iTrust Times

A Quarterly Newsletter

Issue Highlights:

Exercise Crossed Swords 2020 participants

Jan — Mar 2020 | Volume 6 Issue 1

From Centre Director's Desk

i for International

Dear Reader:

Greetings from iTrust! We are well into 2020 and I hope you are working hard towards meeting your yearly goals.

Perhaps Year 2019 can be best labelled as an year of recognition and diversification for iTrust. While iTrust researchers continue to make advancements in the design of critical infrastructure, the technologies developed so far, and our one-of-a-kind infrastructure, led to an invitation from the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

The invitation enabled iTrust to showcase its technologies in Riga, Latvia to over 100 scientists, engineers and administrators from NATO countries during their exercise labelled Crossed Swords (XS2020). The technologies showcased, and actively used by the participants, included VR for critical infrastructure, a plant visualiser, and three integrated design and data-centric anomaly detectors. A team of engineers led by Ivan Lee and myself provided field support to the participants in Riga while another group of five engineers provided ground support from Singapore to enable remote launch of cyber-attacks on the SWaT testbed. Our technologies and effort are well recognised by CCDCOE. Details of XS2020 are in this newsletter.

On the research front, iTrust is actively developing digital twins for water and electric power. The twins will enable researchers to integrate and study the performance of their anomaly detectors and incidence response technologies. A generator for digital twins is also under development that will enable researchers to rapidly prototype digital twins of water treatment and distribution systems and electric power plants.

That's all for this edition of the newsletter! We will be back soon!

Best wishes,

Aditya Mathur
Centre Director, iTrust, Singapore University of Technology and Design
Director, National Satellite of Excellence DeST-SCI
Professor Emeritus, Computer Science, Purdue University

National Research Foundation
Prime Minister's Office
Singapore

Singapore University of Technology and Design

iTrust
Centre for Research in Cyber Security

Research Focus

NATO CCDCOE Exercise Crossed Swords 2020

Exercise Crossed Swords 2020 reached New Levels of Multinational and Interdisciplinary Cooperation, with iTrust providing support

The 6th iteration of the annual cyber exercise Crossed Swords in Riga, Latvia, brought together more than 120 technical experts, Cyber Commands´ members, Special Forces operators and military police.

Organised jointly by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) and CERT.LV, Crossed Swords has evolved from a purely technical red teaming workshop into a one of a kind training event combining different technical skills with kinetic force and taking place in several locations simultaneously. The exercise plays out a number of mutually intertwined kinetic and cyber operations. The focus is on **advancing cyber Red Team members' skills in preventing, detecting and responding to an adversary in the context of full-scale cyber operations.**

"The primary training audiences are cyber Red Teams, but also SOF, and the most a recent addition, a command module," said the Director of CCDCOE Colonel Tarien. "Crossed Swords is unique in combining multidomain with multinational. This year's Crossed Swords practiced a realistic cyber enabled joint operation. The setting is highly experimental, yet authentic and challenging."

"For the first time in exercises' history we had six nations working together as the Cyber Command element: the command function was fully integrated into technical and kinetic gameplay," Lauri Luht, the Director of Technical Exercises at the CCDCOE concurred. "In technical exercises the training audience is not expected to have 100% success rate. The main task and lesson is to understand the coordination between multiple disciplines. At Crossed Swords, we link cyber elements with conventional force," Luht explained.

Crossed Swords as a technical cyber exercise focuses on **training penetration testers, digital forensic professionals, and situational awareness experts,** among them many, who will take up a role in the Red Team at the forthcoming Locked Shields 2020 exercise. Being a joint tactical exercise it brings technical experts, data collection experts and Special Forces operators under the same command working for a united goal. The complexity and interdisciplinary nature makes Crossed Swords one of the most challenging cyber exercises. Altogether the exercise welcomed 26 nations and more than 120 participants.

