iTrust Times

A Quarterly Newsletter

Issue Highlights:

Jul — Sep 2025 | Volume 11 Issue 3

From Centre Director's Desk

Dear readers,

Greetings from iTrust! As part of our sustainability efforts, after 10 years of hardcopies of iTrust Times, we have now moved it online!

iTrust has been growing and evolving as a world-leading research centre in the area of cyber-physical system security for the protection of critical infrastructure under the leadership of founding centre director Prof Aditya Mathur in the past decade. Now, iTrust is looking forward and planning for the development in the next decade. We hosted a roundtable in June 2025, bringing together academia, government, and industry partners for a day of reflection, knowledge sharing, and forward-looking discussions. We would like to extend our sincere thanks to all attendees, partners, and speakers for contributing to the success of this event. The outcomes will help us to shape the new direction and focus for iTrust to explore in the next stage.

iTrust has been active in the cybersecurity community, presenting its research works at top cybersecurity conferences over the past few months. As a founder of ACNS which was initiated in 2003, I was delighted to see a big team from SUTD attending ACNS'25 in Munich, Germany in June 2025. Besides Dr Awais and me from iTrust presenting our papers at the main conference and workshop, our five CiMS scholars had the opportunity to attend the conference and broaden their view in the cybersecurity world by interacting with researchers and students from around the globe. We may also support our new CiMS scholars to attend ACNS'26 in New York.

As the steering committee chair of ACM AsiaCCS, I attended AsiaCCS'25 in Hanoi, Vietnam in August 2025. 2025 is an important milestone as it celebrates the 20th anniversary of AsiaCCS. It was a great pleasure for me to grow AsiaCCS to become a top cybersecurity conference. iTrust was also the main organiser of CPSS'25, which is a flagship workshop on cyber-physical system security associated with AsiaCCS. This year we had two former AsiaCCS steering committee chairs Prof Robert Deng and Prof Winston Shieh as the keynote speakers at CPSS'25.

iTrust researchers made a significant contribution to 5G security. The team led by Prof Sudipta Chattopadhyay developed a new attack toolkit SNI5Gect and demonstrated that hackers can sniff and hijack 5G traffic without even a fake base station. This novel attack CVD-2024-0096 affects the 3GPP standard. The work was recently presented at USENIX Security'25 in Seattle, USA, and was covered widely in the media. We thank Sudipta for his contributions to iTrust and wish him all the best in the next chapter of his career.

iTrust is also doing impactful work on maritime cybersecurity and actively exploring opportunities for collaboration with local and overseas partners, by leveraging our new MariOT testbed. Stay tuned.

Jianying Zhou

Centre Director, iTrust, SUTD

Professor of Cyber Security, SUTD

CSA SINGAPORE

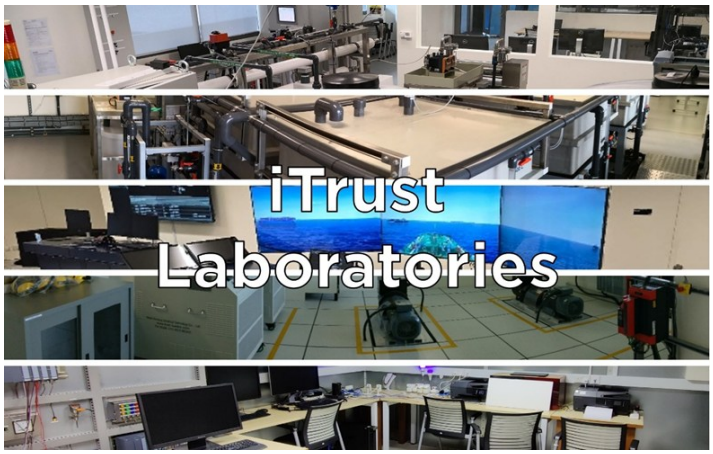
SINGAPORE UNIVERSITY OF TECHNOLOGY AND DESIGN

iTrust Centre for Research in Cyber Security

Announcement

Revised Testbed Rental Rates

iTrust is the proud host of several world-class testbeds and training platforms. These testbeds and training platforms together constitute a one-of-a kind facility for research and training in the design of safe and secure large-scale cyber-physical systems. The interconnected testbeds support R&D, technology validation, international cyber exercises, education and training programmes towards the safety and security of cyber-physical systems.



