF, noted that alongside technology advancements cyber threats have evolved in a non-linear and unpredictable manner and across "every physical domain across land, sea, air, and even space." In opening the Think-in sessions, he acknowledged the significance of "collaboration not only between national security agencies, but also amongst individuals and businesses to strengthen our collective capabilities in cyber security." To this end, a hopeful result is a "tight network (of international cyber security counterparts) to police, counter and prevent cyber security threats worldwide."

RADM Harris Chan at his opening address

"From a security perspective, crime and warfare has become even more non-linear and unpredictable since cyber threats can transcend physical boundaries."

RADM Harris Chan, Future Systems and Technology Architect, MINDEF

Keynote Address

Mr Neil Hershfield's keynote address **"Managing Cyber Risks"** set the tone for the two days of discussions. In it, he presented a worldwide threat assessment where cyber attacks have hit critical sectors such as education, healthcare, and finance, and in which the threat actors range from non-state (individuals, small groups, criminals), terrorists, to state. Regardless of their motivations behind the attacks, Neil noted that while cyber threats cannot be eliminated, cyber risk must be managed. Echoing RADM Chan on the increasing sophistry of cyber attacks, Neil shared how adversaries are becoming more advanced in their modus operandi. Expenditure in cybersecurity is forecast to at least double by 2020 (compared to the 2015 figures) thus supporting the need for risk management. He then gave an overview of the ICS-

Neil Hershfield on ICS-CERT's cyber risk management strategies

CERT's mission in risk reduction and response and recovery operations in the event of a cyber incident, and encouraged the use of ICS-CERT's resources including advisories, courses and reports.

"Ransomware...is going to be growing in the ICS space, and is grower faster than we originally thought."

Neil Hershfield, Deputy Director, ICS-CERT

Session 1: Threats

Mr Lim Soon Chia, Director of Technology at the Cyber Security Agency (CSA) of Singapore presented **Singapore's cyber security threat landscape** that has grown alongside Singapore's digital transformation. These emerging threats have necessitated a cyber security strategy spanning four areas to continue to keep Singapore safe: building a resilient infrastructure; creating a safer cyberspace; developing a vibrant cybersecurity ecosystem; and strengthening international partnerships.

Exploring two sides of the same coin, **Ms Marina Krotofil**, a cyber security researcher at Honeywell Industrial Cyber Security Lab, opined that there were some **threats that were *unlikely* to occur in the near future**. Such threats include complex cyber physical attacks – as high engineering precision and a high level of coordination, time and effort are required – and attacks that require a feedback loop, to ensure that the intended effects of the attacks are actually realised.

Session 1 panellists Lim Soon Chia (left) and Marina Krotofil (right) share on their threats assessment and management

Session 2: Interconnected Systems

To assess the **risks that operators of cyber physical systems face, Prof David Nicol** of the University of Illinois at Urbana–Champaign argued that a system model – containing that of the physical system, cyber-based control (and their connections) and the attacks on control – needs to be constructed first. This involves identifying touch points between cyber and physical systems and characterising how the connections between the cyber and physical systems (i.e. actuators) change the state of the physical system etc. Such a model would then provide a predictive assessment of the system thus allowing stakeholders an overview of a baseline vulnerability of their existing CPS, evaluate the effectiveness of new cyber defenses, and compare cost and effectiveness of alternative mediation strategies, among other things.

(From left to right) Session 2 panellists David Nicol, Sahra Sarvestani and Robert Kooij on security of interconnected CPS

Critical infrastructure (CI) (e.g., power and water plants) face the triple challenges of added complexity, interdependency, and vulnerability which can lead to degradation due to failure propagation channels. In view of the **interdependencies among CPS, Assoc Prof Sahra Sedigh Sarvestani** of Missouri University of Science and Technology stressed the importance of studying the effects of component failure on the system to determine how each failure impacts the system's functionality, and whether the failure can cascade to other components, both from the point of view of dependability and security. **Prof Robert Kooij** of TNO South East Asia deep dived into **interdependent CIs by exploring their interconnected and interacting networks**, for example, between communication networks and power networks. His simulation studies showed that, beyond a threshold of the fraction of nodes that are removed as a result of a cyber attack, the resulting cascade failure starts to escalate. From these results, he posited that a system-of-systems approach would help CI designers and operators better understand inter-dependencies and mitigation responses to cyber attacks.