"The participants have to make decisions about the means to achieve effects. The process of figuring out the optimal approach is instrumental in learning to operate as a joint force. At Crossed Swords, the participants have freedom to experiment and a licence to fail – this is how the learning takes place," said Dr Rain Ottis, the Head of Exercise Control.

"Fail, fail again, fail better," summarised Dr Bernhards Blumbergs, the exercise founder and technical director, a cyber security expert from CERT.LV. "Training tasks such as attribution and the collaboration of units from very different fields and nations with integrating sub-teams are meant to push participants out of their comfort zone. This is when learning happens."

The exercise benefits largely from having industry partners on board and providing hands on integration of military and industry technology. Their technology and know-how are of key importance to make the endeavour authentic and similar to real world challenges. **This year's training event integrated water purification system** and a specialized communication network to name just a few.

The exercise was organised jointly by the NATO CCDCOE, a NATO-accredited cyber defence hub in Tallinn, and CERT.LV, the Information Technology Security Incident Response Institution of the Republic of Latvia, in partnership with the Latvian Cyber Defence Unit, Cyber Command of the EDF, Latvian National Armed Forces Joint HQ, NSHQ, **iTrust – Singapore University of Technology and Design**, CybExer Technologies, Greycortex, Stamus Networks, Latvian Mobile Telephone (LMT), Evolution Gaming and Thinnect.

Fig 1: It takes a village…Ground and supporting teams for Exercise Crossed Swords. (Top photo, from left): Ivan Lee, Siddhant Shrivastava, Aditya Mathur, Muhammad Syuqri Bin Johanna; (bottom photo, from left): Ian Teo, Desmond Wan, Beebi Siti Salimah Binte Liyakkathali, Mark Goh, Francisco Furtado

iTrust Labs Governance Board

The Governance Board for iTrust Laboratories and the National Cybersecurity R&D Laboratories (NCL) convened on 11 Feb 2020. iTrust and the NCL provided an overview of their work and roadmap, and sought the Board's directions going forward. The Governance Board is chaired by the Cyber Security Agency's Deputy Chief Executive Officer Mr Teo Chin Hock. The board comprises members from government agencies and the academia, and they are:

- Mr CHAI Chin Loon, Senior Director (Cyber Security Group), Government Technology Agency
- Mr Philip HEAH, Assistant Chief Executive, Info-communications Media Development Authority
- Prof HO Teck Hua, Senior Deputy President (Research & Technology), National University of Singapore
- Mr Kiren KUMAR, Assistant Managing Director, Economic Development Board
- Prof LAM Khin Yong, Vice President (Research), Nanyang Technological University
- Mr LIM Soon Chia, Director (Technology), Cyber Security Agency
- Mr George Loh, Director (Services & Digital Economy), National Research Foundation
- Prof Steve MILLER, Vice Provost (Research), Singapore Management University
- Dr LYE Kin Mun, Chief Risk Officer, Agency for Science, Technology and Research
- Prof YEO Kiat Seng, Associate Provost, Research & International Relations, Singapore University of Technology and Design

Logs Integrity and Backup Using Blockchain

Honeywell

Who moved my data?

By Research Assistant Aung Maw

In Feb 2020 iTrust Research Assistant Aung Maw successfully completed the deliverables set out in the 3-month project "Logs Integrity and Backup Using Blockchain" funded by, and in collaboration with, Honeywell. The objectives of the project were to **provide integrity of the transactions and the associated transactions in Honeywell's historian data by using blockchain, and retrieve those transactions in the event of data loss or unauthorised changes.**

Aung proposed's solution, named "Blockops," uses blockchain to provide data integrity to the logs stored in the historian database. The logs are grouped into data blocks with time intervals. The hash for each data block is generated and stored inside the blockchain. The integrity of each data block can then be verified by generating the hash again and comparing this generated hash with the stored hash inside the blockchain. Identical hashes imply that the block's integrity is intact. In the blockchain layer, the hashes are fully replicated across all the blockchain nodes.