We strive to make our testbeds accessible to as many cyber professionals as possible, and are pleased to announce revised rental rates *(yes, they are revised downwards!)* for our testbeds. Use of iTrust SUTD's world-class testbeds are now more affordable than ever, and are available for use onsite and via remote access. Contact us at **itrust@sutd.edu.sg** or visit **https://itrust.sutd.edu.sg/itrust-labs_overview/** to find out more!

iTrust Roundtable 2025

A Decade of Innovation, A Future of Collaboration

On 3 June 2025, iTrust hosted its first roundtable, bringing together academia, government, and industry partners for a day of reflection, knowledge sharing, and forward-looking discussions. The event was a milestone occasion, marking over a decade of iTrust's contributions to advancing research and innovation in critical infrastructure security.

The roundtable began with Prof Aditya Mathur, Founding Centre Director of iTrust, who shared opening remarks and reflected on iTrust's journey over the past thirteen years. His address highlighted the centre's achievements in fostering collaboration and driving impactful research across multiple sectors.

Prof Jianying Zhou, Centre Director of iTrust, then presented

Fig 1.: Prof Aditya, iTrust Founding Centre Director, giving his opening remarks.

the vision and plans for the next decade of iTrust. His sharing set the stage for how iTrust will continue to evolve, building on past successes while exploring new directions in technology and security research.

Fig 2.: Prof Jianying Zhou, iTrust Centre Director, presenting the plans for the next decade of iTrust.

We also had the privilege of hearing from four of our valued collaborators and industry partners:

- Mr Edwin Chin, Chief Information Security Officer, PUB
- Mr Lim Minhan, Head of Consulting, Ensign Infosecurity
- Mr Loh Teng Joo, Head of IT, SBS Transit
- Mr Ong Chin Beng, Chief Information Security Officer, MPA

Fig 3.: Presentation by iTrust's collaborations and partners (Clockwise from top left: Mr Edwin Chin (PUB), Mr Lim Minhan (Ensign Infosecurity), Mr Ong Chin Beng (MPA), and Mr Loh Teng Joo (SBS Transit))

Their insights provided an industry driven perspective on the initiatives and directions iTrust could pursue in the coming years, underscoring the importance of strong partnerships in shaping the future.

Following the plenary sessions, attendees took part in breakout discussions that explored specific domains including

Fig 4.: Breakout group discussions following the presentations

water and energy, IoT and healthcare, artificial intelligence, maritime and land transport, and aviation. These conversations allowed them to exchange ideas and identify opportunities for collaborative research and innovation.

Fig 5.: Summarising findings from the breakout session. (From left: Dr Jit Biswas, Senior Research Fellow, iTrust, and Assoc Prof Liang Zhenkai, NUS)

The day concluded with group sharing, before participants gathered over lunch and networking to further strengthen connections and partnerships. These focused sessions encouraged rich discussions, sparking ideas for collaboration and innovative solutions.

Fig 6.: Group photo of the attendees of iTrust Roundtable 2025.

We would like to extend our sincere thanks to all attendees, partners, and speakers for contributing to the success of this event. Your presence and input are vital to shaping iTrust's journey ahead. As we look forward, iTrust remains committed to fostering collaboration and delivering impactful research that addresses the evolving challenges of critical infrastructure cyber security.

International Society of Automation (ISA) OT Cybersecurity Summit 2025

By: Mark Goh, Assistant Director, iTrust

ISA OT 2025

The ISA OT Cybersecurity Summit was held in Brussels on 18 and 19 June 2025. Organised around two tracks, "**Threat Intelligence: Transforming Business and Driving Progress**" and "**Securing the Supply Chain: Strategies for Mitigating Risk**", the summit provides practical insights about IEC 62443 and best practices for its implementation. Developed by ISA, the **ISA/IEC 62443** is an international cybersecurity standard designed specifically for industrial automation and control systems, which includes SCADA, PLCs, HMIs, and other OT systems. Unlike IT security standards such as ISO/IEC 27001, which focus on protecting data, IEC 62443 revolves around OT. Hence, IEC 62443's focus shifts from protecting data to ensuring the reliability, safety, and availability of physical processes.

In his presentation "**Mind Games in ICS: Turning PLCs into Honeypots with SDN**," Dr Sam Maesschalck, Lead OT Cybersecurity Engineer at Immersive Labs, shared that he believed honeypots have a place in the defence against OT attacks, in that they act as "scarecrows" that are designed to not just attract attackers, but to also lead attackers to believe that honeypots might be deployed to monitor them, thereby discouraging interactions with the real system. Terming it "obfuscated honeypot", his team's primary goal was not to create the most realistic honeypot for the entire system, but just a PLC, thereby saving otherwise significant investment in resources.

