The UQ Cyber Security Research Conference (CSRC 2023)

17-18 July 2023

Full program information

Contents

Welcome

We extend our warm welcome to you for the inaugural UQ Cyber Security Research Conference 2023.

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

- A/Prof Guangdong Bai, The University of Queensland, Australia
- 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
- Mrs Tiani Viscarra, Project Coordinator, 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

Keynote Speeches

Keynote 1

Mr Rob Champion - Queensland Government Chief Information Security Officer - ‘Challenges, interested research topics, problems and opportunities'.

Rob has over 30 years’ experience in Queensland Government ICT in infrastructure, architecture, strategy and projects. Rob has been Queensland Government’s Chief Information Security Officer since 2018. He has been a motivating force in government cyber security, helping prepare for events such as G20 Leaders’ meetings and the Commonwealth Games. Rob and his team are driving continuous improvement and collaboration in cyber security across Queensland Government and its partners. His keynote speech will cover the challenges, interested research topics, problems and opportunities for the Queensland Government.

Keynote 2

Dr David Stockdale - Director, Cyber Security, Information Technology Services - 'The challenges AusCERT faces and how researchers can work together with them'.

David is currently the Deputy Director with responsibility for IT Infrastructure, Data Services and operational security at The University of Queensland (UQ). He is also the Director of AusCERT, one of the oldest CERTs (Computer Emergency Response Teams) in the world and a not-for-profit organisation based at The University of Queensland.

Keynote 3

Dr Nick Tate - President of the Australian Computer Society (ACS) - 'I wouldn’t start from here if I were you'.

Nick is President of the Australian Computer Society (ACS) and a senior executive, with a strong background in Information Technology (IT) and Cybersecurity. He has considerable experience as a Company Director and at the level of CIO and has been a CEO. Nick has 20 years’ experience as a Company Director in 16 Australian and 2 US companies. He has a PhD in Cybersecurity, is an Adjunct Professor at the University of Queensland (UQ) and a member of the James Cook University (JCU) Council. From 2016 to 2017, he was CEO of BCI Technology. He is also director of an APEC project to establish an ICT Skills Framework for the Asia-Pacific region.

Program at glance on Monday 17 July 2023

Session	Speaker	Title	Time
Top conference paper session	Mr Hao Guan	A Comprehensive Study of Real-World Bugs in Machine Learning Model Optimization	11:00 - 11:30
	Ms Baiqi Chen	Investigating Users' Understanding of Privacy Policies of Virtual Personal Assistant Applications	11:30 - 12:00
IoT& CPS security	Ms Wenlu Zhang	Honeypot for Industrial Control System	14:00 - 14:20
	Ms HongNhung Nguyen	Security Modeling and Analysis for In-vehicle Networks	14:20 - 14:40
	Ms Tina Moghaddam	Intelligent Cyber Attacks for Moving Target Defense Techniques in Software-Defined Networking	14:40 - 15:00
UQ Seed funding - session 1	Dr Moya Kate Baldry	Safe Gaming Metaverse	15:00 - 15:20
	Dr Steffen Bollmann	Privacy preserving federated deep learning for medical imaging	15:20 - 15:40
	Dr Rocky (Tong) Chen	Cybersecurity Defence Strategies of Distribution Synchrophasor in Smart Grids	15:40 - 16:00
	Prof Janet Wiles	Secure digital identities for older Australians	16:00 - 16:20

Top conference paper talks

Hao Guan

Talk title: A Comprehensive Study of Real-World Bugs in Machine Learning Model Optimization

Abstract: With the great advance of machine learning (ML) techniques, ML models are expanding their application domains since the last decade. To adapt for resource-constrained platforms such as smart devices, pre-trained models need to be optimized to enhance their efficiency and compactness, using techniques such as pruning and quantization. Similar to optimizations in other areas, e.g., compilers and databases, optimizations for ML models can contain bugs, leading to severe consequences such as system crash and financial loss. While bugs in the training stages have been extensively studied, the research community still lacks a systematic understanding and characterization of optimization bugs. In this work, we conduct the first systematic study to explore the strategies on overcoming the model optimization bugs (MOBs). We collect a comprehensive dataset from popular open-source ML frameworks and investigate them from various perspectives.

Short biography: Mr Hao Guan received his Bachelor's Degree in Computer Science and Technology in 2020, from Southern University of Science and Technology (SUSTech), China. He is now a PhD student in UQ-SUSTech joint PhD program, under the supervision of Dr. Guangdong Bai in UQ and Dr. Yepang Liu in SUSTech. His main research interests are machine learning and software quality.

