An iTrust Newsletter

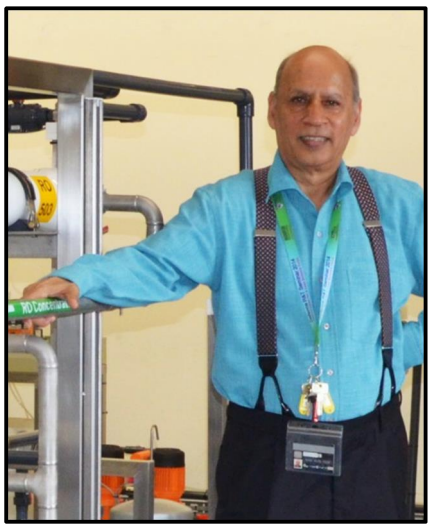
Apr – Jun 2015 | Issue 1

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 inaugural issue of iTrust Times.

iTrust was established at SUTD in 2012 through a grant from the Ministry of Defence (MINDEF). Since then iTrust has evolved into a fast maturing research organisation. It is a multidisciplinary umbrella for nearly all of cyber security research at SUTD. iTrust now has research projects funded by various government agencies. Its international partnership is growing and already includes MIT and Imperial College.

Research in cyber security is not new. Brilliant people at centres around the world are conducting cutting-edge research in this area. Sharp focus on the design of secure and safe Cyber Physical Systems (CPS) uniquely positions iTrust among its peers. iTrust researchers are investigating existing designs of public infrastructure for its safety and security in the presence of cyber attacks. These researchers have access to an in-house Secure Water Treatment (SWaT) testbed. Two additional testbeds, one for water distribution and another for Smart Grid, are in design and expected to be available for experimentation by early 2016.

Design of secure enterprise networks is another research track in iTrust. Professor David Yau leads the Cross-functional Information Systems for Decision Making project. This project focuses on network security threats. It adopts an inter-disciplinary research view - spanning systems security, natural language processing, machine learning, signal processing, and networking - to protect mission-critical network infrastructures.

The fast rise of connected devices has led to the Internet of Things (IoT). Research in the design of secure IoT devices and their interactions is yet another track within iTrust. This track is led by Professor Yuval Elovici who is establishing a state of the art laboratory for designing and testing secure IoT devices and their networks.

iTrust has designed a rich outreach program under the leadership of Mr. Ivan Lee. The LEET laboratory designed by Mr. Lee and his colleagues at SUTD, is where students in secondary and junior colleges are exposed to understanding cyber threats, and techniques for cyber defence, using active learning.

That in brief is what I would like to share with you in this inaugural issue of iTrust Times. Through this newsletter, my colleagues and I will continue to share with you the various events and research outcomes in iTrust.

Thank you for reading, and best wishes,
Aditya Mathur
Professor and Head of Information Systems Technology and Design Pillar
Centre Director iTrust

