An iTrust Newsletter

Jul – Sep 2015 | Issue 2

iTrust Times

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

Established in collaboration with MIT

From Centre Director's Desk

Dear Reader:

Greetings, and welcome to the second issue of iTrust News.

A lot has happened since I wrote this column for the inaugural issue in April. Prime Minister Lee Hsien Loong visited the Secure Water Treatment (SWaT) testbed together with several other dignitaries. This visit was a part of the SUTD's opening event held on May 8, 2015. The PM did evince keen interest in the testbed and asked us how and why we are using it in our research, and about our collaborators.

The SCy-Phy Systems Week 2015 is now behind us. Given how young iTrust is, I consider this as our first mega-event! During the week over 200 people from academia, government, industry, and local schools, participated in various activities hosted at SUTD. About 100 people attended the two-day Think-in session that focused on "Design of safe and secure Cyber Physical Systems." Academics from US, Europe, and Singapore teamed up with others from government and the industry to create a well-crafted sequence of short presentations and discussions. each and every one of the presentations was followed by a series of Q&A's from the attendees. The second day saw a standing room only hands-on session at the SWaT laboratory. Attendees were shown how a Cyber Physical System can be attacked and its impact. A well-planned series of demonstrations and exercises were offered to the attendees by researchers in Prof Nils Tippenhauer's and my research groups.

Prof Yuval Elovici and Mr. Dave Aucsmith teamed up and offered a Cyber Defence workshop to about 25 attendees from the government sector. The workshop included brief talks on cyber crime, espionage and warfare. Participants were given several exercises to work through relating to metasploits and big-data security analytics. They also got a taste of upcoming challenges in the areas of digital manufacturing and side channel attacks. The workshop was conducted in the Learning Environment for Experimental Technology (LEET) laboratory allowing participants to engage in active learning.

Ivan Lee and Toh Jing Hui conducted not just one, but two full days of Reverse Engineering Malware (REM) workshop for secondary and tertiary school students. The workshop, conducted in LEET laboratory, introduced REM techniques and offered hands-on exercises to enhance the students' learning experience. About 50 students attended the workshop.

The last item during the SCy-Phy week was a sequence of technical presentations by invited speakers. Alvaro Cardenas, UT Dallas, Yuval Elovici, iTrust and Ben Gurion University, Dina Hadžiosmanović, Delft and Mardavij Roozbehani, MIT, spoke to well attended audience about their work in cyber security.

Overall the SCy-Phy week was a success at an unexpected scale. As a consequence new collaborations are now in the works with faculty and research organisations in the US and Europe. These collaborations will allow deeper interactions among bright minds from iTrust with those from the other parts of the world. The tremendously positive response to the SCy-Phy week has led us to consider making it an annual event. Do expect more information on SCy-Phy Systems Week 2016 in the next newsletter.

SWaT continues to attract a broad stream of visitors from Singapore and other parts of the world. During the past few months we hosted about 60 visitors from the Agency for Science, Technology and Research (A*STAR), Defence Science & Technology Agency (DSTA), Google, the Ministry of Education and University of Illinois.

That in brief is what I would like to share with you in this issue of iTrust Times. As always, through this newsletter, my colleagues and I will continue to share with you the various events and research outcomes in iTrust. You are welcome to share your thoughts on this newsletter with us by writing to itrust@sutd.edu.sg. Thank you for reading and best wishes.

(Left to right): Alvaro Cardenas, Bert Jan te Paske, Daniel Trivellato, Jeroen Laarakkers, Marina Krotofil, Kasper Rasmussen, Aditya Mathur, Avi Ostfeld, Dina Hadžiosmanović, Mardavij Roozbehani, Bruno Sinopoli, Sylvain Frey

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

News

PM Lee visits iTrust's Secure Water Treatment System (SWaT) Testbed

Prime Minister Lee Hsien Loong was at SUTD on 8 May 2015 to officiate its opening as Singapore's fourth public university. Part of his itinerary was a tour to iTrust's SWaT testbed. Together with him were Emeritus Senior Minister Goh Chok Tong, Minister for Education Heng Swee Keat, Chief Defence Scientist Professor Quek Tong Boon, SUTD's Board of Trustees Chairman Philip Ng and PUB Chief Executive Ng Joo Hee.

Prof Aditya explaining to PM how a possible attack on the system can take place

iTrust Centre Director Prof Aditya Mathur guided the visitors around the laboratory and explained the water treatment processes and the ongoing cyber security research on the testbed. He also highlighted how the research would contribute to Singapore's push towards being a Smart Nation as we become increasingly connected. Two members of the SWaT elite team – comprising students from different pillars in SUTD with interest in cyber security – were also available to explain how cyber attacks could be carried out to disrupt a water treatment plant's operations.

The SWaT testbed has generated a lot of interest and is heavily utilised since its opening in Mar 2015. SUTD researchers have been busy designing research experiments and building attack and defence models of the testbed. To raise awareness of the testbed and iTrust's capabilities, these experiments and models were also demonstrated to international and local visitors from the academia, government and industry (see following articles).