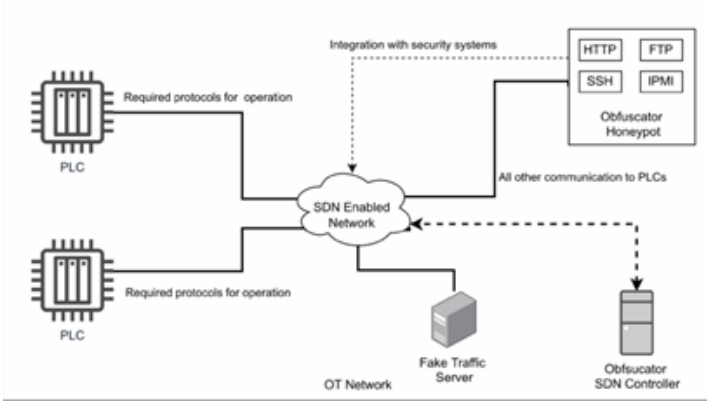


Fig 7.: ICS Obfuscator – A tool for enhancing the benefits of honeypots (picture credit: Dr Sam Maesschalck)

By exposing a mix of services (e.g., HTTP, FTP, Modbus) on what appears to be a single device, it prompts attackers to doubt its authenticity, as a typical PLC would not run such diverse services. Sam's obfuscated honeypot utilised a PKI switch, SDN controller running OpenFlow, and a Siemens PLC. A fake traffic server was added to create a realistic network environment with activity, providing attackers with proof of something to investigate.

Sam's team also invited two experts to evaluate the honeypot, and they were in agreement that the setup could be effective in a real environment by putting doubt in the

attacker's mind, implying 'one wrong step and you might be discovered' and that the system could be a honeypot, thereby reducing attackers' willingness to interact.

His next steps include evaluating and refining the deployment strategies for integrating the obfuscated honeypot near actual PLCs. A comprehensive risk assessment should also be conducted for SDN-based controller implementation before deployment in operational environments. Once deployed, "blind" penetration testing" would need to be performed to validate honeypot effectiveness. Finally, the deployment should also be checked against compliance and alignment with ISA/IEC 62443 and other industry standards.

Fig 8.: Brandon explaining why IT security is insufficient to secure OT assets (photo credit: ISA)

Brandon Cho's (Director of Cybersecurity Excellence & Innovation and Cyber Infrastructure & Technology at Honeywell), presentation "**Beyond Compliance: How Applied Security Strengthens OT Defence**" focused on OT cybersecurity as distinct from traditional IT security frameworks, emphasising that OT environments face unique risks and challenges requiring specialised approaches. This also meant that traditional IT standards such as ISO27001 would not be adequate for adoption in securing OT environments. Similarly, he noted that there were many vendors that offered solutions tailored for IT (and not OT control systems), leading to potential miscommunication, confusion, operational disruption, and safety risks. Adding to the complexity, security teams often faced siloed solutions, excessive logs, and a lack of clear prioritisation for real threats, contributing to operational and alarm fatigue. Citing Honeywell's' own experience, evaluating e suitable solutions could be a lengthy and painful process, as exemplified by Honeywell's team taking almost a year to evaluate over 50 vendors.

To this, he offered some tips for organisations who are evaluating solutions: they must first clearly define the problems they need to solve, then map out their mandatory requirements, and finally, evaluate, validate, and test the solutions before them. Evaluation criteria should include: functionality, ease of use, integration, vendor support and training, cost effectiveness, and compliance with industry regulations and standards. Finally, Brandon stressed that even with significant investment in advanced cybersecurity tools, threats can remain undetected if organisations lack skilled personnel and operational readiness.

Wrapping up, Brandon espoused two strategies for defending OT: defence-in-depth, which requires multiple integrated layers of security that address both cybersecurity and operational resilience. As each layer is designed to catch or slow down an attacker, it can help ensure that if one control fails, another defence layer can step in. These defence layers include network segmentation, layered controls that combine firewalls with next-generation features such as network IDS/IPS, anti-virus, malware features, application control, and application whitelisting to provide additional benefits and redundancy against threats like zero-day attacks, and integration of physical, technical and administrative controls. He also argued for the extension of threat modelling by mapping TTPs to industrial processes, so that threat intelligence can be transformed into actionable and process-specific defences. This in turn helps to anticipate attack paths through the OT network and prioritise critical OT assets and controls.

