An iTrust Newsletter Oct – Dec 2015 | Issue 3

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 third issue of iTrust Times.

iTrust is rapidly moving forward in its mission to create methods and tools to enable design of resilient Cyber Physical Systems (CPS). In this edition of iTrust Times, I will focus on iTrust's growing research programme and new international collaborations.

First, congratulations to Professor Yuval Elovici and his team of researchers for receiving a research grant for the project on Research & Security Innovation Lab for IoT. This project adds Internet of Things (IoT) to the existing iTrust research focus. The ready availability of microprocessors at low cost and high computing power, and systems on a chip, has led to an explosion of Internet-enabled consumer devices. These devices allow communication with the mobile phone, are often Wi-Fi enabled, and are programmable. Researchers have pointed to security risks associated with these devices; some have even renamed IoT as the Internet of Insecure Things. The project will enable Professor Yuval's research group to study security risks in realistic settings and offer experimentally validated proposals for securely architecting such devices. A state-of-the-art testbed is being built to demonstrate security risks often associated with such devices and enable product evaluation. This testbed includes a shielded room to identify and demonstrate security risks with a variety of IoT devices. The shielded room will also enable companies to test their products against a set of security related criteria.

iTrust welcomes commercial organisations to make the best use of our facilities for the assessment of security products for CPS. The Secure Water Treatment (SWaT) testbed at iTrust is a world-class facility that allows experiments with cyber attacks and techniques for defence. We welcome Elbit Systems, Check Point and ICS^2 who will soon be using SWaT to assess and demonstrate the effectiveness of their products in defending a CPS. Their engineers will work closely with iTrust researchers. Together we will learn the strengths and limitations of the companies' products. We hope that this collaborative exercise, made possible by Defence Science & Technology Agency (Singapore), will lead to even better products for improving the resiliency of CPS.

So much for this edition of iTrust Times – expect a lot of interesting news in the next edition. Thanks for reading iTrust Times and best wishes for the season.

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

SUTD students at the Singapore Cyber Conquest, GovWare 2016

In This Issue

Advancing Security of Public Infrastructure using Resilience and Economics

By Aditya Mathur

The project was officially launched in January 2015. Experimental work began in April 2015 soon after the Secure Water Treatment (SWaT) testbed was available. This project is to conduct fundamental scientific research to improve the resilience of CPS that offer key services such as water and power.

Researhcers have made rapid progress since the project launch. In addition to the nine PI/Co-PIs, the project now has a staff of 10 that includes researchers, lab engineer, and administrators. Four undergraduate students are also engaged in the project.

A range of experiments has been conducted using SWaT, and more are ongoing. These experiments are aimed at understanding the response of SWaT to cyber attacks, ways to launch attacks, and the attack detection mechanisms. Attack detection has been experimented with invariants derived from the physics of water flow across the tanks as well as using the CUSUM method. The CUSUM method has been used successfully in the past on a simulated chemical process. SWaT has enabled its assessment in a realistic process. Novel attacker and attack models have been proposed. These models are used to design a variety of cyber attacks and launched on SWaT.

A Water Distribution (WADI) testbed is expected to be operational in early 2016. However, while we wait for WADI, researchers are using EPANET to simulate cyber attacks on water distribution systems. EPANET is software developed by the US Environmental Protection Agency (EPA) to simulate hydraulic and water quality behaviour within pressurised pipe networks.

A power grid testbed (Electric Power and Intelligent Control, or EPIC) is expected to be available in mid-2016. Meanwhile, researchers have been using the testbed at the NTU's Laboratory for Clean Energy (LaCER) to look into scalable and predictive safety assessment of power grids. They are conducting a systematic evaluation of Extreme Machine Learning (ELM) in the context of power grid.

Work is also underway to look into ways to attest software running inside a PLC. Existing software and hardware-based methods for attestation are being studied for their applicability and effectiveness in the SCADA domain. This work is currently underway in the context of SWaT.

Progress has been made towards a unified economic model for CPS. In addition, the researchers aim at developing models for fair cost allocations to various stakeholders. These models will be applied to SWaT, WADI and EPIC.

