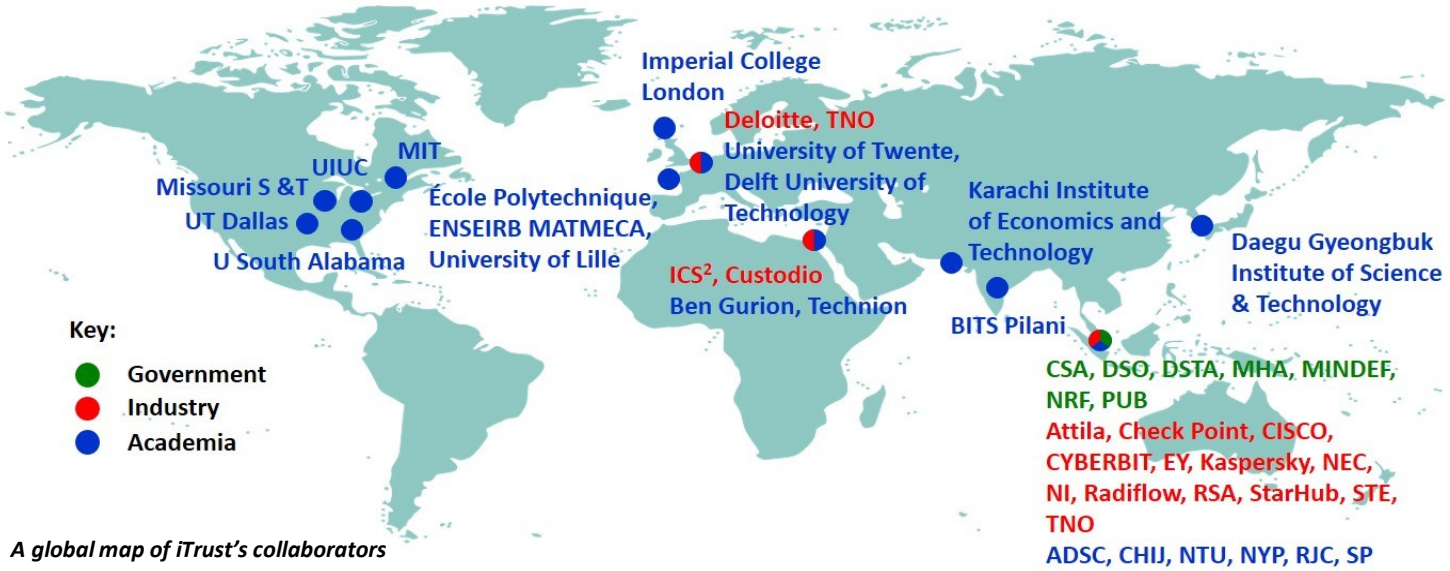
iTrust Times

SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

From Centre Director's Desk



A global map of iTrust's collaborators

Dear Reader:

Greetings from iTrust! A very Happy 2018 and welcome to the 12th issue of iTrust Times!

This issue coincides with the end of Phase I of iTrust. Since its establishment in 2013, iTrust has attracted a number of collaborators from academia and industry. Our faculty and one-of-a-kind testbeds have been the key sources of attraction. Our collaborators use the testbeds in one way or another and collaborate actively with faculty on jointly funded projects . This issue of the iTrust Times is devoted almost in its entirety to brief articles from some of our collaborators. These articles should expose you to the nature and value of research in iTrust.

It is worth to look at iTrust by numbers. Since its launch in 2013, here is what iTrust has accomplished. Publications: 94; Delegations hosted: more than 130; Funded international collaborations: 2; Research funds received: SG$22.7M; Full-time researchers (Research Scientists, Post-docs, Research Assistants) supported: 52; Fully operational testbeds: 4; Technology disclosures: 5. I believe that for a young centre such as iTrust these statistics are impressive.

Phase II of iTrust is expected to start soon. Our focus in Phase II will be on Design Science and Technologies for Secure Critical Infrastructure (DeST-SCI). University of Illinois, Urbana -Champaign, is our newest research partner in Phase II. UIUC has launched a major research initiative in Singapore titled "Trustworthy and Secure Cyber-Plexus (TSCP)." TSCP is housed in NRF's Campus for Research Excellence and Technological Enterprise (CREATE). iTrust faculty will work with UIUC researchers on projects related to secure power grid. In addition, under DeST-SCI, iTrust researchers will continue contributing to the design of secure critical infrastructure.

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

Best wishes,

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

In This Issue

Projects with collaborators

Since iTrust's inception in February 2013, we have made remarkable progress in cybersecurity research as well as the inflow of research funding. As a consequence of this, we have collaborated with an increasing number of local and international companies and academia to advance the field. This issue features the work with seven of our collaborators on their research work with iTrust.

Fostering Industrial Research with iTrust, SUTD

By Toh Jing Hui, Cyber Security Consultant, Attila Cybertech Pte Ltd

2017 went by in a flash. For Attila Cybertech, we celebrated our first birthday with a bang. We established cyber security R&D collaborations with a few Institutes of Higher Learning (IHL), the Singapore University of Technology and Design (SUTD) being one of them. Currently, the security posture – an overall security plan that a business adopts to security, from planning to implementation – for industrial control systems (ICS) is severely lacking. We aim to translate and foster industrial research done with our partners into robust and comprehensive solutions for the Critical Information Infrastructure (CII) sectors.