Baiqi Chen

Talk title: Investigating Users' Understanding of Privacy Policies of Virtual Personal Assistant Applications

Abstract: The increasingly popular virtual personal assistant (VPA) services, e.g., Amazon Alexa and Google Assistant, enable third-party developers to create and release VPA apps for end users to access through smart speakers. Given that VPA apps handle sensitive personal data, VPA service providers require developers to release a privacy policy document to declare their data handling practice. The privacy policies are regarded as legal or semi-legal documents, which are usually lengthy and complex for users to understand. In this work, we conducted a subjective study to investigate the level of users' understanding of the privacy policies, targeting the VPA apps (i.e., skills) of Amazon Alexa, the most popular VPA service. Our study focused on technical terms, one of the greatest hurdles to users' understanding. We found that 84.2% of our participants faced difficulty in understanding technical terms appeared in the skills' privacy policies, even for participants with IT background. Additionally, 64.3% of them reported that explanations for the technical terms are generally lacking. To address this issue, we proposed two principles, i.e., domain-specificity principle and implication-oriented principle, to guide skill developers in creating easy-to-understand privacy policies. We evaluated their effectiveness by creating explanation sentences for 23 representative terms and examining users' understanding through a second user study. Our results show that using explanation sentences based on these principles can significantly improve users' understanding.

Short biography: Baiqi Chen is a first-year PhD candidate at the University of Queensland, under the supervision of Assoc Prof. Guangdong Bai and Dr. Yanjun Zhang. She received the Bachelor degree of engineering in Tiangong Univeristy in 2019 and the Master degrees of Information Technology in the University of Queensland in 2022. Then, she start her PhD focus on privacy and security. Her research interests include human-centric security, security usability, user privacy, privacy compliance.

HDR students talk

IoT& CPS security

Wenlu Zhang

Talk title: Honeypot for Industrial Control System

Abstract: Industrial Control Systems (ICS) are widely used in critical infrastructure areas like water treatment, chemical transportation and power grids. Since ICS are critical for business continuity and our daily lives, any interruption or damage to ICS can lead to huge business losses and even threaten the safety of citizens. However, legacy ICS devices have been designed to physically connect and communicate within closed Operational Technology (OT) networks without considering network security. Therefore, it is necessary to develop technologies to protect ICS from cyberattacks.

Honeypots are used as a deception technology which simulate the functionalities of real ICS devices to fool attackers to interact with them. Attackers' hacking strategy will be collected during the hacking process and the real device will remain safe. Existing ICS honeypots are grouped into low-interaction honeypots and high-interaction honeypots. Low-interaction honeypot simulates limited functionalities of ICS protocols which cannot support deep interaction with attackers. It is less time-consuming and cheap to design and build while can be easily identified by network reconnaissance tools and attackers. To make up for the loopholes of low-interaction honeypot, the high-interaction honeypot is invented with more protocol services and dynamic system values. The additional functions of high-interaction honeypot make the honeypot stronger to confront reconnaissance tools and stealthier to experienced attackers. On the other hand, more functions mean extra cost and time which significantly increase the cost of design and implementation. Currently, there are no clear standards to distinguish low-interaction and high-interaction ICS honeypots and the physical processes of ICS devices are not well simulated. This talking will analyze the research gaps of existing ICS honeypots and propose potential solutions to solve the problems.

Short biography: Wenlu is a third-year Ph.D. student at UQ and researching the cybersecurity of Industrial Control Systems (ICS). She graduated from UQ with an Honour of Software Engineer degree in 2020 and had internships in Domino‘s Pizza Enterprises Limited and the Department of Agriculture and Fisheries. Her current research is using ICS honeypots to collect hacking strategies from attackers and use the collected data to develop Intrusion Detection System to protect ICS."

Nhung Nguyen

Talk title: Security Modeling and Analysis for Autonomous Vehicle Networks

Abstract: Autonomous vehicles (AVs) are like computers on wheels, composed of numerous control units, network components, and protocols that enable them to operate effectively and communicate with their surrounding environment. While these technologies provide vehicles with more capabilities, they also create a dozen new attack surfaces, leaving AVs vulnerable to cyberattacks. Successful cyberattacks on AVs can have profoundly serious consequences, such as traffic congestion and even life-threatening situations.

To protect cyber-physical systems like AVs, security modeling is crucial, as it allows for the simulation and analysis of AV security before an attack occurs. However, there is still a lack of research on AV security modeling, as well as methods to analyze AV security and evaluate the effectiveness of different security protections.

In this talk, we will discuss the following: (1) Introducing the security of autonomous vehicles; (2) Presenting some challenges in AV modeling; (3) Proposing a method to model the AV security during the early stages of the system development process.

Short biography: Nhung Nguyen is a second-year PhD student at the University of Queensland, under the supervision of Assoc Prof. Dan Kim and Assoc Prof. Guangdong Bai. She received her Engineering degree in Information Technology from the Hanoi University of Science and Technology in Vietnam. Afterward, she worked for the Vietnamese government on developing cybersecurity systems and countering cybercrime. Her research interests include autonomous vehicle security, system security, and graphical security modeling."