Results from experiments conducted so far indicate that regardless of the attack detection and defence mechanisms installed to protect the PLCs and the communications network in SWaT, attackers will likely succeed in penetrating the system and disturbing its operation. To make SWaT highly resilient to cyber attacks, our researchers are looking into a layered defence mechanism. The top layer and the most difficult to penetrate, is at the design stage using the concept of intelligent checkers.

The progress made is evident in terms of publications, some of which have appeared while others will appear soon at top conferences relevant to the design of resilient CPS.

Cyber Physical System Protection

By Aditya Mathur

The Cyber Physical System Protection project is now in its third year. The most recent project review was completed successfully on October 9, 2015. The project is on target; so far our researchers have met the requirements for the deliverables at each of the four milestones. Research in this project has led to a number of publications in journals and conferences.

In addition to the four PI/Co-PIs, the project now has

a research and admin staff of nine. At the recent six-monthly review, three Co-PIs shared on their progress. Co-PI Sun Jun presented a tool named TAuth that focuses on verifying the properties of components of CPS. In addition he presented another tool named HyChecker that can be used to model hybrid CPS such as the SWaT testbed. Currently HyChecker uses LabView to model SWaT. Controller code from the six PLCs in SWaT was manually translated into Python and included in the LabView model. The model is huge: 2^{23} operation modes. Using heuristics, the model was simplified for an initial assessment. Several questions are being answered using this simplified model. For example, one question that relates to the backwash process in SWaT is: "Is it possible to reach a state where the backwash water tank overflows or drains, within K steps?"

Co-PI Nils Tippenhauer presented a simulation platform focusing on faithful reproduction of Ethernet/IP traffic, SWaT network and physical link topology. This toolbox, named MiniCPS, can simulate attacks and physical layer effects. It contains a set of tools (Scapy extensions) to analyse the Ethernet/IP traffic exchanged by Allan Bradley devices used in SWaT. MiniCPS aims to combine real time network simulation with physical process simulation. Physical process simulation is connected to component simulation through a simple API. Currently, an SQL database is used to store real-time values of tags. The toolbox has been released as open source[1] and is co-authored by Daniele Antonioli and Nils.

Co-PI Yuen Chau presented his group's work on security in data acquisition. Several attack scenarios including active attacks, integrity, and passive attacks, were examined. Confidentiality and availability of data transmission over both single-hop and 2-hop networks were mathematically derived. Amplify-and-Forward and Decode-and-Forward relaying schemes were considered. The objective was to obtain an achievable secrecy outage capacity with closed form expression, and design simple relaying schemes. Explicit expressions were derived for the secrecy outage capacity for both AF and DF relaying schemes, and their performance compared under different conditions.

Events

Singapore
Cybersecurity R&D Conference

Riding on the success of SCy-Phy Systems Week 2015, iTrust is organising the inaugural Singapore Cybersecurity R&D Conference (SG-CRC 2016) on 14 and 15 January 2016 at the campus of the Singapore University of Technology and Design. The event is supported by the National Research Foundation (NRF).

The conference will bring together academics and practitioners from across the world to participate in a vibrant programme consisting of research papers, industrial best practices, and tools exhibition. Students, undergraduate and graduate, are encouraged to participate in specially organised sessions. Several cash awards and certificates will be given to the best contributions in various student categories.

This year's theme – Cybersecurity by Design – focuses on the importance of bringing a technically grounded element of design that integrates cyber security into a system early in the process rather than an afterthought. The element of design is integral to a process be it a purely software system, such as one engaged in managing online transactions, or a combination of hardware and software such as in Industrial Control Systems, pacemakers, and a multitude of IoT devices. This design element pervades the entire development process from the beginning till the end, and even during operation and maintenance. SG-CRC 2016 will focus on how design as an element can be made explicit early in the development process using novel techniques based on sound mathematical tools and engineering approaches.

Authors are invited to submit original work on any of

[1] http://www.researchgate.net/publication/280221159_MiniCPS_A_toolkit_for_security_research_on_CPS_Networks

the topics listed on the conference website via EasyChair: http://itrust.sutd.edu.sg/sg-crc-2016/. Accepted papers will be made available online about one week after the conference has ended. The proceedings will be published with Open Access by IOS Press in the Cryptology and Information Security Series.

iTrust Seminar Series - Understanding Cyber Risk as Business Risk in Industrial Control Environments

Professor Awais Rashid was invited to speak at iTrust Seminar Series on 25 Sep 2015. The title of his presentation was "Understanding Cyber Risk as Business Risk in Industrial Control Environments".