Using a water tank setup in his organisation, Dr Ric Derbyshire, Principal Security Researcher at Orange Cyberdefense, demonstrated a simple attack that simulated the opening and closing of valves. The attack blinded the HMI and hid the true status of the outlet valve. While simple, the objective of the attack was to highlight how the misconception of the phrase "game over" when an attacker has gained access into the OT network trivialises the complexity of operational processes and specific OT attacks to cause meaningful adverse impacts of a plant. These complexities include understanding the physical environment, how OT automates it, how cybersecurity elements secure it, and mechanical and human safeguards in place to react to and prevent cascading process faults.

Hence, Ric argued that OT environments are complex and require targeted, nuanced manipulation, not just broad, destructive actions, especially for an adversary unfamiliar with the physical process, security controls, and safety features. Case in point: he cited that the data collected by Orange Cyberdefense showed that highly sophisticated attacks, where adversaries gain deep operational understanding (process comprehension) to cause a very specific and meaningful impact, represent "only" 8% of cases over the past 36 years. He also cited Dillion Beresford's work on replay attacks on Siemens PLCs as ineffective for specific process manipulation, as they simply render systems inoperative without achieving meaningful process changes.

John Fitzpatrick, Founder of Lab539, opened his keynote

presentation "**Proven Resilience: Trusting in OT's Own Path to Cybersecurity**" by touching on the oft-cited perception that OT networks are insecure, running on legacy technology, lacking updates, and using insecure protocols.

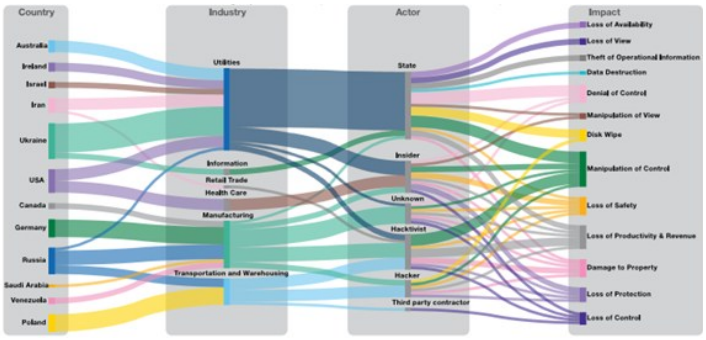


Fig 9.: Spread of OT attacks across various sectors and their impact (picture credit: Dr Ric Derbyshire)

Despite this common belief, it is IT networks - which have received significant investments, dedicated security teams, and advanced tools - that are frequently compromised, while older OT systems often demonstrate resilience and continue to function effectively. In that, there is a real concern that cybersecurity approaches (standards, solutions etc.) devised in an IT world may be inappropriately lifted and shifted to an OT world, potentially introducing new risks. As an example, the IT world typically focuses on patching all known vulnerabilities (CVEs). On the other hand, the OT work adopts a mindset focused on "resilience against future threats," which distinguishes between a general vulnerability and an exploitable one, prioritising patching only if a flaw can be actively exploited within the specific OT environment.

Fig 10.: John sharing his experience securing OT assets for an O&G client (photo credit: ISA)

Echoing the difficulty in achieving meaningful adverse impacts on OT environments, John argued that unencrypted protocols (e.g., Modbus) within a closed, segmented OT environment are less critical if an attacker must first compromise the SCADA system directly to achieve disruption. The focus should be on whether a vulnerability is truly exploitable within the operational context, rather than simply the presence of an unencrypted protocol. Extending this into the context of pentesting, John emphasised that the goal should be to identify viable routes for achieving operational disruption, not merely to generate a list of vulnerabilities that may not be patchable or exploitable in the OT context.

Dr Marina Krotofil, an engineer with 15 years of experience in industrial security, specialising in cyber-physical security, and a friend of iTrust, shared her insights into whether cyber -physical attacks that are capable of causing long-term, significant damage are becoming common. "**From Spotlighting to Shadows - The Current Dormant Phase of Cyber-Physical Attacks**" highlighted Marina's work in analysing a trove of "Vulkan files" – thousands of documents and emails – that implicated a Russian company NTC Vulkan in acts of cybercrime, political interference in foreign affairs. It was clear from the documents that Russia was developing nation-state cyber capabilities to carry out cyber attacks on telecoms, undersea cables, data centres, critical infrastructures and conduct information warfare.

Fig 11.: Marina using iTrust's SWaT testbed to demonstrate the complexity in causing adverse impacts in an OT environment

However, creating reliable and impactful cyber-physical attacks – and ensuring that they work in the field as intended - is exceptionally difficult and expensive. A case in point: an attack on a safety controller took 12 months for the initial intrusion and another 12 months to develop the implant's communication module – yet, the attack ultimately failed and was discovered because the sophisticated exploit did not perform as expected in the live environment, causing the plant to trip. Recognising this, Russia began using Ukraine as a testing ground by conducting more than 6,000 attacks in just two months in 2016, so that it could test and refine its cyber capabilities.