Session 3: Models

To say that **modelling and model checking of a CPS** requires considerable effort is an understatement. The task is made much more tricky when taking security into consideration. In his presentation **Prof Sjouke Mauw** from the University of Luxembourg lists some of these enduring and evolving difficulties, despite the recent progress in overcoming them including available computing power. Some difficulties include the state-explosion problem for finite state concurrent systems (especially in large and complex ICS), model checking security of hybrid systems as well as compositional verification (from compositing two previously secured isolated protocols), and the integration of human behaviour into the so-called "Physical-Cyber-Social System."

Asst Prof Alvaro Cardenas from the University of Texas at Dallas took the approach of developing **adversary models in ICS**, such as deception attacks where an attacker changes the sensor measurement forcing the controller to make the wrong decision. In trying to develop stronger adversary models, Alvaro stressed the importance of the "...need to be pessimistic with (the performance of) our models," in the hope "that in reality the adversary will never match our worst case scenario, and therefore, we expect our systems to perform better in practice than in our pessimistic assessments."

(From left to right) Session 3 panellists Sjouke Mauw, Alvaro Cardenas and Dieter Gollmann on CPS modelling

In performing a **model-based security analysis of CPS**, one needs to understand and familiarise with an attacker's perspective so that potential gaps and attack paths can be identified and closed. In his presentation **Prof Dieter Gollmann** (Hamburg University of Technology) highlighted two key challenges. First, since a CPS model cannot be perfect there will exist gaps, unknown to the operator, between the model and the actual system thus enabling attackers to launch an attack. Second, identifying attacks based on the assumption that an attacker does not have a full picture of the system may turn out to be infeasible, since specific features of the system under analysis may not have been captured. Furthermore, incorporating these insights when performing a model-based security analysis tends to be devilishly complex.

Session 4: Defences

Assoc Prof Mauro Conti (University of Padua) called for and shared new solutions to **secure industrial IoT**. In remote attestation, the Secure and Scalable Aggregate Network Attestation (SANA) protocol can be adopted to verify the integrity of a network of interconnected devices (via "swarm attestation") within realistic constraints. Updating software in IoT devices presents a different challenge as a far larger number of deployed devices need patching. "Updaticator", an efficient, scalable and secure software update distribution may help. FlowFence requires companies (that develop apps that collect sensitive data) to only use the data in an intended manner (i.e. intended flow patterns), and in doing so, protects consumers' privacy. **Asst Prof Gerhard Hancke** (City University of Hong Kong) discussed the transfer of promising software and hardware technologies from mobile computing and smart cards space for use as a **hardware security platform for IIoT**. Three technologies were presented: Rich mobile OS offers an open and versatile environment upon which software can be developed. Trusted Execution Environment (TEE), a secure area of the main processor, ensures confidentiality and integrity of sensitive data within, thereby ensuring a higher level of security than provided by the rich mobile OS. While a TEE has more functionality than an Secure Element (SE), the latter offers

(From left to right) Session 4 panellists Gerhard Hancke, Mauro Conti and Biplab Sikdar on security and defences

a higher level of protection due to the tamper-resistant platform that is capable of running secure applications and storing cryptographic data. Moving to defences in CPS, **Assoc Prof Biplab Sikdar** (National University of Singapore) proposed the use of **physical laws to detect anomalies and attacks.** He presented these in the context of a power grid and water distribution system. Highlighting several limitations, he also called for complementary mechanisms such as intrusion detection, redundancy and hardware isolation for critical logical components to be put in place.

Session 5: Translating Research to Industry

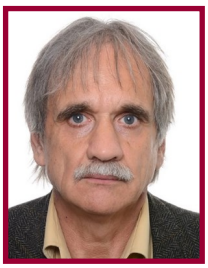
In an effort to encourage the translation of useful and feasible research results into commercial(isable) products, this panel was created and industry experts invited to share their insights. **Dr Jorge Cuellar** (Siemens AG) sees future research directions, applications and corresponding challenges in the areas of privacy and security, including Privacy-Enhancing Technologies (PET) in IoT devices, tokens for authorisation (among other applications), and local reasoners. Some of these challenges include the authentication of devices against each other, efficiency and energy consumption vis-à-vis security mechanisms and enforcement of restricted workflows (to prevent abuses). As a security solutions company, Secure-IC has more than 15 years of research experience in hardware, CPS and IoT security. **Mr Matthieu Lec'Hvien** presented some of the research at the company, use cases in the CPS and mobile space, as well as its experience with industrialisation of these technologies into products that help protect its clients against cyber attacks. He also highlighted the use of machine learning to accelerate evaluation of the research results.

