The UQ Cyber Security Research Conference (CSRC 2024)

11 July 2024

Full program information

Contents

Welcome 3

Organisation committee 4

Keynote Speeches 6

Keynote 1: Dr Jonathan Pan (Home Team Science and Technology Agency (HTX), Government of Singapore & UQ Alumnus) – To be added 6

Keynote 2: Dr Padmanabhan Krishnan (Oracle) - ***'Intelligent Application Security'*** 6

Keynote 3: Dr David Lacey (Founder, IDCARE) - ***'Brains, Bytes and Blame'*** 6

Invited speaker 7

PhD research talks 8

UQ seed funding projects 14

TinyRange project 16

Welcome

We extend our warm welcome to you for the inaugural UQ Cyber Security Research Conference 2024.

This conference represents a notable accomplishment in the field of cyber security research & development at UQ, as we assemble to exchange insights, investigate cutting-edge technologies and methodologies, and establish new partnerships.

As we all know, the need for effective cyber security has never been greater. Our world is becoming increasingly interconnected, and as a result, we face ever more complex and sophisticated threats to our digital infrastructure. Cyber-attacks can have serious consequences, ranging from financial losses to damage to our critical infrastructure, and even to threats to national security.

This is precisely why events such as this conference hold tremendous significance. By convening preeminent researchers, HDR students, practitioners, industry experts, and policymakers from UQ and worldwide, we possess an exceptional prospect to gain knowledge from each other, share ideas, and work together towards ground-breaking resolutions to the obstacles that confront us.

We have prepared various research talks in the field of cyber security research. We will explore topics such as AI for cyber security, cyber defence for industrial control systems, applied cryptography and formal methods, novel cyber defence techniques and much more. We will also have ample opportunities to network, exchange ideas, and build new relationships that will help to advance the state of the art in this critically important field.

On behalf of the organising committee, we would like to welcome to each and every one of you. Thank you for joining us at this event, and I look forward to a productive and enlightening few days ahead.

Sincerely,

Ryan Ko and Dan Kim

General chairs

Organisation Committee

General Chairs

- Prof Ryan Ko, Chair & Director, Cyber Security, The University of Queensland, Australia
- A/Prof Dan Kim, Deputy Director, Cyber Security, The University of Queensland, Australia

Program Chairs

- Dr Guowei Yang, The University of Queensland, Australia

Industry Liaison Chair

- Mr Grant Ferguson, Senior Manager (Industry & Development), The University of Queensland, Australia

Local Organisation Chair

- Mrs Kana Smith, Project Manager, UQ Cyber, The University of Queensland, Australia
- Ms Wenlu Zhang, PhD student, The University of Queensland, Australia

Web Chair

- Mr Shunyao Wang, PhD student, The University of Queensland, Australia

Program at Glance

Time (Brisbane time, UTC +10)	Session information	Session chair
8:00 - 9:00	Registration open	
9:00 - 9:05	Welcome by A/Prof Dan Kim, Deputy Director of UQ Cyber	Dan Kim
9.05 - 9.10	Welcome remarks by Prof Michael Bruenig, Head of School of EECS	Dan Kim
9.10 - 9.30	Remarks by Mr Rob Champion, QLD Government Chief Information Security Officer (Confirmed)	Dan Kim
9.30	Guidance remarks by A/Prof Dan Kim	Dan Kim
9:30 - 10:10	Keynote 1 - Dr Jonathan Pan, Home Team Science and Technology Agency (HTX), Government of Singapore & UQ Alumnus (Confirmed)	Dan Kim
10:10 - 10:40	Morning tea break	
10:40 - 11:20	Keynote 2 - Dr Padmanabhan Krishnan, Oracle (Confirmed)	Mark Utting
11.20 - 12.00	Keynote 3 - Dr David Lacey, Founder, IDCARE (Confirmed)	Guowei Yang
12:00 - 13:00	Lunch	
13:00 - 13:05	Welcome remarks by Prof Sue Harrison, EAIT Executive Dean	Dan Kim
13:05 - 13:10	ASD introductions by Mrs Kyla Quinn, Technical Director Data & Analytic Services, ASD	Dan Kim
13:10 - 15.00	PHD research talks	Guowei Yang
15.00 - 15.30	Afternoon tea break	
15.30 - 16:30	UQ seed funding research + TinyRange	Naipeng Dong
16:30 - 17:00	Wrap up by AusCERT	