Prof Rashid spoke about how industrial control systems (ICS) were increasingly interacting with enterprise IT systems, leading to an increase in the level of threats to critical infrastructures. As a result, being able to understand and respond to cyber security risks from a business continuity and recovery perspective in order to evaluate and prioritise their mitigation responses was important for decision makers.

He shared about his ongoing work of his team in Lancaster Research Centre in which they studied and found that, in recent ICS accidents, more often than not, latent flawed designs within the ICS were the (main) causes of failures, rather than human failures, intentional or otherwise. Prof Rashid then discussed how the role of perception in understanding and articulating cyber risks could mitigate these risks and incidences should they occur.

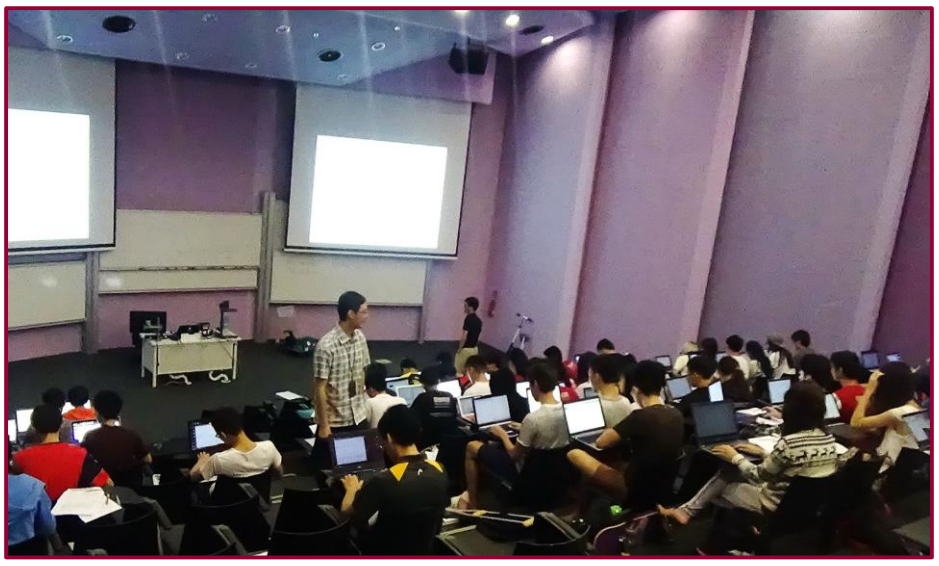
Prof Rashid is Director of Security Lancaster Research Centre, one of the UK's Academic Centres of Excellence in Cyber Security Research. He is particularly focused on sense-making of large, heterogeneous data sources and human factors in order to unravel impacts on cyber resilience of individuals, organisations and infrastructure.

Summer Camp

By Tan Yong Sheng

iTrust organised a two-day Python Summer Camp in SUTD to introduce students to the fundamentals of Python programming. The workshop was conducted by a team of expertise from iTrust: Senior Associate Director for Cyber Security Technologies Ivan Lee, Research Technician Toh Jing Hui and Technical Officer Tan Yong Sheng. Besides SUTD students, the Summer Camp was extended to secondary school, junior college, polytechnic and ITE students. Participation was encouraging: 70 students turned up for the workshop.