(From left to right) Session 5 panellists Jorge Cuellar, Matthieu Lec'Hvien and David Ong share their experience on research translation

Mr David Ong (Excel Marco, a local solutions provider of process automation and safety systems) provided an overview of his company's experience in the adoption of cyber security in its systems, and its recent collaboration with iTrust in cyber security research. David sees these two parties as a "marriage of researchers who have the knowledge of the latest know-how and their applications in the real world and the actual adopters to use, give feedback, and refine on the technologies."

Invited Talks

Four Think-in panellists were invited to give a more in-depth talk in their research domain on 7 and 8 June. **Prof Dieter Gollmann** discussed the current state of research on employing **Brain Computer Interfaces (BCI) for user authentication**, with a particular focus on the feasibility of using cheap gaming headsets in this context along with its challenges. He also described how BCI could serve as a subliminal channel out of the brain and its underlying privacy implications. Social scientists, market researchers, and public institutions make use of anonymised social network graphs - generated from the collection of data from online social networks - for research and market evaluation, among other things.



Prof Dieter Gollmann

Prof Sjouke Mauw

Through his talk, **Prof Sjouke Mauw** explained why **anonymised social network graphs continue to be vulnerable** to attacks on the privacy of users, and discussed strategies to measure and mitigate this loss of privacy. Based on her study of recent attacks in Ukrainian infrastructures such as power substations, airports and banks, **Marina Krotofil** provided an overview of a **typical attack time-line**, which is derived from real-world forensic investigation. She shared some techniques used by the attackers to overcome perimeter protections using backdoor attacks, revealing the increase

Ms Marina Krotofil

Assoc Prof Sahra Sarvestani

in their competence and capabilities. **Assoc Prof Sahra Sarvestani's** presentation on **"Model-Based Fortification of Large-Scale Cyber-Physical Systems"** touched on survivability analysis as a means to quantify and predict service degradation caused due to a malfunction or security breach. Doing so helps stakeholders make investment decisions on strengthening CPS, and targeted fortification of these components enables continual, if partial, delivery of critical services.

Outreach Workshop

By Sita Rajagopal and Elaine Cheong

An outreach workshop on **Cyber Security Essentials** was organized for students from secondary schools, junior colleges, polytechnics and the Institute of Technical Education (ITE). The workshop was held on 7 and 8 June at SUTD's Learning Environment for Experimental Technology (LEET) laboratory and attended by 80 students. As cyber threats have become more prevalent than ever, the workshop aimed to raise awareness about these dangers to students and remind them to remain vigilant.

Led by Research Assistants Franscisco Furtado and Toh Jing Hui and assisted by SUTD students, topics covered in the workshop included Advanced Computing, Ciphers and Cyber Threats. In the Advanced Computing segment, students learnt how to utilise Windows Command Prompt and introduce the Command Line Interface. Cisco's Packet Tracer was used as a teaching tool to create awareness of basic wired and wireless networking knowledge. Students were then introduced to common cyber threats such as password cracking, Distributed Denial of Service (DDoS) Attacks and Cross-Site Scripting (XSS) vulnerabilities.

The workshop ended with a tour of iTrust's Cyber-Physical Systems and Internet-of-Things (IoT) Automatic Security testbeds, to gain first hand account of how iTrust's research work is validated and translated to useful commercial products.

Students trying out one of the many hands-on exercises during the workshop

SUTD Security Showdown '17 (S3-17)

Verizon's Data Breach Digest 2017[1] described how a water treatment plant in March 2016 suffered a cyber attack in which hundreds of PLCs controlling the valves and ducts were manipulated to change the dosing levels of chemicals used to treat tap water. The attackers gained access through the plant's online customer paying portal. Post-mortem analysis showed that SQL injection and phishing techniques were used in the attack. Yet, many more attack vectors remain unknown.

