Erin Kenneally

U.S. Department of Homeland Security

Talk Title: *Responsible cyber security innovation*

Abstract: TBA

Trust is necessary for sustainable and scalable technology innovation yet we cannot assume their coevolution without deliberate design and

supporting processes. This is even more paramount as we build and deploy systems that autonomously observe, interact, decide, and take actions with consequence. Yet neither trust nor innovation easily lends itself to mathematical formulae or universal specifications. The talk will frame an approach this challenge through several applied cybersecurity R&D programs that comprise the 'Body, Mind, and Spirit' of trusted cyber-risk innovation: data and analytics, economics, and ethics, respectively.

First is the Information Marketplace for Policy and Analysis of Cyber-risk & Trust (IMPACT) program, [https://www.dhs.gov/csd-impact] a unique distributed platform that supports the global cyber risk community by coordinating and provisioning real world data and information sharing capabilities (tools, models, and methodologies). The second is the Cyber Risk Economics (CYRIE) program [https://www.dhs.gov/science-and-technology/csd-cyrie] that supports empirically-based measurement, modeling and evaluation of cybersecurity investments in cyber risk controls, impacts of those investments on outcomes, and the resulting value and incentives that drive optimal decisions. At a time of high opportunism and when cybersecurity may be in tension with other rights and interests, the third trust proxy is the Cyber Risk Ethics Decision Support (CREDS) tool [https://www.impactcybertrust.org/ethos], a project that assists cybersecurity stakeholders identify, articulate and mitigate ethical risk in the design and deployment of their cybersecurity R&D.

Prof. Christopher Lecke

University of Melbourne

Talk Title:Anomaly detection in cyber security

Abstract:

A major challenge in detecting cyber attacks is how to identify stealthy or zero-day attacks, which do not match a known signature. To address this problem, there has been considerable interest in methods based on anomaly or outlier detection, where the aim is to model normal behaviour and detect activities that do not fit that model of normal behaviour. A major issue for anomaly detection is the potentially high rate of false positive alarms due to changes in normal behaviour in complex systems, and the ability of adversaries to “poison” the training data and bias the learned model of normal behaviour. This talk will give a brief introduction to anomaly detection in cyber security, and highlight some recent research on adversarial attacks on anomaly detection techniques.

Dr. Marthie Grobler

CSIRO's Data

Talk Title:

Conceptualising human resilience within the cyber context: Putting cyber epidemiology into context

Abstract:

The human element is perceived as the weakest link in otherwise provably secure socio-technical systems. We therefore place human centric cyber security at the forefront of enabling online health resilience. The research challenge that we face is that people in general are not resilient enough to identify and remediate cyber risks and therefore continue to create online risks for others through their online actions and interactions. Cyber security in particular is a complex global phenomenon where different populations interact, and the infection of one person creates risk for another. Given the dynamics and scope of cyber campaigns, studies of local resilience without reference to global populations are inadequate. It is therefore advantageous to look at cyber from an epidemiological viewpoint, and investigate how human resilience can be hardened to remediate the rippling and cross-infectious effects from cyber attacks.

Prof. Robert Deng Huijie

Singapore management university

Talk Title:

Secure sharing and computation of encrypted data in untrusted servers

Abstract:

Outsourcing data to third-party cloud servers brings many benefits to individuals and organizations; however, software and hardware platforms in the cloud are not under direct control of data owners and may subject to various attacks. Storing electronic medical records in a patient's mobile device allows ubiquitous access of such records, especially in emergency situations; however, mobile devices could be lost or stolen. In this talk, we present a cryptographic and system integrated approach to protecting data security and privacy in "untrusted servers". In particular, we introduce a framework for scalable access control of encrypted data and for secure computation over encrypted data. We provide an overview of the underlying techniques, a prototype implementation, and performance evaluation.

Prof. Yang Xiang

Swinbourne University of technology

Talk Title:

Data-driven cyber security to counterfeit malicious attacks

Abstract:

Cyber security has become one of the top priorities in the research and development agenda globally today. At the same time, data is more prevalent and pertinent than ever before. Cyberspace generates 2.5 quintillion (1018) bytes of data per day. Threat data is no exception: with continuously growing cybercriminal activities contributing to its abundance. New and innovative cyber security technologies that can effectively address this pressing danger are critically needed.