Events

SCy-Phy Systems Week 2015

iTrust organised the inaugural Secure Cyber-Physical (SCy-Phy) Systems Week from 22 to 26 June 2015, attracting over 200 international and local attendees to the event. The event was supported by the Ministry of Defence. Stretched over a week, SCy-Phy started off with a 2-day Think-in session, focusing on the theme "Design of safe and secure Cyber Physical Systems."

Participants at Day 1 Think-in Session

Think-in Session (Day 1)

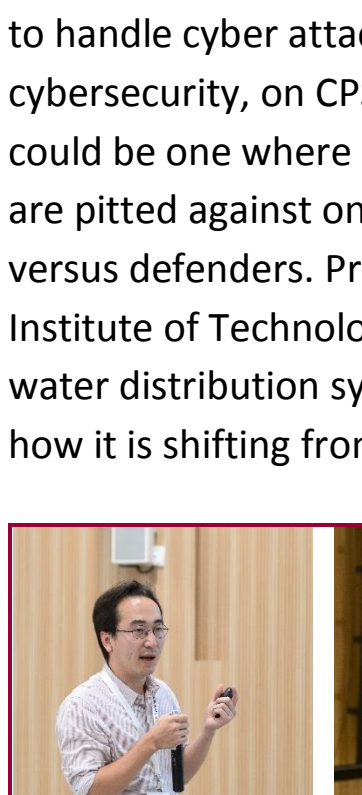
The brainstorming sessions on the first day spanned four themes: Threats; Defences; Models; and Safe and Secure Controls. A selected panel of international and local experts were invited to share key issues within the sessions and the state of the art techniques and tools to address these issues. Following presentations by the panellists, key discussants and event attendees engaged in lively discussion and exchange of ideas on the strengths and limitations of the existing tools and techniques

Assoc. Prof Bruno Sinopoli (Carnegie Mellon University) started off the Threats session with an introduction to CPS, and general security concerns with those systems. Ms Marina Krotofil (Hamburg University of Technology) followed with a discussion on the adequacy of traditional cyber-security measures in the context of CPS, and how a better understanding of attackers and their methods might

help build robust attack-resilient processes. Prof Yuval Elovici (Ben Gurion University and Research Director, iTrust) closed the session with a detailed case study of a real-world CPS, its existing security considerations and countermeasures, and real-world trade-offs when securing such a system.

Top (left to right): Session 1 panellists Assc Prof Bruno Sinopoli, Ms Marina Krotofil, Prof Yuval Elovici. Bottom (left to right): Discussants Mr Mohd Raihan, Mr Lim Hwee Kwang, Dr Sylvain Frey, Dr Lim Woo Lip, Dr Nilanjan Raghunath

In "Defences", Dr Dina Hadžiosmanović (Delft University of Technology) presented the concept as a marriage of traditional safety measures (such as alarms) with those of cybersecurity control measures (such as intrusion detection), where one complements the other. Mr Daniel Trivellato (SecurityMatters) presented three important industrial control system protection of awareness and visibility, specialised control and actionable intelligence in the face of threats resulting from threat actors and vectors. Dr Kasper Rasmussen (University of Oxford) delved into the defence of embedded systems via remote attestation, which uses a trusted verifier to verify the internal state of the embedded device. He ended his presentation with a call for more realistic adversary models, such as one where the attacker, being able to compromise the system at will, can "leave and come back" whenever there is an attestation request.



GOH Prof Quek at his welcome address

Following lunch, Guest of Honour Prof Quek Tong Boon, Chief Defence Scientist, gave a welcome address to the participants. He said that while many had embarked on CPS research, he saw how the Think-in session could be a platform to bring together expertise from all over the world to generate new projects and catalyse collaborations.

Dr Sicun Gao (MIT) began Session 3 on "Models" by presenting the use of automated reasoning - teaching machines to scan cybersecurity systems for glitches - to handle cyber attacks against, and hence improve cybersecurity, on CPS. He opined that the future could be one where automated reasoning engines are pitted against one another as cyber attackers versus defenders. Prof Avi Ostfeld (Technion – Israel Institute of Technology) presented on the current water distribution systems security modelling and how it is shifting from offline design/decisions to

Top (left to right): Session 2 panellists Dr Kasper Rasmussen, Dr Dina Hadžiosmanović, Mr Daniel Trivellato. Bottom (left to right): Discussants Mr Tan Ee Sin, Mr Mark du Plessis, Mr Bert Jan te Paske

Top (left to right): Session 3 panellists Dr Sicun Gao, Prof Avi Ostfeld, Asst Prof Stefano Galelli. Bottom (left to right): Discussants Mr Tan Ee Sin, Mr Jeroen Laarakkers, Dr Sylvain Frey

online/real time modelling, and the inherent challenges in place. These include obtaining a real time and reliable hydraulic flow, pressure distribution and water quality. In the same vein, Asst Prof Stefano Galelli (SUTD) discussed how increased model complexity and the corresponding computational requirements, pervasiveness of conventional sensors and the use of unconventional sensors, and model validation-- all presented themselves as challenges in process-based modelling of water resources management systems.