Marina noted that while high-precision cyber-physical attacks are difficult, the ongoing digitalisation of industrial environments is creating a massive and easily exploitable attack surface. This meant that the focus of future attacks will likely shift to causing costly downtime by targeting less-defended, internet-connected systems. She encouraged organisations to adopt a more 'military mindset and discipline' in their corporate defence strategies, rather than drive solely by business processes.

A common thread observed from the speakers was that even if an attacker managed to penetrate into the OT network, it was far from "game over," as it was extremely

difficult to launch a cyber attack that caused catastrophic and lasting physical impacts on the critical infrastructure; indeed, it would have been much easier to resort to "kinetic means" such as "throwing a match into the fuel depot." This is owning to the depth of technical know-how of the OT environment and its intricate web of a multitude of processes, interlocks and dependencies that is demanded of an attacker. The resources and investments notwithstanding in gaining this technical know-how, the attacker must then design the attack with razor-sharp precision, all this without a platform to test the attack and hence no guarantee that the resources invested will yield any success.

CPLAS 2025

Cyber-Physical Learning Alliance Summit 2025

By: Andy Tay, Senior Research Assistant & Education Lead, iTrust

On 5th June 2025, I had the privilege of representing iTrust to present my findings on evaluating technologies developed within iTrust. My research paper, titled "**Evaluating GURU: Transforming Cyber-Physical System Education**," was accepted for oral presentation at the Cyber-Physical Learning Alliance Summit (CPLAS 2025) held at the Hong Kong University of Science and Technology (HKUST). Cyber-physical learning today goes beyond the virtual classroom.

Fig 12.: Andy Tay, iTrust Education Lead, presenting his research paper "Evaluating GURU: transforming Cyber-Physical System Education"

It also encompasses the integration of generative AI, such as ChatGPT, into academic assignments. Many educators are grappling with how to regulate AI use in tertiary education.

CPLAS marked my first experience attending an academic conference as both an author and a participant. It was an eye-opening experience, allowing me to learn from researchers across the globe with vast experience and deep insights in their respective fields. The conference covered both breadth and depth of cyber physical learning — from ethical considerations in cyber-physical learning to the design of parallel learning assignments that address both the use and non-use of ChatGPT.

During the summit, Prof Danny Liu presented a compelling concept: a program-level assessment design using a "two-lane" approach. This strategy enables educators to embrace generative AI while still maintaining academic integrity. I believe this is an important concept that could be widely adopted in the coming decade, as students increasingly incorporate tools like GPT into their learning processes.

Technology will always evolve faster than policy, but how can educators remain relevant and ensure effective knowledge transfer? Prof Liu's two-lane approach offers a promising direction for empowering future educators to adapt while preserving the integrity of learning.

Throughout the conference, it became evident that the topic of cyber-physical learning has inspired many researchers to develop innovative solutions addressing the challenges faced by both students and educators. These solutions aim to improve engagement and strengthen the connectedness between students and instructors. Witnessing the work of others has inspired me to explore potential collaborations with other universities and potential enhancements for improving GURU.

ACNS 2025

5th International Workshop on Critical Infrastructure and Manufacturing System Security 2025

By: Dr Awais Yousaf, Research Fellow, iTrust

After a long hiatus from academic travel, I was thrilled to present my research paper at the 5th International Workshop on Critical Infrastructure and Manufacturing System Security (CIMSS - 2025), one of the satellite workshops of the 23rd International Conference on Applied Cryptography and Network Security (ACNS 2025) in Munich. With great anticipation, I arrived at the airport, navigated through immigration and baggage checks, and finally settled at my gate, eagerly awaiting the journey ahead.

The conference began on Monday, June 23, 2025 with opening remarks, followed by a series of engaging sessions. One of the highlights was a keynote presentation by Bart Preneel titled Crypto Wars Revisited, emphasizing the need for a broader societal debate to balance security with fundamental rights. A poster and networking session followed, offering a chance to connect with world-class researchers, including my professor, Prof Jianying Zhou.