Data-driven approaches to solve security problems have been increasingly adopted by the cybersecurity research community. They have two areas of focus: detection and prediction of security events. Early research focuses primarily on detection of various kinds of security events, such as cyber-attacks, vulnerabilities, and data breaches. More recently, there have been efforts to predict or forecast cyber security events, such as predicting attackers' next move, estimating attacks' ultimate goal, intrusion prediction, and security situation forecasting. Data and its analytic methods are the key tools to underpin all of these activities.

New methods and tools, consequently, must follow up in order to adapt to this emerging security paradigm. In this talk, we will discuss the concept of Data-Driven Cyber Security and how the data-driven methodology can be used to address the security and privacy problems in cyberspace. Addressing the challenges will allow us to deliver solutions that can safeguard one of the central and critically important aspects of all of our lives from attacks that are real, ongoing and damaging

Prof. Vijay Varadharajan

University of Newcastle

Talk Title:

Data – centric security – challenges and issues

Abstract:

In this talk, we will look at some of the challenges and issues in data-centric security. We will start by outlining the data context and related challenges in security, privacy and trust in a distributed system context. Then we will outline three specific research areas that emphasize a data-centric approach to security namely secure policy based control of flow of data in a distributed system, security in named data networks, and enforcing security policies on encrypted cloud data storage.

Prof. Prof. Wanlei Zhou

University of technology Sydney

Talk Title:

Propagation of Malicious Attacks and Identification of their Sources

Abstract:

In the modern world, the ubiquity of networks has made us vulnerable to various malicious attacks. For instance, computer viruses propagate throughout the Internet and infect millions of computers. Misinformation and fake news spread incredibly fast in online social networks, such as Facebook and Twitter. Researchers and manufacturers evolve new methods to produce detection systems to detect suspicious attacks. However, to build effective detection systems, we need to have a good understanding on the mechanisms of malicious attacks propagation and the ways to identify where these malicious attacks come from. Moreover, we need to understand how can we build effective and efficient prevention systems to stop malicious attacks before they do damage and have a chance to infect our systems. This talk presents various models on propagation of malicious attacks and reviews the state-of-the art in source identification techniques, esp. the application of these techniques in social networks, and discusses the pros and cons of current methods. In order to gain a quantitative understanding of current methods, we provide a series of experiments and comparisons based on various environment settings. Our experiments reveal considerable differences in performance by employing different network topology, various propagation schemes and diverse propagation probabilities. We then present our work in modelling the propagation of rumours and truths in social networks. This talk is mainly based on our following recent publications:

1.Jiaojiao Jiang, Sheng Wen, Shui Yu, Bo Liu, Yang Xiang, Wanlei Zhou: Malicious Attack Propagation and Source Identification. Advances in Information Security 73, Springer 2019, ISBN 978-3-030-02178-8, pp. 1-181.
2. Jiaojiao Jiang, Sheng Wen, Shui Yu, Yang Xiang, Wanlei Zhou: Rumor Source Identification in Social Networks with Time-Varying Topology. IEEE Trans. Dependable Sec. Comput. 15(1): 166-179 (2018).
3. Bo Liu, Wanlei Zhou, Longxiang Gao, Haibo Zhou, Tom H. Luan, Sheng Wen: Malware Propagations in Wireless Ad Hoc Networks. IEEE Trans. Dependable Sec. Comput. 15(6): 1016-1026 (2018).
4. Jiaojiao Jiang, Sheng Wen, Shui Yu, Yang Xiang, Wanlei Zhou: Identifying Propagation Sources in Networks: State-of-the-Art and Comparative Studies. IEEE Communications Surveys and Tutorials 19(1): 465-481 (2017).
5. Chao Chen, Yu Wang, Jun Zhang, Yang Xiang, Wanlei Zhou, Geyong Min: Statistical Features-Based Real-Time Detection of Drifted Twitter Spam. IEEE Trans. Information Forensics and Security 12(4): 914-925 (2017).
6. Mohammad Sayad Haghighi, Sheng Wen, Yang Xiang, Barry G. Quinn, Wanlei Zhou: On the Race of Worms and Patches: Modeling the Spread of Information in Wireless Sensor Networks. IEEE Trans. Information Forensics and Security 11(12): 2854-2865 (2016).
7. Sheng Wen, Mohammad Sayad Haghighi, Chao Chen, Yang Xiang, Wanlei Zhou, Weijia Jia: A Sword with Two Edges: Propagation Studies on Both Positive and Negative Information in Online Social Networks. IEEE Trans. Computers 64(3): 640-653 (2015).
8. Jiaojiao Jiang, Sheng Wen, Shui Yu, Yang Xiang, Wanlei Zhou: K-Center: An Approach on the Multi-Source Identification of Information Diffusion. IEEE Trans. Information Forensics and Security 10(12): 2616-2626 (2015).