In the last session on "Safe and Secure Controls", Asst Prof Alvaro Cardenas (UT Dallas) presented the current methods for protecting control systems. Agreeing with Dr Hadžiosmanović, he pointed out that future research into holistic systems that combine security and controls would be essential for designing attack-resilient CPS.

Top (left to right): Session 4 panellists Asst Prof Alvaro Cardenas, Dr Mardavij Roozbehani, Asst Prof Roland Bouffanais. Bottom (left to right): Discussants Dr Lim Woo Lip, Mr Raymond Ung, Mr Samuel Yee

Drawing on the well-understood design issue of tradeoffs between robustness and performance in industrial control systems, Dr Mardavij Roozbehani (MIT) explained how the tradeoffs can be improved with a reconfigurable control setup, albeit at the cost of increased complexity of the control system. Asst Prof Roland Bouffanais (SUTD) drew parallels between thousands of animals moving together as a coordinated unit - swarms - and CPS, and discussed how these commonalities and emulating nature could be used for the design of secure reconfigurable CPS.

Wrapping up the Think-in sessions, Prof Aditya and Mr Yu Chien Hsiang thanked the panellists for their thought-provoking presentations as well as the discussants and attendees for the fruitful discussions that followed. Even before the day concluded, small groups were already forming to discuss new projects and collaborations, thus achieving the primary objective of the Think-in session.

Think-in Session (Day 2)

By Sridhar Adepu & Daniele Antonioli

Participants, fresh from intense discussions at the previous day's Think-in session, gathered at the SWaT lab for specially designed demonstrations by researchers to showcase their current work and the capabilities of SWaT for research purposes. They were introduced to iTrust's current and upcoming testbeds: SWaT, WADI, EPIC and IoT.

The first demo session by researchers Mr Sridhar Adepu, Mr Daniele Antonioli and Mr Nicolas Iooss was on the concept of "security by design," i.e., how to design code that would be resilient to an attack affecting a sensor reading. The researchers simulated attacks on different sensors by compromising the communication in real-time. They then introduced a defence strategy and demonstrated its effectiveness by comparing the responses of the systems with the defence mechanism switched on and off.

Participants and researchers discussing the hands-on experiments

During the experiments session, participants were provided with tools to connect to and explore the SWaT internal network through a dedicated wireless access point. A second experiment focused on the SWaT protocol suite, in which the participants were able to collect and analyse packets in real-time, discover the services provided by the testbed and eventually perform a basic network attack.

They were also given access to iTrust's simulation environment through a set of dedicated virtual machines, so that the researchers could show the simulation tools and to test attack and defence mechanisms without adverse impacts on the actual testbed. These interactive experiments also allowed participants to experience the same developing environment as that of an iTrust researcher. During lunch, the participants also had the opportunity to tour the SWaT testbed, led by Prof Aditya.

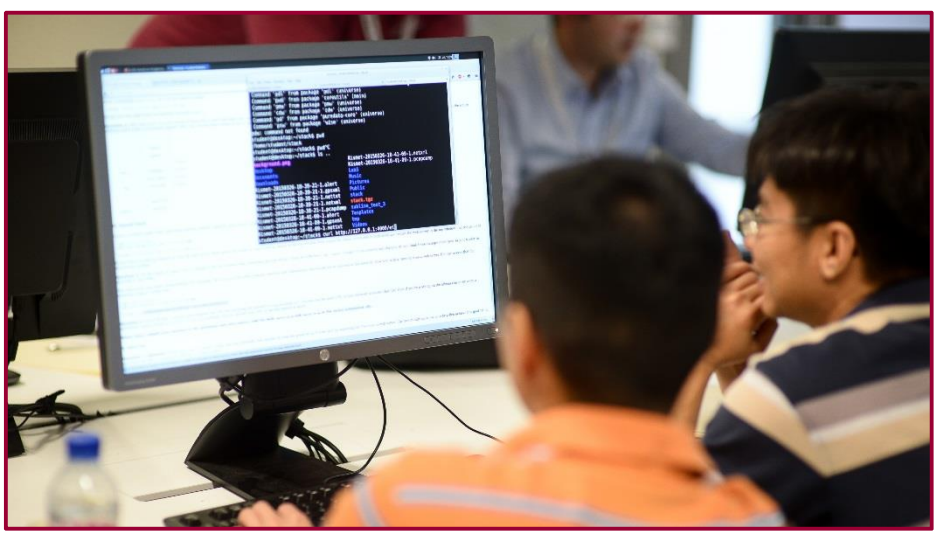
A couple of technical demo followed the lunch break. The first demo showed how during the study of the testbed, the researchers used network protocol analyser to sniff out packets of data between the PLC and SCADA so as to analyse and determine that CIP (Common Industrial Protocol) was used on top of the Ethernet/IP as the communication protocol. The second demo addressed Software-Defined Networking (SDN) in the context of CPS. SDN was presented as a novel architectural way of thinking about network design, and continues to be one of the hot research topics in networking. Core concepts of SDN were shared with the participants followed by a live demo on the implementation of an SDN controller for the SWaT testbed.

