An iTrust Newsletter Oct - Dec 2016 | Issue 7

iTrust Times

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN
Established in collaboration with MIT

From Centre Director's Desk

Dear Reader:

Greetings from iTrust, and welcome to this seventh issue of iTrust Times.

I invite all readers to participate in the 18th IEEE High Assurance Systems Engineering (HASE) 2017 conference. The conference is scheduled for January 12-14, 2017. We have a vibrant and exciting conference programme that includes keynote and invited speakers from US, Europe, and Singapore, research talks, and two panels. Details are at http://itrust.sutd.edu.sg/hase2017.

iTrust is proud to have completed Cyber Physical System Protection – the first 3-year research project funded by the Ministry of Defence. Thanks to our brilliant faculty and research staff, I am happy to report that ALL deliverables, as approved in the original proposal, were met at each of the six deadlines! This project resulted in new technologies and tools. Our accomplishments include: design and operationalisation of two testbeds for water treatment and distribution; a novel CPS simulation and verification tool; technologies for secure communications in CPS; and a novel open source tool named MiniCPS. In addition to research publications at top venues, the project generated two provisional patents for novel PLC-based attack detection technologies, namely Water-Defence and Argus. Negotiations are underway with investors to commercialise these technologies.

The international footprint of iTrust continues to expand. We now have 11 collaborators in countries spanning North America, Europe and Asia. iTrust's educational landscape is also expanding. iTrust will be a key partner in SUTD's recently launched Master of Science in Security by Design (MSSD) programme. This is a one-of-a-kind graduate level programme is designed specifically for engineers. Details are available at https://istd.sutd.edu.sg/mssd/message-mssd-committee.

As always, we would like to hear from you, and are always looking for collaborators who may wish to use our unique testbeds for security research here at iTrust!

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

In This Issue

- Masters of Science in Security by Design
- Research project updates
- HASE 2017
- GovWare 2016

Events

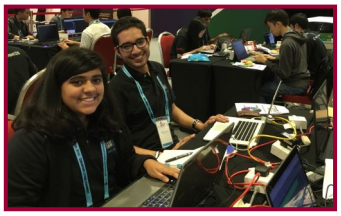
Singapore International Cyber Week (SICW) 2016

The inaugural SICW is organised by the Cyber Security Agency of Singapore (CSA). Held over three days from 10 to 12 Oct 2016, it featured multiple events, including the 25th edition of GovernmentWare (GovWare), the inaugural Smart Nation IoT Security Conference 2016 and the 7th Singapore Cyber Conquest (SCC).

At this year's GovWare, iTrust was given the opportunity to showcase its research projects. Leveraging on the conference theme of "Building a Secure Smart Nation", iTrust showcased three related projects related: Advancing Security of Public Infrastructure using Resilience and Economics, Research & Security Innovation Lab for IoT and Security by Design for Interconnected Critical. iTrust received a stream of conference attendees who were keen to find out more about iTrust and its work.

iTrust's Research Director Prof Yuval Elovici was invited to present at the Smart Nation IoT Security Conference. Titled "Detecting Compromised Consumer IoT Devices: Challenges and Research Directions", he presented on the capabilities of the IoT security testbed available at iTrust, such as testing an IoT device's security against a set of security requirements. In response, he also presented on the challenges and research direction of developing innovative technologies that can act as a preventive mechanism (see following article in "Research Focus".)

iTrust also sent two teams of four SUTD undergraduates to compete in the SCC, a computer and network security challenge that is designed to test the participants' skills and wit in a cyber range. Participants were scored based on the computer and network security challenges that they had to resolve. The challenges covered topics such as penetration testing, malware analysis and digital forensics and incident response.



SUTD undergraduates at the SCC (left to right): Claudia Aw, Muhammad Syuqri, Dhanya Janaki and Arjun Singh

18th IEEE International Symposium on High Assurance Systems Engineering (HASE)

This is the first time HASE is held in Singapore, and iTrust is proud be the organiser for next year's symposium. At the close of the Call for Papers, we received about 50 submissions. These are being reviewed by panel of a high quality of Programme Committee members; authors whose papers are accepted will be notified by 24 Oct 2016. We thank you for your submissions and support!

HASE 2017 will be held from 12 to 14 Jan 2017 at Grand Copthorne Waterfront Hotel. The draft programme and other details can be found on HASE 2017 website: http://itrust.sutd.edu.sg/hase2017.