Dr Alexey Loginov

GrammaTech Inc

Talk Title:

Machine-Code Analysis: it's all binary but it's not black and white

Safety- and security-critical infrastructure is increasingly dependent on software, most of which is delivered in binary form only. Reverse engineering and analyzing binaries for vulnerabilities pose many challenges, starting with the undecidability of one of the first steps—disassembly.

At GrammaTech, we contributed to early efforts in extending traditional program-analysis techniques to apply to binaries, but we now find it difficult to obtain acceptable precision, recall, and performance while relying solely on traditional program analysis. In recent years, we have begun to explore heuristic techniques, as well as approaches based on machine learning and evolutionary computation.

In this talk, I will illustrate some challenges in machine-code analysis and present examples of how our approach to the problem has been evolving.

Rachael Falk

Cybersecurity CRC

Talk Title:

Research with impact in the cyber ecosystem

Abstract:

Cyber security is a crowded space, with many actors offering their particular viewpoint, services, or products. CRCs are unique entities because they bring together the isolated research ideas and perspectives from different silos or sectors to address a particular problem. The Cyber Security CRC is a newer entrant into the cyber security ecosystem, with 24 Participants from industry, government and research institutions. Our voice is unique because we stand at the intersection of tech and policy, as a hub of interdisciplinary and cross-sectional research. We aim to develop and potentially commercialise cutting-edge research and solve real-world problems that will strengthen Australia's sovereign cyber security capabilities.

Prof. Wenke Lee

Georgia Tech

Talk Title:

User interface and security: Two sides of the story

Abstract:

TBA

Prof. Ryan Ko

University of Queensland

Talk Title:

Returning data control to users

Abstract:

Not many people know how to help themselves in cyber security situations. Worse, many do not even know that they are victims or perpetrators of cyber attacks or privacy breaches. This talk will discuss these issues and the crux of most cyber security problems — the lack of control of our data in digital environments. With control over our own data, we will be able to address several related issues in security attribution, trust, accountability and privacy. I will also demonstrate my recent breakthroughs in data control and human-centric cyber security, covering areas including provenance, practical homomorphic encryption, security visualization and ransomware detection technologies, and briefly demonstrate wider control challenges in vehicles and drones.

Prof. Vitaly Shmatikov

Cornell Tech

Talk Title:

What are machine learning models hiding?

Abstract:

Modern machine learning models exhibit super-human accuracy on tasks from image classification to natural-language processing, but accuracy does not tell the entire story of what these models have learned. Does a model memorize and leak its training data? Does it contain hidden backdoor functionality? In this talk, I will explain why common metrics of model quality may hide potential security and privacy vulnerabilities, and outline recent results and open problems at the junction of machine learning and privacy research.

Dr. Olivier de Vel

Defence Science & Technology (DST) Group

Talk Title:

Machine Learning Security

Abstract:

Machine Learning (ML) techniques and technologies are developing at a rapid pace, and have demonstrated remarkable success across a broad range of application areas. However, despite this ongoing success, there are significant challenges in ensuring the trustworthiness of ML systems. Recent work has shown that the use of ML can introduce additional vulnerabilities into a system, which arise from weaknesses in the algorithms themselves, or from the exploitation of weaknesses in the ML system’s goals. We will outline some of the concepts, techniques, applications and challenges in the area of machine learning security

Prof. Sanjay Jha

University of New South Wales

Talk Title:

Security Challenges in Internet of Things (IoT)

Abstract:

In this talk, I will discuss how the community is converging towards the IoT vision having worked in wireless sensor networking and Machine-2-Machine (M2M) communication. This will follow a general discussion of security challenges in IoT. Finally, I will discuss some results from my ongoing projects on security of bodywork devices and Secure IoT configuration management. Wireless body worn sensing devices are becoming popular for fitness, sports training and personalized healthcare applications. Securing the data generated by these devices is essential if they are to be integrated into the current health infrastructure and employed in medical applications. In this talk, I will discuss a mechanism to secure data provenance and location proof for these devices by exploiting symmetric spatio-temporal characteristics of the wireless link between two communicating parties. Our solution enables both parties to generate closely matching `link' fingerprints, which uniquely associate a data session with a wireless link such that a third party, at a later date, can verify the links the data was communicated on. These fingerprints are very hard for an eavesdropper to forge, lightweight compared to traditional provenance mechanisms, and allow for interesting security properties such as accountability and non-repudiation. I will present our solution with experiments using body worn devices in scenarios approximating actual device deployment. I will also touch upon other research on secure configuration management of IoT devices over wireless networks.