Participants at the Day 2 Think-in Session

Cyber Defence Workshop (Day 2)

While the Think-in session continued with demonstrations and experiments at SWaT lab on Day 2, government agency representatives gathered for the Cyber Defence Workshop at the Learning Environment for Experimental Technology (LEET) laboratory. The workshop was jointly conducted by Mr David Aucsmith, a senior computer scientist and technology leader with a deep technical understanding of computer and communications security, and Prof Yuval Elovici, iTrust's Research Director.

Mr Aucsmith began the workshop by introducing the concept of cyber attacks in its various forms: crime, espionage and war. In the second session, he focused on how an attacker can control the target process' execution by exploiting the buffer overflow vulnerability, and some of the tools such as Metasploit Framework and resources available to guide users in penetration testing and IDS signature development. In the hands-on session, participants were given pre-written codes to run on the workstations to demonstrate and see the effects of buffer overflow.



In the afternoon sessions, Prof Elovici presented an array of topics, from big data security analytics to techniques on bridging the air-gap as well as his future work relating to IoT. Assisted by Mr Toh Jing Hui, the participants continued with a second practical session on data analytics. Using data prepared by the workshop conductors, the participants were taught how to use WEKA (a freeware for performing big data analytics) to assist in learning and understanding how security analytics is able to help them detect attacks that are happening in their network.

Reverse Engineering Malware Workshop (Day 3 & 4)

To generate interest in cyber security among students, iTrust conducted a 1-day Reverse Engineering Malware (REM) workshop at the LEET laboratory. Students from secondary schools, junior colleges and tertiary institutions were invited to the workshop. Due to the overwhelming response and to ensure that each student has ample hands-on experience, the workshop was extended by another day. In total about 50 students participated in the workshop.

Ivan Lee conducting the REM workshop

The REM workshop was conducted by Mr Ivan Lee and Mr Toh Jing Hui, who introduced the students to how REM is being carried out in the industry. There was a dedicated workstation for each student to enhance their learning experience. Participants were also encouraged to share a workstation to discuss and learn from one another. The students were taught how to perform two techniques which they then used to study and analyse several malware provided to them. The two techniques were behaviour analysis, which allows the user to understand how a piece of malware works, and the classification of malware and code analysis, where using dissection a user can learn how the hacker wrote the malware.

During the workshop, one student commented that "Together with some basic understanding, the hands-on exercises helped me understand the concepts better." Agreeing, another said he "…liked that there was hands-on learning, where we had to learn how to decode using the "commands panel" to see what the virus had done to our computer and how to make full use of apps to understand the virus we were dealing with."

Toh Jing Hui showing a video on AirHopper demonstration to students

At the end of the workshop, the students were also given a tour of SUTD's campus and laboratories to experience university life.

Cyber Security Technical Talks (Day 4 & 5)

Concluding SCy-Phy Systems Week were technical talks by four invited speakers over two days. Asst Prof Alvaro Cardenas highlighted the communication gaps between security practitioners and control engineers and how it limited the security benefits of their interactions. With improved understanding and communication, he argued how leveraging research in both areas could be used to design a novel secure and private CPS. Dr Mardavij Roozbehani presented a bird's-eye view of the factors at play in infrastructure vulnerabilities, from physical, cyber, economic to social. Combining these with examples of vulnerabilities, he proposed a unified framework and discussed some of the existing methodologies, challenges and open problems in addressing CPS security.

Prof Yuval Elovici presented several methods of advanced cyber attack i.e. bridging air gapped networks for data in/exfiltration via different

communication mediums including sound, light, heat emissions and radio frequencies. Dr Dina Hadžiosmanović presented her research work on a detection approach that aims to address current shortfalls in network intrusion detection systems. This approach continuously tracks updates to corresponding process variables to then derive variable-specific prediction models as the basis for assessing future activity.

Profiles

Justin Ruths

Justin is an Assistant Professor at the Singapore University of Technology and Design (SUTD). At SUTD, Justin develops theoretical tools that determine the fundamental properties of large-scale control systems and also computational methods to solve the optimal control problems corresponding to these dynamical systems, which are usually analytically intractable. In particular, his work is motivated by applications in the control of quantum systems and neuroscience as well as understanding the role of structure in the control of dynamical networks.

Justin received his PhD in Systems Science & Mathematics at Washington University in 2011, following his BS in Physics from Rice University in 2004 and his MS in Mechanical Engineering from Columbia University in 2006.