Keynote Speeches

Keynote 1: Dr Jonathan Pan (Home Team Science and Technology Agency (HTX), Government of Singapore & UQ Alumnus) – To be added

Keynote 2: Dr Padmanabhan Krishnan (Oracle) - ***'Intelligent Application Security'***

Abstract: I will present an overview of our vision for security tooling as part of DevSecOps and the progress we have made towards it. I will also outline open problems that need more research. Our approach includes a mixture of static and dynamic program analysis and the use of LLMs. These techniques are applied to protect applications from known injection attacks, address software supply chain security issues and attempt to remediate security issues in an autonomous fashion. To prevent known injection attacks, we use ideas of synthesis from programming by example to generate security monitors that are based on program-point specific allowlists. We analyse build systems and scripts (e.g., GitHub Actions, bash scripts) to ensure that third-party artifacts consumed are properly built and published. We also help developers harden their build pipelines and make their artifacts tamper resistant via associated provenances. We are exploring the role of LLMs in the process to automate the remediation.

Short biography: Paddy Krishnan is the Research Director and head of Oracle Labs in Brisbane, Australia. His current research interests are in the areas of program analysis, automatic test generation, and program repair focusing on application security. Prior to joining Oracle Labs in 2013, he was an academic for over 20 years with various visiting positions in industry. He got his B. Tech from IIT Kanpur-India, M.S and Ph.D. from the University of Michigan-USA all in Computer Science and Engineering. He is a senior member of the ACM and the IEEE.

Keynote 3: Dr David Lacey (Founder, IDCARE) - ***'Brains, Bytes and Blame'***

Abstract: Cybercrimes rely significantly on plausibility of deceptive techniques. But little is understood about what influences a victim of cybercrime in their belief of criminals that can have catastrophic impacts for organisations, individuals and economies. This presentation unpacks research on the belief influences of online deception and questions whether we have the orientation of our cyber security practices geared towards countering instances where belief of such attacks may prevail.

Short biography: David Lacey is Managing Director of IDCARE and researcher in human factors of cyber security. He has published widely on inter-organisational performance, control effectiveness and behavioural impacts and influences of crimes of deception. In his work at IDCARE he remains exposed to many tens of thousands of cases of cybercrimes impacting our community each year, providing rich insights into how well Australia is performing in countering these impacts.

Invited Speaker

Speaker: Kyla Quinn, Technical Director Data & Analytic Services, ASD

Talk title: To be added.

Abstract: To be added.

Short biography: To be added.

PhD Research Talks

Speaker: Taejun Choi

Talk title: Cyber autonomous to protect smart grid from price attack

Abstract: "The pressure for wide adoption of renewable energy has been forced due to climate change's effects across the globe, increasing the number of smart homes with photovoltaic power panels and batteries called prosumers. Although the trend's effects are positive, its potential negativity, cyber attacks via smart homes, should be taken into consideration.

In the case of nano-grids or smart homes, it is estimated market size of global microgrids to reach US $47.4 Billion by 2025 by having an annual growth rate of 10.6%. Despite the expected increase in the market, it will cause an expansion in attack surface due to its widespread control systems and the possible attacks demonstrated by academic research. Utilising the attacks demonstrated in other research, attackers may be able to commit pricing cyber attacks and manipulate electricity demands.