One of the few projects on which we are working with SUTD is a state-of-the-art **anomaly detection system for ICS**. The difference between this project, in collaboration with iTrust, and what the industry currently offers is that we are employing physics for anomaly detection. As far as we know, this system is the first of its kind to offer such detection mechanisms. The beauty of this project is twofold. Firstly, we bring to the industry a new and unique approach to detecting faults in their critical systems. Secondly, this project shows how far technology has progressed, from using hard rules for anomaly detection to using the behaviour of the malware and now finally, to using physics. This shows how the physical and digital world are actually closely intertwined.

Another interesting project that Attila is collaborating with SUTD is a Capstone Project titled "Cyber Security for the Maritime Industry". This project is offered to SUTD undergraduates as their final year project. Currently, the maritime industry has numerous cyber security loopholes which have not received much attention until recently. According to an article by The Maritime Executive, there have been cases of GPS spoofing involving more than 20 vessels over the month, in which navigations experts have no clear way of detecting it. It is a challenging problem to address as the environments for the ships are usually a combination of IT and ICS system, which makes anomaly detection difficult. We aim to design and develop a working prototype of a cyber security solution for ships.

With these projects on hand, 2018 looks set to be a busy year for us. We look forward to the completion of these projects and bringing the final product to the industry. The detection solution developed will be validated in iTrust's testbed, and likely then deployed in selected plants across Singapore.

Source:
https://maritime-executive.com/editorials/mass-gps-spoofing-attack-in-black-sea#gs.bW94JbY

SUTD and BGU collaborate on IoT Security and Privacy Research

By Yair Meidan and Shachar Siboni, Asaf Shabtai, Ben-Gurio University of the Negev (BGU), and Sachidananda Vinay Mysore, SUTD

The Internet of Things (IoT) is a global ecosystem of information and communication technologies which connects everyday appliances to each other and the Internet. These connected appliances are typically referred to as smart IoT devices. Unfortunately, the proliferation of those devices is accompanied by various challenges, particularly in the areas of security and privacy. While

studying such IoT-related emerging threats, an initial collaboration between researchers from iTrust and BGU has led to further collaboration and new research directions.

SUTD faculty and researchers include Prof. Yuval Elovici, Asst Prof. Nils Ole Tippenhauer, Dr.-Ing. Vinay Sachidananda, Dr. Yan-Lin Aung, Juan-David Guarnizo, Amit Subhashchandra Tambe, and Dominik Breitenbacher; their counterparts at BGU are Dr. Asaf Shabtai, Shachar Siboni, Yair Meidan, Michael Bohadana, and Yael Mathov.
One of the areas of collaborative research aims at automating the enforcement of security policies in large enterprises in the age of the IoT. For that, they defined and implemented an innovative patent-protected security **testbed framework targeted at IoT devices**. This security testbed is aimed at testing all types of IoT devices, with different configurations and various scenarios, by performing standard and advanced software and hardware security testing (Figure 1). Several joint publications and a patent were submitted on this topic.

In another joint research, a **multi-stage meta-classifier** which leverages already-monitored network traffic data, **differentiates between connected PCs, smartphones, and IoT devices**, and maps the various types of IoTs into categories, e.g., smart TVs, watches, cameras, etc. A modification of this approach proposes a multi-class classifier for IoT white-listing, which prevents unauthorised (insecure) types of IoT devices from connecting to the organisational network.

This technology was extended further in order to detect compromised IoT devices that are part of botnets. In this research the researchers use deep neural networks to identify anomalous traffic which serves as an indication of malicious activity. This method operates on the network level, and in an extension of this study they suggest a hybrid approach, which combines data collected from both the network and the hosts. In a recent initiative, they also leverage a novel IoT honeypot infrastructure developed at SUTD to detect zero-day botnet attacks.

The researchers from both universities enjoy working together on innovative, interesting, and impactful research endeavours and are looking forward to continuing their collaboration.

Imperial College London

Security by Design for Interconnected Critical Infrastructures

By Venkat Reddy, Postdoctoral Researcher, SUTD

A new infrastructure when designed will need to co-exist with existing and connected infrastructures. This joint research with Imperial College London aims to generate a prototype tool that **integrates physical design with security analysis prior to system construction**. This tool will allow designers to investigate the cascading effects of attacks,

