isi UPDATE

ISSUE 3 | APRIL 2009

NEWSLETTER OF THE INFORMATION SECURITY INSTITUTE

Mr Eric Hall, General Manager and Director of Business Development

from the **directors**

Biannual Directors Report – April 2009

It is timely to reflect on the establishment of the ISI in 2005 and the key drivers which led to this. What was the university thinking which led to a decision to invest in this activity, when the breadth of different research activities is as diverse as they are at QUT?

Perhaps this is somewhat of an oversimplification because I wasn't here at the time, but it seems to have boiled down to two key criteria:

1. To grow a pre-existing research strength in information assurance into a nation leading concentration in the university sector.
2. To target and nurture a holistic, systematic approach to research program design in information assurance which would require multidisciplinary participation to deliver solutions which have practical utility in the real world.

The prospect of a Research Quality Framework under the Howard government and now the Excellence in Research for Australia (ERA) under the current federal leadership requires universities to quantitatively demonstrate through predefined indicators and a peer review process that their research is world class in terms of its quality and impact.

Historically, the middle ranking Australian universities have tended toward a model which provides a "one size fits all" or an egalitarian program mix to capture the broadest possible cross-section of the local demographic as was possible. This was driven by the Commonwealth funding model. The ERA regime is about to change all that and no institution will be able to continue to be all things to all people.

ISI had and continues to have a national reputation in information assurance. We are growing rapidly and expect that our profile as the largest group of its kind in the Australian university landscape to consolidate over the next few years.

ISI has some way to go in the multidisciplinary space. But there are some promising signs that augur a new cultural predisposition to consider collaboration outside the researcher's traditional silos and an acceptance that this will deliver more meaningful outcomes for end-users.

Some examples:

Law: There is a fundamental intersection between law and security issues. Our clients include the Attorney Generals Department and the Australian Federal Police. Project work includes the development of policy and legal frameworks for transnational prosecution of originators of cyber attacks on our national information infrastructure,

isi diary

CONFERENCE:

The ISI will be hosting/co-hosting the following events this year:

- In April 2009, the ISI will be co-hosting the India Australia Conference on Information Technology Security (IACITS 09) to be held 1–2 April, 2009 in New Delhi, India.
- An Indo/Australian Collaborative DDoS project workshop to be held 3–4 April 2009 in New Delhi, India
- The 14th Australasian Conference on Information Security and Privacy (ACISP 2009) to be held 1–3 July at Queensland University of Technology, Brisbane

in this issue

QUT isi Information Security Institute

visitors to the isi

VISITING RESEARCHERS:

- Professor Changji Wang, ***Department of Computer Science***, Sun Yat-sen University, PR China, 1 August, 2008 until 31 July, 2009.
- Professor Andreas Steffen, ***Head of the Institute for Internet Technologies and Applications and Professor in Security and Communications***, University of Applied Sciences Rapperswil, Switzerland, 14 September, 2008 until 30 January, 2009.
- Professor Ji Hong Kim, ***Department of Information Security***, Semyung University, Korea, 24 September, 2008 until August, 2009.
- Dr Kiam Keliher, Associate Professor, ***Department of Mathematics & Computer Science***, Mount Allison University, Canada, 1 November, 2008 until 30 December, 2008
- Professor Jung-Tae Kim, ***Network and Information Security Laboratory***, Mokwon University, South Korea, 1 January, 2009 until 29 February, 2010.

international conferences

ISI KEYNOTE TALKS AT INTERNATIONAL CONFERENCES

- Dawson, E., (Keynote), Clapperton, D., Corones, S., Foo, E., Lane, W., McCullagh, A., Reid, J., Salim, F.: ***Leveraging ICT for Information Sharing: Challenges and Opportunities*** presented at CIP and ISAC Workshop, 21 October 2008, Taipei, Taiwan.

ISI BEST STUDENT PAPER AWARD AT INTERNATIONAL CONFERENCES

- Huseyin Hisil (FST)* was awarded best student paper:
- Hisil, H., Wong, K., Carter, G and Dawson, E., Faster Group Operations on Elliptic Curves: Australasian Information Security Conference (AISC 2009), 20-23 January 2009, Wellington, New Zealand.

the development of novel e-contracting tools and information sharing of government held information to the public and special interest groups.