However, the main issue in the situation is the response of the smart home residents and grid participants. Regarding the traditional incident response, the Security Operations Center (SOC) is an organisation that detects, analyses and responds to cyber security incidents according to their operational processes or playbooks (workflows. 94\% of SOCs in organizations use Incident Response Plan (IRP) which is a sequence of tasks. Also, the huge number of security events(up to 11,000 per day is an issue; yet having a security analyst for each smart home is an issue.

In many research, AI plays an important role, but it requires a trigger program to activate playbooks as the proposed solutions using AI can only monitor the SOC, and the actual response must be executed by SOC staff. However, if you use an AI planner, you can respond to changes in the situation. We have explored AI planners to test those planners' compatibility with electricity consumption rates. After preliminary testing of different planners, we chose GTPyhop which is a Goal Task Network planning system in Python. We tested the planner with publicly available data with some interpolating them. The planner shows it can generate action plans to remediate the over-electricity consumption in minute-step monitoring."

Short biography: "I worked at LG Electronics as an embedded S/W developer for around 12 years. I am currently working as a Research Programmer at UQ and concurrently doing a part-time PhD student. Also, I have a Certified Information Systems Security Professional (CISSP) and Certified Information Systems Auditor (CISA) certificate"

Speaker: Omar Jarkas

Talk title: Solving End-to-end Data Processing Encryption with Confidential Computing

Abstract: "Loud computing has transformed the IT landscape by offering scalable resources that enable rapid application deployment and foster innovation without significant capital investment in physical infrastructure. However, This technological democratization brings forth profound privacy and trust challenges. Users are compelled to entrust their sensitive data to cloud providers, depending heavily on the providers' security protocols and service-level agreements. This dependency often leads to a considerable relinquishment of data control, exposing businesses to potential risks and breaches.

The field of cloud security has become pivotal in tackling these challenges, focusing on devising sophisticated security measures that ensure user autonomy while providing robust privacy protections. Among these advancements, end-to-end encryption stands out as a vital technology. It safeguards data by encrypting it at the source and decrypting it solely at its final destination, thereby preserving confidentiality and integrity, even across the insecure terrains of cloud infrastructures.

Nevertheless, while end-to-end encryption addresses many security concerns, its application in cloud computing has been limited due to traditional CPUs' inability to process encrypted data directly. This gap has spurred the emergence of confidential computing—a comprehensive approach underpinned by hardware-based technologies that create secure enclaves for data processing. These enclaves ensure that data remains protected during processing, shielded from other applications, the operating system, and even the cloud provider, effectively simulating the processing of encrypted data.

This presentation underscores the critical role of end-to-end encryption in preventing unauthorized data access. It explores innovative pathways to expand this encryption into full-scale, end-to-end data processing encryption by integrating confidential computing technologies. This approach promises to revolutionize cloud services by offering unprecedented security and compliance assurances."

Short biography: Omar Jarkas is a Ph.D. Candidate at the School of Information Technology and Electrical Engineering, University of Queensland, Australia. He graduated in 2022 with two masters in Software Engineering and Cyber Security. He also holds a Bachelor's in Computer Engineering. His research interest is Confidentiality and Trust using Hardware-based Security Protocols in the Cloud.

Speaker: Rita Lok

Talk title: Justice for sexual assault and rape: Digital and legal discourses in Australia

Abstract: "Sentencing in many commonwealth jurisdictions has persistently become harsher on sex crimes; some have attributed this punitive turn to the fact that the court's sentencing decisions were informed by specific public concerns. To explore the current public conversations and conceptualisations around sexual assault/rape against the backdrop of the #MeToo movement, I investigate the ways in which Twitter users make sense of and respond to high-profile sexual assault/rape cases in Australia. In other words, how do "networked publics" utilise digital spaces as "counterpublics" to challenge cultural narratives of sexual assault/rape and the judicial processing of the offence. This, as a result, has revealed the gap and relationship between judicial and public views in the pursuit of rape justice in this "human/technical hybrid world". I will present the findings derived from one of the five selected cases in this presentation. By manually coding a total of 2,072 tweets, four main themes were identified in the context of Jarryd Hayne's allegation: (1) a tug of war between acceptance and rejection of rape myths; (2) "Scumbag, lock him up and throw away the key"; (3) challenging the court's legitimacy when disagreeing with judicial processes and decisions; and (4) advocacy for better institutions and encouraging social actions.