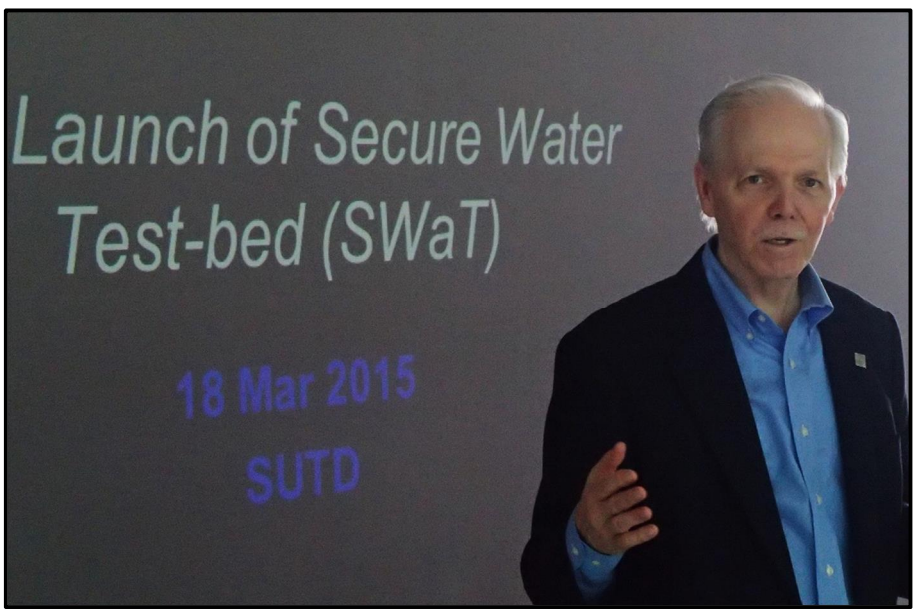
Overall process layout of SWaT

News

Launch of Secure Water Treatment System (SWaT) Testbed

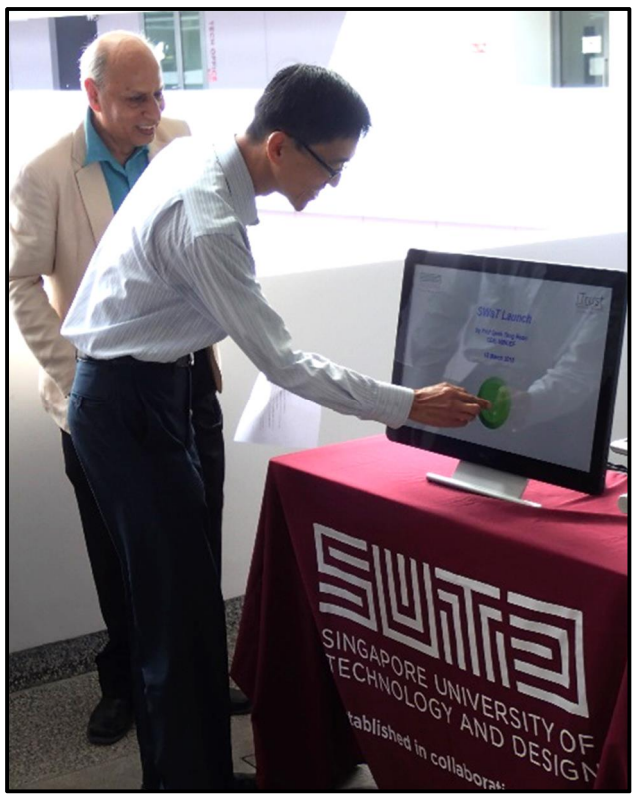
To enable experimentally validated research in the design of secure and safe CPS, iTrust is setting up a series of testbeds, with the SWaT testbed being the first. These testbeds will enable researchers to investigate issues through experiments related to the design of secure CPS.

The SWaT testbed was officially opened on 18 Mar 2015. In his welcome address, SUTD President Prof Tom Magnanti said, “We at SUTD and in this lab will be focusing on the security of CPS. We intend to do so by blending theory and applications, conducting foundational work, validated in experimental testbeds. We envision many opportunities and are excited as we undertake this journey and work alongside many collaborators.”



Prof Tom Magnanti giving his welcome address

The Guest of Honour at the event was Chief Defence Scientist (CDS) of MINDEF Prof Quek Tong Boon, who officiated the launch of the testbed. He noted in his opening remarks that the opening date coincided with the day “the world lost a scientific genius in Norbert Wiener,” considered the originator of cybernetics, and how "the foundations of the testbed - whether it is the controls, the connections between the physical and the computer systems - were laid by, and encapsulates the vision and genius of Norbert Wiener." Prof Quek was also joined by members from the National Research Foundation’s (NRF) International Advisory Panel (IAP).