Business: Using enterprise resource planning software and specially developed tools to automatically detect fraudulent transactions or money laundering has become a priority for government agencies and financial institutions. New legislation has mandated onerous reporting requirements which, without automation, would prove costly and time consuming.

Built Environment and Engineering: ISI researchers have been involved in surveillance projects for airport security and the development of new biometric technologies for financial and law enforcement applications.

Science and Technology: On a worldwide basis national critical infrastructure such as water and electricity is increasingly exposed to cyber attack. To secure such infrastructure, researchers within the ISI have developed new tools and techniques to improve the resilience of communities facing disruption because of natural or man-made events.

Professor Colin Boyd, Research Director

Professor Colin Boyd

Ten years ago information security was widely regarded as a purely technical challenge. Many of us in the field at that time believed that within a few years the security challenge of the Internet would be solved. The cryptographic protocols needed to be tweaked, the public key infrastructure put into place, the firewalls tightened up, and then the era of cheap and secure electronic business would be with us. As we all know now, the reality has been quite different. Not only are the original problems still unsolved, but a whole new list of malicious tools has entered the vocabulary, including phishing, spamming and rootkits.

In the last few years information security researchers and practitioners have begun to appreciate that a purely technical approach is doomed to failure. Therefore they have been looking to the social sciences to help understand the problem. Economics was perhaps the first non-technical discipline to be drafted in to help the information security cause. By understanding the incentives behind attacks such as denial of service or spamming, researchers were able to suggest new defensive schemes. Another discipline that has a lot to offer to information security is psychology. We need to understand how people think, both attackers and legitimate users, in order to design security measures that not only defend against attackers but which are easy and natural enough for everybody to use with confidence.

The ISI is in a unique position to contribute to the new way of looking at information security. Our breadth of coverage across our different Faculties gives a comprehensive perspective. In the few years since the Institute was founded as an interdisciplinary entity, a wide variety of projects has brought together different strands of understanding. Many of our projects combine research input across two or more of the ISI Faculties. We aim to maintain and increase our interdisciplinary focus in the coming years, not only by including differing perspectives but also by integrating the separate strands of knowledge to obtain a deeper understanding of the information security problem.

visiting academic

Professor Andreas Steffen

My name is Andreas Steffen. I'm a professor for Security in Communications with the University of Applied Sciences Rapperswil located on Lake Zurich in Switzerland. Thanks to an invitation by Ed Dawson I spent my sabbatical leave with the ISI from September 2008 to January 2009. Upon my arrival in Brisbane I was very lucky to find a nice two-bedroom apartment in picturesque New Farm, just in walking distance (4 km) from the CBD. Thus I was able to accomodate my family when they visited me in Australia over the Christmas holidays.

During my stay I profited from the ISI's expertise in the area of cryptographic e-voting systems while preparing a seminar on this topic for my university's master curriculum. Together with Jason Smith I worked on novel ways to secure Mobile IPv6 binding updates. I also hope that I succeeded in sharing some of my knowledge of the IPsec protocol acquired through my group's ongoing development of the Linux strongSwan VPN software (www.strongswan.org).

Back in snowy Switzerland I badly miss the joyful rides on the CityCat river ferry on a hot summer day and I'm eagerly looking forward to revisiting Brisbane sometime in the future.

money laundering from an economic and policy perspective

Professor
Benno Torgler

The term 'Money Laundering' originates from the US describing the Mafia's attempt to 'launder' illegal money via cash-intensive washing salons in the 30s, which where controlled by criminal organisations. A modern day definition sees money laundering as the process of transferring money between the official and the unofficial economy. Money laundering has received attention in the political arena due to an increasing focus on the finances of drug trafficking and terrorism. The IMF estimates that 2-5% of the world gross domestic product (GDP) stems from illicit (criminal) sources and thus has to be laundered. Money laundering can be seen as a threat to the integrity of the financial system and can increase fiscal instability. It also induces distortion of investment patterns since money launderers do not seek the most effective investment. Estimating the true amounts of money being laundered is difficult due to its hidden nature. To fight against money laundering is also extremely difficult, as we have no efficient and powerful international organizations, which can effectively fight against organized crime and money laundering. It is therefore essential to understand the process of money laundering and identify its major feeders and receivers. To be able to derive policy implications, suggest counter measures and to control for potential problems of efficiency we need to isolate potential harmful incentives and behaviours.