On the one hand, social media is considered an unprecedented avenue for public civil participation in the governance and criminal justice arena. On the other hand, scholars are mindful of how technology shapes our understanding and knowledge of a social topic since social media platforms tend to foster opinion "nodes" or "echo chamber". This is the reason why some social media communities and feeds tend to be formed or populated by niche opinions where beliefs are affirmed and reinforced by reiterative exposure with limiting room for different points of view. Consequently, Twitter serves as a "loudspeaker" for those who support rape victims (i.e., engage in Rape Myths Debunking) and those who engage in victim blaming (i.e., engage in Rape Myths Acceptance). In light of it, populism can be a double-edged sword in the context of pursuing rape justice, including the protection and violation of fundamental human rights and judicial independence/rule of law."

Short biography: Rita is a Year-2 PhD student in Criminology at the University of Queensland (UQ). She is a qualitative researcher and has an interest in criminal justice policy and social media analysis. In her PhD project, she explores the public and legal discourses of sexual assault/rape allegations against the backdrop of the #MeToo movement in Australia. Alongside her studies, she is currently working as a research assistant on a cyber security research project titled "Anatomy of a successful online scam: Design, composition, proliferation, and harm" (led by Dr Jonah Rimer). Previously, she was engaged in one of the Australian Research Council (ARC) funded projects titled "Government Web Portals as New Government Actors" (led by Professor Paul Henman). In addition, she was a tutor in various Criminology courses at UQ, including Introduction to Criminology (CRIM1000) and Introduction to Criminal Justice (CRIM1019). Before studying at UQ, Rita obtained her master's degree in Criminal Justice Policy at the London School of Economics and Political Science (LSE). She also worked as a senior research assistant at the University of Hong Kong (HKU) on an array of projects (led by Dr Frances Law), including studies on the evaluation of drug use rehabilitation programs, suicide prevention initiatives, and the associations between mental ill-being and traditional masculinity.

Speaker: Hetong Jiang

Talk title: Data provenance in the Era of Distributed Computing

Abstract: The era of distributed computing, where large volumes data and research are moved to distributed storages, distributed collaborations, and distributed infrastructure, has provided better scalability, higher throughputs and lower the requirements of proximity for many research activities. Provenance, an effective way to monitoring data lineage, tracking workflows and enhance the trustworthiness of data sources, is facing challenges in adapting distributed environments. As a result, fine-grained data provenance systems in distributed setups are either introduce significant runtime overhead and leaves vulnerability that could results in untrustworthy data. Several factors are contributing to these challenges, one of the major factors is due to many designs that scales the existing provenance system into a multi-host setup, each user was treated as a part of the distributed system (a server) rather than considering the distributed system as a backend infrastructure. Another major cause is tightly coupled backend of provenance systems, where provenance storage, managing and analysing modules needs to be synchronised in real-time. My research aims to address the challenges by design a distributed-native data provenance system for distributed file system - one of the core modules of the distributed infrastructure. The design consists of the whole lifecycle of the data provenance from the collection and storage, to managing and access; it considering the distributed infrastructure from the beginning where each node only handles a part of the provenance, and no runtime syncing is required. As a trade-off, overhead have been shifted to the querying procedures, which is much less frequent than collection.

Short biography: Hetong Jiang is a fourth year PhD student at The University of Queensland. He received his bachelor degree majoring in mechanical engineering from the Queensland University of Technology, Australia in 2018, and Master of IT degree from The University of Queensland, Australia in 2020. He is currently a PhD student in the cybersecurity group under the supervision of Prof. Ryan Ko, Dr Guangdong Bai, Prof. David Abramson and Dr Mohan Baruwal Chhetri. His research interests include data provenance in distributed systems and any cybersecurity-related areas.