Tuesday began with another captivating keynote by Shweta Shinde: Confidential Computing in Three Acts. The day featured parallel workshops (SPIQE, PrivCrypt, and

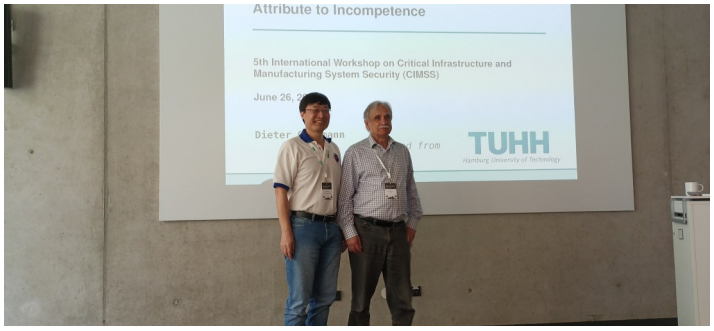


Fig 13.: Prof Jianying Zhou pictured with Prof Dieter Dieter Gollmann (TUHH)

CrossFyre), but I chose to attend the main conference sessions, which aligned more closely with my curiosity. I was also pleased to see my iTrust colleague Nadhirah and one of my graduate students, Sharma Sanjay Kumar, along with his Master of Science Security by Design (MSSD) classmates, who were attending the conference to increase their exposure to cyber security.

Wednesday brought two exciting events: the awards ceremony and the conference dinner at the Löwenbräukeller. The dinner provided a rich opportunity to engage with researchers from diverse backgrounds and interests.

Thursday marked the final day of the conference, which began with opening remarks by Chair Zengpeng Li, while Co-Chair Ahmed Amro joined online. After the first presentation, I presented my paper titled "**Spying by SPi, I got the Birds-Eye**". Co-chair Ahmed Amro asked couple of questions too and expressed his keen interests in exploring joint collaboration on the topic.

Fig 14.: iTrust representative at the conference (from left: Siti Nadhirah, Tan Qi Feng, Madhan Selvapandian, Dr. Awais Yousaf, Sanjay Kumar Sharma, Jermyn Sng, Krishnan Parthipan, Prof Jianying Zhou).

After the conclusion of the CIMSS 2025 Workshop, another workshop, AIoTS 2025 began, where Prof Jianying Zhou was the keynote speaker. His talk, titled "**Generative AI for Internet of Things Security**", was both insightful and forward-looking. Following his keynote and the subsequent presentations, I returned to the main conference hall for the formal closing remarks, marking the end of an enriching academic experience.

Fig 15.: Dr. Awais Yousaf presenting his paper at the conference

CiMS x ACNS Reflections

Experiencing ACNS 2025 – A Gateway to Global Cybersecurity Research

By: Jermyn Sng, CiMS 2024 Recipient

The 23rd International Conference on Applied Cryptography and Network Security held in Munich, Germany was a gathering of intellectuals sharing on the latest research and development in the Cybersecurity industry. The seminars were indeed highly technical, and I would be lying if I said that I understood all of it. From improvement of post-quantum cryptographic equations and application of new Machine Learning algorithms to proposing new protocols in blockchain technology, the research was as varied as they were intriguing.

We all gathered to listen to Prof Jianying Zhou's lecture on Biometric Identification. His idea of using MPC-enabled cryptographic techniques was novel!

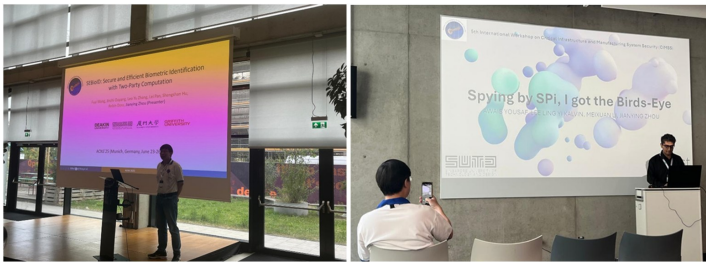


Fig 16.: (left) Prof Jianying Zhou's lecture on Biometric Identification, and (right) Dr Awais sharing about MariOT.

Aside from seminars, there were a variety of workshops that were more specialised. These were smaller groups of people who were able to ask more nuanced questions and form connections in the same field.

Dr Awais gave an excellent talk about the MariOT project under iTrust, and many participants lined up to ask questions

and show interest in the project.

Aside from the talks, and equally as important was the networking. We had lunch and coffee with various people from different aspects of life, each with a unique study to talk about. It was not all about work exchanged though, we talked about our countries, hobbies and more. I would like to believe that we made as many friends as network connections.

Overall, ACNS 2025 was a great experience in term of academics, networking and seeing fresh perspectives. I would definitely recommend those who have the opportunity to go for it.