Martin Ochoa

Assistant Professor Martin Ochoa joined SUTD's Information Technology and Systems Design Pillar on 3 Aug 2015. Martin is from Bogotá, Colombia. He studied Systems Engineering in San José, CR (Universidad Latina, B.Sc.) and Mathematics in Rome (La Sapienza, B.Sc.). He continued his math studies in Munich (LMU, M.Sc.) and Sophia-Antipolis (INRIA). Thereafter, Martin completed a PhD in Computer Science (TU Dortmund) on model-based security for evolving systems. He then worked as a consultant and researcher in IT security for Siemens Corporate Technology in Munich. In 2013 Martin joined the Technical University of Munich as a post-doctoral researcher, where he received an innovation in teaching award for a practical course on Software Security based on an attacker/defender gamification.

Martin is interested in various aspects of Software Security, including Information Flow Analysis, Security Testing and Software Diversity. In particular he is interested in applications to side-channel analysis and quantification, software obfuscation and polymorphic malware analysis. At SUTD Martin will be involved in teaching and research activities in the field of security for cyber-physical systems.

iTrust also welcomes **Tan Yong Sheng** who joined iTrust on 29 Jun 2015 as a Technical Officer. He carries out both administrative and technical duties including organising student seminars and assisting in cyber security workshops and technical needs of iTrust. Yong Sheng graduated from the School of Information Technology at Republic Polytechnic. Before joining SUTD, he worked for an IT support services company for two years and constantly seeks to expand his knowledge in IT.

On 1 Jul 2015, **Toh Jing Hui** joined Prof Yuval Elovici's team as a Research Technician to work on a SEED project titled "Preventing New Bridging for Air-Gap Attacks using Deception Techniques". The project is supported by TL@SUTD, which aims to develop a system that can automatically detect and remove security vulnerabilities in an organisation before any damage is done. Jing Hui holds a Diploma in IT from Kaplan Institute of Higher Education and is currently pursuing a degree in Cyber Forensics. Prior to joining TL, Jing Hui was a Laboratory Technologist with the ISTD team, as well as SUTD's IT department to resolve IT issues that the staff or faculty faced.

Research Focus

Advancing Security of Public Infrastructure using Resilience and Economics (Water)

By Stefano Galelli

This project is an extension of the main Advancing Security of Public Infrastructure using Resilience and Economics project, an interdisciplinary project on the cyber security of large-scale, public infrastructures. Funded by PUB – the national water agency – it complements the main project with a three-year focus on public water infrastructure systems. The project team consists of researchers from SUTD and PUB engineers.

The project, which is motivated by the rise of cyber attacks to critical infrastructures, aims at investigating the vulnerability of SCADA systems and mitigating the effect of such attacks to water infrastructures, such as water treatment and distribution systems. To this purpose, the team will analyse different threats and design secure and economically viable countermeasures. Particular emphasis will be given to the development of dynamic control solutions that defend the systems during cyber attacks.

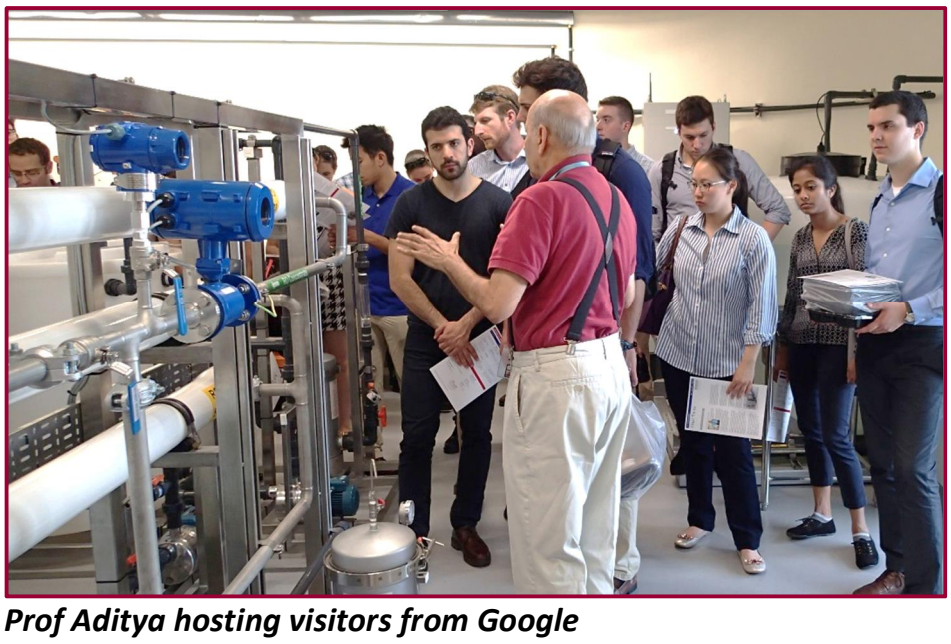
The team will investigate the interaction between physical and cyber layers, leveraging two testbeds available at SUTD, namely SWaT and WADI (Water Distribution). The former features the most common steps in water treatment, including filtration and chemical dosing, whereas the latter faithfully represents automated water distribution systems in cities such as Singapore.