Thus, in a CRC ISI Anti-Money Laundering Project we shed some light on the causes and consequences money laundering and to provide better bases to be able to take more efficient measures against money laundering. Our empirical results indicate that governance and institutional quality is extremely important to reduce money laundering activities. In particular, a solid law and order enforcement reduces the incentives to conduct money laundering activities. Thus, a well-functioned state appears to be an essential precondition in preventing money laundering. On the other hand, a failure of a country's legal system enhances the use of money laundering activities. Currently, we are also exploring the link between money laundering, globalization and terrorism. Globalisation has changed the way the world functions and new opportunities for transnational organised crime have emerged. Money laundering techniques have become increasingly sophisticated and have been used by terrorists to finance their activities around the world. Thus, it is important to provide good insights how to optimize anti-money laundering strategies in a globalized environment.

Project	Research Team	Funding Sources	Contact
Money Laundering from an Economic and Policy Perspective	Professor Benno Torgler, Professor George Mohay Dr Nic Chantler Professor Colin Boyd Dr Yuke Sakurai Dr Joanne Fuller	Smart Services CRC	Professor Benno Torgler +617 3138 2517 Benno.torgler@qut.edu.au

spoken term detection: the search for information in audio collections

Dr Robbie Vogt

Our speech is being collected and stored in unprecedented volumes. The utilisation of the vast amounts of information contained in this speech urgently requires the development of technologies that make these collections accessible and useful. Providing intelligent access to large collections of spoken audio is one of speech technology's most important challenges. There is demand from a vast range of industries including speech analytics, surveillance, consumer search and media monitoring.

In pursuit of this goal, there has been a recent surge in interest in the field of spoken term detection (STD), which involves the detection of all occurrences of a specified word or phrase of interest, rapidly and accurately in large heterogeneous audio archives. STD systems first pre-process the audio to create an index that subsequently allows for very rapid searching. This index is usually based on an automatic word-level transcription produced by a large-vocabulary speech recogniser. A word-level index can provide quite accurate term detection, however, indexing is slow and new and rare terms cannot be easily detected if they are not in the recogniser's limited vocabulary. Importantly, these rare and out-of-vocabulary terms are often precisely the terms that users are most likely to be interested in as they are often the most informative (for example, names of people, places, companies and products).

A phonetic index, on the other hand, represents sounds in terms of phonemes, the basic building blocks of speech. For example, the word 'security' consists of 9 phones: 's', 'ih', 'k', 'y', 'uh', etc. This kind of representation allows for search terms of any kind, has potential for languages with limited training data and avoids the costly training, development and runtime requirements associated with large vocabulary speech recognition. This is the approach researchers at QUT are taking.

Applying well-established speech recognition techniques to the task of spoken term detection raises a number of challenging issues. For example, the speed of indexing and searching is critical for STD, as is the accuracy and precision of the results. Ultimately, a balance is necessary to produce a system which best meets the needs of the user. Current research at QUT is suggesting that, from this perspective, real solutions can be developed to allow us to tap into one of the last remaining vast information resources: our speech.

graduate destination

Dr Kim Kwang (Raymond) Choo

- Dr Kim Kwang (Raymond) Choo
  Awarded PhD in 2006 from ISI
  Thesis Title: ***Key Establishment: Proofs and Refutations***
  Supervisors: Professor Colin Boyd (Principal), Dr Yvonne Cliff and Dr Greg Maitland (Associates)

Recipient of the 2009 Fulbright DFAT Professional Scholarship

'Cybercrime is one of the top issues in crime today. Opportunities for organised crime groups to engage in cybercrime have increased with globalisation and improvements in ICT.'

Dr Kim Kwang (Raymond) Choo, a Research Analyst with the Australian Institute of Criminology (AIC), has received the 2009 Fulbright Professional Australia-U.S. Alliance Studies Scholarship, sponsored by the Department of Foreign Affairs and Trade. He is also a Visiting Fellow at The Australian National University's ARC Centre of Excellence in Policing and Security, and a member of the International Consultant Group (Research) in the joint United Nations Office on Drugs and Crime and Korean Institute of Criminology 'Virtual Forum against Cybercrime' Program.