Prof Quek launches the SWaT testbed by starting its operations

<u>Research</u>

Researchers at SUTD are building models of SWaT. These models will be used to conduct experiments aimed at understanding the response of SWaT to a variety of cyber attacks as well as conditions of natural disasters. The focus is on secure communications through coding and CPS redesign, and on the design of a layered defence mechanism that ensures a safe and secure system when cyber attackers are successful in entering the system through the network or internally. Experiments will lead to a better understanding of the strengths and weaknesses of existing defence mechanisms in SWaT that conform to current industry standards. This understanding will enable researchers to create novel designs, and assess their effectiveness through experiments, with the goal of defending a CPS against cyber and physical attacks as well as the effects of natural disasters.

“Our water treatment plants are key national infrastructure. Physically, they are heavily guarded and secured against intrusion and attacks. Housed within are complex and highly automated systems. These must also be safeguarded from cyber-attacks. The research that will come out of this SWaT testbed will help make our plants even more resilient against sabotage, making our water system to be that much more secure,” said Mr Peng Kah Poh, PUB’s director of Information Systems.

<u>Collaboration</u>

iTrust is collaborating with Cisco, National Instruments, NEC, Starhub, as well as several Singapore Government agencies in research on secure CPS and in the design of SWaT.

Prof Aditya explaining the operations of SWaT to members of NRF's International Advisory Panel. From left to right: Prof Howard Schmidt Partner, Ridge-Schmidt Cyber, LLC; Prof Quek Tong Boon, CDS, MINDEF; Sir John Beddington, Senior Adviser, Oxford Martin School; Prof Lui Pao Chuen, Advisor, NRF; Mr Khoo Boon Hui, Senior Advisor, Ministry of Home Affairs

iTrust: A Garden of Testbeds

In addition to the currently operational Secure Water Treatment (SWaT) testbed, iTrust is in the midst of designing three additional testbeds for research in cyber security. The Water Transmission and Distribution (WADI) testbed is designed to understand the impact of cyber attacks on the water storage and distribution systems. WADI, with its reconfigurable distribution network, will be integrated into SWaT as an extension. This integration will allow for a comprehensive study of the impact of cyber attacks on a city's water infrastructure and enable the assessment of new designs for defence against such attacks.

To enable investigations into the response of a power grid to a variety of cyber attacks, an end-to-end electric power testbed is being designed. This testbed, named Electric Power and Intelligent Control (EPIC), will consist of three distinct though interconnected subsystems, namely, power generation, transmission, and distribution. Both AC and DC generation sources will be available. A variety of reconfigurable and switchable loads, connected through smart meters, will be available for experiments with demand response strategies, as well as to understand the impact of cyber attacks on customers and grid equipment.

A myriad of challenging issues relating to security and privacy are rising, as simple as well as complex devices get connected to the Internet. Such devices, when connected over a network, form what is generally referred to as the Internet of Things (IoT) or Internet of Devices (IoD). iTrust is in the midst of designing a testbed for IoT that will allow researchers to experiment with devices to better understand the nature of attacks and design practical defence mechanisms. It will enable the researchers to understand the risks associated with IoT and demonstrate standards for secured IoT architecture.

Soon, iTrust will host a rich collection of testbeds mentioned above. A project to connect these testbeds via a CPS-bus is underway. The objective of this project is to allow iTrust's collaborators to access these testbeds for experimentation from anywhere in the world.

Profiles

Yuval Elovici

Professor Yuval Elovici joined iTrust in Sep 2014 as Research Director. In addition to his role at iTrust, he is also the director of the Telekom Innovation Laboratories at Ben-Gurion University of the Negev (BGU), head of BGU Cyber Security Research Centre, Research Director of iTrust at SUTD, and a Professor in the Department of Information Systems Engineering at BGU.

Yuval holds B.Sc. and M.Sc. degrees in Computer and Electrical Engineering from BGU and a Ph.D. in Information Systems from Tel-Aviv University. He served as the head of the software engineering program at BGU for two and a half years. For the past 11 years he has led the cooperation between BGU and Deutsche Telekom. Yuval has published articles in leading peer-reviewed journals and in peer-reviewed conferences. In addition, he has co-authored books on social network security and on information leakage detection and prevention.