Outreach

Visits to SWaT lab

By Ivan Lee

On 3 Jul 2015, about 50 Associate Product Managers (APM) from **Google** visited iTrust. As part of Google's APM programme, they are sent to meet companies and research organisations and build connections and knowledge that will bring about change. Their visit to iTrust and the SWaT testbed was hosted by Prof Aditya Mathur and Mr Ivan Lee.



Prof Aditya hosting visitors from Google

Prof Aditya explained the different stages of the SWaT testbed's treatment process, followed by the possible attack vectors and cyber security implications in such a design. He also shared some of the research work being carried out by iTrust researchers and elaborated on a few possible attack and defence scenarios. The Google APM displayed keen interest and knowledge in the testbed and raised many questions during their visit, such as security design and validation in CPS, as well as possible international collaboration.

The **Defence Science & Technology Agency (DSTA)** visited the SWaT lab on 23 Jul 2015. Prof Aditya hosted the visitors and briefed them about iTrust's research in the Internet of Things (IoT), Gamification and Cyber Security. The next day, iTrust welcomed a group of scholars from the **Agency for Science, Technology and Research's (A*STAR)** Academia Pathways Programme who have completed their PhD education and embarking on a teaching career. Prof Aditya Mathur, Prof Martin Dunn and Asst. Prof Nils Tippenhauer met with Prof William Sanders, Prof Rakesh Nagi and Prof Klara Nahrstedt from the **University of Illinois at Urbana-Champaign** on 27 Jul 2015 to discuss current and future research projects at iTrust, and potential for collaborations in the future. In particular, the discussion was focused on exchange of researchers (faculty and students), and shared use of existing and new testbeds. On 30 and 31 Jul 2015, the **Ministry of Education (MOE) Curriculum Planning & Development Division** arranged for some 40 ICT Heads of Departments and teachers to visit SWaT lab to learn more about the current research into cyber physical systems.

World Readiness Programme Symposium

About 300 lower secondary students from Catholic High School, CHIJ St Nicholas Girls' School (SNGS) and Singapore Chinese Girls' School, packed the school hall of SNGS for the Joint Integrated Programme (IP) World Readiness Programme (WRP) Symposium. The WRP's aim is to equip IP students with the knowledge and skills to become well-informed and responsible global citizens.

The theme for the symposium was Cyber Security and Combatting Cyber Crime. Ivan Lee, iTrust's Senior Associate Director for Cyber Security Technologies, was invited to speak on cyber security. Ms Viola Veiderpass, a Digital Crime Officer from Interpol, was also present to speak on Interpol's efforts in combatting cybercrime.

The focus of Ivan's talk was on the impact of cyber security on individuals, organisations and society at large, as well as the next generation of cyber crimes and the efforts to keep these attacks at bay.

Through a series of demonstrations using everyday gadgets and home appliances, Ivan and his team – Toh Jing Hui and Dabin Lee – showed how these devices could be (ab)used for criminal activities. The first demonstration - a flying drone – drew shrieks of excitement from the students. It was used to demonstrate how a cyber criminal could penetrate an unprotected WiFi network and steal data even if he did not have physical access to the source.

Students showing great enthusiasm during the drone demonstration

Another demonstration involved a vacuum cleaner which, when modified and unknown to its owner, allows a cyber criminal to gain control of the device remotely.

(Left to right): Mr Ivan Lee, Mr Loh Chih Hui (HOD, Integrated Programme, CHIJ SNGS) and Mr Leo Hwa Chiang (Director, Asia Business Development, IEEE Asia Pacific Operations Centre) answering questions from students

After an introduction of iTrust and the work we do, the enthusiasm of the students during the Q&A session took the presenters and teachers by surprise. At least 20 students lined up to ask thought-provoking questions on cyber attacks and defences, as well as the presenters' motivation to join their organisations and the skill sets that were required in this field.

In preparing these young and bright students to be leaders of the future, such displays of eagerness and curiosity are indeed an encouraging start.

Research Publications

1. D. Antonioli and N. O. Tippenhauer, "MiniCPS: A toolkit for security research on CPS Networks," in Proceedings of Workshop on Cyber-Physical Systems Security & Privacy (SPC-CPS), co-located with CCS, 2015.
2. 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 International Conference on Communication (ICC), London, UK, Jun. 2015, pp. 1-6.
3. Fire, M., Elovici, Y., "Data Mining of Online Genealogy Datasets for Revealing Lifespan Patterns in Human Population", ACM Transactions on Intelligent Systems and Technology, 6(2):28, 2015.
4. Guri, M., Kachlon, A., Hasson, O., Kedma, G., Mirsky, Y., Elovici, Y., "Data Exfiltration from Air-Gapped Computers over GSM Frequencies", 24th USENIX Security Symposium (USENIX Security'15), Washington, D.C., August 12-14, 2015.
5. Guri, M., Kedma, G., Kachlon, A., Elovici, Y., "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies", 9th International Conference on

Malicious and Unwanted Software (MALWARE 2014), Puerto Rico, October 28-30, 2014, 58-67.