In the event is is discovered that the data integrity has been affected (intentionally or otherwise) through the hash validation process, the user interface is able to pinpoint the exact data block(s) in question. An option in the interface enables for data recovery. The solution also provides a dynamic replication mechanism for the

historian data. To do that, Aung programmed the data from the source historian to be partially and selectively replicated to numerous clone databases, known as replicators, that are distributed across the system network and authorised by blockchain.

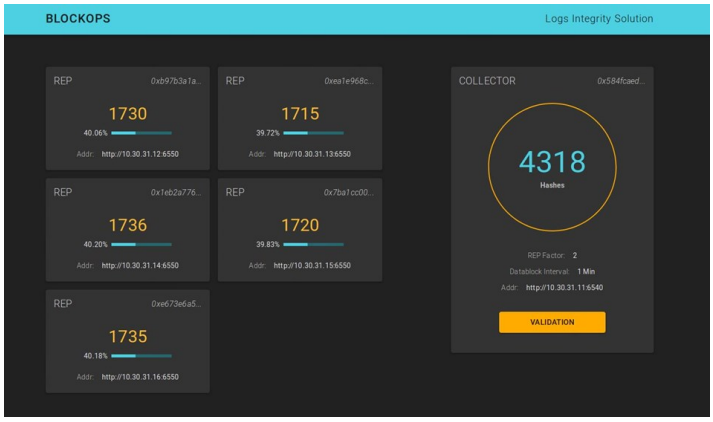

Fig 2: Blockops' GUI showing the total number of hashes generated from data blocks, and how the hashes are replicated across various nodes. Operators can also validate the hashes before retrieving and using the data

Dr Qian Zhang, a Cyber Security Architect at Honeywell, worked with Aung to deploy Blockops on Honeywell's Process History Database, from node creation to setting up a blockchain network and database, as well as setting up the user interface.

Fig 3: Aung Maw (centre) with Honeywell's (left to right) Senior Cyber Security Consultant Gokul Kumar Nanda Gopal, Cyber Security Regional Operations Leader (Asia & Pacific) Rajan Patil, Qian Zhang and Senior Cyber Security Architect Mary Sebastian

Cybersecurity Camp V

Singapore Cybersecurity Consortium

iTrust Centre for Research in Cyber Security

The Singapore Cybersecurity Consortium (SGCSC) holds its first Cybersecurity Camp outside NUS

By Research Associate Siti Nadhirah Shaik Nasair Johar

For the first time, the Camp was **jointly organised by iTrust and the SGCSC.** The two-day camp, held on 12 and 13 Dec 2019 and hosted at SUTD, featured talks related to Secure Critical Infrastructure on Day 1 and a hands-on workshop on Day 2.

A total of seven distinguished speakers from academia and industry were invited to speak at the camp. In their welcome addresses, **Consortium Chairman Prof Abhik Roychoudhury** highlighted the role of translation, manpower training and technology awareness in the area of cybersecurity whereas iTrust **Co-Centre Director Prof Jianying Zhou** spoke about the importance of securing critical infrastructure.

From Control Model to Control Program: A Cross-Layer Approach to Robotic Vehicle Security

The first keynote speaker, **Prof Xu Dongyan, is a Professor of Computer Science at Purdue University** who advocates a multidisciplinary methodology – spanning cyber, control, and domain physics – for an industrial control system (ICS) security research. He shared his recent efforts in vetting and retrofitting robotic vehicle control programs that comprises outlaying a cross-layer framework for investigating robotic vehicle accidents caused by control model implementation bugs in the control program. He presented a **control-guided technique to proactively discover control parameter validation bugs** in control program binaries and the current challenges in retrofitting control programs with reinforcement learning-based attack recovery capability.

Towards Secure and Resilient Critical Infrastructure by Design

Assistant Prof Eunsuk Kang from Carnegie Mellon University presented on how there is little tool support for system designers and operators to predict the impact of cyber-attacks on the system-wide level and proposed potential mitigation and response strategies at the design stage. He described a **model-driven approach to secure infrastructure design,** where a high-level design of a system is captured using a formal model and an automated analysis is applied to systematically identify and address vulnerabilities in

the design. He discussed how the benefits and challenges of this type of approach affects security and how they are applied to critical infrastructure systems, including water treatment plants and intelligent vehicles.