His primary research interests are computer and network security, cyber security, web intelligence, information warfare, social network analysis, and machine learning. Yuval also consults professionally in the area of cyber security and is the co-founder of Morphisec, a startup company that develops innovative cyber-security mechanisms that relate to moving target defence.

Nils Ole Tippenhauer

Assistant Professor Nils Tippenhauer joined SUTD in February 2014 as an Assistant Professor at the Information Systems Technology and Design Pillar. He is also an adjunct research scientist with the Advanced Digital Sciences Centre (ADSC) in Singapore. Nils earned his Dr. Sc. in Computer Science from Swiss Federal Institute of Technology in Zurich (ETHZ) in 2012.

Before ETH Zürich, Nils received a degree in Computer Engineering (Dipl. Ing.) from the Hamburg University of Technology (Germany) in 2007, for which he received the K.-H. Ditze Award for best Master's Thesis, which was on side-channel attack-resistant embedded crypto.

Nils is interested in information security aspects of practical systems. In particular, he is currently working on security analysis of large heterogeneous systems such as (smart) power grids. In addition, Nils is interested in physical layer security aspects of wireless and embedded systems, for example secure ranging, distance measurements and communication using wireless signals. To date, he has (co-)authored more than a dozen publications in this field and received the best paper award at IFIP Wireless Days 2012.

Research Focus

Advancing Security of Public Infrastructure using Resilience and Economics

By Nils Ole Tippenhauer

Advancing Security of Public Infrastructure using Resilience and Economics is an interdisciplinary project combining the fields of Machine Learning, Control, Software, Water and Power Engineering for the security of CPS. The project team is a consortium comprising expert collaborators from the government, industry and local and overseas academia which will enhance the chances of real-world impact of the outcomes.

The project focuses on the cyber- and physical security of public infrastructure against malicious attacks. Our researchers will develop fundamental principles, techniques and soft- and hardware tools to enable the detection of, and defence from, cyber-attacks on CPS. In addition to network-based defence mechanisms, the team will also investigate more resilient control algorithms, economic incentives for defences and attestation mechanisms to ensure the correct programming of logic controllers.

The foundational theoretical work in this project will be complemented by the existing iTrust SWaT testbed, in addition to two testbeds simulating water and electrical power distribution (currently planned) will be constructed to provide a realistic operational environment for the researchers to demonstrate and assess the tools and methods developed.

Project collaborators include government agencies as well as those from the industry industry including Cisco, National Instruments, NEC Asia Pacific and Starhub; and academia collaborators from Massachusetts Institute of Technology (MIT), Nanyang Technological University (NTU) and University of Illinois Urbana-Champaign (UIUC).

Cyber Physical System Protection

By Aditya Mathur

This project lays the groundwork for research in Cyber Physical Systems (CPS) at SUTD. The focus of this project is to improve our understanding of cyber threats to CPS and to develop and experiment with strategies to mitigate such threats. The approach is based on well-understood technical foundations borrowed from the interdisciplinary fields of control theory, artificial intelligence, game theory, networking, and software engineering. The techniques we propose will be evaluated against, and demonstrated in, scaled and/or simulated versions of critical CPS in the iTrust laboratory environment.

The entire project is composed of three distinct tasks. Task A: Modelling and validation of a CPS. Task B: Protection of communications in a CPS. Task C: Design and construction of two realistic CPS testbeds for experimentation. Professors Daniel Jackson from MIT and Sun Jun from SUTD are the Co-PI's for Task A. Professor Nils Tippenhauer is the Co-PI for Task B and Professor Aditya Mathur for Task C. Significant progress has been reported during the first 18-months of the project. This is indicated in some of the publications listed in this newsletter. A Secure Water Treatment (SWaT) testbed is now operational. A smart grid testbed is under design and expected to be operational by early 2016.