It is with such "unknown unknowns" that the second round of the two-day S317— a hands-on cyber security event— returned to SCy-Phy Systems Week on 8 and 9 June. This security exercise is intended to help researchers discover hitherto unknown attack models so that they can strengthen their defence and design a resilient CPS. Through an "online phase" the organisers shortlisted five finalists comprising of four from universities (Lancaster, Oxford, TU Graz and TUM) and one from a company (Good Hackers Alliance), for the "live phase." The teams flew into Singapore a week before S317 for the "exploration phase"

[1] http://www.verizonenterprise.com/verizon-insights-lab/

One of the S317 judges Nils Tippenhauer (left) with the team from Oxford as they conduct reconnaissance on SWaT

to conduct reconnaissance on the Secure Water Treatment (SWaT) testbed. Each team was given two hours during the "live phase" to demonstrate their attacks to the judges. Concurrently, several detection mechanisms from academia and industry were installed to try to (passively) detect and report the attacks as they happened. A scoring system for the attackers was used to determine which team was most successful in its attacks.

iTrust's defence mechanism, the Water Defence Historian, detecting attacks (red boxes) as they occur

After two days of intense competition GHA claimed first place in the event. They were followed by TU Graz (runner up) and TUM (third place). A detailed report will be made available on iTrust's website in the coming months.

The winning team (GHA) for S317, together with judges (back row, left to right) Martin Ochoa and Nils Tippenhauer, and (front row, second from right) iTrust Centre Director Aditya Mathur

Research Focus

Launch of EPIC testbed

The completion of the Electric Power and Intelligent Control (EPIC) testbed in March 2017 adds to the stable of testbeds— the water treatment (SWaT) and distribution (WADI), and IoT testbeds—in iTrust. Funded by the Ministry of Defence (MINDEF) Singapore and the SUTD-MIT International Design Centre (IDC), EPIC serves as an important platform for researchers to investigate the precipitating effects of cyber attacks on upstream CPS to other CPS in its network. Already, a student intern has done preliminary work on attack models for EPIC, and visiting researchers from Missouri University of Science and Technology are working on understanding the information paths of EPIC with the aim of enhancing the cyber-physical security of the EPIC infrastructure using the Multiple Security Domain Nondeducibility (MSDND) model.

The EPIC testbed was officially opened on 22 May 2017, suitably by the Chief Executive of the Energy Market Authority (EMA) of Singapore, Mr Ng Wai Choong. Together with him were Deputy Chief Executives Mr Kng Meng Hwee (Industry Regulation Division and Power System Operation Division) and Mr Bernard Nee (Energy Planning & Development Division and Corporate Services Group). The group was hosted by SUTD President Prof Tom Magnanti, IDC Co-Director Prof Kristin Wood, and iTrust Centre

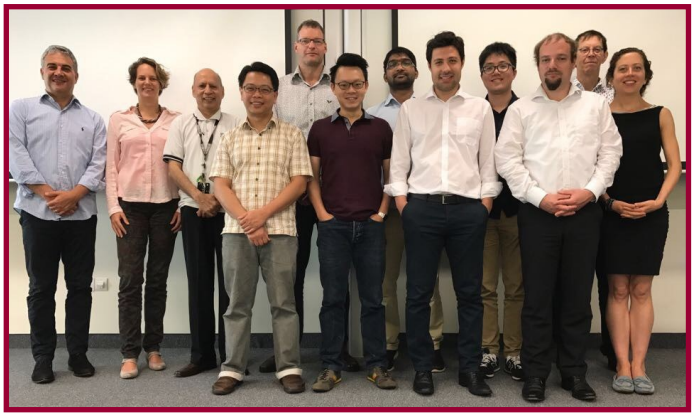
SUTD President Prof Tom Magnanti (right) presenting a plaque to EMA Chief Executive Mr Ng Wai Choong

Director Prof Aditya Mathur, who provided the visitors with a tour of the testbed and an understanding of how EPIC, along with other testbeds, could facilitate research that leads to designs of a more resilient and secure power plant.