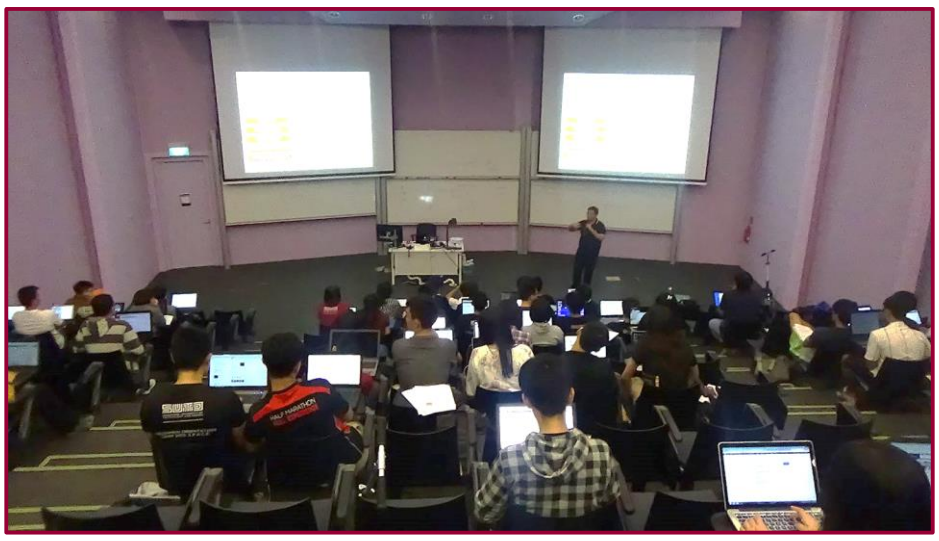
On the first day, basic Python commands were introduced, such as String Operators, String Formatting, Raw Input, Loops, Function, Class and Object, which helped to lay the groundwork in meeting the workshop objectives. On the second day, to help students better appreciate the language and its relevance to cyber security, the workshop conductors introduced to students on cyber security and the Cyber Kill Chain model and its various phases: Reconnaissance, Weaponisation, Delivery, Exploitation, Installation, Command and Control and Actions on Target.



Students carrying out Python commands under Ivan's supervision

To marry these two concepts and enable the students to apply what they had learnt over the two days, they were taught to write simple programmes to carry out cyber security reconnaissance. Beyond the theory, students were given plenty of hands-on exercises that were designed to test the students' understanding

and logical thinking. Year 2 and 3 student helpers were also on hand to guide the participants during the hands-on exercises.



Jing Hui covering the topic on cyber security on Day 2

As this was an introductory workshop to Python with application in cyber security, iTrust was heartened to hear that students felt that the workshop was "beginner friendly" and the conductors had a "very thoughtful way of introducing the Python concepts to beginners". They also appreciated that "assistance was always given and everyone was very helpful and patient".

GovWare 2015

iTrust was at this year's GovernmentWare (GovWare) 2015 to showcase its research projects. Held from 6 to 8 Oct, the annual conference was organised by the Cyber Security Agency of Singapore (CSA), in partnership with the Ministry of Home Affairs (MHA) and the Infocomm Development Authority of Singapore (IDA). The event was graced by Minister for Communications and Information Dr Yaacob Ibrahim, who was the Guest-of-Honour.

Leveraging on the conference theme of "Building a Secure Smart Nation", iTrust showcased projects related to cybersecurity of cyber physical systems: Advancing Security of Public Infrastructure using Resilience and Economics, Cyber Physical System Protection, Cyber Security Patrol and Network Engineering Techniques for Wireless Security.

iTrust received a stream of conference attendees who were keen to find out more about iTrust and its work. In particular, the Cyber Security Patrol project received a lot of interest from visitors, including Minister. In this project, the research team demonstrated the feasibility of launching a cyber-attack using a drone and an application running on an Android smartphone. The research, led by iTrust Research Director Prof Yuval Elovici, was published in Wired (US) magazine as well as more than a dozen tech websites. A video of the demonstration was uploaded onto YouTube and garnered more than 15,000 views at the time of printing.

Student Muhammad Hatib explaining the Cyber Security Patrol project to Minister Dr Yaacob Ibrahim (Photo credit: MCI)

SUTD's students also participated at the 6th Singapore Cyber Conquest held during the conference. The competition, targeted at tertiary students to enhance their cybersecurity situational awareness, comprised two tracks – Offensive Track and Defensive Track. In the Offensive track participants had to think like a cyber attacker to identify and exploit the loopholes found on the target network. Participants in the Defensive track were tasked to respond to cyber attacks.