Events

Secure Cyber-Physical (SCy-Phy) Systems Week 2015

SUTD will host its inaugural Cyber Security week, named SCy-Phy Systems Week, during June 22 to 26, 2015. Three key events are planned during this week. A Think-in event is scheduled for June 22 and 23 where researchers and practicing engineers from academia and the industry will discuss issues in securing large public infrastructure such as that for power and water. Participants will also have a unique opportunity to conduct carefully designed experiments with the Secure Water Testbed (SWaT) facility at SUTD. Dave Aucsmith and Yuval Elovici will conduct a cyber defence workshop on June 23 for members of various government agencies in Singapore. On June 24, Ivan Lee will lead a workshop on cyber security for students of junior colleges and polytechnics. Several invited talks are planned during the remainder of the week.

Outreach

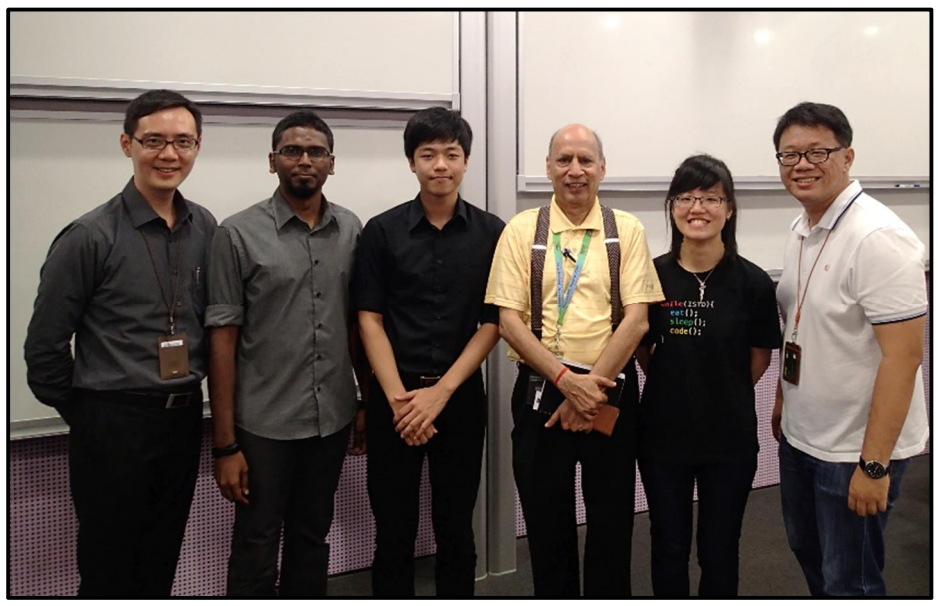
Student Seminar on Cyber Security

iTrust's inaugural cyber security student seminar was held on 25 Mar 2015. The objective of this seminar series is to interest students in the emerging field of cyber security and raise awareness of cyber crimes. Three Year 2 students from the Information Systems Technology and Design (ISTD) pillar presented varying topics on cyber security.

Dabin Lee opened the seminar by introducing the audience to the adware SuperFish. SuperFish was pre-installed on certain models of a commercial notebook with the intention of accessing private data for advertisement purposes. He discussed how SuperFish worked, how its vulnerabilities were exploited to make it easy for hackers to gain unrestricted access and steal private data, and the countermeasures that affected users can adopt to prevent their devices from being compromised.

The Internet of Things (IoT) is gaining popularity in its application in systems and devices such as smart grids and wearable technologies. Tiang Hui Hui presented how Advanced Persistent Threats – an attack in which there is unauthorised, prolonged, and undetected access to a network – can cause loss of data and privacy in IoT, especially in sensitive sectors such as national defence and finance.