By: Krishnan Parthipan, CiMS 2023 Recipient

Attending the 23rd International Conference on Applied Cryptography and Network Security (ACNS 2025) in Munich, Germany was an eye-opening and enriching experience. The event brought together cybersecurity professionals, researchers, and students from around the globe, providing a vibrant platform for knowledge exchange and technical discussions.

As a scholar under the CiMS programme, I had the opportunity to attend a wide array of sessions covering cutting-edge research in cryptographic protocols, AI in cybersecurity, machine learning threats, hardware security, and critical infrastructure protection. I found the CIMSS (Critical Infrastructure and Manufacturing System Security) seminar particularly relevant to my interest, with practical insights on how emerging cyber threats are reshaping industrial systems and national resilience strategies.

Fig 17.: Photo collage of interactions at ANCS (photo credit: Krishnan Parthipan)

Beyond the technical sessions, ACNS 2025 provided valuable networking opportunities. I connected with researchers from academia and industry leaders from Europe, Asia, and the US. These discussions sparked new ideas and potential collaboration opportunities, which I look forward to exploring further with the iTrust team.

Connecting with international researchers and cybersecurity professionals at ACNS 2025 in Munich. The conference offered countless opportunities to exchange ideas, build collaborations.

This experience has deepened my appreciation for the global cybersecurity research community and reinforced my commitment to contributing to national-level security challenges. I am grateful to iTrust for making this opportunity possible.

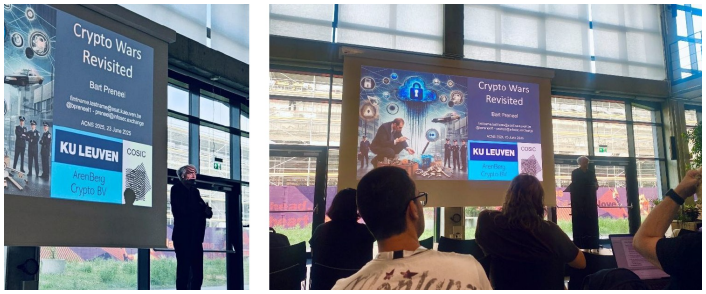


Fig 18.: 'Crypto Wars Revisited' Keynote presentation by Prof. Bart Preneel.

By: Madhan Selvapandian, CiMS 2024 Recipient

Attending ACNS 2025 in Munich was a highly rewarding experience. Representing SUTD at a major global conference allowed me to engage directly with cutting-edge cybersecurity research and discussions shaping the future of the field.

My focus areas include AI security, secure multiparty computation (MPC), industrial protocol analysis, and IoT security, all of which aligned well with several sessions and workshops at the conference. I found the AI for Hardware Security (AIHWS), Security in Machine Learning and its Applications (SIMLA), and Artificial Intelligence and IoT Security (AIoTS) workshops particularly insightful. Topics such as side-channel resilience, adversarial robustness in machine learning, and MPC for secure analytics were especially relevant to my research interests.

It was exciting to see how researchers are combining theory with real-world applications, particularly in securing critical infrastructure like smart grids, water treatment systems, and industrial IoT networks. The technical sessions were well-structured and packed with insightful ideas, some of which sparked new thoughts on how to improve current cybersecurity approaches within my own work.

Fig 19.: CiMS recipients (from left) Madhan Selvapandian, Tan Qi Feng, and Jermyn Sng (photo credit: Madhan Selvapandian)

Beyond the formal sessions, I enjoyed the informal discussions and networking opportunities. Interacting with fellow students, researchers, and industry professionals offered fresh perspectives and helped me understand how

various research efforts around the world are converging to address emerging cyber threats.

ACNS 2025 provided me with a broader and deeper view of the field, and the experience has greatly strengthened my resolve to contribute meaningful solutions in cybersecurity.

By: Sanjay Kumar Sharma, CiMS 2023 Recipient

Thanks to the generous support of iTrust, I had the privilege of attending the 23rd International Conference on Applied Cryptography and Network Security (ACNS 2025) in Munich, Germany. As a Master's student in Security by Design at SUTD, this opportunity was especially meaningful, having been selected based on interest to pursue research, merit and course performance.

The lecture theatre buzzed with excitement on Day 1, and I found myself absorbing a wealth of information presented by postdoctoral researchers and domain experts.

As the conference progressed, I focused on sessions related to Industrial IoT, maritime security, and critical infrastructure, these are areas closely tied to my research interests.

Fig 20.: Sanjay pictured with Karim Baghery, a postdoc from Belgium.