Fuzz Testing for Embedded Device Security Assurance (EDSA)

Mr Pang Ying Kiat, Director of Network and Software Security at Beyond Security, walked through on what it takes to conduct fuzz testing on ISA Security Compliance Institute EDSA Certification program. Using the ARP protocol, one of several protocols under the scope of EDSA, he demonstrated the steps taken to meet the test requirements. He also illustrated why **smart fuzzers are needed when it comes to delivering fuzzed data** at different layers of a protocol for proper testing such as the IEC 61850 MMS protocol and the process of monitoring the Device under Test (DUT) during fuzzing.

Fig 3 (left to right): Assistant Prof Eunsuk Kang (Carnegie Mellon University), Mr Pang Ying Kiat (Beyond Security) and Prof Xu Dongyan (Purdue University) at the morning panel discussion.

Digital Transformation – Are We Forgetting Something?

Fortinet's Mr Anthony Lim spoke about how organisations have engaged various aspects of digital transformation, from apps, to cloud, fintech, IoT, data analytics and artificial intelligence. He addressed the issues on how organisations must **consider cybersecurity, data protection and governance risks** while embracing such new innovative technologies and services, so that, in their pursuit to attract new customers and enjoy operational efficiencies, they and their customers are still protected.

AIoT & Embedded Security

Mr Charles Thooris from Secure-IC presented on the Artificial Intelligence of Things (AIoT) and embedded security using the FD-SOI technology. He highlighted how the **effects of convergence and layered technology must be considered** and how protection and security is as equally important when making improvements in technology. He concluded by reminding participants that there is an absolute need to protect threats to privacy and data at the device level with AIoT.

Securing Industrial Control Systems – People, Process, Technology (Raihan)

Mr Raihan Sultan from PUB Singapore shared how people, process and technology were key factors in securing ICS. He mentioned that **trainings and cyber exercises are key to maintaining a safe ICS**. Both information technology and operational technology are important to regulate the guidelines and procedures available.

Smart Cyber Sensor at the Edge

Mr Chang Seng Keong from ST Engineering shared on anomaly detection using deep learning at the edge of a network. The algorithms designed by ST are lightweight and can be implemented in a resource constrained Field Programmable Gate Array (FPGA) instead of deploying embedded GPUs. Advantages of such a technology include providing a **fast and secure detection, small form factor, lower power consumption and can be implemented at the edge for detection localisation**. One flexibility of the technology is that it can be extended to operational solutions on land, sea and air.

Hands-on Workshop

On Day 2, Research Scientist Dr Nandha Kumar Kandasamy conducted a workshop for the participants. It aimed to train participants in **developing PLC programs and a SCADA system with key elements for cyber security consideration.** They had the opportunity to develop a mock system for small substation or distribution board using the open source soft-PLC runtime package from 'OpenPLC project' and an open source SCADA package called 'SCADAbr'.

Fig 4 (left to right): Dr Kandasamy conducting the workshop for the Camp's participants

iTrust-NSoE Seminar

DeST-SCI National Satellite of Excellence
Design Science and Technology for Secure Critical Infrastructure

The Landscape of Ethereum Smart Contracts

After cryptocurrencies, smart contracts are the second major innovation of the blockchain era. Leveraging the immutability and accountability of blockchains, these event-driven programs form the basis of a new form of digital economy with tokens, wallets, exchanges, and markets, but facilitate also new models of peer-to-peer organisations. To judge the long-term prospects of particular projects and the technology in general, it is important to understand how smart contracts are used. While public announcements, by their nature, make promises of what smart contracts might achieve, openly available blockchain data provides a more balanced view on what is actually going on.