23rd ACM Conference on Computer and Communications Security

The exponential increase of Internet of Things (IoT) devices has resulted in a range of new and unanticipated vulnerabilities associated with their use. IoT devices from smart homes to smart enterprises can easily be compromised. iTrust post-doc researcher Dr Vinay Sachidananda presented on "Towards Exposing Internet of Things: A Roadmap" at the ACM CCS, Vienna, Austria, in Oct 2016. The paper included preliminary work and results on the security analysis of vulnerabilities of IoT devices using penetration testing methods and capabilities available at iTrust's IoT security testbed, such as fingerprinting and vulnerability scan. Dr Sachidananda also introduced an Adaptable and Tunable Framework (ATF) for testing IoT devices.

11th International Conference on Critical Information Infrastructures Security

PhD student Adepu Sridhar presented two papers at CRITIS,Paris, France, on 11 and 12 Oct 2016. In "A Six-Step Model (SSM) for Safety and Security Analysis of Cyber-Physical Systems," the proposed SSM incorporated six hierarchies of a CPS: functions, structure, failures, safety countermeasures, cyber-attacks, and security countermeasures. The inter-dependencies between these dimensions were defined using a set of relationship matrices. SSM enabled comprehensive analysis of CPS safety and security, as it used system functions and structure as a knowledge-base for understanding what effect the failures, cyber-attacks, and selected safety and security countermeasures might have on the system.

Owing to the limited availability of operational datasets in in securing CPS, the second paper on "A Dataset to Support Research in the Design of Secure Water Treatment Systems" provided a realistic dataset that could be utilised to design and evaluate CPS defence mechanisms. The large scale labelled dataset that was presented included data obtained from SWaT during normal operation and when it was under attack. both normal data and attacked data obtained from the SWaT testbed.

Research Focus

Network Engineering Techniques for Wireless Security

This project aims to establish a new paradigm to secure wireless networks by developing network engineering techniques exploiting intrinsic physical channel properties and network configuration such as spatial node distribution and communication protocol for enhancing wireless security. Achievements in the various tasks under this project are described below.

In wireless communication, users are subject to eaves-dropping due to the broadcast nature of the medium. Taking into account the bursty nature of the sources in a communication network, the researchers investigated the **stability region of a two-user broadcast channel**, where one of the receivers with secrecy constraint has full duplex capability. The stability region is obtained when Receiver 2 can perform successive decoding. In this case, the role of jamming signal to ensure secrecy of the packets intended to Receiver 1 becomes more crucial. It is also found that performing power control at the Transmitter or Receiver 1 can enlarge the stability region significantly. When the self-interference cancelation is not efficient, performing power control at Receiver 1 can help to increase the stability region significantly.

With the emergence of ultra dense networks, cooperation can be performed by more transmitters to achieve a better performance. While more transmitters translate to more power received by the legitimate user (LU), it also means more power leakage to potential eavesdroppers. For an LU to efficiently connect to transmitters, a cooperative range is used. The researchers investigated the optimal **cooperative range for communications secrecy in an ultra -dense network** where the source nodes and eavesdroppers are randomly distributed. The secrecy outage probability was analysed for two cooperation modes - analytical expressions and analytical approximations. Simulation results showed that the optimal cooperative range which minimises the secrecy outage depends on the densities of both the source nodes and eavesdroppers as well as the cooperation mode adopted at the transmitters. Compared with direct transmission, the independent phase adjusting mode exploiting the downlink CSI can achieve lower secrecy outage probability with a larger optimal cooperative range.

A new secure group based **device-to-device (GD2D) communication (with functional fine-grained access control)** is proposed for mobile networks to support the needs of performance and location awareness applications. In addition, to protect user privacy, the access control adopts the predicate-based encryption (PBE) to overcome Sybil attacks – a type of security threat when a node in a network claims multiple identities and thus has a disproportionally large influence – and enhance privacy protection and membership management.

In smart grid, the total electrical consumption of a particular area is determined by aggregating the measurements of smart meters (SMs) in that area. While cryptographic systems can help to ensure the privacy of the individual measurements of the SMs, they require complicated computations and key-management infrastructural support. The team proposed a novel physical **channel-based scheme for privacy preservation in**

data aggregation, without the use of a cryptographic system, for both slow–fading and fast–fading scenarios and imperfect channel estimation. This is done by adding jamming signals that are designed to cancel out each other at the aggregator. The scheme can also resist different types of attacks such as eavesdropping, compromising, and differential attacks even when they are colluding. Simulation results show that the mean squared error of the total measurements is significantly lower than that of a traditional scheme.