It was a candid exchange on navigating the research journey, which in turn allows me to gain clarity on topic selection, motivation, and the PhD path. The one-on-one networking also helped demystify the process of selecting my research topics and building meaningful contributions.

Fig 21.: CiMS recipients at a post-conference dinner with Prof Jianying Zhou.

With ACNS 2026 announced in New York, I'm motivated to present my thesis on modelling attack sequences in maritime systems. This experience has deepened my appreciation for the global cybersecurity community and reaffirmed my commitment to academic research. I return to SUTD energised, more focused, and ready to contribute meaningfully to Singapore's security landscape through both collaborative engagement and technical rigor.

My heartfelt thanks to Prof Jianying Zhou for his mentorship and to iTrust for making this transformational experience possible.

By: Tan Qi Feng, CiMS 2024 Recipient

Thanks to the CiMS scholarship, I had the opportunity to attend the ACNS 2025 conference, held this June in Munich, Germany. The experience was both enriching and eye-opening, allowing me to engage with leading experts in cybersecurity and gain valuable insights into the latest research and emerging trends.

"**Crypto Wars Revisited**," thoughtfully exploring enduring tensions between cryptographic innovation and regulatory pressures, and a keynote by Dieter Gollmann, "Do not attribute to malice what you can attribute to incompetence," which reminded us of the importance of building resilient systems capable of recovering from failures as well as deliberate attacks. It was deeply rewarding to see our own SUTD researchers present their work and share important insights with the international community.

During the conference, we connected with students, researchers, and industry professionals from many different countries. They shared their research interests and diverse perspectives, offering valuable insights into how cybersecurity challenges are approached across various contexts. It was a wonderful opportunity to exchange ideas and gain a broader understanding of how people worldwide contribute to this critical field.

Fig 22.: Some highlights from the conference presentations; (Clockwise from top left: Prof Bart Preneel presenting his keynote, Prof Jianying Zhou presenting a paper, Prof Jianying Zhou presenting a keynote, Dr Awais Yousaf presenting his paper)

Farewell Prof Sudipta

iTrust extend its heartfelt thanks to Prof Sudipta for his leadership and dedication as the IoT Sector Lead for iTrust's NSoE Phase II project. His guidance and commitment have made a lasting impact on the team and the project's success. We wish him continued success and happiness in his next chapter!

Fig 23.: Prof Sudipta picture with Prof Jianying Zhou and the iTrust team and researchers during his farewell gathering on 18 September.

Featured on Media

Sni5Gect

One of iTrust's works from the IoT sector, Sniffing 5G Inject (Sni5Gect), was recently presented at USENIX Security'25. Sni5Gect is a proof-of-concept attack toolkit that demonstrates that even without a rouge base station, hackers can still sniff and hijack unencrypted messages sent between the base station and the user equipment, and inject messages to target User Equipment (UE) over-the-air at specific states of 5G NR communication. Sni5Gect can be used to carry out attacks such as crashing the UE modem, downgrading to earlier generations of networks, fingerprinting, or authentication bypass. Sni5Gect's sniffing and injection capabilities have been successfully demonstrated using srsRAN and Effnet as legitimate 5G base stations. Demos of the toolkit can be found on Sni5Gect's info page: **https://asset-group.github.io/Sni5Gect-5GNR-sniffing-and-exploitation/#/**

Researchers who were involved in this work, Shijie Luo, Matheus E. Garbelini, were led by Prof Jianying Zhou and Assoc Prof Sudipta Chattopadhyay.

Scan to view previous issues of iTrust Times

iTrust Matters

General Enquiries

iTrust: *itrust*
NSoE: *nsoe_destsci*
CiMS: *cims*
Email addresses end with the domain ***@sutd.edu.sg***

Management

Prof. Jianying ZHOU
Centre DirectorProfessor, Information Systems Technology and Design (ISTD), SUTD
jianying_zhou

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

Mark GOH
Assistant Director, iTrust
mark_goh

iTrust Laboratories

Siddhant Shrivastava
Cyber Tech Lead
shrivastava_siddhant

Andy TAY
Education Lead
andy_tay

Aanand R
Cyber Security Technology Engineer
aanand_r

Jash Jignesh VERAGIWALA
Cyber Security Technology Engineer
jash_veragiwala

Andrew TAY
Research Senior Technologist
andrew_taykongngee

National Satellite of Excellence

Jillian CHIN
Senior Manager
jillian_chin

Angie NG
Manager
angie_ng

Vanessa LEE
Manager
vanessa_lee

Siti Nadhirah Shaik NASAIR
Deputy Manager
siti_nadhirah