SUTD-TUD Workshop

Even as Wilco's Jeff Tweedy sighed that "distance has no way of making love, understandable", this is not so for two like-minded universities wishing to foster a closer research relationship. Hailing from countries at the vanguard of cybersecurity and innovation, and which are more than a distance apart (a quarter of the Earth's circumference, to be exact), SUTD and Delft University of Technology (TUD) gathered for a workshop in Singapore on 29 and 30 June 2017. Co-organised byProf Robert Kooij of Delft University of Technology (TUD) and Prof Aditya Mathur, Head of Pillar at SUTD's Information Systems Technology and Design (ISTD) pillar, the aim of this workshop was to kick-off the SUTD-TUD 2+2 PhD programme, in which a PhD student each from SUTD and TUD will jointly work on a project and supervised by faculty members from both universities.

SUTD's faculty members included Prof Aditya Mathur, Assoc Profs Tony Quek and Sun Jun, and Asst Prof Nils Ole Tippenhauer. TUD's cybersecurity delegation was led by Prof Inald Lagendijk, Chair of the Computer Science Department of Intelligent Systems at TUD. Ms Elsbeth Nijhuis, project manager innovation from the Embassy of the Kingdom of the Netherlands also joined in.



Participants at the SUTD-TUD Delft workshop: (back row, left to right) Inald Lagendijk, Elsbeth Nijhuis, Aditya Mahutr, Robert Kooij, Sridhar Adepu, Qin Lin, and Pieter Hartel, (front row, left to right) Shaowei Lin, Mark Goh, Mauricio Aniche, Christian Doerr, and Eveline Vreede

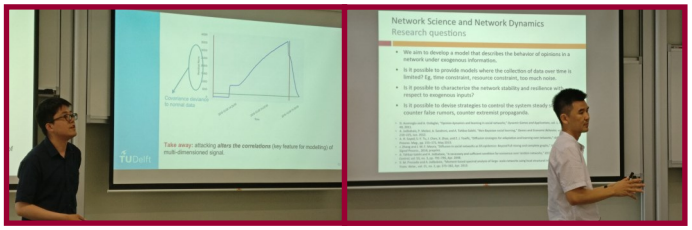
To kick start the workshop, Prof Aditya Mathur and Prof Pieter Hartel, head of TUD's Cyber Security Group, gave an overview of the cybersecurity research efforts at their respective universities.

Four project proposals were presented over two days; each project was proposed jointly by a faculty member from SUTD and TUD and the audience was invited to give their feedback to strengthen the proposal. On the first day, Asst Prof Nils Ole Tippenhauer and Dr Christian Doerr, Assistant Professor at TUD's Cyber Security Group, presented "Advanced Analytics for ICS honeypots". Nils had separately worked on MiniCPS - a lightweight real-time network emulation of a CPS - and IoT honeypots (IP cameras acting as honeypots to induce attackers to hack into them so as to enable gathering of different attack models). Together with Christian, they proposed a merger of these two technologies to grow the list of attack models on CPS. This would also help the research community and industry to better understand potential attacks on CPS.

(Left to right): Christian Doerr, Asst Prof Nils Tippenhauer and Dr Mauricio Aniche present their proposal on CPS research

Assoc Prof Sun Jun and Dr Mauricio Aniche, Software Engineering Researcher at TUD, proposed the innovative use of formal methods and machine learning to improve verification of access controls in CPS, and by doing so improve the privacy of software systems. Their approach also seeks to improve the privacy of systems with a focus on its application to CPS.

On the second day of the workshop, PhD students Sridhar Adepu (SUTD) and Qin Lin (TU Delft) proposed to develop methods that capture the SWaT system state from physical and network data in interpretable models such as Markov chains and state machines. Both the physical and network data are then conditioned on model states representing normal operating conditions of the system (e.g., water filling in a tank or chemical properties of water such as pH), thus providing the ability to detect anomalies such as irregular valve changes, or exchanges of network packets between hosts that normally do not communicate under the current system state. In doing so, they aimed to improve the attack detection accuracy while limiting false positives.