SUTD's representatives at the Singapore Cyber Conquest. (From L to R: Arjun Singh Brar, Hiang Cheong Kai, Tiang Hui Hui, Pavithren S/O V S Pakianathan, Dhanya Lakshmi Janaki, Randolph Wong Wai Kit, Koh William, Muhammad Hatib Bin Abdul Aziz, Chiew Jun Hao)

Profiles

David Yau

Prof David Yau obtained the B.Sc. from the Chinese University of Hong Kong (CUHK), and M.S. and Ph.D. from the University of Texas at Austin, all in computer science. He joined SUTD in May 2013 as a Professor in the Information Systems Technology and Design pillar. Since 2010, he has been Distinguished Scientist at the Advanced Digital Sciences Centre, Singapore, where he is Cybersecurity Program Director. He is also Qiushi Chaired Professor in the Department of Control, Zhejiang University, China. From 1997 to 2013, he was Assistant Professor and then Associate Professor in Computer Science at Purdue University (West Lafayette).

David's research interests are in network protocol design and implementation, network and cyber-physical system privacy and security, quality of service, network incentives, and wireless and sensor networks. He received a CAREER award from the U.S. National Science Foundation in 1998, for research in network QoS provisioning.

David served as Associate Editor of IEEE/ACM Transactions on Networking (2004-09) and (Springer) Networking Science (2012-13). Since 2014, he's been on the editorial board of Journal of Big Data Research (Elsevier). He was technical program committee (TPC) co-chair (2006) and steering committee member (2007-09) of IEEE International Workshop on Quality of Service (IWQoS); vice general chair (2006), TPC co-chair (2007), and TPC area chair (2011) of IEEE International Conference on Network Protocols (ICNP); TPC track co-chair (2012) of IEEE International Conference on Distributed Computing Systems (ICDCS); and TPC track co-chair (2013) of IEEE International Conference on Green Computing and Communications (GreenCom). In 2010, he co-organised the first ADSC Smart Grid Symposium with the Experimental Power Grid Center of the Agency for Science, Technology and Research (A*STAR).

Sun Jun

Jun received Bachelor and PhD degrees in computing science from National University of Singapore (NUS) in 2002 and 2006. In 2007, he received the prestigious Lee Kuan Yew postdoctoral fellowship in School of Computing of NUS. In 2010, he joined Singapore University of Technology and Design as an Assistant Professor. He was a visiting scholar at MIT from 2011-2012. Jun's research interests include software engineering, formal methods, software engineering, programme analysis and cyber-security. He is the co-founder of the PAT model checker. To date, he has more than 100 journal articles (including TSE, TOSEM, etc.) or peer-reviewed conference papers (including ICSE, FSE, CAV, TACAS, FM, etc.). Jun is also the general co-chair of ICECCS'13 and PRDC's and program co-chair of FM'14. He is a number of conference programme committee including FM'15 and ICSE'16.

Priscilla Pang

iTrust welcomes Priscilla, who joined iTrust on 8 Oct 2015 as Manager. She assists iTrust Research Director Prof Yuval Elovici in project management for projects related to IoT. Priscilla graduated with a Masters of Science (Information Studies). Prior to joining iTrust, she was working in a national research agency in various capacities ranging from admin management, event coordination, and project management. Priscilla was involved in various project implementation to improve the administration and process flow of the organisation. Building on her core strength, she was instrumental in the implementation of document management guidelines and information sharing policies for the shared service Business Centre. Priscilla enjoys meeting and working with different people. In her leisure time, she loves spending time with her family.

Jonathan Goh

Jonathan joined iTrust as Research Scientist on 2 Nov 2015. Prior to joining SUTD, he was at the Institute for Infocomm Research (I^2R), A*Star where he was the Lab Head of the Multimedia Forensics & Security Lab. During his time in I^2R, he was involved in identifying new research domains related to the changing technology landscape. He was the Principal Investigator (PI) for various research projects and also the Co-PI of the recently awarded NRF Cyber Security grant.

Jonathan received both his PhD and BSc degrees from the University of Surrey in 2011 and 2006 respectively. His research interest includes cyber security and forensics, computer vision and machine learning. During his career, he has published multiple publications and filed for patents in the Cyber Forensics domain. He is particularly interested in the application of deep learning to the areas of forensics and security. His work on deep learning helped his team to win the Cyber Security and Data Mining Competition in 2014.

Outreach

Visits to iTrust and SWaT lab

Over the past few months, iTrust and the SWaT lab continued to attract distinguished visitors locally and worldwide. They were keen to understand more about the exciting work iTrust was embarking on, and explore commercial, research and educational collaborations.