6. Guri, M., Kedma, G., Kachlon, A., Elovici, Y., “Resilience of Anti-malware Programs to Naïve Modifications of Malicious Binaries”, IEEE Joint Intelligence & Security Informatics Conference (JISIC2014), Hague, Netherlands, September 24-26, 2014, 152-159.
7. Guri, M., Kedma, G., Zadov, B., Elovici, Y., “Trusted Detection of Sensitive Activities on Mobile Phones Using Power Consumption Measurements”, IEEE Joint Intelligence & Security Informatics Conference (JISIC2014), Hague, Netherlands, September 24-26, 2014, 145-151.
8. Guri, M., Monitz, M., Mirsky, Y., Elovici, Y., “BitWhisper: Covert Signaling Channel between Air-Gapped”, 28th IEEE Computer Security Foundations Symposium, Verona, Italy, July 13-17, 2015.
9. Guri, M., Poliak, Y., Shapira, B., Elovici, Y., “JoKER: Trusted Detection of Kernel Rootkits in Android Devices via JTAG Interface”, The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-15), Helsinki, Finland, August 20-22, 2015.
10. Mirsky, A., Cohen, R., Stern, L., Felner, A., Rokach, L., Elovici, Y., “Search Problems in the Domain of Multiplication: Case Study on Anomaly Detection Using Markov Chains”, The International Symposium on Combinatorial Search (SoCS 2015), Ein-Gedi, the Dead Sea, Israel, June 11-13, 2015, 70-77.
11. Mirsky, Y., Shapira, B., Rokach, L., Elovici, Y., “pcStream: A Stream Clustering Algorithm for Dynamically Detecting and Managing Temporal Contexts”, Pacific-Asia Conference on Knowledge Discovery and Data Mining (PAKDD 2015), Ho Chi Minh City, Vietnam, May 19-22, 2015, 119-133.
12. N. O. Tippenhauer, H. Luecken, M. Kuhn, and S. Capkun, "UWB Rapid-Bit-Exchange System for Distance Bounding," in Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2015.
13. Nakibly, G., Sosnovich, A., Menahem, E., Waizel, A., Elovici, Y., “OSPF vulnerability to persistent poisoning attacks: a systematic analysis”, 2014 Annual Computer Security Applications Conference (ACSAC 30), New Orleans, Louisiana, USA, December 8–12, 2014, 336-345.
14. Nissim, N., “ALPD: Active Learning Framework for Enhancing the Detection of Malicious PDF Files”, IEEE Joint Intelligence & Security Informatics Conference (JISIC2014), Hague, Netherlands, September 24-26, 2014, 91-98.
15. Nissim, N., Boland, M.R., Moskovitch, R., Tatonetti, N.P., Elovici, Y., Shahar, Y., Hripcsak, G., “An Active Learning Framework for Efficient Condition Severity Classification”, 15th Conference of Artificial Intelligence in Medicine 2015 (AIME-2015), Pavia, Italy, June 17-20, 2015.
16. Nissim, N., Cohen, A., Glazer, C., Elovici, Y., “Detection of APT Attacks Initiated by Malicious PDF Files Attached to Emails: a State of the Art Survey”, Computers and Security, 48, 2015, 246-266.
17. Nissim, N., Rokach, L., Moskovich, R., Elovici, Y., "Efficient Active Learning Methods for Improving the Detection of Unknown PC Malwares", Expert Systems with Applications, 41(13), 2014, 5843-5857.
18. Puzis, R., Zilberman, P., Elovici, Y., Dolev, S., Brandes, U., “Topology Manipulations for Speeding Betweenness Centrality Computation”, Journal of Complex Networks, 3 (1), 2015, 84-112.
19. R.-H. Hsu and J. Lee, "Group Anonymous D2D Communication with End-to-End Security in LTE-A," Proc. IEEE Conference on Communications and Network Security (CNS), Florence, Italy, Sep. 2015, pp. 1- 9.
20. Rui Tan, Varun B. Krishna, David K. Y. Yau, and Zbigniew T. Kalbarczyk. "Integrity Attacks on Real-Time Pricing in Electric Power Grids," ACM Trans. Information and System Security (TISSEC). Accepted for publication.
21. Sepetnitsky, V., Guri, M., Elovici, Y., “Exfiltration of Information from Air-Gapped Machines Using Monitor's LED Indicator”, IEEE Joint Intelligence & Security Informatics Conference (JISIC2014), Hague, Netherlands, September 24-26, 2014, 264-267.
22. X. Chen, C. Zhong, C. Yuen, H.-H. Chen, "Multi-antenna relay aided wireless physical layer security," IEEE Communications Magazine, accepted on Apr 2015.
23. X. Chen, L. Lei, H. Zhang, C. Yuen, "Large-Scale MIMO Relaying Techniques for Physical Layer Security: AF or DF?" IEEE Trans. On Wireless Communications, accepted on May 2015.
24. Yinxing Xue, Junjie Wang, Yang Liu, Hao Xiao, Jun Sun, "Mahinthan Chandramohan: Detection and classification of malicious JavaScript via attack behaviour modelling," ISSTA 2015: 48-59