(Left to right): TUD PhD student Qin Lin and Assoc Prof Tony Quek present their research ideas

The proliferation of fake news and extremist propaganda in social networks at its worst can lead to mass hysteria and social unrest. This prompted Assoc Prof Tony Quek and TUD's Prof Piet van Mieghem to propose an approach to model describing the behaviour of opinions in a network under exogenous information and devise strategies to control and counter false rumours and extremist propaganda.

The candid exchanges brought forth fresh ideas for the proposals. Upon further refinements and discussions among the project teams, both universities will together decide which complementary research projects to collaborate on.

iTrust Brainstorming Session

At the ideation phase of Design Thinking, a design methodology for solving complex problems, practitioners are taught to encourage wild ideas as they can often give rise to creative leaps, as well as to build on the ideas of others. In this, Linus Pauling, a chemist and a two-time Nobel Prize winner had already recognised such benefits when he said: "The best way to have a good idea is to have lots of ideas."

Fresh from research discussions during SCy-Phy Systems Week, iTrust organised a brainstorming session on 23 June to solicit research ideas and focus on cyber security as it moves towards its next phase of growth. This is not a closed group discussion; iTrust's close collaborators from thirteen government agencies and industry were there to share their insights on future needs.

Having presented where iTrust is now, its landmarks and achievements, Prof Aditya Mathur invited SUTD faculty members who are involved in cyber security research to present their current work and new research ideas, and solicit feedback. Topics presented ranged from cyber security in traditional and non-traditional CPS (ICS, maritime, and land transport) to autonomous vehicles, artificial and swarm intelligence, IoT and smart manufacturing.

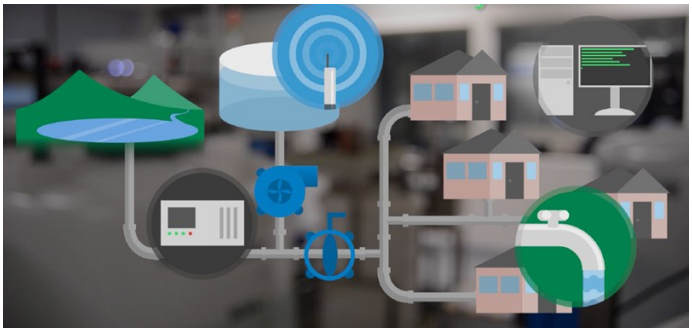
Aditya presenting iTrust's past and future five years

A thrust-technology matrix matched research thrusts to technologies proposed to address issues in those thrusts. Feedback and discussion points are being distilled into a research proposal. iTrust thanks all participants for their contribution towards designing and building a more secure future!

Conferences

World Environmental & Water Resources Congress 2017

By Stefano Galelli



BATADAL is a competition jointly organised by iTrust (Dr Riccardo Taormina, Asst Profs Stefano Galelli and Nils Ole Tippenhauer), Technion—Israel Institute of Technology (Prof Avi Ostfeld) and Optiwater (Mr Elad Salomons). The goal is to objectively compare the performance of algorithms for the detection of cyber attacks on water distribution systems. The need for such comparison stems from the increasing number of cyber attacks launched against the monitoring and control systems of water utilities—as recently reported by the U.S. Department of Homeland Security ICS-CERT (2016). BATADAL ran from September 2016 to May 2017 and saw the participation of seven teams from both academia and industry.

The competition followed a phased approach, consisting of calibration, testing and result announcement. In Fall 2016, the participants received the competition rules and calibration datasets, containing information about the operation of a benchmark water distribution system (e.g., water flows, pressures) under normal and attack conditions. The data were generated with epanetCPA¬, a software toolbox recently developed at SUTD to simulate the response of water networks to cyber-physical attacks (Taormina et al., 2017). In February 2017, the organisers released the test dataset, which contains a handful of new, unlabelled attacks. The performance of all algorithms was then assessed in terms of timeliness and accuracy (i.e., the capability of detecting attacks, without issuing false alarms). Results and final team ranking were presented at the Annual Water Distribution Systems Analysis Symposium, World Environmental & Water Resources Congress—held in Sacramento, California, on May 21-25 (2017).

The organisers and participants are now in the process of preparing a jointly-authored manuscript for the Journal of Water Resources Planning and Management. Future developments may include a new battle (with data provided by water agencies) and the setup of an online repository for algorithms and data. Additional details about BATADAL are available at www.batadal.net.