Speaker: Shunyao Wang

Talk title: Assessing the Vulnerability of Self-Supervised ML Models in CPS under Evasion Attacks

Abstract: In the evolving landscape of Cyber-Physical Systems (CPS), the robustness of anomaly detection models based on self-supervised learning (SSL) against evasion attacks has emerged as a critical concern. Although most research on evasion attacks has focused on supervised machine learning models, this study explores the unique challenges and feasibility of such attacks on self-supervised models within CPS. We introduce a model-agnostic framework that incorporates a Proximal Policy Optimization (PPO) agent-based Evasion Attack approach, named PEAttack, to generate optimal adversarial perturbations. Additionally, we have developed several new metrics to thoroughly assess the effectiveness of evasion attacks, considering the distinct characteristics of CPS environments.

Short biography: Shunyao Wang is a third year PhD student in UQ Cyber, School of EECS. His research focuses on machine learning model's resilience evaluation under adversarial attacks in Cyber-Physical Systems.

Speaker: Cheng MIAO

Talk title: SCP-BP Framework: Situational Crime Prevention for Managing Data Breaches in Business Processes

Abstract: Although the development of ICTs and the use of the internet brings significant benefits to businesses, it also brings opportunities for criminals who challenge cyberspace safety. Business processes are fundamental to organisations and the primary assets of organisations. Therefore, cybercrime prevention in business processes is important. Situational Crime Prevention (SCP) is a criminological practice with five strategies and 25 criminal opportunity-reducing techniques that can provide holistic cybercrime prevention by considering human and technical aspects. My literature review suggests that there is limited research on cybercrime prevention for business processes. From the People, Process and Technology perspectives, there is low engagement and involvement by business managers (People), inadequate criminology perspectives and thinking in business process design (Process) and overemphasis on technical controls (Technology). There is also limited research on the evaluation of the effectiveness of cybercrime prevention in business processes. To address these issues, we propose the use of SCP and Crime Script Analysis concepts to offer insights into cybercrime prevention for business processes, which incorporate SCP and Crime Script Analysis with Business Process Reengineering methodology to provide holistic cybercrime prevention in business processes.

Short biography: Mr Cheng MIAO is a second-year PhD student in the UQ cyber. His research interest is in the application of Situational Crime Prevention to prevent cybercrimes in business processes.

Speaker: Wenlu Zhang

Talk title: Proactive security of Industrial Control Systems via a Hybrid Honeypot Approach

Abstract: Industry Control Systems (ICS) are widely used in critical infrastructure and common services like water treatment, power grid and fuel transportation. Due to the essential roles of ICS, the security and consistency of industrial control systems are vital since any interruption or damage can cause environmental degradation, financial losses and safety compromises. However, traditional ICS devices were designed to be physically connected and communicate within closed Operational Technology (OT) networks without considering the security of Information Technology (IT) networks. In recent years, ICS networks have increasingly interconnected with the Internet to achieve remote monitoring and control for engineers. However, this provides attackers with chances to get access to ICS networks and conduct malicious attacks on vulnerable industrial devices. For example, Stuxnet malware rapidly spread in the system of the Iran nuclear station and stealthily changed the industrial device settings without being noticed by engineers which lead to the degradation of physical machines in 2010. Moreover, around 30 substations of Ukraine's electricity distribution companies were maliciously turned off which caused more than 200,000 people to lose power for almost 6 hours in 2015.