In their talk, Assoc. Prof. Gernot Salzer and Asst. Prof. Monika Di Angelo presented a comprehensive picture of the smart contract landscape on Ethereum, currently the major platform for smart contracts. Based on 20+ million contract creations and 1.5 billion interactions, they **grouped contracts with respect to common properties, characterised them quantitatively and qualitatively, and observed their temporal evolution.** Using static methods they analysed the byte code of contracts as well as dynamic methods for aggregating and classifying the communication between contracts.

Gernot Salzer is an associate professor at TU Wien, Austria. His research interests and teaching cover mostly theoretical computer science and computational logic, but more recently also distributed computing, in particular blockchain and smart contracts.

Monika Di Angelo currently works at the Institute of Computer Engineering in the Automation Systems Group, TU Wien. Monika does research mainly in Computer Science and occasionally in Social Sciences, Arts and Humanities. Her current research focus is in Smart Contracts and Cryptocurrencies. She has also worked in Informatics Didactics and Digital Heritage.

Visits

ETH Zurich

ETH Zurich learns more about iTrust's cybersecurity research and testbeds

By Research Associate Siti Nadhirah Shaik Nasair Johar

As the leading centre in cyber security in Singapore, iTrust welcomes many visitors. On 5 Dec 2019, SUTD interim Provost and Associate Provost, Student Affairs Prof Lim Seh Chun, Associate Provost for Research and International Relations Prof Yeo Kiat Seng and co-Centre Director of iTrust, Prof Zhou Jianying hosted the **President of ETH Zurich Prof Joël Mesot and his colleagues, ETH Vice President for Research and Corporate Relations Prof. Detlef Günther, the Singapore-ETH Centre Director and Managing Director Prof. Gerhard Schmit and Mr. Thomas Rufener respectively.**

The visitors were given a comprehensive tour on iTrust's Secure Water Treatment (SWaT) and Water Distribution (WADI) testbeds and a series of

demonstrations by our research assistants.

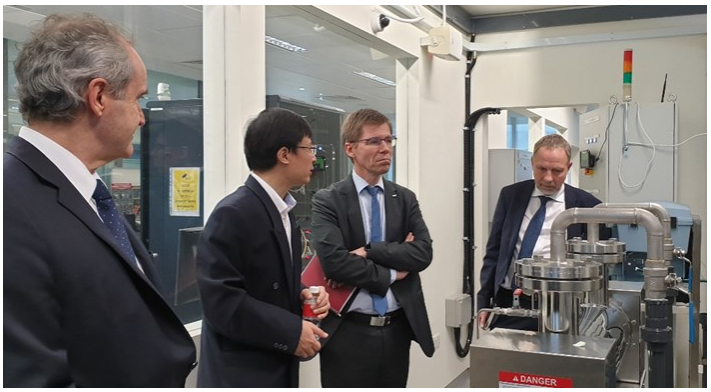

Fig 5. Prof Zhou (second from left) giving a tour of SWaT to (left to right) Prof Schmit, Prof Mesot and Prof Gunther

Profiles

iTrust welcomes three new staff to the team

Beebi Siti Salimah Binte LIYAKKATHALI

Cyber Security Technology Engineer

With her keen interest in cybersecurity, Salimah changed her field of study from biotechnology to cybersecurity. She graduated from the University Of Wollongong in 2018 where she studied Computer Science and majored in Digital System Security.

Upon graduation, Salimah worked as a Research Assistant in Project ASPIRE (Advancing Security of Public Infrastructure using Resilience and Economics) under Prof Aditya Mathur where she focused on critical infrastructure security from an offensive perspective that includes launching cyber-physical attacks, creating attack vectors and validating against defence mechanisms using iTrust testbeds. She is also a part of iTrust red team.

Salimah joined iTrust as a Cyber Security Technology Engineer in Jan 2020. In addition, she is a SG:D Postgraduate Scholar pursuing her Masters of Science in Security by Design in SUTD. In her free time, she still executes attacks, but this time round in the form of combat sports.