Panel Abstract

Prof. Ali Babar – *University of Adelaide*
Prof. RK Shyamasundar – *IIT Bombay*
Dr. Jackie Craig – *Independent Consultant*
Prof. Vallipuram Muthukkumarasamy – *University of Griffith*
Prof. Anton Van Den Hengel – *Australian Institute for Machine Learning*

Talk Title:

Data-Driven Technologies for Cybersecurity: Opportunities, Challenges, and Solutions

Abstract:

Organisations are increasingly adopting big data technologies for harnessing and analysing security related data available from Open-Source Intelligence (OSINT) and/or Organisational specific security events data to secure the mission-, business-critical software systems and ICT infrastructures against cyber attacks. The role of data-driven technologies in general and the Artificial Intelligence (AI) and Machine Learning (ML) in particular is vital in developing innovative approaches, tools and techniques to predict, prevent, detect, and respond to cyber threats.

This panel aims at distilling the observations and reflections from the panellist and the audience about the data-driven nature of the cybersecurity threats and required solutions; the panel would also debate the challenges of identifying and leveraging the full potential of Data-driven technologies for cybersecurity, and the current and/or envisioned AI/ML based solutions to build resilience against the cybersecurity threats, vulnerabilities, and attacks.

Prof. Ali Babar

University of Adelaide

Talk Title:

Panel Discussion & Brainstorming

Abstract:

M. Ali Babar is a Professor in the School of Computer Science, University of Adelaide. Professor Babar leads the University of Adelaide's participation in the **Cyber Security Cooperative Research Centre (CSCRC)**, one of the largest Cyber Security initiative the Australasian region. Within the CSCRC, he leads the theme on Platforms and Architectures for Cyber Security solutions as service. At the University of Adelaide, Professor Babar has established an interdisciplinary research centre, CREST - Centre for Research on Engineering Software Technologies, where he leads a research and development team of more than **15** members. He has been involved in attracting several millions of dollar worth of research resources over the last ten years. Professor Babar has authored/co-authored more than 2**00 peer-reviewed articles** in the premier Software Technology journals and conferences. With an **H-Index 45,** the level of citations to his publications is among the leading Software Engineering researchers in Aus/NZ. Further details can be found on: http://malibabar.wordpress.com

Dr. Jackie Craig

Independent Consultant

Talk Title:

Panel Discussion & Brainstorming

Abstract:

Jackie Craig graduated with a PhD in physics from St. Andrews University in 1981 and was employed by the UK Ministry of Defence for nine years.

In 1990 she emigrated to Australia and began her 26 year science career with the Australian Defence Science and Technology Group, rising to become Chief of Cyber and Electronic Warfare Division where she led a team of 350 scientists, engineers and technical specialists. Jackie has held several executive leadership positions within Defence and the five-eyes Defence and Intelligence S&T forums, spanning the areas of space, digital systems, autonomous systems, big data, cyber and ISREW.

Jackie has 57 publications in the open literature, 27 classified publications, numerous conference presentations and keynote addresses, and is the lead author on four strategic S&T plans. She was awarded the 2001 Ministers Award in Defence Science for her substantial contribution and influence on imagery ISR systems, and has received several awards for scientific leadership from the five-eyes community in the areas of ISR, space, EW and cyber. She was elected as an ATSE Fellow in 2016.

With time running out and so many Alpine mountains and rock walls to climb, Jackie retired in 2016. In between climbing, she is very active in the ATSE Digital Futures Forum, and whilst an Honorary Fellow of DST Group she contributed to the development of Australian Defence Space S&T Strategy.