Through his Fulbright Scholarship Raymond will travel to Rutgers University's School of Criminal Justice and the Palo Alto Research Center for three months to undertake a project looking at the future cybercrime threat environment.

'Attempting to anticipate the likely actions of organised crime groups has long been a key role of law enforcement and intelligence agencies. Opportunities for organised crime groups to engage in transnational activities have expanded with globalisation and improvements in ICT. My study will look at the cybercrime risks likely to arise in the short to medium term and to consider how these threats may develop.' Raymond said.

'My research aims to contribute to future planning and responses to neutralise these crime opportunities before they arise. Particular focus will be placed on the impact these future developments will have for law enforcement and policy makers. This will include the need for additional resources, law reform and the development of cooperative arrangements between public and private sector organisations in Australian and overseas, and the creation and dissemination of public information and educational resources to minimise the risk of harm to the community.'

Raymond is a British Computer Society's Chartered IT Professional. Since starting at the AIC in July 2006, he has authored and co-authored a number of publications in the areas of cybercrime and anti-money laundering, including the 'Future directions in technology-enabled crime : 2007-09' research report, 'Zombies and botnets' article and 'Money laundering risks of prepaid stored value cards' article. Recent awards include a 2008 Australia Day Achievement Medallion, Wilkes Award for the best paper published in the 2007 volume of Oxford University Press's The Computer Journal and the 2007 Queensland University of Technology Faculty of IT Executive Dean's outstanding Ph.D. thesis commendation.

The prestigious Fulbright program is the largest educational scholarship of its kind, created by U.S. Senator J. William Fulbright and the U.S. Government in 1946. Aimed at promoting mutual understanding through educational exchange, it operates between the U.S. and 150 countries. In Australia, the scholarships are funded by the Australian and U.S. Governments and corporate partners and administered by the Australian-American Fulbright Commission in Canberra.

Raymond is one of 23 talented Australians to be recognised as a Fulbright Scholar in 2009. Applications for Fulbright Scholarships in 2010 open on 1 June, visit www.fulbright.com.au

awards and achievements

- **Dr Robbie Vogt [BEE] and Dr Juanma Gonzalez-Nieto [FST]** recipients of the Vice-Chancellor's Excellence Awards
- **Associate Professor Andrew Clark** appointed as a Research Advisory Committee member for the Defence Systems Innovation Centre at the University of South Australia.

promotions and new appointments

PROMOTIONS:

Faculty of Science and Technology

- Dr Andrew Clark
  – Promoted to Associate Professor
- Dr Leonie Simpson
  – Promoted to Senior Lecturer
- Dr Jason Reid
  – Promoted to Senior Research Fellow
- Dr Jason Smith
  – Promoted to Senior Research Fellow
- Dr Juanma Gonzalez-Nieto
  – Promoted to Senior Research Fellow

Faculty of Built Environment and Engineering

- Dr Wageeh Boles
  – Promoted to Professor

Faculty of Business

- Associate Professor Benno Torgler
  – Promoted to Professor

NEW APPOINTMENTS:

- Dr Alan Tickle
  – Adjunct Professor (FST)
- Dr James Birkett
  – Postdoctoral Research Fellow (FST)
- Dr Douglas Stebila
  – Postdoctoral Research Fellow (FST)
- Dr Khandoker Islam
  – Postdoctoral Research Fellow (FST)
- Dr Simon Denman
  – Postdoctoral Research Fellow (BEE)
- Dr Brendan Baker
  – Postdoctoral Research Fellow (BEE)
- Dr George Mamic
  – Research Fellow (BEE)
- Ms Eugene Gerogiades
  – Senior Research Assistant (LAW)
- Dr Desmond Schmidt
  – Programmer (ISI)
- Mr Suriadi Suriadi
  – Research Assistant (ISI)
- Mr Edward Chang
  – Computer Systems Support Officer (ISI)