The 2017 IEEE International Conference on Software Quality, Reliability & Security (QRS)

A bumper crop of five papers – co-authored by Prof Aditya Mathur, PhD students Sridhar Adepu, Chuadhry Mujeeb Ahmed, Jay Prakash and Gayathri Sugumar and visiting student Gyanendra Mishra – were accepted at QRS 2017. Sridhar, Mujeeb and Gayathri presented these papers at the conference in Prague in July.

Research in security of cyber physical systems is focused on threat models where an attacker can spoof sensor readings by compromising the communication channel. Mujeeb's work on **"Hardware Identification via Sensor Fingerprinting in a Cyber Physical System"** proposed a method to detect potential attacks on physical components in a CPS. Physical attacks are detected through a comparison of noise pattern from sensor measurements to a reference noise pattern (a "fingerprint"); any deviation from this fingerprint suggests that a sensor is probably compromised or is defective. Extensive experimentation with ultrasonic level sensors in the SWaT testbed points to the effectiveness of the proposed fingerprinting method in detecting physical attacks. Gayathri's paper on **"Testing the Effectiveness of Attack Detection Mechanisms in Industrial Control**

Systems" detailed an approach using Timed Automata to assess the effectiveness of an attack detection mechanism based on process invariants. In a case study, one stage of the SWaT testbed was simulated through a network of models for plant components along with an attack detection mechanism to test their effectiveness against various cyber attacks.

Sridhar Adepu presented three research papers. The first, co-authored with Gyanendra Mishra, **"Access Control in Water Distribution Networks",** highlights inadequacies in access control in CPS that allow malicious entities to compromise system security. The study will to lead to guidelines for secure access control implementation in CPS. The second paper, co-authored with Jay Prakash, focuses on how **jamming attacks** can be performed on ICS and their impact. The observed response to various attacks was then used to propose attack detection mechanisms. The third paper is **"From Design to Invariants: Detecting Attacks on Cyber Physical Systems"**, which proposes an approach to derive state-based invariants that proved to be effective in detecting cyber attacks on a Cyber Physical System (CPS). The proposed approach begins with the CPS design and models its process dynamics using extended hybrid automata from which the invariants are derived. The invariants are active during CPS operation and serve to check on the validity of the system state in accordance with the system design. This approach was evaluated on a fully operational six-stage water treatment plant (SWaT) that uses a distributed process control system.

CommunicAsia 2017

On 23 May 2017, Prof Yuval Elovici, iTrust' Research Director, shared preliminary research results in "Detecting Compromised IoT Devices" under the track "Security of Things: Threat-proofing the Future with Agility and Resilience" at CommunicAsia 2017. Early results showed that compromised IoT devices were detected based on the developed algorithms on machine learning techniques applied on IP network traffic.

Visits

By Mark van Staalduinen, Innovation Manager, TNO

TNO's COO Mr Wim Nagtegaal, leading a delegation of young researchers from TNO, visited SUTD on 20 April as part of their study tour to Singapore. At iTrust's CPS testbeds, it was very impressive to see how the small scale albeit realistic representations of physical systems such as water processing and power facilities are used by SUTD's researchers to put the cyber security of those systems to the test.

Following the testbed tour, four TNO researchers gave short lectures on topics spanning from health to clean energy, chemistry and naturally, cyber security. The first encouraged the adoption of the power of sensors to improve health and work conditions. The second shared on the application of TNO's solar technology in less-than-conventional places including roads and building facades. The third presenter showed how electrochemistry can play a part in a circular economy, where resources are kept in use for as long as possible to extract the maximum value from them). Finally, an approach in detecting cyber attacks through sense making of DNS chaos was presented.

Marloes van Put presenting on expanding the possible places for the installation of solar panels

TNO also organised a parallel breakout session where SUTD and TNO researchers could share their experiences on working in a research environment and brainstorm on innovative solutions for today's problems.

Young TNO would like to thank the iTrust staff and researchers for their warm welcome and interesting tours

and presentations. It was truly a pleasure to visit such world-class facilities and we are looking forward to future opportunities to collaborate.

iTrust Matters

Research Openings

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

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

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

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 Information

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

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

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

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

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

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

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

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

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

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