Research & Security Innovation Lab for IoT

The exponential increase of IoT devices has resulted in a range of new and unanticipated vulnerabilities associated with their use. The lab focuses on identifying these IoT security risks, develops and demonstrates various security perspectives of IoT. The project addresses four major security challenges common in IoT: security, privacy, integrity, and authorisation. The project is led by iTrust's Research Director Prof. Yuval Elovici, in collaboration with Ben-Gurion University, Israel.

Automatic Security Testbed

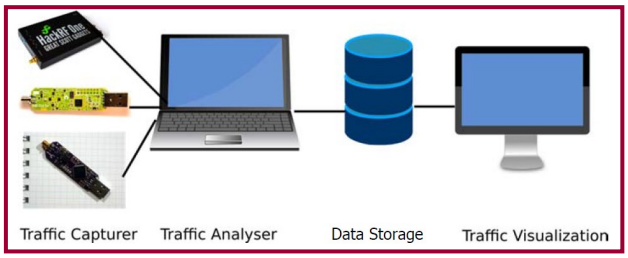
One of the first deliverables for this project is the setting up of an automatic security testbed for IoT devices, which enables the testing of various IoT devices against a set of security requirements with predefined use cases. The testbed consists of hardware and software components for experiments of wide-scale testing deployments. A variety of tests can be conducted: standard, context-based, data, and side-channel. The IoT testbed offers different types of testing environments which simulate various sensor activity (GPS, movement, Wi-Fi, etc.) and performs predefined and customised security tests. In addition, any predefined and customised security tests. In addition, any relevant simulator and/or measurement and analysis tool can be deployed in the testbed environment in order to perform comprehensive testing. The testbed also collects data while performing the security analysis to conduct a security forensic analysis. Finally, a report is produced, which lists the type of IoT device tested, its connectivity and the communication protocols supported, and the security test cases executed and their status (PASS or FAIL).

The IoT automatic security testbed at iTrust

Use Cases

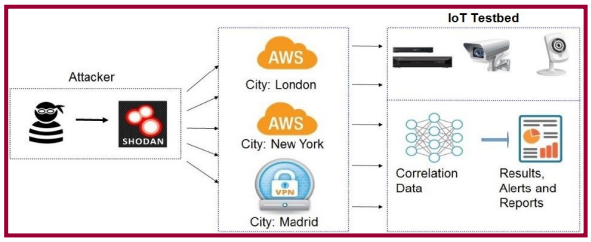
In the first phase of this project, two use cases were identified – an IoT scanner and an IoT honeypot. Initial results on the use cases are described below.

IoT Scanner: The first use case integrates a range of radios to allow local reconnaissance of existing wireless infrastructure and participating nodes. The architecture of the scanner is shown in the figure below. The scanner intercepts Wi-Fi and Bluetooth signals and applies a set of filters to identify traffic of interest. Relevant extracted information such as MAC addresses are sent to the data storage for further analysis and visualisation. The visualisation component displays the connectivity graph of the underlying network and a summary of network, and allows the researchers to interact with the data.



IoT Scanner architectural view

IoT HoneyPot: The motivation is to learn common attack vectors, gather statistics on the attacks and understand the relationship between the geographic location of IoT devices and their risk of being attacked. Researchers have deployed 35 cloud servers, each designated as a honeypot (but not identified as one by SHODAN), from three different cloud service providers in various cities. All the traffic (device solicitations or attacks) are then diverted to actual IP cameras or Network Video Recorders. Current work is focusing on the process of maximising the amount of traffic received and analysing the data gathered.



High level design of the IoT honeypot

Cyber Physical System Protection

Project Cyber Physical System Protection was launched in October 2013 and funded by the Ministry of Defence, Singapore. The focus of the project is to improve our understanding of cyber threats to CPS and develop and experiment with strategies to mitigate such threats. Throughout its three years, the research team has discovered, implemented, and experimentally evaluated several fundamental techniques that will go a long way in helping to defend Singapore's public infrastructure from malicious actors.