detecting fraud in ERP systems

Professor George Mohay

Enterprise resource planning (ERP) systems provide an enterprise-wide information system designed to coordinate all the resources, information, and activities of an enterprise needed to complete business processes such as order fulfillment, billing, HR etc. This ARC Linkage project addresses the development of an integrated fraud detection framework for use with SAP's ERP software and focuses on transaction mining to detect anomalous transaction patterns as well as transaction patterns known to be indicative of fraud. The concepts developed in the project will be applicable to ERP systems in general. The project, led by Adjunct Professor George Mohay and Associate Professor Andrew Clark, commenced in 2007 and involves an inter-disciplinary team of investigators also including Professor Benno Torgler from QUT and Dr Sarath Indrakanti from SAP. Also working on the project are QUT's Malcolm Corney, PhD student Roheena Khan and Dr Asadul Islam who is about to join the project. The project is a collaboration with SAP Research and is developing research prototypes which will monitor processes like invoicing and salary payments, to try to identify unusual instances and patterns that may indicate fraudulent behaviour by people inside an organisation. SAP Research is the technology research department of SAP.

Detection and analysis of anomalous transaction patterns and transaction patterns known to be indicative of fraud enables the detection of new as yet unknown financial fraud scenarios as well as fraud arising from inadequate role separation, a common occurrence in SME's. The project also addresses visualization of fraud situations and security policy inference and assessment. A number of SAP customers have expressed an interest in pilot studies which are expected to get underway in the next few months.

Project	Research Team Leaders	Funding Sources	Contact
Integrated Financial Fraud Detection in Enterprise Applications	Professor George Mohay Professor Benno Torgler Associate Professor Andrew Clark Dr Sarath Indrakanti (SAP)	Australian Research Council Linkage (06-09)	Professor George Mohay +617 3138 9569 g.mohay@qut.edu.au

advances in identity based cryptography

Dr Juanma González-Nieto

Cryptographic pairings represent a very promising frontier technology from which new products and services can be expected to emerge. The ability to replace the failing current technologies for PKI with identity based infrastructure will allow a wide range of security services to be robustly provided. Innovative applications are extensively promoted in the literature such as in healthcare and new products in network security are already being offered. These are exciting times for cryptographic research and the ISI is playing a leading role.

The discovery of public key cryptography more than 25 years ago promised to solve all the problems of key distribution by allowing open distribution of public keys. In combination with the development of ubiquitous networking and internetworking, the possibility of secure communications on demand between any two corners of the world seemed assured. During the 1980s and 1990s elaborate schemes for certification of public keys, including many standards, seemed to be moving towards a worldwide public key infrastructure. However, in recent years it has been widely recognised that this infrastructure has more problems than was at first realised. Business confidence in public key infrastructure has faltered. Apart from the many commercial, legal and political issues, a recurring dilemma has been how best to manage the processing, storage and revocation of public key certificates.

The idea of identity based cryptography is to replace both public keys and certificates with the identity of an entity. Simply by knowing the correct identity string, anyone can encrypt a message intended for the entity described by that string. This means that there is no longer need for an elaborate directory structure and there are savings in storage (certificates do not need to be stored), computation (certificates do not need to be verified) and communications (certificates are not required to be included in protocol messages). Identity based cryptography was first proposed by Adi Shamir (the 'S' behind RSA) in the early 1980s. However until the recent discovery of cryptographic pairings, it was largely an open question how to implement identity based cryptography.

Despite its many clear advantages there remain some problems with identity-based cryptography. Further research is still needed to improve the efficiency and the security assurance of identity based systems. With this goal in mind a group of ISI researchers lead by Prof Colin Boyd and Dr Gonzalez have been investigating identity based cryptography. Highlights to date of this research include the following:

- Efficient pairing algorithms. Computation of pairings, the underlying cryptographic primitive in identity based systems, is an important bottleneck in many applications. ISI researchers have developed the most efficient pairing implementations known so far, thus pushing further the practicality of identity based cryptography.
- Protocols and security models for identity based authentication and key establishment. Key establishment is a fundamental part of most practical uses of cryptography and protocols must be free of all security flaws in order to provide their role. ISI researchers have devised security models in which to analyse the security of identity-based protocols, as well as new protocol designs that they have rigourously proven secure.