iTrust Staff

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

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

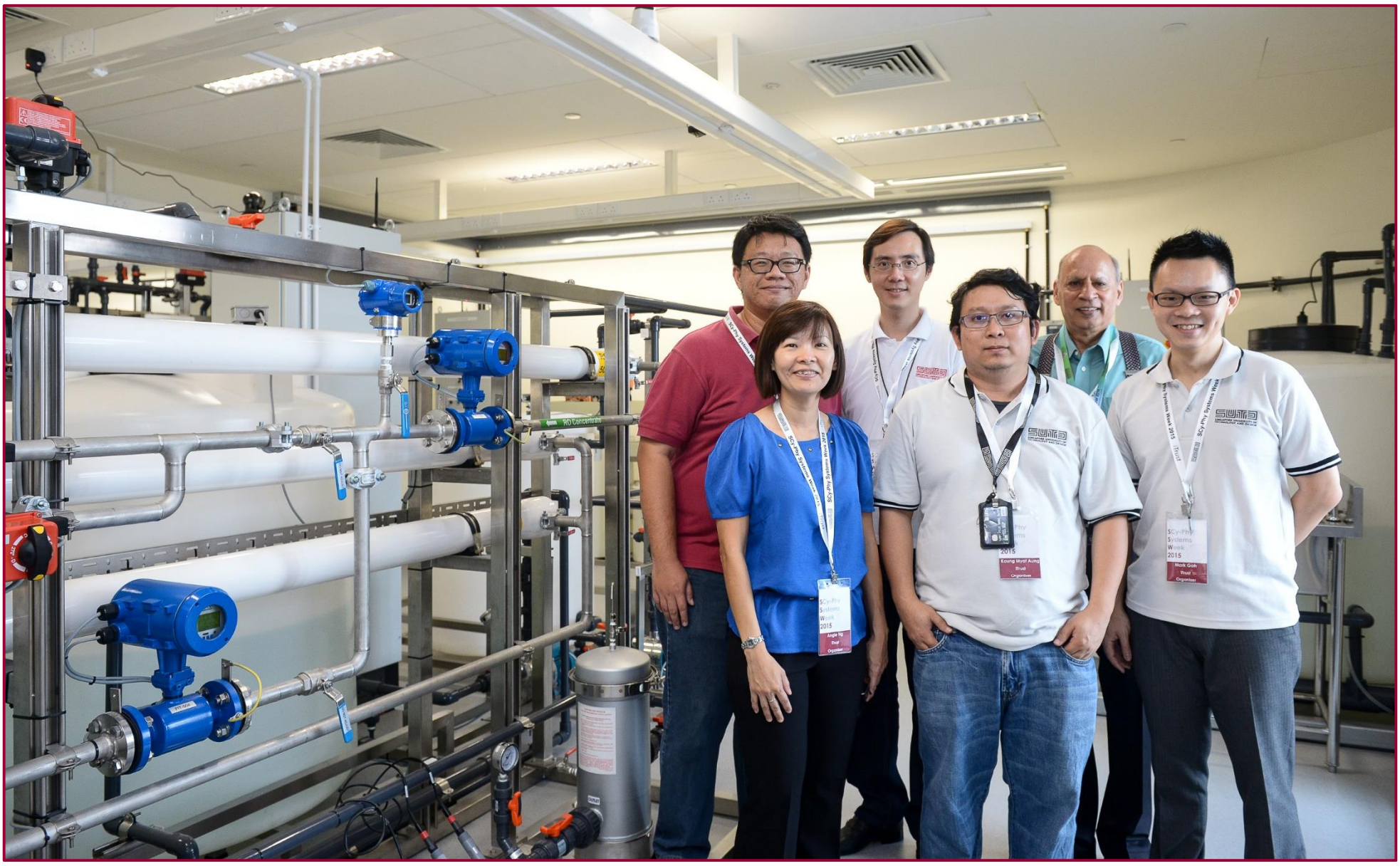
Mr Ivan LEE
Senior Associate Director, Cyber Security Technologies
ivan_lee@sutd.edu.sg

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

Mr KAUNG Myat Aung
Laboratory Engineer
kaungmyat_aung@sutd.edu.sg

Mr Mark GOH
Manager
mark_goh@sutd.edu.sg

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



Left to right: Toh Jing Hui, Angie Ng, Ivan Lee, Kaung Myat Aung, Aditya Mathur, Mark Goh

iTrust
Centre for Research in Cyber Security

itrust.sutd.edu.sg

This issue of the iTrust Times is designed and edited by Mark Goh.