Tina Moghaddam

Talk title: Intelligent Cyber Attacks for Moving Target Defense Techniques in Software-Defined Networking

Abstract: While moving target defense (MTD) techniques have been shown to be effective in thwarting cyberattacks, and their application in software-defined networks is growing in popularity, they are generally evaluated against simple automated attacks. However, with the increased knowledge of and ease of access to AI techniques, automating intelligent behaviours is becoming increasingly accessible, and AI is starting to be used to enhance existing attacks or create new ones that were not previously possible. Given these developments, evaluation of MTDs against simple automated attacks is no longer enough to demonstrate their effectiveness in increasing system security. With this in mind, this talk will present a framework for evaluating MTD techniques in software-defined networks against intelligent, AI-powered attacks. It will present a taxonomy of possible intelligent attacks that could target MTD techniques, then show how the framework can be used to generate datasets and realize these intelligent attacks, which can then be used for evaluating and enhancing the MTD techniques.

Short biography: Tina Moghaddam is a Ph.D. candidate at The University of Queensland, Brisbane, Australia, under the supervision of Assoc. Prof. Dan Kim and Dr. Guowei Yang. Prior to commencing her Ph.D. she completed a dual Bachelors of Software Engineering (Hons) and Science at the University of Queensland in 2021. Her research interests include cybersecurity, networking, and machine learning.

UQ Seed funding - session 1

Dr Moya Kate Baldry

Talk title: Safe Gaming Metaverse

Abstract: The UQ Safe Gaming Metaverse project has investigated the breadth and scope of socio-technical threats on shared gaming platforms with the objective of researching the efficacy of innovative threat-detection systems to improve safety in the metaverse.

The project has used codesign to engage with industry and researchers to identify how malicious and harmful human behaviour will present in these platforms. Across two workshops, participants identified concerns relating to hate crimes, data sovereignty and data privacy, identity theft, child grooming and physical assaults of avatars. Using diegetic fiction, these harms were extrapolated to allow communities to better understand the types of harms that people may experience and to allow us to better prepare mitigation strategies.

Currently, the project is investigating user preferences and behaviours relating to differing reporting mechanisms. As an embodied medium that allows 6DoF (6 degrees of freedom), we explored whether users would prefer to use embodied reporting mechanisms rather than traditional reporting interfaces and buttons. Today's presentation discusses the research findings and future directions.

Short biography:

Dr Moya Kate Baldry is a postdoctoral research fellow in the Human-Centre Computing department in the School of ITEE. She has been working on the UQ Safe Gaming Metaverse project with Dr Mashhuda Glencross, Assoc Professor Stephen Viller, and international research partners, Dr Jassim Happa from Royal Holloway University London and Prof Anthony Steed, University College of London.

Dr Baldry holds a Doctor of Creative Industries, Grad Cert (AI), MBA and B. Bus (Journalism). She has experience as an innovative digital media designer and developed one of the first location-based games for phones. She became interested in the expanded capacities presented by XR technologies to capture our data and to engage users in complex, emergent systems while conducting her doctoral research.

Through the cybersecurity seed funding project, Dr Baldry has engaged with a human-centered focus to ask pertinent questions relating to our safe participation in the metaverse, but also the need to mitigate the scope of harms presented by humans using these technologies.

Dr Steffen Bollmann

Your talk title: Privacy preserving federated deep learning for medical imaging

Abstract:

Introduction

Deep learning requires large amounts of training data and currently involves the acquisition and central aggregation of large amounts of patient data. These centrally aggregated patient datasets are used to train central models that are distributed to different sites in production.

This results in a bottleneck currently limiting the impact of deep learning in medical imaging, because it is challenging to securely aggregate the training data in a central location due to privacy and data ownership concerns. Another problem arising from this centralized approach is the cyber security threat that patient data could be extracted via model inversion and membership inference attacks.

Federated Learning enables the distributed training of a global model without sharing or aggregating the actual data. Although the data are not shared between sites the global model can contain sensitive patient information that can be leaked and extracted via model inversion attacks. To overcome this problem, Zhang et al. (2021) proposed a new algorithm named Confined Gradient Descent (CGD) that enables each participant to contribute to the model without exposing any patient information.

Here, we aim to investigate the use of confined gradient descent for the secure distributed training of deep learning models using magnetic resonance imaging data.

Methods

We implemented the Confined Gradient Descent algorithm for a proof-of-concept application on MRI data and combined it with a self-supervised learning technique (Autoseg, Meissen et al. 2022). We simulated 5 clients that jointly train a segmentation task over 510 epochs and we simulated a lack of labeled data. First, every client randomly selects an un-annotated MRI scan (1057 images in total), simulates a tumor and this simulated training data are used for the first 415 epochs and the last 95 epochs are fine-tuned with real annotated images (337 images in total). 15172 images are kept for testing the model performance. Each client initializes their own model parameters, and the gradient is computed on the local data and model. This gradient is shared with the central server and an aggregated gradient update is sent out to all clients. Every client uses the same gradient step for an update and then computes a new gradient step in the next epoch.