To mitigate ICS from cyberattacks, we propose metrics for measuring ICS honeypot interaction ability and present the ICSHIve framework based on the metrics parameters and rules. ICSHIve is a device-independent framework that can be used for high-interaction honeypot development of various PLC models, vendors and physical processes. To demonstrate the reproducibility of ICSHIve, we apply the framework to build Allen-Bradley and Schneider honeypots with comprehensive protocol and physical processes simulation. Our evaluation results show ICSHIve honeypots provide indistinguishable simulations that cannot be identified by common reconnaissance tools and are better at collecting attack data and identifying attack patterns compared with existing honeypots.

Short biography: I'm currently a fourth-year PhD student at UQ Cyber. I'm supervised by Prof Ryan Ko, A/Prof Guangdong Bai and Dr Naipeng Dong. I'm working on the ICS honeypot and intrusion detection technologies for my research.

Speaker: Subrat Swain

Talk title: PANDA: Practical Adversarial Attacks Against Intrusion Detection Applications

Abstract: "While adversarial machine learning (AML) attacks have become prevalent in the computer vision (CV) domain, their applications in other domains, such as network intrusion detection systems (NIDS), remain limited. This gap stems from the lack of a well-defined input space in non-image domains, hindering the generation of adversarial examples. Unlike CV problems, where the input space is the feature space, other domains generally lack a precise inverse mapping from the feature space to the problem space. In this work, we propose PANDA, a novel approach that bridges this gap and enables AML attacks against NIDS. PANDA represents a series of packets as images for training a surrogate NIDS model. Benefiting from the invertibility of this representation, PANDA leverages well-evolved image-based AML attacks to generate adversarial examples against the surrogate model. It then repurposes the adversarial examples from the surrogate model to evade the target NIDS model. We demonstrate the effectiveness of PANDA by successfully crafting adversarial network intrusions with the UQ-IoT dataset. This work establishes a framework for transferring AML attacks from the CV domain to the network domain, opening new avenues for attack modelling and defence strategies in NIDS."

Short biography: Subrat holds a degree of Bachelor of Technology in Computer Science and Engineering from VSS University of Technology, Sambalpur. He worked at Cognizant Technology Solutions, Bengaluru for a year as a Machine Learning Engineer for an Auto-ML platform called NEXA. Prior to his work with Cognizant, he worked with a San Francisco based stealth financial AI start-up as a Machine Learning Engineer. He was also a part of UC Berkeley's Skydeck start-up accelerator program in Fall 2020. Subrat also enjoys sketching and dancing.

Speaker: Isha Pali

Talk title: "Protecting Autonomous Vehicles: Safeguarding Against Modern Intrusion Detection System Attacks"

Abstract: "This research introduces a comprehensive framework aimed at addressing cybersecurity threats in Controller Area Network (CAN) networks, integral to modern vehicles. The focus is on developing and evaluating an innovative adversarial attack methodology designed to test and enhance the robustness of CAN intrusion detection systems (IDSs). Leveraging the concept of adversarial transferability, the framework creates adversarial packets capable of potentially evading existing IDSs, crucial for safeguarding against real-time threats that could pose life-threatening consequences. Evaluation utilizes the Carla simulator to generate a tailored dataset and assess the performance of adversarial packets within a simulated environment, providing critical insights into CAN network vulnerabilities.

The research objectives encompass the entire spectrum of addressing CAN network cybersecurity concerns, including generating and evaluating adversarial attacks, developing effective defence mechanisms. This comprehensive approach aims to contribute to the ongoing efforts to secure automotive systems against evolving cyber threats."

Short biography: Isha Pali is a Joint PhD student currently in her second year of study, specializing in Information Security with a focus on Automotive Security. She is enrolled in a collaborative program between the Indian Institute of Technology Delhi (IIT Delhi) and the University of Queensland (UQ). Under the guidance of her supervisors, Dr. Dan Kim from UQ and Dr. Vireshwar Kumar from IIT Delhi, Isha is deeply engaged in researching the intricacies of cybersecurity within automotive networks. Her research interests encompass understanding and mitigating the unique challenges posed by adversarial threats in vehicular systems. Isha aspires to contribute significantly to enhancing the security protocols and resilience of automotive technologies, thereby advancing both theoretical insights and practical solutions in the field of information security.