Among the deliverables for this project is the Secure Water Treatment (SWaT) testbed, which has enabled iTrust to host researchers and engineers from universities and commercial organisations for research, testing and collaborations. From it, two provisional patents have been filed. One patent, titled "Water Defence," encapsulates software mechanism for the distributed detection of multi-point attacks on water treatment plants. Another, titled "Argus: An Orthogonal Defence Mechanism for Water Treatment Systems," encapsulates a hardware/software mechanism for defending water treatment plants.

There are two tracks for this project: (A) Develop and experiment with design strategies and tools for achieving end-to-end resilience to attack; and (B) Develop and experiment with trustworthiness and security for data Acquisition and communications in CPS. Deliverables for these two tracks are described below.

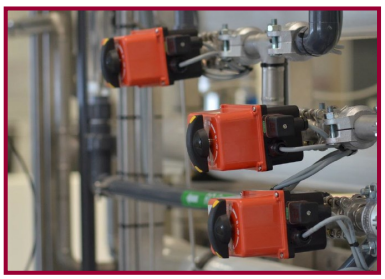
Track A: Two tools, TAuth and HyChecker, with guidelines for systematic application, were developed. In using TAuth, researchers were able to identify known and unknown security vulnerabilities in real-world security protocols. TAuth is suited for small critical components in a CPS system like the security protocols. On the other hand, HyChecker is used to model and analyse complex CPS, based on different models as well as analysis methods. HyChecker takes a model of a CPS in the form of a Python programme and systematically samples behaviours of the system and evaluates the likelihood of the system violating certain safety or security property. HyChecker is available publicly at http://apps.liyi.website/SMC/.

Track B1: Researchers extended an attacker model by assuming that the attacker has complete system knowledge such as knowing the thresholds selected to raise alerts, thereby carrying out a stealthy attack. Such a model would allow defenders to develop stronger intrusion detection metrics to safeguard against such attacks. While developing the MiniCPS - an extensible, reproducible research environment simulating communications and physical-layer interactions in CPS - the team discovered that the MiniCPS could be employed as a CPS Honeypot to attract malicious users and gain knowledge on attack strategies.

Track B2: Researchers evaluated the vulnerability of physical topology of electric grids, and in the process defined a new performance metric that could identify which power lines would lead to cascading failure when under attack, and the severity of those attacks. They also developed a coordinated cyber-physical attack strategy against state and topology, to help identify which power line to attack coupled with the intention to mislead the grid operator.

Track B3: An extension to the project, this track analyses security against performance trade-offs. Researchers developed a Selective Packet Authentication, in which a deep packet analysis is performed to determine if the data that passes through is critical or not. As a result, only critical data is signed, thereby reducing the network latency. More importantly, such a process increases the security of the existing network protocol and ensures that the data from industrial controller is protected from man-in-the-middle attacks.

Masters of Science in Security by Design



SUTD is proud to announce that it will be offering the Master of Science in Security by Design (MSSD) programme from Sep 2017. The MSSD is aimed at educating and training manpower to develop expertise in the design, analysis, implementation and testing of secure enterprise and cyber physical systems.

This one-year full-time programme is specially designed for working engineers and computer scientists. Students can expect to gain knowledge on securing public infrastructure, and supplement their knowledge via ready access to some of the world's best testbeds in cyber physical systems.

Selected students will also have the opportunity to complete their Masters thesis or project at collaborating universities in the US, UK and the Netherlands.

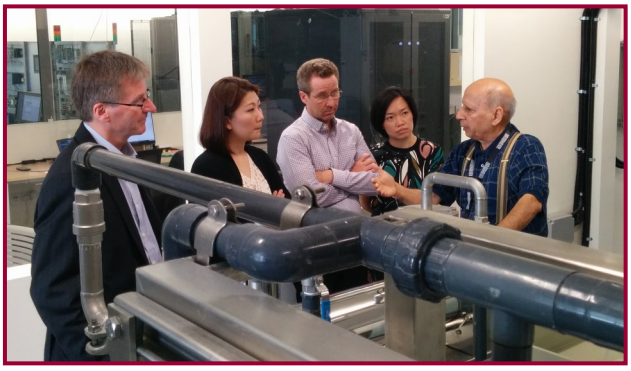
To cater to a range of students, full-time (three academic terms in one year) and part-time (six academic terms in two years) courses for MSSD are available. Other than coursework, students are required to undertake a project in Term 3. MSSD is open to graduates with a degree in engineering, physics, chemistry or mathematics, with sound mathematical background and computer programming skills.