Results and Discussion

We found that the self-supervised learning with Autoseg delivered a dice score of 0.45 and fine-tuning with real data improved the dice score to 0.7. We also found that CGD (0.68) performed similarly to FedAvg (dice 0.69) and both federated algorithms achieved a similar performance to a centralized model (dice 0.71).

Conclusion

Confined Gradient Descent performs similarly to FedAvg and a central model. In addition, we simulated the lack of labeled data and found that the Autoseg self-supervised learning technique can help in training a model with limited labeled data.

References

- Zhang, Yanjun, Guangdong Bai, Xue Li, Surya Nepal, and Ryan K. L. Ko. 'Confined Gradient Descent: Privacy-Preserving Optimization for Federated Learning'. ArXiv:2104.13050 [Cs], 2021.
- Felix Meissen, Georgios Kaissis, and Daniel Rueckert. Autoseg – steering the inductive biases for automatic pathology segmentation, 2022.

Industry Partner Name(s): Siemens Healthineers: Kieran O'Brien; Jin Jin

Industry Partner Emails: (for our invitation emails) kieran.obrien@siemens-healthineers.com; Jin.jin@siemens-healthineers.com

Short Biography: After a PhD on multimodal imaging at the University Children's Hospital and ETH Zurich, Switzerland, Dr Bollmann joined the Centre for Advanced Imaging at the University of Queensland, where he pioneered the application of deep learning methods for quantitative susceptibility mapping. In 2019 Dr Bollmann joined the Siemens Healthineers collaborations team at the MGH Martinos Center in Boston where he worked on the translation of deep learning reconstruction techniques into clinical applications. Since joining the School of Information Technology and Electrical Engineering at the University of Queensland in 2020 Dr Bollmann develops computational methods to process magnetic resonance imaging data.

Dr Tong Chen
Talk title: Cybersecurity Defence Strategies of Distribution Synchrophasor in Smart Grids

Abstract: Distribution Synchrophasors (DS) are the signatures of power distribution systems that are directly recorded from the power outlets. Variations of DS collected at different locations possess local environmental characteristics, which can be used as a potential fingerprint for authenticating measurements' source information. Within this presentation is proposed a computational intelligence-based framework to recognize the source locations of DS signals within a distribution network in the Queensland state. To be more specific, a set of informative location-sensitive signatures from DS measurements are initially extracted with such measurements representative of local grid characteristics. Then these distinctive location-dependent signatures are further fed into a data mining algorithm yielding the "source-of-origin" of DS measurements. Experimental results using DS data from multiple intra-grid locations have validated the proposed methodology.

Short Biography: Rocky (Tong) Chen is currently a Lecturer and ARC DECRA Fellow with the Data Science Discipline, School of Information Technology and Electrical Engineering, The University of Queensland. His research has been focused on developing accurate, efficient, and trustworthy data mining solutions to discover actionable patterns and intelligence from large-scale user data to facilitate prediction and recommendation in a wide range of domains. To date, he has published 60+ peer-reviewed papers in the most prestigious conferences (e.g., KDD, SIGIR, WWW, ICDM, ICDE, AAAI and IJCAI) and journals (e.g., VLDBJ, IEEE TKDE, IEEE TNNLS, ACM TOIS and WWWJ). His publications have won 3 Best Paper Awards, 1 Best Paper Nomination, and 2 Travel Awards.

Industry Partner Name(s): David Dart from NOJA Power Switchgear Pty Ltd

Industry Partner Emails: (for our invitation emails): DavidD@nojapower.com.au

Prof Janet Wiles
Team: Janet Wiles, William Bingley, Alex Haslam, Nicole Gillespie, Ryan Ko, Alina Bialkowski, Peter Worthy

Abstract: Secure digital identities are increasingly required to participate in important aspects of society such as banking, accessing government services, and staying connected to others. Our research investigates how older Australians engage with and secure their digital identities. We have conducted a systematic literature review on how older people can secure their digital identities, as well as an online survey of older Australians' experiences with and attitudes towards digital identity security. Furthermore, we are currently in the process of conducting semi-structured interviews. These data will be combined to create a report in conjunction with KPMG, which in turn will be utilised to build towards an ARC Linkage grant application.
Industry Partner Name(s): KPMG

Short Biography: Janet Wiles is a Professor in Human Centred Computing at the University of Queensland. Her multidisciplinary team co-designs language technologies to support people living with dementia and their carers; new tools to enable language communities to develop their own speech recognition systems; and social robots for applications in health, education, and neuroscience. Her most recent research on Human-centred AI focuses on how older Australians perceive and manage their digital identities.