UQ Seed Funding Projects

Speaker: Yuexi Xu

Talk title: Formal Verification Techniques for Post-Quantum Cryptography

Abstract: "As quantum computing advances, securing digital communications through post-quantum cryptography is becoming increasingly critical. Computer-aided cryptography verification tools are essential in this context, simplifying the verification process for post-quantum cryptographic primitives and protocols, thus reducing the reliance on complex manual proofs. This talk provides a comprehensive review of research in four key areas: quantum computing, post-quantum cryptography, cryptanalysis, and verification.

We will begin by discussing the rapid progress in quantum computing and its potential to undermine current cryptographic systems, necessitating a swift transition to post-quantum cryptography. Quantum computers pose a significant threat to traditional cryptographic schemes, such as RSA and ECC, which are widely used today. The talk will then cover the current state of post-quantum cryptographic primitives and protocols, emphasizing the challenges and advancements in developing these new schemes. Various approaches, including lattice-based, code-based, multivariate polynomial, and hash-based cryptographic schemes, will be highlighted for their unique advantages and trade-offs.

A significant focus will be on categorizing and analysing state-of-the-art computer-aided cryptography verification tools. These tools are crucial for validating the security properties of post-quantum cryptographic schemes. We will explore their features, including modelling capabilities, adversary models, security properties, validation methods, and limitations. By examining these aspects, we can identify the strengths and weaknesses of current verification tools and understand where improvements are needed.

The talk will conclude with insights into the limitations of existing verification tools and recommendations for future research and practical applications. Potential future research directions include developing more sophisticated verification tools, integrating machine learning techniques, and exploring new cryptographic primitives and protocols. By understanding the intersection of post-quantum cryptography and computer-aided verification, we can better prepare for the future of digital communication security in the quantum era."

Short biography: "I am originally from China and pursued my higher education in Australia. I earned a Bachelor of Information Technology degree and a Master of Cybersecurity degree from the University of Queensland. My academic journey has been marked by a strong focus on emerging technologies and their security implications.

During the final year of my master's program, I had the privilege of joining Dr. Dong's research team, where I delved into the intriguing world of post-quantum cryptography. This experience was pivotal, allowing me to apply theoretical knowledge to practical research problems and contribute to the growing body of work in this cutting-edge field. My research focused on the challenges and solutions associated with securing digital communications against the looming threat of quantum computing.

After graduation, I continued to work on the project, dedicating my efforts to advancing our understanding and developing robust cryptographic protocols. This perseverance paid off when our comprehensive survey paper was accepted by the International Conference on Engineering of Complex Computer Systems (ICECCS) 2024. This achievement has been a significant milestone in my career, highlighting the impact of our research and our contribution to the global discourse on cybersecurity.

Beyond my academic and research endeavours, I am passionate about staying abreast of the latest developments in technology and cybersecurity. I actively participate in related conferences and workshops, seeking to expand my knowledge and engage with experts in the field. My journey in cybersecurity is driven by a commitment to innovation and excellence, and I am excited about the future opportunities to contribute to this ever-evolving domain.

In addition to my technical skills, I bring a multicultural perspective and a collaborative approach to my work. I believe in the power of teamwork and interdisciplinary collaboration to solve complex problems and advance our collective understanding of cybersecurity challenges in the quantum era."

Speaker: Djamahl Etchegaray

Talk title: RoadAtlas 2.0 – A Resilient and Privacy-Preserving Platform for Automated Road Defect Detection and Asset Management

Abstract: "Most local governments in Australia rely on manual methods to survey road surfaces, monitoring for damages such as cracks and potholes. This traditional workflow, which involves lodging visual evidence into a single machine, is not only time-consuming but also poses significant risks of cyber-attacks and data leaks due to its single point of failure. In collaboration with the Logan City Council and the School of Civil Engineering, we propose the construction of a resilient and privacy-preserving platform for the efficient monitoring of road network performance.