The first yearly intake for the MSSD will commence in Sep 2017. The academic year for the MSSD is from Sep to the following Aug. Application for the Sep 2017 intake will commence on 21 Nov 2016 and close on 30 Mar 2017. For further updates on the MSSD programme, please subscribe to the mailing list at http://tinyurl.com/sutdmssd. You may also contact Office of Graduate Studies, Ms Ong Ai Ling at 6303 6683 or email to mssd@sutd.edu.sg.

Visits

ISTD External Advisory Board

The Information Systems Technology and Design (ISTD) pillar's External Advisory Board (EAB) saw a new makeup of its board members, with Chairperson Prof Richard A. DeMillo extending his appointment. As part of its annual meeting on 25 and 26 Aug 2016, some EAB members from the Information Systems Technology and Design (ISTD) pillar visited iTrust's testbed facilities. This year, other than the Secure Water Treatment (SWaT) testbed, the members also got a walkthrough of the Water Distribution (WADI) testbed by Prof Aditya Mathur, as well as the upcoming Electrical Control and Intelligent Control testbed.



Prof Aditya explaining the SWaT testbed processes to EAB members (from left to right) Prof Ross Murch, Ms Angeline Poh, Mr Shamus Weiland, Prof Alexander Pretschner, and Ms Peggy Mah

Ministry of Defence, Singapore

Prof Aditya describing to Mr Ng (right) how the Electrical Power and Intelligent Control (EPIC) testbed could contribute to iTrust's research in CPS

Permanent Secretary (Defence Development), MINDEF, Mr Ng Chee Khern visited Temasek Lab@SUTD, iTrust and the SUTD-MIT International Design Centre (IDC) on 10 Oct 2016 to better understand the projects funded by MINDEF. He was given an overview by the respective directors, SUTD Provost Prof Chong Tow Chong, Prof Aditya Mathur, and Prof Kristin Wood, as well as project demonstrations during his tour of the labs. Mr Ng was accompanied by Chief Defence Scientist Mr Quek Gim Pew and DSO National Laboratories Chief Executive Mr Cheong Chee Hoo respectively. Mr Ng was impressed with the laboratories and research work done TL@STUD and iTrust and how they could contribute to the defence of Singapore.

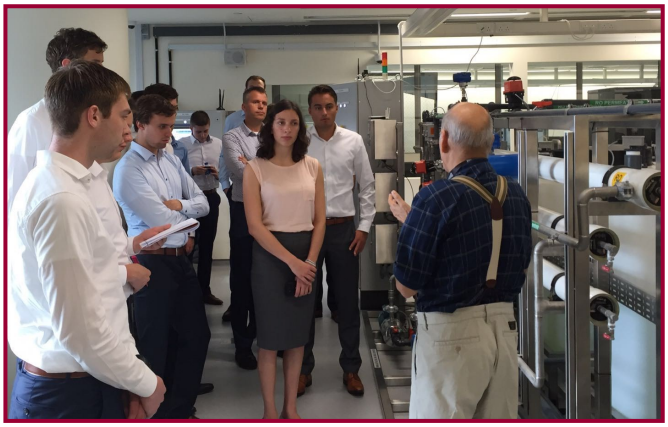
Ministry of Defence, Brunei

Prof Aditya presented with a token of appreciation from the Deputy Permanent Secretary (Technology)

At MINDEF's invitation, the Deputy Permanent Secretary (Technology) from Brunei, Captain (Rtd) Haji Mohammad Amirul Shahnoel bin Haji Mohammad Noeh was given an overview of iTrust's research capabilities in cyber security by Prof Aditya and Prof Yuval, and was given a tour of iTrust's four testbeds - SWaT, WADI, EPIC and IoT. Such exchanges and discussions with neighbouring countries aid in fostering cyber capacity building among ASEAN member states, one of the areas to enhancing cybersecurity in ASEAN (Association of Southeast Asian Nations), announced by Dr Yaacob Ibrahim, Minister for Communications and Information & Minister-in-Charge of Cybersecurity at the opening ceremony of the Ministerial Conference on Cybersecurity on 11 Oct 2016.