Program at Glance on Tuesday 18 July 2023

Session	**Speaker**	Title	Time
AI security & Security for AI	Mr Kun Han	Temporal Analysis for Cyber Attacks Detection	9.30 - 9.50
	Mr Subrat Swain	SPAT: Semantic Preserving Adversarial Transformation for Generating Perceptually Similar Adversarial Examples	9.50 - 10.10
	Mr Shu Peng	Quantitative Explainable AI for Face Recognition	10.10 - 10.30
UQ Seed funding - session 2	A/Prof Mark Utting	Automated Verification of Ethereum Smart Contracts	11:00 - 11:20
	Dr David Mount	Assessing the Impacts of Enhanced Cybertip Alerts on AFP Child Abuse Material Triaging and Investigative Referral Processes	11:20 - 11:40
	A/Prof Gianluca Demartini	The UQ Election Ad Data Dashboard	11:40 - 12:00
Incident response & governance	Ms Elinor Tsen	Contextualising cyber resilience: how can we encourage its adoption?	13:40 - 14:00
	Mr Hee Meng Ho/Mr Cheng Miao	Using Situational Crime Prevention (SCP) to Prevent Cybercrimes	14:00 - 14:20
Software & Systems security	Mr Joshua Scarsbrook	TinyRange: Tiny run everywhere Linux networks for Cyber Security education	13:00 - 13:20
	Mr Omar Jarkas	Leveraging Hardware-Based Solutions for Robust Cloud Container Security	13:20 - 13:40
UQ Seed funding - session 3	Dr Ivano Bongiovanni	Evidence-based decision-making in cybersecurity: A comparison between research and practice	14:30 - 14:50

AI Security and Security for AI

Kun Han

Talk title: Temporal Analysis for Cyber Attacks Detection

Abstract: Cyber-attacks are a growing concern for organisations and individuals, emphasising the need for effective, quick, automated methods. This research endeavours to tackle the challenge of efficient real-time cyber-attack detection, despite limited resources and the need for a quick response time.

Cybersecurity domains often involve multivariate time series data related to network traffic, user behaviours, and system logs. This data can exhibit missing values due to sensor failures or inconsistent sampling, which can impede traditional machine learning methods. To solve this issue, we examine the potential of utilising a graph relationship among time-series data to enhance cyber-attack detection. Specifically, the proposed encoder-decoder framework utilizes a recurrent neural network, such as a Gated Recurrent Unit with message passing from a Graph Neural Network (GNN), to address the challenges posed by data irregularities, including missing values and varying lengths. Note that, our proposed methods do not require any prior information and can adaptively learn the graph structure with the streaming data. Empirical experiments demonstrate that our proposed framework enhances the performance of state-of-the-art methods by 10% on both synthetic and real-world datasets. The findings of this research are expected to make a significant contribution to the field of real-time cyber-attack detection by providing new insights and techniques.

Short biography: Mr Kun Han is a second-year PhD student in the School of ITEE at the University of Queensland (UQ). Growing up with a passion for both computer science and engineering, Kun pursued a bachelor's degree in communication engineering at the Beijing University of Post and Telecommunication, China. After graduating with honours in 2018, he enrolled in UQ's master's program in computer science. At UQ, Kun works under the joint supervision of Professor Ryan, Dr Miao Xu, Dr Weitong and Dr Abigail. His research focuses on temporal analysis-based machine learning techniques for cyber-attacks detection. Although still in the early stages of his PhD, Kun has already achieved some academic milestones. He presented his work at Australasian Joint Conference on Artificial Intelligence (2022) and actively participated in cybersecurity events. Kun has also attended the Algorand Centre of Excellence on Sustainability Informatics for the Pacific (ACE-SIP) summer school, further expanding his knowledge and expertise in the field.

Kun is dedicated to being an active participant in the cybersecurity community, consistently involving himself in various events and conferences to further enhance his research and knowledge.

Subrat Kumar Swain

Talk title: Generating Semantic Preserving Adversarial Samples

Abstract: Achieving adversarial robustness remains a significant challenge in deep learning due to the lack of an exact mathematical description of semantic correctness. Most current adversarial attack and defence strategies rely on bounded threat models such as L2, Linf distance, or spatial perturbations, that do not consider semantic and perceptual closeness to the original data. To address this ue, we propose Semantic-X attacks, a semantic implementation of existing adversarial attack algorithms. We modify the objective function of an existing adversarial attack X to maintain semantic similarity between the adversarial and original input. Our method achieves robust accuracies

comparable to prior methods while generating adversarial input while maintaining the semantic correctness and perceptual similarity to the original inputs.

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 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. In 2022, he received the most prestigious PhD fellowship in India, the Prime Minister's Research Fellowship (PMRF). Currently, he is a second year joint-PhD scholar in The University of Queensland - IIT Delhi Academy of Research.

Shu Peng

Talk title: Quantitative Explainable AI For Face Recognition

Abstract: Face recognition is widely adopted in our daily life in recent years. It usually relies on sophisticated techniques to achieve high accuracy in identifying or verifying the identities of given face images.

Artificial intelligence (AI), especially deep learning, is a popular technique used in face recognition due to its high accuracy, known as the \emph{deep face recognition}.

However, the reliability of the deep face recognition models becomes a concern, especially in security-critical applications.