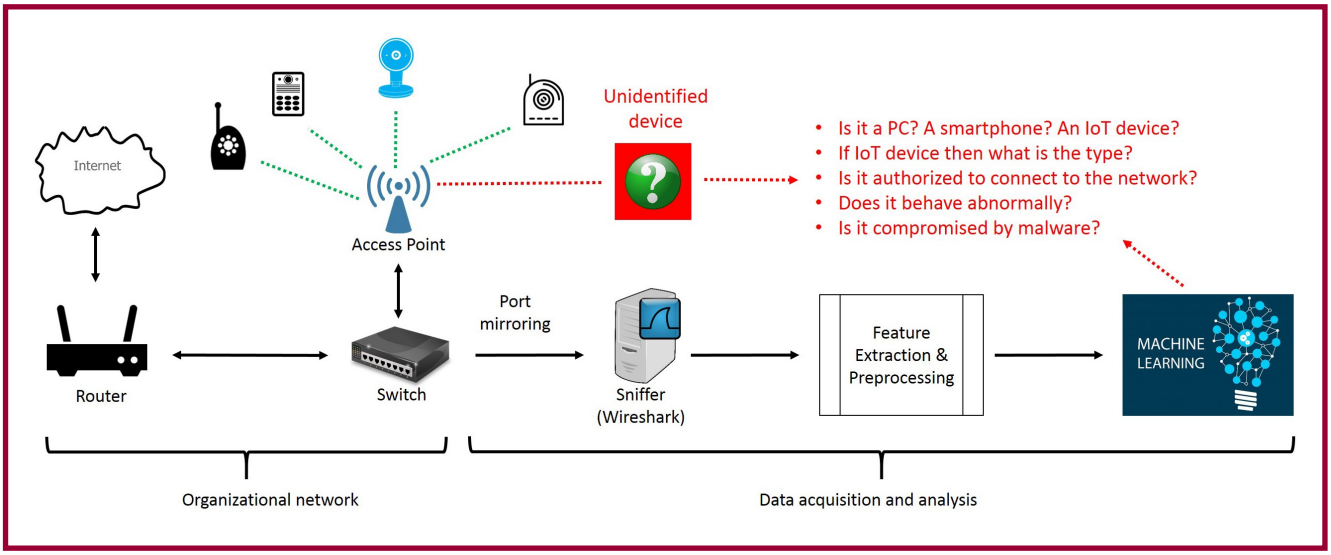


Figure 1: The infrastructure and process for IoT security analysis, jointly developed and implemented by BGU and SUTD researchers

and their mitigation, during the design stage. It will help tackle how to best model cyber-physical critical infrastructures (CI) and their dependencies. It will also help in determining the response of these CI to cyber-attacks, extracting the relationship between two or more properties and how an attack on one affects the others. It will be able to incorporate different types of CI including hybrid CI. Furthermore, it will generate reports that help with analysing the model, its response to different cyber-attacks and suggest improvements in the design of the CI. This tool will also include a generic attack model and potential attacks that can be performed on the CI.

Axiomatic design theory principles from system design are used to model CI. This modelling provides an abstract representation of CI to **understand the behaviour of infrastructures under potential attacks**. Axiomatic Design principles start with functional requirements and define the design parameters that meet those functional requirements. The design parameters represent the CPS components, and the process of defining these parameters automatically sets their inter-relations.

Researchers at iTrust consider the Water Distribution (WADI) testbed as a case study for modelling and analysis. The design matrices are derived for the second stage of WADI which establishes the relationship between the set of functional requirements and design parameters. These design matrices can help with the detection of potential attacks and analyse the impact of real attacks in a CPS. Attack detection follows two approaches: system design invariants and data invariants. Design invariant rules that define the physical conditions that must be maintained for the normal operation of a CPS provide a means by which early detection of anomalous system states may be achieved, allowing for timely mitigating actions – such as fault checking, system shutdown – to be taken. However, many hidden invariant rules can be extremely challenging to identify, particularly in circumstances where insights are needed across numerous subsystems and where dependencies between a wide range of physical metrics may be implicit rather than explicit. Therefore, a combination of machine learning and data mining techniques is used to systematically learn invariant rules from information contained within ICS operational data logs. The data logs are collected every second by running WADI non-stop for a total of 16-days. The system is operated under normal conditions (without any attacks) for a period of 14 days. During the remaining two days, 15 different types of attacks are launched on the testbed.

Deployment of Kaspersky's Industrial CyberSecurity (KICS) Solution, Leveraging on iTrust's Test Bed

By Vikram Kalkat, Kaspersky Lab Singapore

Earlier this year, Kaspersky Lab deployed its Kaspersky's Industrial CyberSecurity (KICS) solutions at iTrust's Secure Water Treatment (SWaT) testbed. The solutions deployed aim to support Kaspersky engineers to **detect and deter cyber attacks in real world and real time environments**.

SWaT, Singapore's first water treatment test bed for cyber security research is a collaborative project headed by researchers from SUTD, international consultants, and stakeholders. It is managed by iTrust, and aims to provide a real world environment for developing advanced tools and methodologies to ensure the security and safety of current and future large scale infrastructure against cyber attacks in Singapore.

The test bed is a unique and sophisticated facility that mimics the functions of a water treatment system in a live setting. The test bed allows multi-disciplinary researchers to conduct live simulations and testing that will enhance their understanding of the strengths and weaknesses of new and existing defence mechanisms intended for the cyber security industry. SWaT will serve as a valuable platform for researchers in Singapore and globally, who are planning to design secure Cyber Physical Systems (CPS) for water treatment, power generation and distribution as well as oil and natural gas refinement.

Industrial control systems (ICS) have been known to be a target of malicious and sophisticated cyber attacks

worldwide. One such attack was the Ukrainian power grid attack in 2015 that left hundreds of thousands of residents in the Ivano-Frankivisk region in the dark for a period of one to six hours. Another example was the anonymous regional U.S. water utility hack, where cyber criminals managed to gain access to the valve and flow control systems and manipulated the settings, handicapping water treatment and production capabilities.

It is evident that the repercussions of such attacks can be devastating, not only in financial losses but affecting citizens' lives as well. According to the Kaspersky Lab Industrial Control Systems Cyber Emergency Response Team (Kaspersky Lab ICS CERT), every third industrial control system computers worldwide has been targeted by cyber threats in the first half of 2017 .

Protection of industrial systems requires a different approach and technologies – a security that keeps availability of process on top of all. Kaspersky Industrial CyberSecurity is a portfolio of technologies and services designed to secure every industrial layer, including SCADA servers, HMIs, engineering workstations, PLCs, network connections and people – without impacting on operational continuity and consistency of the industrial process.