University of Twente

A group of 30 visitors from University of Twente, comprising Bachelor and Master students, researchers and committee members were at SUTD on 28 Sep 2016 as part of their "Intelligent & Secure Cities" theme-related study tour. They were briefed by Asst Prof Tony Quek on ISTD's Graduate Programme, and also invited by Prof Aditya Mathur, who holds concurrent appointments as ISTD's Head of Pillar and iTrust Centre Director, to collaborate in cyber security research at iTrust. The visitors were given a tour of iTrust's testbeds to better understand iTrust's research focus and capabilities.



Prof Aditya interacting with students and researchers from University of Twente

Profiles

Tony Quek

Tony Quek received the B.E. and M.E. degrees in Electrical and Electronics Engineering from Tokyo Institute of Technology, Tokyo, Japan, respectively. At MIT, he earned the Ph.D. in Electrical Engineering and Computer Science. He joined the Singapore University of Technology and Design (SUTD) from July 2012 and he is currently a tenured Associate Professor. He also serves as the deputy director of the SUTD-ZJU Innovation, Design and Entrepreneurship Alliance. His main research interests are the application of mathematical, optimisation, and statistical theories to communication, networking, signal processing, and resource allocation problems. Specific current research topics include heterogeneous networks, green communications, wireless security, internet-of-things, big data processing, and cognitive radio.

Dr. Quek has been actively involved in organising and chairing sessions, and has served as a member of the Technical Program Committee as well as symposium chairs in a number of international conferences. He is serving as the Workshop Chair for IEEE Globecom in 2017 and the Special Session Chair for IEEE SPAWC in 2017. He is currently an Editor for the IEEE Transactions on Communications and an Executive Editorial Committee Member for the IEEE Transactions on Wireless Communications. He was Editor for the IEEE Wireless Communications Letters, Guest Editor for the IEEE Signal Processing Magazine (Special Issue on Signal Processing for the 5G Revolution) in 2014, and the IEEE Wireless Communications Magazine (Special Issue on Heterogeneous Cloud Radio Access Networks) in 2015. He is a co-author of the book "Small Cell Networks: Deployment, PHY Techniques, and Resource Allocation" published by Cambridge University Press in 2013 and the book "Cloud Radio Access Networks: Principles, Technologies, and Applications" by Cambridge University Press.

Dr. Quek was honored with the 2008 Philip Yeo Prize for Outstanding Achievement in Research, the IEEE Globecom 2010 Best Paper Award, the 2012 IEEE William R. Bennett Prize, the IEEE SPAWC 2013 Best Student Paper Award, the IEEE WCSP 2014 Best Paper Award, the IEEE PES General Meeting 2015 Best Paper, and the 2015 SUTD Outstanding Education Awards - Excellence in Research.

Giedre Sabaliauskaite

Giedre is the co-principal investigator for the joint-project between Nanyang Technological University and SUTD on Cyber Security for Autonomous Vehicles. She joined SUTD in 2013 as a post-doctoral researcher. Giedre received her PhD degree in Software Engineering from the Osaka University, Japan, in 2004, following her BSc and MSc degrees in Information Systems from the Kaunas University of Technology, Lithuania. After completing her PhD, she worked in academia and industry in several countries. This includes the Fraunhofer Institute for Experimental Software Engineering (IESE) in Germany, where she worked as a scientist and a consultant. She then worked as a software quality engineer at Critical Software, a Portuguese-based software development transnational company. Prior to joining SUTD, Giedre was a post-doctoral

researcher at the Lund University in Sweden.

Giedre is interested in cross-disciplinary and emerging complex topics in relation to the organisations, the design and management of systems, the role of customers, and the strategies to deal with increasingly uncertain environments. Her current research focuses on safety and security of cyber physical systems.

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. Autonomous Vehicle Security
   c. Research & Security Innovation Lab for IoT
2) **Research Assistant** in the following projects:
   a. Advancing Security of Public Infrastructure using Resilience and Economics
   b. 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

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

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

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

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

Mr Mark GOH
Manager
mark_goh@sutd.edu.sg

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

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

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

Kandasamy MURUGANANDAM
Specialist (IoT)
Kandasamy_m@sutd.edu.sg

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

Ms Priscilla PANG
Manager
priscilla_pang@sutd.edu.sg

iTrust
Center for Research in Cyber Security
itrust.sutd.edu.sg