The main challenge is the ``black-box"" nature of the sophisticated internal structure of the models.

Explainable AI has emerged as a solution that provides meaningful explanations to help humans understand the complicated internal structure of the deep learning models, and increase the transparency and interpretability of the ``black box". However, this is often at the cost of model accuracy. In this paper, we propose an approach to increasing both the accuracy and interpretation of quantitatively explainable AI models for face recognition. It increases the accuracy of the explainable face recognition models by applying improved loss functions and enhances quantitative interpretability by adding a new visualisation feature. The proposed approach is validated using advanced deep face recognition models and is compared with existing approaches to demonstrate its better performance.

Short biography: My name is Shu Peng, I'm a first year master student studying Software Engineering at The University of Queensland, my research i focus on developing explainable AI models for face recognition to address the lack of transparency and interpretability in many AI systems. I interested in building models that can provide concise, intuitive explanations of their decision-making processes to help establish trust and enable effective oversight of AI systems. the aim is to contribute to the development of more transparent AI systems that are not only more accurate, but also more ethical and understandable."

UQ Seed funding - session 2

A/Prof Mark Utting
Your talk title: Automated Verification of Ethereum Smart Contracts

Abstract: We explore the use of Microsoft's Vale framework to guarantee correctness of low level Ethereum Virtual Machine (EVM) bytecode, while affording smart contract developers higher-level language and reasoning features. We encode EVM-R (a subset of EVM semantics and instruction set) into F*, and raise the EVM-R into Vale design-by-contract components in an intermediate language supporting conditional logic. The specifications of Vale procedures constructed from these verified EVM bytecodes carry integrity to the bytecode level, which is not guaranteed by current EVM compilers. Furthermore, raising the instruction set to Vale allows opportunity for refinement of the instructions, which we did ensuring safety properties of overflow protection, invalid memory access protection, and functional correctness. We demonstrate our contributions through two case study smart contracts, a simple casino, and a subcurrency coin.

Short Biography: Associate Professor Mark Utting's research interests include software verification, model-based testing, automated reasoning, and the correctness of smart contracts. He has worked in the software industry for several years, developing next generation genomics software and manufacturing software. He is author of the book 'Practical Model-Based Testing: A Tools Approach'.

Industry Partner Name(s): Consensys

Dr David Mount

Talk title: Assessing the Impacts of Enhanced Cybertip Alerts on AFP Child Abuse Material Triaging and Investigative Referral Processes

Abstract: The AFP recently introduced a new reporting and intelligence system (Hubstream Intelligence Server Enterprise - HISE) to manage Child Abuse Material (CAM) triaging and prioritization of cases for investigative action. HISE provides triage staff with access to international Cybertip reports that contain more detailed user generated content and geo-locational data than was available using the old reporting and referral system. This joint research project aimed to assess the impacts of HISE and the associated enhanced Cybertip reports on the AFP's existing CAM triage and referral decision-making processes and the ongoing operational viability of the UQ-AFP designed Triage Referral Investigation Support Tool (TRIST).

Short biography: Dr David Mount is a Lecturer in Cyber Criminology and since 2019 has been working collaboratively with the Australian Federal Police on a series of research projects associated with the triaging of online child abuse material reports. David's research interests span law enforcement training regimes, information warfare, countering online child exploitation and the nexus of intelligence and law enforcement in the cyber realm.

A former Australian Army officer, David's career in the Australian Intelligence Corps provided wide-ranging experience and specialist qualifications in the intelligence and security domains. He served at the strategic, operational and tactical levels of command providing advice and support to commanders and decision makers both in Australia and deployed on operational service. The culmination of David's military career came with his appointment as Commandant of Australia's Defence Intelligence Training Centre. Levering his knowledge and experience of working as a member of the Australian Intelligence Community for 30 years, David has provided consultancy services to several major Defence projects.

He has also developed and delivered intelligence training to organisations including the Australian Federal Police, Victoria's Office of Police Integrity and the Australian Security Intelligence Organisation.

Associate Prof. Gianluca Demartini

Your talk title: The UQ Election Ad Data Dashboard

Abstract: In this talk we will discuss the work that led to the creation of the UQ Election Ad Data Dashboard which was used to track Facebook ads published during the 2022 Federal election campaign in Australia. This system serves as a continuous social media monitoring of political campaigning to understand how untruthful communication may be used to influence an audience (e.g., the electorate) and further an agenda. We will present key findings from our monitoring system as well as the results of a post-hoc analysis of the collected data aimed at automatically detecting propagandist strategyes used during the campaign.

Short Biography: Dr. Gianluca Demartini is an Associate Professor in Data Science at the University of Queensland, School of Electrical Engineering and Computer Science. His main research interests are Information Retrieval, Semantic Web, and Human Computation. His research has been supported by the Australian Research Council (ARC), the UK Engineering and Physical Sciences Research Council (EPSRC), the EU H2020 framework program, Meta, Google, and Wikipedia. He has published more than 200 peer-reviewed scientific publications including papers at major venues and received several best paper awards. He is a senior member of the ACM, an ACM Distinguished Speaker, and has been a TEDx speaker in 2019.