Prof. RK Shyamasundar

IIT Bombay

Talk Title:

Panel Discussion & Brainstorming

Abstract:

Prof RK Shyamasundar is a JC Bose National Fellow and Distinguished Visiting Professor at the Department of Computer Science and Engineering, IIT Bombay. He was the Founding Dean of School of Technology and Computer Science at Tata Institute of Fundamental Research. He is a Fellow IEEE, Fellow ACM and Fellow of all National Science and Engineering academies and a Fellow of the World Academy of Sciences (TWAS), Trieste. He has authored over 300 peer reviewed publications, 8 patents, and 8 books. More than 35 Ph.D. students have graduated under his guidance in India and USA. He has been a consultant to ESPRIT projects, Industries, Govt. of India etc. He is on the editorial board of Journal of parallel and distributed computing, Sadhana etc. He has served as Faculty/Visiting Scientist at various places like IBM TJ Watson Research Center, UCSD, UIUC, SUNY at Albany, INRIA, IRISA, University of Cambridge, JAIST at Japan, Max Planck Institute at Saarbrucken, Visiting Distinguished Fellow of Royal Academy of Engineering, UK twice etc. One of his principal areas of research has been cyber security and is leading the Information Security Research and Development Center (ISRDC) funded by MEITY at IIT Bombay. He has/had been on the boards of IIIT Allahabad, IIIT Jabalpur, IDRBT, Bombay Stock Exchange etc.

Prof. Vallipuram Muthukkumarasamy

University of Griffith

Talk Title:

Panel Discussion & Brainstorming

Abstract

Muthu obtained PhD from the University of Cambridge, England (Christ's College Scholar) and BScEng with 1st Class Hons from University of Peradeniya, Sri Lanka. He has pioneered the Network Security research and teaching at Griffith University and has been leading the Security Research Group at the Institute for Integrated and Intelligent Systems.

Muthu is attached to School of Information and Communications Technology, Griffith University, Australia as Associate Professor. His current research areas include blockchain technology, cyber security, wireless sensor networks, trust management, and security protocols. He has been successful in attracting national and international funding for his research activities. He has a passion for innovation and had successful collaboration with Data61, Gold Coast Hospital, IBM Security Research lab etc. Recent funded projects on blockchain technology involved industry, inter-disciplinary and international elements.

He has published over 150 articles in top ranking journals and conferences in his area of expertise. He has supervised over 30 PhD and research Masters students for successful completion. Google Scholar: h-index of 24, and i10-index of 51. He has also been leading a number of academia-industry workshops and symposiums on DLT since 2016. Muthu has been invited as keynote speaker at international conferences, various government departments, leading universities, and professional organisations on blockchain technology and cyber security.

Muthu's excellence in teaching and leadership has been recognised by a number of awards. During his tenure as the Deputy Head L&T, the School of ICT had become the No. 1 in Australia for Overall Student Satisfaction. He is now leading the Master of Cyber Security as Program Director.

Prof. Willy Susilo

University of Wollongong

Talk Title:

Securing Cloud Storage: Challenge and Research Directions

Abstract:

Cloud storage offers low-cost solutions for small and medium-sized enterprises. Nevertheless, cloud storage security remains an elusive research problem. Merely encrypting the data prior to storing them to the cloud is not an ideal solution either. This talk will discuss issues and research challenge in securing cloud storage, and provide some future research directions.

Dr. Jin-Song Dong

Griffith University

Talk Title: Formal Analysis in security

Abstract:

This talk introduces the process analysis toolkit (PAT) which integrates the expressiveness of state, event, time, and probability-based languages with the power of model checking. PAT has attracted thousands of registered users from hundreds of organizations and been successfully applied in verifying security. In the work TrustFound, a formal framework is built based on PAT for model checking of trusted computing platforms (TPM). The formal framework has been used to analyse two TPMs, leading to the identification of a total of six implicit assumptions and two severe previously-unknown logic flaws. In the work AppGenome, the call-back relations in Android applications are automatically constructed into PAT models. Using PAT, two logic flaws in Android application have been automatically identified. In addition, a security protocol module (including a specification framework and a set of verification algorithms) is built in the PAT framework, particularly for timed security protocols and stateful security protocols. Security of these two types of protocols can be automatically proved or disproved, e.g., a previously unknown timing attack is found in Kerberos V protocol using the security protocol module. In this talk, we will also present some ongoing research projects, i.e., “Silas: trusted machine learning” in collaboration with Dependable Intelligence (www.depintel.com).