On 13 Aug, the **External Advisory Board** members from SUTD's Information Systems Technology and Design (ISTD) Pillar visited the SWaT lab as part of its annual meeting. Senior management representatives from a group of member companies in the **Finnish Information Security Cluster (FISC)** paid a visit to iTrust on 28 Aug to explore cooperation opportunities with Singapore government agencies and educational and research institutes. These companies include Bittium, Codenomicon, DISE, Flashtec, Fujitsu Finland, Granite Partners, Jykes, Nixu Corporation, SSH Communications Security and VTT Technical Research Centre of Finland. The senior management team of **Certis CISCO** - a security organisation offering a range of physical, IT and data security services - visited SUTD and iTrust on 16 Sep. They were keen to understand the capabilities of our ISTD Pillar students, with the view of offering scholarship and employment opportunities. Representatives from **Ernst & Young's** Advisory Services (IT) visited iTrust and SWaT lab to gain insight on iTrust's capabilities. From the discussions, there were several potential areas of collaboration, such developing policies, framework and awareness programmes in cyber security for the energy sector. Prof. Isaac Ben-Israel, Director of Blavatnik Interdisciplinary Research Centre (ICRC) at **Tel Aviv University** led a team of representatives on his visit to iTrust on 23 Oct. They were accompanied by the National Cybersecurity R&D (NCR) directorate from NRF as well. Following a tour to SWaT testbed, hosted by Prof Aditya Mathur, the two universities shared and exchanged ideas on their current research work.

Student intern from CHIJ St Nicholas Girls' School

iTrust also welcomes its first secondary school student intern! Tan Ying Ting is a Secondary One student from CHIJ St Nicholas Girls' School. After attending the Reverse Malware Engineering Workshop organised by iTrust in June this year, Ying Ting's interest and curiosity in cyber security was piqued. She took the initiative to write in to iTrust seeking for opportunities to gain more knowledge in this area, and was offered a student research assistant role in the project on Research & Security Innovation Lab for IoT. In this project, she will assist the project team in discovering ways in which hackers can hack into a drone. Ying Ting will be with iTrust from Nov 2015 to Jan 2016.

Publications

1. S.-Y. Chang, J. Lee, and Y.-C. Hu, “Noah: Keyed Noise Flooding for Wireless Confidentiality," in Proc. ACM International Conference on Modeling, Analysis and Simulation of Wireless and Mobile Systems (MSWiM), Cancun, Mexico, Nov. 2015, pp. 1- 8.

2. J. Ryu, J. Lee, and T. Q. S. Quek, “Trust degree-based cooperative transmission for communication secrecy,” in Proc. IEEE Global Communication Conference (Globecom), San Diego, CA, Dec. 2015, pp. 1-6.

3. Y. Sun, W.-T. Li, W. Song. and C. Yuen, “False Data Injection Attacks with Local Topology Information against Linear State Estimation", IEEE ISGT-Asia 2015.

4. W.-T. Li, C.-K. Wen, J.-C. Chen, K.-K. Wong, J.-H. Teng, and C. Yuen, "Location Identification of Power Line Outages Using PMU Measurements with Bad Data", IEEE Transactions on Power Systems, Oct 2015.

5. 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 Communication Conference (Globecom), San Diego, CA, Dec. 2015, pp. 1-6.

6. J. Wang, J. Lee, and T. Q.S. Quek, "Secure Communication for Massive MIMO Uplink in the Presence of Co-located and Distributed Eavesdroppers" in Proc. IEEE Int. Conf. Wireless Commun. and Signal Processing, Nanjing, China, Oct. 2015, pp. 1-5, Invited Paper.

7. J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, “Jamming-aided secure communication in massive MIMO Rician channels,” IEEE Transactions on Wireless Communication, vol. 14, no. 12, Dec. 2015.

8. J. Zhang, C. Yuen, C.-K. Wen, S. Jin, K.-K. Wong, H. Zhu, "Large System Secrecy Rate Analysis for SWIPT MIMO Wiretap Channels", IEEE Information Forensics and Security, Aug 2015.

iTrust Staff

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

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

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

Mr Mark GOH
Manager
mark_goh@sutd.edu.sg

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

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

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

Ms Priscilla PANG
Manager
priscilla_pang@sutd.edu.sg

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

iTrust
Centre for Research in Cyber Security

itrust.sutd.edu.sg

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