Our approach leverages advanced deep defect detection algorithms integrated with distributed databases deployed in the cloud. This innovative system ensures the secure and efficient detection of road surface damages while mitigating the risks associated with centralized data storage. By enabling the real-time identification of both physical and cyber threats, our platform offers a robust solution to the challenges faced by local governments in road maintenance. Join us as we explore the future of smart infrastructure management through the convergence of civil engineering expertise and cutting-edge technology."

Short biography: Djamahl Etchegaray is a second-year PhD student at the School of Electrical Engineering and Computer Science (EECS) at the University of Queensland (UQ), studying under the supervision of Dr. Yadan Luo and Prof. Helen Huang. As the lead research assistant on a groundbreaking project aimed at improving road surface monitoring, Djamahl has demonstrated significant expertise and leadership in his field. In 2023, Djamahl's innovative work on the Open-Roadtlas project earned him the prestigious Best Demo Award at the ACM Multimedia conference. The Open-Roadtlas project integrates large Vision-Language Models (VLMs) into a comprehensive road distress detection system, enabling detailed surveys of road, kerb, and channel conditions, and enhancing asset management capabilities.

Speaker: Liuhuo Wan

Talk title: SATB: A Testbed of IoT-Based Smart Agriculture Network for Dataset Generation

Abstract: Agriculture has seen many revolutions since the booming Internet of Things (IoT) was embedded to enable the smart agriculture (SA) scenarios. SA integrates end devices, gateways and clouds to digitalize and automate traditional farming methods. Due to the open deployment and wide range accessibility, SA systems face a new attack surface that may lead to security and privacy concerns. It is expected that the cyber security and data science research communities will set off on constructing advanced technologies to safeguard this critical infrastructure, e.g., data-driven protection and AI-enabled defense. In this work, we set up an SA testbed named SATB that can facilitate SA dataset generation. SATB is designed to be extensible so that it is capable of incorporating sensors (e.g., SenseCAP sensors) and protocols (e.g., LoRaWAN) that are extensively adopted in real-world SA systems. To test the usability of SATB, we use it to create a comprehensive SA network dataset for research use. With SATB, our dataset can capture data that rigorously covers the whole lifecycle of SA scenarios, from the authentication stage to the runtime functioning stage.

Short biography: Guangdong Bai is an Associate Professor in School of Electrical Engineering and Computer Science, The University of Queensland, Australia. His research spans on responsible machine learning, security and privacy. His work has appeared in top security and software engineering venues such as IEEE S&P, NDSS, USENIX Security, ICSE and FSE. He has served as program/general (co-)chair of international conferences such as NSS, ICECCS, and ICFEM. He is an Associate Editor of IEEE Transactions on Dependable and Secure Computing.

TinyRange Project

Speaker: Joshua Scarsbrook

Talk title: TinyRange: Next-generation Virtualisation for Cyber and beyond

Abstract: "TinyRange is a open source (https://github.com/tinyrange/tinyrange) virtual machine orchestration system with an integrated build system. TinyRange has been a work in progress for 2 years and during that time has been used in high-school workshops and for packaging software for neuroimaging.

TinyRange is designed to be a faster, easier, and safer alternative to using containers or virtual machines for application sandboxing. It uses MicroVMs to boot virtual machines in less than a second and contributes a novel filesystem driver enabling it to construct pre-populated ext4 file systems in a matter of milliseconds. This presentation will be a high-level overview of TinyRange along with a short tutorial demonstrating some use cases."

Short biography: "Joshua Scarsbrook is a Research Officer in the Computational Imaging Group of the School of EECS with 8 years of experience in Cyber Security research and development. His main research area is operating systems and orchestration. He is a founding coach for the Oceania team for the International Cybersecurity Challenge and has years of experience organising and playing in capture the flag challenges."