Muhammad Hatib presented the vulnerabilities of BIOS (basic input/output system) in OS boot processes in which cyber criminals could gain access into one's computer. While a newer system – the UEFI (Unified Extensible Firmware Interface) – is designed to replace BIOS and helps to overcome some of BIOS' vulnerabilities, Hatib also reminded users that they also play a part to keep their systems secure.



Students pose for a picture with iTrust staff: (From left) Ivan Lee, iTrust Associate Director, Hatib, Dabin, Prof Aditya Mathur, iTrust Centre Director and Head of Pillar (ISTD), Hui Hui and Toh Jing Hui, Laboratory Technologist

Research Publications

1. Chen, X.; Sun, J.; and Sun, M. A., "Hybrid Model of Connectors in Cyber-Physical Systems." In Proceedings of International Conference on Formal Engineering Methods (ICFEM), pp. 59-74, 2014
2. X. Chen, C. Yuen, Z. Zhang, "Exploiting Large-Scale MIMO Techniques for Physical Layer Security with Imperfect CSI", Globecom 2014
3. X. Chen, L. Lei, H. Zhang, C. Yuen, "On the Secrecy Outage Capacity of Physical Layer Security in Large-Scale MIMO Relaying Systems with Imperfect CSI", ICC 2014
4. Sheng-Yuan Chiu, Hoang Hai Nguyen, Rui Tan, David K.Y. Yau, and Deokwoo Jung. JICE: Joint Data Compression and Encryption for Wireless Energy Auditing Networks. In Proc. IEEE Int'l Conf. Sensing, Communication, and Networking (SECON), Seattle, WA, June 2015
5. H. S. Dau, W. Song, C. Yuen, "On the Existence of MDS Codes Over Small Fields With Constrained Generator Matrices", ISIT 2014
6. H. S. Dau, W. Song, C. Yuen, "On Block Security of Regenerating Codes at the MBR Point for Distributed Storage Systems", ISIT 2014
7. H. S. Dau, W. Song, C. Yuen, "On Block Security of Regenerating Codes at the MBR Point for Distributed Storage Systems", ISIT 2014
8. S. H. Dau, W. Song, C. Yuen, "On Simple Multiple Access Networks", IEEE JSAC – Network Coding for Wireless Communications, Nov 2014
9. S. H. Dau, W. Song, C. Yuen, "Secure Erasure Codes With Partial Decodability", ICC 2015
10. S. H. Dau, W. Song, C. Yuen, "Weakly Secure MDS Codes for Simple Multiple Access Networks", ISIT 2015
11. Li, L.; Hu, H.; Sun, J.; Liu, Y.; and Dong, J. S., "Practical Analysis Framework for Software-Based Attestation Scheme." In Proceedings of International Conference on Formal Engineering Methods (ICFEM), pp. 284-299, 2014
12. Chris Y.T. Ma and David K.Y. Yau. On Information-theoretic Measures for Quantifying Privacy

Protection of Time-series Data. In Proc. ACM Symp. Information, Computer, and Communications Security (ASIACCS), Singapore, April 2015

10. Nageswara S.V. Rao, Stephen W. Poole, Chris Y.T. Ma, Fei He, Jun Zhuang, and David K.Y. Yau. Defense of Cyber Infrastructures Against Cyber-Physical Attacks Using Game-Theoretic Models. Risk Analysis. Accepted for publication

11. G. Sabaliauskaite, A. P. Mathur, “Aligning Cyber-Physical System Safety and Security”, in Proceedings of the 1st Asia-Pacific Conference on Complex Systems Design & Management (CSD&M Asia 2014), 2014, pp. 41-53, doi: 10.1007/978-3-319-12544-2_4. (Best academic paper award)

12. G. Sabaliauskaite, A. P. Mathur, “Countermeasures to Enhance Cyber-Physical System Security and Safety”, in Proceedings of the 11th IEEE International Workshop on Software Cybernetics (IWSC 2014), 38th Annual IEEE International Computers, Software, and Applications Conference (COMPSAC 2014), pp. 13-18, 2014, doi: 10.1109/COMPSACW.2014.6.