Project	Research Team Leaders	Funding Sources	Contact
Cryptographic Protocols Proofs and Designs	Professor Colin Boyd Dr Juanma González-Nieto	Australian Research Council Discovery Grant	Dr Juanma Gonzalez-Nieto +617 3138 9552 j.gonzaleznieto@qut.edu.au

technical and legal models in virtual information-sharing networks for critical infrastructure protection – the FOI implications – bill lane

Professor Bill Lane

Protection of 'critical infrastructure' (CI) – such as that relating to transport and telecommunications or the supply of essential services (such as electricity, gas, water), has become a major concern for governments worldwide. Yet it is generally estimated that approximately 90 per cent of CI is privately owned or operated – in other words, CI protection is not the exclusive domain of government.

This means that information sharing between government and the private sector has become a vitally important component of effective CI risk management. Yet establishing effective info-sharing arrangements between the public and private sector must take account of existing legal regimes, particularly, those concerning access to and public disclosure of government-held information.

A project to examine the freedom of information (FOI) implications of CI info-sharing is part of an overall ARC Discovery Grant, Technical and Legal Models in Virtual Information-Sharing Networks (VISN) for Critical Infrastructure Protection (CIP). Consistent with the purpose of the grant as a whole, the aim of this project is to examine the extent to which the current Commonwealth FOI regime might act as an impediment to private sector operators of critical infrastructure participating in government-operated information sharing arrangements like the TISN.

By way of explanation, the underlying basis of FOI legislation (enacted in all Australian jurisdictions) is the recognition that citizens in democratic systems of government have a right to be adequately informed about the processes of government, particularly in relation to the development of policy and the manner in which policy is translated into executive action. The defining feature of FOI is a legally recognised right of access for every person to government-held documents.

The establishment of info-sharing arrangements for CI protection involves a 'trade off' between private and public interests. To that extent FOI does at least recognise that the public interest in open and accountable government must be balanced against the public interest in avoiding prejudice to certain government interests or the business or personal interests of others. However, in the context of info-sharing arrangements for CI protection, the potential remains for FOI to act as a significant impediment to effective participation by private sector operators of CI unless this balance is adequately realised.

Project	Research Team	Funding Sources	Contact
Technical and Legal Models for Virtual Info-Sharing Networks (VISN) for CIP	Professor Stephen Corones Professor Ed Dawson Dr Ernest Foo Professor Bill Lane Dr Adrian McCullagh	Australian Research Council Discovery (07-09)	Professor Bill Lane +617 3138 2004 wb.lane@qut.edu.au

completions

Masters by Research

- Robert Dawson (FST), ***Secure Communications for Critical Infrastructure Control Systems***. Supervisors: Professor Colin Boyd (Principal), Dr Juan Gonzalez-Nieto (Associate)
- Sinclair Hansen (FST), ***An Intrusion Detection System for Supervisory Control and Data Acquisition Systems***. Supervisors: Associate Professor Andrew Clark (Principal), Dr Juan Gonzalez-Nieto (Associate)

PhD

- Stig Andersson (FST), ***Detecting and Characterising Malicious Executable Payloads***. Supervisors: Associate Professor Andrew Clark (Principal), Professor George Mohay (Associate), Dr Jacob Zimmermann (Associate)
- Simon Denman (BEE), ***Improved Detection and Tracking of Objects in Surveillance Video***. Supervisors: Associate Professor Vinod Chandran (Principal), Dr Clinton Fookes (Associate), Professor Sridha Sridharan (Associate)
- Rong Du (FST), ***Secure Electronic Tendering***. Dr Ernest Foo (Principal), Supervisors: Professor Colin Boyd (Associate) and Professor Sharon Christensen (Associates)
- Rouhshi Low (LAW), ***The use of technology to automate the registration process within the Torrens System and its Impact on Fraud: An Analysis:*** Supervisors: Professor Sharon Christensen (Principal), Professor Bill Duncan (Associate) , Dr Ernest Foo (Associate)
- Ake Tritilanunt (FST), ***Protocol Engineering for Protection Against Denial-of-Service Attacks***. Supervisors: Professor Colin Boyd (Principal), Dr Ernest Foo (Associate).

Please contact us
CRICOS No. 00213J

Information Security Institute
Queensland University of Technology
GPO Box 2434 (126 Margaret Street)
Brisbane Qld 4001 Australia

Phone +61 3 3138 9572
Fax +61 7 3221 2384
Email info@isi.qut.edu.au
Web www.isi.qut.edu.au