Incident response & governance

Elinor Tsen

Talk title: Contextualising cyber resilience: how can we encourage its adoption?

Abstract: Cyber incidents are a significant concern for organisations requiring mature cyber security and resilience implementations. However, cyber security and resilience tends to be implemented in isolation within organisations. This isolated implementation appears to be due to the historical technical focus of cyber security. Despite research and practice expanding from this focus, there is little evidence that organisations are as progressive. This can lead to organisations isolating cyber security and resilience from other functions.

Encouraging organisations to evolve and integrate their cyber security and resilience can be difficult. It is unclear what factors can be used to encourage adoption of practices. There is then little certainty of how policies and other mechanisms affect adoption. This lack of clarity on relevant factors for adoption is a current gap in existing research. Though this gap is pertinent for cyber security, it is a critical issue for cyber resilience. The potential utility of cyber resilience, i.e. its focus on incident response and recovery, is severely limited by the current lack of adoption. This research focuses on cyber resilience and determining relevant factors encouraging adoption. Understanding relevant factors can help researchers, policymakers and practitioners develop mechanisms to motivate adoption. In addition, these mechanisms may encourage a cultural shift towards integrating cyber resilience.

This research addresses this gap of little research on relevant antecedents for cyber resilience through a mixed-method study (focus groups, survey and interviews). The findings show cyber resilience is a voluntary practice with limited institutional actors. Further, standards and certifications are key in encouraging higher cyber resilience. Internally, the support of top leadership appears to be critical unlike sector and size.

This research contributes to current understanding of how cyber resilience adoption can be encouraged through identifying relevant mechanisms. These mechanisms may be usable to disseminate relevant techniques and practices to organisations.

Short biography: Elinor is a PhD candidate within the University of Queensland Business School. Her interdisciplinary research focuses on exploring the concept of cyber resilience in organizations to support decision-making.

Cheng MIAO and Heemeng Ho

Talk title: Using SCP to provide a holistic cybercrime prevention in business process management

Abstract: Business processes are fundamental to organisations in achieving their business objectives. Today, business processes benefit from IT development and represent a logical sequence of an interrelated set of tasks involving people, data and business activities. However, IT development and transforming human activities in the physical world to cyberspace bring along the threat of cybercrimes. Although organisations implement cybersecurity controls to prevent cybercrimes, emphasising technical controls leads to a biased cybercrime prevention strategy. Furthermore, business process management naturally focuses more on profitability than cybercrime prevention. Therefore, the lack of emphasis on cybersecurity in managing business processes can lead to increased cybercrime opportunities, resulting in financial losses and reduced customers' confidence and trust in online businesses. To overcome this, a multi-disciplinary approach is needed to implement a cybercrime prevention strategy in business processes holistically. We start by understanding cybercrime opportunities by breaking down the business process components and subsequently linking them to cybercriminal opportunities in business processes. Next, a SCP-based cybersecurity framework integrating SCP techniques and cybersecurity guidelines is introduced to provide a comprehensive set of cybersecurity, business and people controls. We demonstrate the application of this framework with an example of a business process. We also discuss the extendibility of this framework to include other forms of cybersecurity threats in the business processes.

Short biography: Mr Cheng MIAO received his BSc in Tourism Management in 2019 from Beijing International Studies University, his BTHEM in Event Management in 2019 from the University of Queensland (UQ), and his MInfTech in Information Technology in 2022 from UQ. He is currently a first-year PhD candidate in the cybersecurity group in the School of Information Technology and Electrical Engineering at UQ under the supervision of Professor Ryan Ko and Dr John Gilmour. His current research interest focuses on applying Situational Crime Prevention (SCP) to business processes for cybercrime prevention.

Software & Systems security

Joshua David Scarsbrook

Talk title: Type Inference in TypeScript: Uncovering the Magic Behind Type Annotations

Abstract: TypeScript is a popular statically-typed programming language that provides powerful tools for developers to write robust and maintainable code. One of the key features of TypeScript is its type inference system, which allows developers to omit type annotations while still enjoying the benefits of static typing.

In this talk, we will explore the inner workings of TypeScript's type inference system and how it helps us write better code. We will start by reviewing the basics of type inference and how it differs from dynamic typing. We will then dive into the details of TypeScript's type inference algorithm and examine some of the challenges and limitations it faces.

Along the way, we will explore some common pitfalls and best practices for using type inference effectively in TypeScript. We will also discuss some of the trade-offs involved in using type inference, such as code readability, performance, and maintainability.

By the end of this talk, attendees will have a deeper understanding of how TypeScript's type inference system works, and how to use it effectively in their own codebases.