Figure 2 (from left): Eugene Kaspersky, CEO, Kaspersky, and Professor Aditya Mathur, Head of Pillar and Centre Director iTrust, discussing the project, along with Kaspersky Lab's Stephan Neumeier, APAC Managing Director and Vikram Kalkat, Senior Key Account Manager, KICS APAC

Engineers from Kaspersky Lab will be able to conduct a variety of realistic offensive and defensive experiments on the SWaT testbed with KICS. The experiments are aimed at verifying whether what is learnt in simulation applies to the physical testbed. Also, it aims to help engineers to understand the security gaps that a CPS has, enabling them to build effective designs in a real world setting.

Stephan Neumeier, Managing Director, Asia Pacific at Kaspersky Lab (Figure 2) said, "Cyber threats to industrial environments are fundamentally different to traditional 'office' threats in terms of the scale of their potential damage, they can be disastrous. We want to play an active role in helping mitigate cyber attacks in this sector and ultimately help build a more secure infrastructure."

Securing Cyber Physical Systems

By Bruce McMillin, Professor, Missouri University of Science and Technology

The Missouri University of Science and Technology (Missouri S&T) is a focused 9000 student Science/ Engineering university. Our Internet of Things work is largely centred around Fog architectures, essentially to how construct, secure, and improve the resilience of systems that have embedded intelligence near to the physical system. Missouri S&T has been part of a 10 year US National Science Foundation Engineering Research Center to build a Fog distributed electric smart grid system called FREEDM (Future Renewable Electric Energy Delivery and Management). During this work, Missouri S&T researchers have developed inherently secure algorithms for transactive energy management, essentially creating a trusted energy management system out of untrusted components. This insight led to an understanding that Fog computing security architectures have more peer-to-peer domains than hierarchical and to secure such systems, requires looking at the information present in both the cyber and physical interactions among these domains. Encapsulating knowledge into the running system through invariants adds additional information paths that are used to secure the system.

Missouri S&T has additional strengths in Privacy Preserving

system interactions include vehicular networks, work in secure sensor clouds, and work in securing corporate infrastructures using evolutionary computation techniques.

This summer Missouri S&T sent a small team (Figure 3) to iTrust to apply these techniques to both the SWaT and EPIC testbeds. Due to the extensive work done by the SUTD team on the SWaT, the S&T team was able to make only small improvements. EPIC, being a new system, presented a number of vulnerabilities that the S&T team was able to secure.

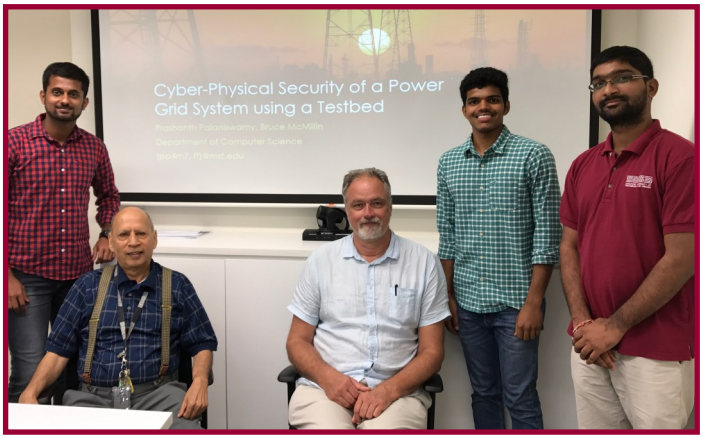


Figure 3 (from left): Prashanth Palaniswamy (S&T-Student), Prof Aditya Mathur, Prof. Bruce McMillin (S&T), Sai Sidharth Patlolla (S&T-Student), and Sridhar Adepu (SUTD)

NEC

Development of Virtual Control System for Security Risk Assessment

By Hiro Ueda, Masafumi Watanabe, Kazuya Kakizaki, and Kyotaro Higuma, NEC Corporation Security Research Laboratory

Given that cyber-attacks on control systems have increased in frequency and intensity, one countermeasure would be to conduct **security risk assessment** on these systems. Doing so provides system operators a **pre-evaluation of cyber-attack risks to the control system and its vulnerability**. This in turn helps them make informed decisions on the appropriate security measures for their systems. However, assessment of security risk for control systems poses the following two key challenges due to their inherent features:

(1) Difficulty in assessing the system directly without interfering with its operations, i.e. downtime.

(2) Difficulty in accurately evaluating the extent of physical damages, such as explosions and overflows, as a consequence of cyber-attacks.

To circumvent these limitations, NEC conducted a security risk assessment of a virtual model instead of doing so on an actual control system. The virtual model provides operators with a damage visualisation that automatically analyses the effects of cyber-attacks. To ensure that the virtual model accurately reflects an actual control system's operations and behaviour, NEC is working in collaboration with iTrust to refine the following techniques, using iTrust's SWaT testbed as a platform:

a) Collecting configurations and behaviour data of control systems; and

b) Determining data relationships and control rules on control systems from the collected data.

To date, NEC has conducted an automated network analysis (Figure 4) and an automated programmable logic controller (PLC) control logic analysis on the SWaT testbed (Figure 5, next page).

The upcoming work includes developing a method to generate relationships between the system behaviour and the testbed's physical processes. NEC's final goal is to create a virtual SWaT model based on these relationships and perform attack simulations to determine the extent of physical damages caused by the attack.