Siti Nadhirah Shaik NASAIR Johar

Research Associate

Nadhirah joined iTrust as a Research Associate in Nov 2019. She holds a BSc (Hons) Specialising in Medicinal Chemistry from NUS. Her research involved studying the response and efficiency of a new cyanide detecting compound.

She previously worked in a freight forwarding MNC as a customer service specialist, managing the importation of goods for various technological and manufacturing companies. She was also involved in a quality improvement project for the company.

She finds comfort in learning new recipes and watching documentaries. She enjoys a good book on a rainy day.

Ian TEO

Cyber Security Technology Engineer

Ian graduated from NTU in 2018 with a Bachelor of Engineering in Electrical & Electronics Engineering (EEE), with a specializsation in Power Engineering. Prior to joining iTrust, he was a Cybersecurity Engineer with ST Engineering Land Systems.

At ST, Ian offered support for autonomous vehicle platform and conducted VAPT (Vulnerability Assessment & Penetration Testing) for the autonomous buses. He participated in the deployment and trial of the driverless bus in Sentosa. He also provided cybersecurity support to the various engineering project teams and while ensuring that cybersecurity programs and tools were updated and ready for deployment.

Professional Accreditation, Achievement & Training

- Certified Ethical Hacker (CEH)
- EC-Council Certified Incident Handler v2
- STECA Cybersecurity Posture Building Workshop
- STECA Cybersecurity by Design (CSBD)
- SUTD Design Innovation Course

Progressively, Ian hopes to complete offensive security certifications like OSCP, ISC2, CISSP, SANS cybersecurity courses and looking into taking up MSc in Security by Design (MSSD) at SUTD in the future.
Ian joined iTrust as a Cyber Security Technology Engineer in Jan 2020.

Awards

Research Assistant Siddhant Shrivastava was presented with the **SUTD Champion award** at the SUTD Awards ceremony on 7 Feb 2020. Since joining iTrust in 2018, Siddhant has helped raise iTrust's international visibility through his work in the use of Augmented Reality/ Virtual Reality (AR/VR) technology in the context of Critical Infrastructure (CI), with plans to integrate AR/ VR with CI to train the those working in Operational Technology Cybersecurity. Siddhant has honed a significant amount of cyber-related skills and has given back to SUTD through mentoring several undergraduates.

Besides research, Siddhant has represented iTrust in hackathons and on multiple occasions, speaking at numerous overseas universities on iTrust and his work.

Well done, Siddhant!

Fig 6: Siddhant poses with his award at the SWaT testbed on which he has done much research

iTrust Matters

Feel free to reach out to us to explore research collaborations, testbed usage and training and testing services. Email addresses end with the domain *@sutd.edu.sg*

Management

Ivan LEE
Deputy Director, Cyber Security Technologies
ivan_lee

Prof. Aditya P MATHUR
Centre Director, iTrust
Director, National Satellite of Excellence, DeST-SCI
Professor Emeritus, Computer Science, Purdue University
aditya_mathur

Prof. Jianying ZHOU
Co-Centre Director, iTrust
Professor, Information Systems Technology and Design
jianying_zhou

National Satellite of Excellence

Siti Nadhirah Shaik NASAIR Johar
Research Associate
siti_nadhirah

Angie NG
Manager

Priscilla PANG
Manager
priscilla_pang

General Enquiries
nsoe_destsci

iTrust Laboratories

Mark GOH
Senior Manager
Editor, iTrust Times
mark_goh

Beebi Siti Salimah Binte LIYAKKATHANI
Cyber Security Technology Engineer
liyakkathali

Ian TEO
Cyber Security Technology Engineer
ian_teo

Desmond WAN
Cyber Security Technology Engineer
desmond_wan

iTrust
Centre for Research in Cyber Security

https://itrust.sutd.edu.sg
itrust@sutd.edu.sg
Singapore University of Technology and Design | 8 Somapah Road, Building 2 Level 7, Singapore 487372