Short biography: Hello, my name is Joshua Scarsbrook and I am an Research Officer and PhD Student in Cyber Security with 7 years of professional research experience. My passion lies in developing solutions to tackle the ever-growing challenges in the field of cyber security.

Throughout my career, I have been involved in numerous projects that have allowed me to hone my skills in the areas of visualisation, software architecture and operating systems. My work has been focused on developing innovative approaches to address complex cyber security issues.

I am committed to advancing the field of cyber security through my research and am constantly seeking out new opportunities to collaborate with other experts in the industry. I am particularly interested in cyber security education, as I believe that empowering individuals with the knowledge and skills to protect themselves and their organisations is essential to building a safer digital environment."

Omar Jarkas

Talk title: Embracing Container Confidential Computing: Enhancing Performance and Privacy in Cloud Environments

Abstract: Lightweight virtualization is one of the services widely used in various applications due to its efficiency in resource utilization. It enables lighter and more agile user space instances, known as containers, than traditional Virtual Machines (VMs). Such agility has encouraged the adoption of multi-cloud and hybrid-cloud environments. However, due to weaker isolation guarantees, security hinders container adoption. Therefore, security researchers actively propose various software and hardware-based container security protocols to address these issues.

In contrast to software-based, hardware-based container security techniques are sought as an alternative to software trust as they enable confidential computing. Confidential computing is an emerging technology that uses hardware security modules to secure remote environments on the dimension of runtime encryption, isolation, remote attestation, and sealing. Examples of confidential computing include processor-based secure cloud environments.

Both confidential computing and containerization have made substantial progress in recent years, but their combination and optimization for various use cases are still being explored and developed. By integrating confidential computing into containerization practices, we can establish a more robust security posture for cloud deployments, addressing the challenges of data protection and privacy compliance in an increasingly interconnected digital world while enjoying the performance advantages of lightweight virtualization. This talk will cover the latest developments in confidential computing, including the role of trusted execution environments, emerging frameworks, and orchestration tools. We will also discuss the growing industry support for confidential computing and its potential to become a must-have feature for cloud and SaaS workloads, transforming the future of computing and ensuring the privacy and security of sensitive data in the cloud.

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 cybersecurity. He also holds a bachelor's in computer engineering. His research interest is Security and Trust in Hardware-based Security Protocols in the cloud, multi-tenant, and micro-service environments. He is also involved in industry research related to application security and machine learning. "

UQ Seed funding - session 3

Dr Ivano Bongiovanni
Abstract: In this presentation, we will illustrate the preliminary findings of a research project aimed at unpacking the factors that mostly affect organisational leaders when making decisions in cybersecurity. Examples for such decisions include, but are not limited to: budget allocation for cybersecurity, selection of cyber-risk controls, reliance on outsourcing, stance towards cyber-insurance, etc. Our study has produced a theoretical, research-based model for how decisions are made in cybersecurity. It has then utilised it for comparison with data collected in 3 organisations in the utility and healthcare sectors, to identify differences and propose recommendations for future intervention. We will conclude our presentation with next steps in the research and strategies for publication of findings which maximise the value for end-users (e.g., participating organisations).

Short Biography: A Lecturer in Information Security, Governance and Leadership with the UQ Business School and a member of UQ Cyber, Ivano helps business leaders and executives make evidence-based decisions in cybersecurity. With a professional background in risk and security management, Ivano's work bridges the gap between technical cybersecurity and its repercussions across organisations. He has advised ministers, policy-makers, board members, and senior executives on strategies, governance structures, policies, and training programs for effective cybersecurity management. Ivano is also an experienced facilitator in the fields of Design Thinking and Design-Led innovation, having run since 2015 more than 50 design-led workshops and longer projects for public and private sector organisations.

Industry Partner Name(s): Avertro
Industry Partner Emails: (for our invitation emails) Ian Yip (CEO): ian@avertro.com

Naipeng Dong

Title: Formal Verification of Post-Quantum Cryptographic Primitives

Abstract: Quantum computers will be a real threat to public-key cryptography which is used to secure all digital communication in today's world. The security of these cryptographic primitives is provided by their complex security proofs which are prone to errors. In the case of post-quantum security, the security proofs are even more complex than in the classical setting. Therefore, to ensure a high guarantee of post-quantum cryptographic security, simple security proofs performed by humans are not sufficient to provide confidence in those primitives. Formal verification methods which are performed by software are highly required. In this project we will investigate formal verification methods for Post-Quantum Cryptographic Primitives.

Short Biography: Dr. Naipeng Dong is an expert in automatic formal verification of security and privacy in cryptographic protocols, Android applications and blockchain systems. She has developed efficient automatic formal verification techniques with a focus on attacker reasoning and analysis on cryptogrpahic protocols, developed algorithms to verify fault-tolerance of systems with dishonest participants, and analysed systems in e-auction, e-health, Single-Sign-on authentication, and blockchain consensus.

Industry Partner Name: DEPENDABLE INTELLIGENCE PTY LTD