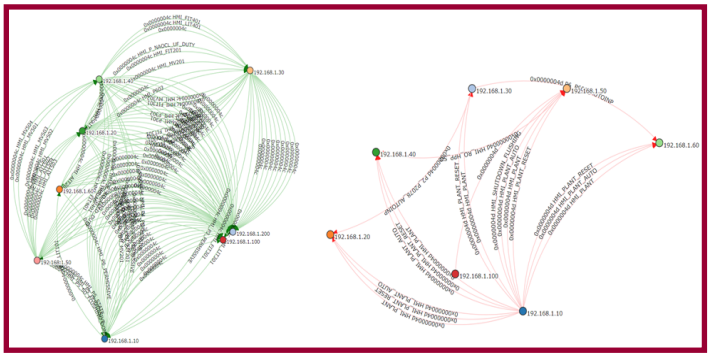


Figure 4: Read/write data flow obtained by NEC network analysis

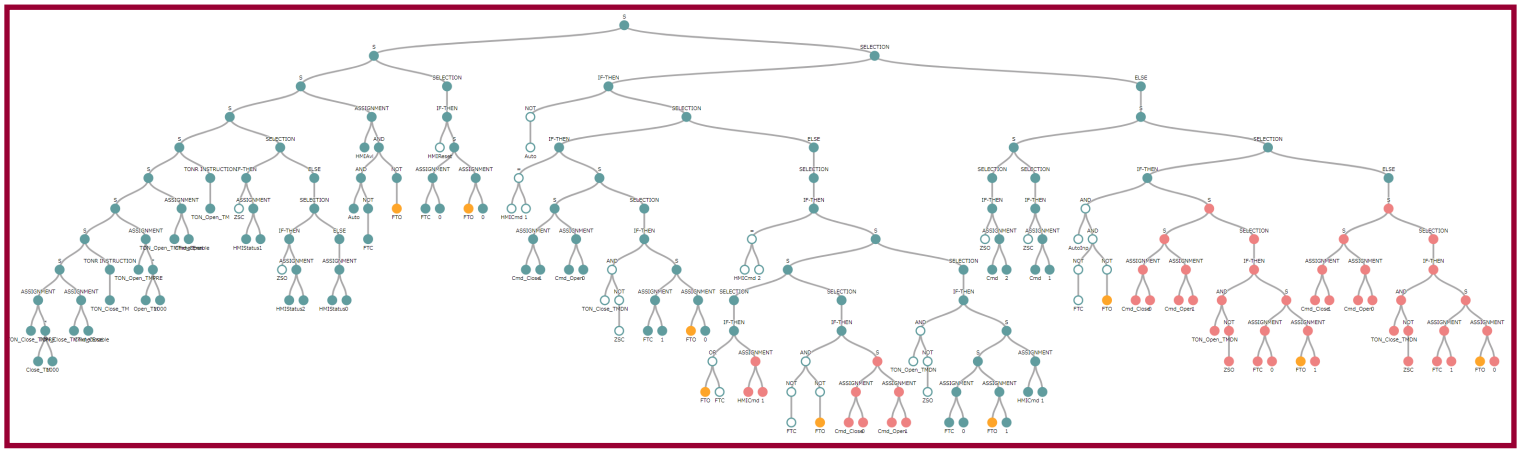


Figure 5: Parameter relationship obtained by NEC PLC logic analysis

TUDelft

TABOR: A Graphical Framework for Anomaly Detection in Industrial Control Systems

By Qin Lin, PhD student, Delft University of Technology

The motivation for this research arose from two key challenges in applying machine learning techniques in the context of anomaly detection for cyber physical systems. Firstly: Can we explain the outcome of attack detection, i.e. why is this an anomaly? Secondly: Can we localise the anomaly, i.e. which sensors and actuators are potentially under attack. These two questions are of importance for operators who need to **diagnose the abnormal behaviour and to undertake one of possibly many follow-up safety actions.**

To deal with these problems, an insightful graphical framework (Time Automata and Bayesian network; TABOR) is learned from the normal operational observation of the Secure Water Treatment (SWaT) testbed at SUTD. Sub-processes of the entire SWaT are modeled. Sets of sensors and actuators in SWaT are partitioned into groups based on their functionalities in order to deal with high dimension and complexity of the problem. Signals from the sensors are symbolically represented and learned using timed automata (TA) (Figure 6) to discover the underlying dynamical fluctuating behaviour of the water level and other sensors. The states in the TA are associated with other actuator's states by dependency/causality inference using the Bayesian network, which show the dependencies of the sensors and actuators. Irregular patterns and dependencies that do not adhere to the learned model from normal behaviour are considered to be anomalies.

TABOR provides a solution for the **interpretation and localisation of anomalies.** The detected anomalous patterns can be located precisely to processes, sensors, or actuators. The model is visualisable and interpretable, thus enabling a better understanding of the system and verification of the model itself. Compared to those detected using methods based on deep neural network (DNN) and the support vector machine (SVM) available in the literature, TABOR is able to detect more attack scenarios.