13. G. Sabaliauskaite, A. P. Mathur, “Design of Intelligent Checkers to Enhance the Security and Safety of Cyber Physical Systems”, in Proceedings of the 11th IEEE International Workshop on Software Cybernetics (IWSC 2014), 38th Annual IEEE International Computers, Software, and Applications Conference (COMPSAC 2014), pp. 7-12, 2014, doi: 10.1109/COMPSACW.2014.128.

14. Li, L., Sun, J., Liu, Y., Dong, J. S., “TAuth: Verifying Timed Security Protocols.” In Proceedings of International Conference on Formal Engineering Methods (ICFEM), pp. 300-315, 2014

15. Li, L., Sun, J., Liu, Y., Dong, J. S., “Verifying Timed Parameterized Protocols.” In Proceedings of International Symposium of Formal Methods, 2015

16. N. O. Tippenhauer, W. G. Temple, A. H. Vu, B. Chen, D. M. Nicol, Z. Kalbarczyk, and W. Sanders, “Automatic Generation of Security Argument Graphs,” in Proceedings of the IEEE Pacific Rim International Symposium on Dependable Computing (PRDC), 2014

17. A. H. Vu, N. O. Tippenhauer, B. Chen, D. M. Nicol, and Z. Kalbarczyk, “CyberSAGE: A Tool for Automatic Security Assessment of Cyber- Physical Systems,” in Proceedings of the Conference on Quantitative Evaluation of SysTems (QEST), 2014

18. Jongho Won, Chris Y.T. Ma, David K.Y. Yau, and Nageswara S.V. Rao., “Proactive Fault- Tolerant Aggregation Protocol for Privacy-Assured Smart Metering. IEEE/ACM Trans. Networking.” Accepted for publication

19. J. Zhang, C. Yuen, C.-K. Wen, S. Jin, K. K. Wong, H. Zhu, “Achievable Ergodic Secrecy Rate for MIMO SWIPT Wiretap Channels”, ICC-Workshop on Physical Layer Security, 2015

20. J. Zhang, C. Yuen, C.-K. Wen, S. Jin, X. Gao, "Ergodic Secrecy Sum-Rate for Multiuser Downlink Transmission via Regularized Channel Inversion: Large System Analysis", IEEE Comms Letters, Sept 2014, pp. 1627 - 1630

SUTD’s Learning Environment for Experimental Technology (LEET) laboratory

R&D Projects in Cyber Security

S/N	Project Title	PI / Co-PIs	Collaborators
1	Cross-functional Information Systems for Decision Making	David Yau Cheung Ngai Man, Duan Lingjie, Lu Wei, Selin Ahipasaoglu, Yuval Elovici, Zhang Mei Hui, Zhang Yue	Starhub; Ravishankar Iyer, UIUC
2	Cyber Physical System Protection	Aditya Mathur Nils Ole Tippenhauer, Sun Jun, Yuen Chau	Daniel Jackson; MIT
3	Empirical Assessment of Techniques for Detecting and Responding to Sensor Attacks in Cyber Physical Systems	Justin Ruths Aditya Mathur	
4	Network Engineering for Wireless Security	Jemin Lee	Sang-Yoon Chang, ADSC; Moe Z. Win, MIT
5	Advancing Security of Public Infrastructure using Resilience and Economics	Aditya Mathur Costas Courcoubetis, David Yau, Duan Lingjie, Justin Ruths, Nils Ole Tippenhauer, Roland Bouffanais, Stefano Galelli, Sun Jun	ADSC; Cisco; National Instruments; Saurabh Amin (MIT); NEC; Gooi Hoay Beng, NTU; Starhub; Ravishankar Iyer, UIUC

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
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

iTrust
Centre for Research in Cyber Security

itrust.sutd.edu.sg

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