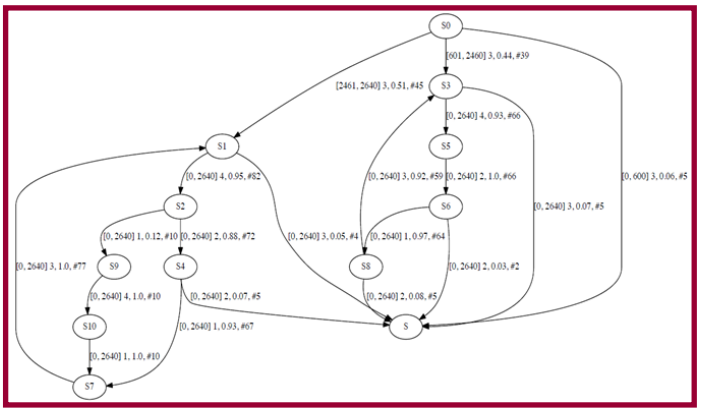


Figure 6: Timed automaton learned from the level sensor in stage 1 of SWaT. S_x denotes the states in stage 1, accompanied by transition

Hacking Competitions

Research in iTrust is aimed at the development of methods and supporting tools to aid in the design of secure critical infrastructure. Such infrastructure must be resilient to cyber attacks. Resiliency requires integration into the

infrastructure software and hardware devices for preventing attackers from entering a plant, detecting attacks in the event the prevention mechanism has been bypassed, and ensuring that doubly authenticated commands are allowed to pass to actuators such as pumps, generators, and circuit breakers. Researchers at iTrust engage in research and development activities aimed at the creation of a robust and practical triple-defence approach that includes prevention, detection, and control in the face of cyber and cyber-physical attacks. While researchers design and perform experiments to assess the effectiveness of various components of the triple-defence mechanisms they develop, it is important that such assessment be also carried out by independent teams consisting of people well versed in the design and launch of cyber attacks.

S317

It is with the above mentioned goal in view that iTrust began organising the **SUTD Security Showdown** event. This event, dubbed as S3, was first held in June 2016 at iTrust. It is organised by a team consisting of faculty, research staff, and administrative staff in iTrust. More than 10 international and local attack and defence teams have been invited to iTrust to participate in S3. Two such events have been organised so far, one in 2016 and the other in 2017. The Ministry of Defence, Singapore, and the SUTD-MIT International Design Centre, funded the S3-17 event. The event consists of two key phases – an online qualifier and a live event held at iTrust. Following the online qualifier, five international teams were invited to participate in the live event. Each team was given the opportunity to design attacks against the realistic SWaT testbed. The goal of each attack team was to meet as many pre-defined challenges as possible within the pre-allocated time. The 2017 report, which focuses on the organisation of the S3-17 event and the performance of various attack and defence teams, is now available on iTrust website.

EPIC BLAQ_0 Hackathon

By Francisco Furtado, Lauren Goh and Jonathan Heng, Research Officers, SUTD

A group of iTrust researchers also organised a hacking competition – **BLAQ_0 Hackathon** – for SUTD undergraduate students to put their skills to the test and gain experience in hacking. For a realistic setup, the competition was held at the Electric Power and Intelligent Control (EPIC), a power testbed at iTrust that mimics a typical power grid. Dr Kandasamy Nandha Kumar and research officer Francisco Furtado helped design the competition with laboratory specialist Muhamed Zhaffi. The BLAQ_0 Hackathon comprises several phases: (1) Briefing on the ethics of hacking and safety measures; (2) reconnaissance of the EPIC testbed; and (3) the actual (supervised) hacking in which the teams demonstrated their prepared attacks.

Five teams – a total of 17 students – participated in BLAQ_0 which ran from 22 to 25 January 2018. Teams comprised of students from different pillars of SUTD: the Engineering Product Development (EPD), Engineering Systems and Design (ESD), and Information Systems Technology and Design (ISTD). Students combined their knowledge from different disciplines to tackle the Cyber-Physical System Hackathon.

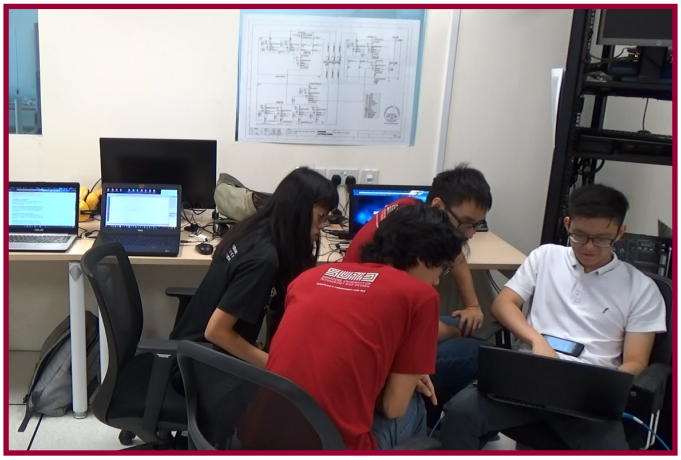


Figure 7: A team of students discussing strategy to gain access into EPIC's network

Each team was given two hours to launch attacks to achieve specified attack goals on the EPIC testbed. Due to safety and ethical issues, teams needed to communicate their plans to the judges prior to launching an attack. The goals of an attack were either physical interruptions to EPIC's operation or digital manipulation of stored/ processing data values. The points were then scaled according to the degree of control over the physical

process or data values: random, or specific.

All teams were able to launch attacks. With many open source resources, most teams used Kali Linux and Metasploit as a pen-testing framework. This framework provided teams with known vulnerabilities which could be exploited to gain unauthenticated access into the system. Teams had to have a plan of attack to cause damage to the system as gaining access is only the beginning of an attack. Successful attacks lead to disruption of operations in the EPIC testbed, loss of control of the operating system, and corruption of the database.

The winning team, **Rainbow Rocket** (Figure 8), exposed multiple vulnerabilities (e.g. EternalBlue, default passwords) in the existing system. The top three teams walked away with cash prizes of $500, $300, and $150, respectively. Monica Nathalia, from the 3rd placed team, said that the hackathon "has exposed me to the cyber physical field which otherwise I would have never tried. The hackathon stages were very comprehensive and I got to learn at my own pace. The organisers are also very responsive and make sure that we understand the whole system. Overall an enriching experience and great start to the cybersecurity world!"

Figure 8: Amish Bhandari (right) from winning team Rainbow Rocket receiving the cash prize and certificate from iTrust Deputy Director Ivan Lee

As the competition was specially organised for SUTD undergraduates, the organisers felt it was encouraging to see them bridge the gap between what is learnt in class and what happens in the real world. Participating in such hands on events will help them gain experience towards designing and building more secure CPS in the future.

iTrust Seminar Series

Dr Ralph Holz

Over the last years, blockchains have developed into a mainstream technology that entire industry sectors are talking about. The latest generation even supports smart contracts - programs that are executed by all participants and that may govern everything from simple transactions to the setup of organisations. Beyond the hype, however, there is little deployment beyond the two most prominent examples, Bitcoin and Ethereum.

Some of the reasons why this is so is explored in **"Consensus, security and the network - measuring Blockchain"** by **Dr Ralph Holz**, a lecturer in Networks and Security at the School of IT at the University of Sydney, where he leads the Node for Cybersecurity in the Human-Centred Technologies cluster. He showed that the P2P (peer to peer) networks that underlie blockchains impact their functionality in decisive ways. Ralph also looked at the dependability and abortion of transactions, both of which are crucial for enterprises, as well as inspected the network structure and its influence on transaction execution. He presented some early numbers from more than 2,500 scans of a blockchain network and discussed some research directions that could prove fruitful in a number of systems, blockchains or beyond.

Conferences

The Driving Automation System (DAS) can be considered the brain of the Autonomous Vehicle (AV), providing it with decision making and driving automation capabilities. Since any failure – intentional or accidental – can cause various losses, such as safety, privacy, financial and operational performance losses (Figure 9, next page), which could lead to disastrous effects, the integration of safety and security aspects in the AV is crucial.

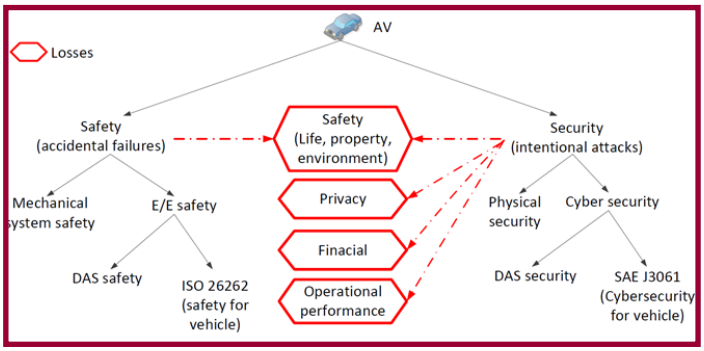


Figure 9: Safety and security in Autonomous Vehicles

On this topic, post-doctoral researcher Dr Jin Cui presented two papers at the International Academy, Research, and Industry Association (IARIA) conference in Nov 2017, held in Barcelona, Spain, in which they make mention of the adoption of international standards, namely ISO 26262 (functional safety of road vehicles), SAE J3061 (vehicle cyber-security), and SAE J3016 (vehicle driving automation).

The first paper, titled **"On the Alignment of Safety and Security for Autonomous Vehicles,"** proposes an approach for aligning safety and security lifecycle processes, defined by the international standards. The proposed approach uses a model – the Failure, Attack, and Countermeasures (FACT) graph – to analyse consistency and completeness among safety and security countermeasures.

The second paper, **"Integrating Autonomous Vehicle Safety and Security"**, proposes a more complex model, the Six-Step Model, which is used as a backbone for achieving and maintaining integration and alignment among safety and security artefacts throughout the entire AV life-cycle. It incorporates six hierarchies of AVs, namely, functions, structure, failures, attack, safety countermeasures, and security countermeasures (Figure 10).

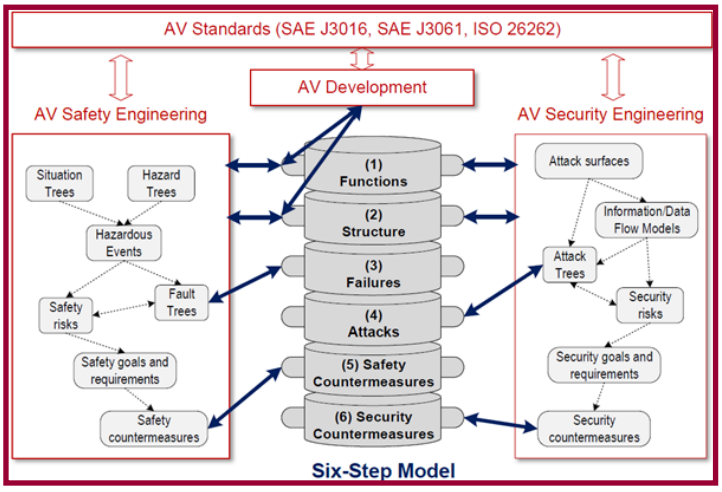


Figure 10: The Six-Step Model as a backbone for integrated AV safety and security analysis

The Six-Step Model enables comprehensive analysis of AV safety and security, as it uses system functions and structure as a knowledge base for understanding the effect of failures and attacks on AV.

Profiles

Prof Pieter Hartel

Prof Dr Pieter Hartel is head of the Cyber Security research group of the faculty of Electrical Engineering, Mathematics and Computer Science at Delft University of Technology. He also holds part time professorial positions at the University of Twente and at SUTD. He has 24 years of research and teaching experience in Cyber Security in the Netherlands, the UK, the US, Malaysia, and Singapore. Pieter is also the coordinator of the 4TU Cyber Security Master Specialisation where he teaches a course Cybercrime science with Prof Marianne Junger from the University of Twente and the Capstone courses on Social, Business, and Entrepreneurial skills in cyber security with Dr Victor Scholten and Dr Hanieh Khodaei from TU Delft.

A/P Georgios Piliouras

Georgios Piliouras is an Assistant Professor at the Engineering Systems and Design pillar. He received his PhD in Computer Science from Cornell University under Eva Tardos in 2010. His work lies on the intersection of game theory, learning theory, dynamical systems, and algorithms. Before joining SUTD, Georgios was the Wally Baer and Jeri Weiss postdoctoral scholar in Computing and Mathematical Sciences at Caltech and a Berkeley/Simons Fellow. During his Georgia Tech postdoc at the Electrical and Computer Engineering department, he was involved in the DARPA Physical Intelligence program which explored and prototyped novel, neuron-inspired computer

architectures. Finally, he has held visiting positions at the Center for Information and Computation (CWI/ Amsterdam) and the economics departments of Oxford and Johns Hopkins University.

Georgios' main research interests lie in the areas of algorithmic game theory, computational learning theory, multi-agent learning and dynamical systems. He is interested in exploring dynamic phenomena that arise from the interaction of numerous adapting agents. Georgios is a Co-PI in the project "Testing for Blockchain Security by Design."

Dr Vinay Sachidananda

Vinay Sachidananda joined iTrust as a postdoctoral researcher in February 2016 and was promoted to Research Scientist in December 2017. He received his M.Sc. degree in Computer Science (networking and mobility) in 2008 from University of Trento, Italy. Vinay successfully completed his PhD in Computer Science at the Technical University of Darmstadt, Germany. He had been working as post-doctoral research fellow in iTrust Centre of Cyber Security in Singapore University of Technology and Design, focusing mainly on Internet of Things. Currently, he is working as Research Scientist in iTrust and mainly focusing on topics of Cyber Security of Internet of Things and Cyber Physical Systems.

Vinay's research interests include the area of Wireless Sensor Networks, Internet of Things, Cyber Physical Systems, Machine-to-Machine, Mobile Ad Hoc Networks, Peer-to-peer networks and Solving Optimisation problems. Vinay is a member of the IEEE. Born and raised in Mysore. Vinay is zealous traveller, cheerful and music lover.

Pawel Szalachowski is an Assistant Professor at the Information Systems Technology and Design Pillar, having joined the university in 2017. Prior to joining SUTD, he was a senior researcher at ETH Zurich, where he led the design and implementation of the SCION architecture. He

A/P Pawel Szalachowski

received his PhD degree in Computer Science from Warsaw University of Technology in 2012. His research interests are in building and analysing secure networked systems. In particular, he is interested in the blockchain security (Bitcoin, Ethereum, cryptocurrencies, smart contracts) and network and systems security (Internet, SSL/TLS, PKI, SDN, IoT). Pawel is a Co-PI in the project "Testing for Blockchain Security by Design."

Visits

At the invitation of MINDEF to showcase Singapore's cybersecurity efforts and advancements, iTrust welcomed several foreign delegations in February.

The **Netherlands Ministry of Defence's** Strategy Advisor on Research & Technology to the Minister of Defence and R&T Director at the General Directorate of Policy Affairs, **Mr Auke Venema** toured iTrust's testbeds on 1 February. He was joined by Col Rene Pals, Defence Attaché (Jakarta), and Dr Peter van Hooft, Branch Office Director TNO South East Asia.

From left: Prof Hartel and Ivan hosting Col Rene Pals and Mr Auke Venema

The same day also saw a visit by **MG Olivier Bonnet de Paillerets**, General Chief of Staff and Cyber Defence Commander of the **French Armed Forces**. MAJ Valerie Mauvais, Assistant Defence Attache, French Embassy in Singapore and MAJ Lucas Baratin, Staff Officer, Cyber Command, French Armed Forces were also with him.

Ivan explaining SWaT's capabilities to (from left) MG Olivier Bonnet de Paillerets, MAJ Lucas Baratin and MAJ Valerie Mauvais

These visits were followed by one from the Estonian Ministry of Defence on 5 February. The delegation was led by Dr Kusti Salm, National Armaments Director. He was accompanied by his colleagues from the Defence Investments Departments Ms Getter Oper, Chief Scientific Officer, and Mr Andri Rebane, Executive Project Manager.

Ivan at the EPIC testbed with the Estonian delegation (from left) Mr Andri Rebane, Ms Getter Oper and Dr Kusti Salm

iTrust Matters

Research Openings

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

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

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

iTrust Contact Information

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

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

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

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

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

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

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

Ms Stacey Zhang
Senior Associate, iTrust
stacey_zhang@sutd.edu.sg

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