

isi UPDATE

ISSUE 2 | JULY 2008



NEWSLETTER OF THE INFORMATION SECURITY INSTITUTE



Mr Eric Hall,
General Manager
and Director
of Business
Development

from the directors

Biannual Directors Report – July 2008

The national security landscape and especially the segment related to e-security continues to evolve toward the development of organisations and national infrastructure which are inherently more resilient than was evident in the previous decade. In tandem, ISI continues to regard the federal government as the most fruitful source of research funding because of its need for informed decision making in a rapidly changing environment.

The Australian Government released its significantly revised *E-Security National Agenda* last year. It introduces new coordination mechanics to address e-security threats and a number of new initiatives. The agenda has been allocated a budget of \$73.6 million over four years.

Three key priorities have been identified with policy development and implementation responsibility being shared between multiple agencies, including the Attorney-General's Department, the Defence Department and the Department of Broadband, Communications and Digital Economy, and agencies such as the Australian Federal Police, Australian Government Information Management Office (AGIMO) and Australian Communications and Media Authority (ACMA). The priorities identified are:

- Priority 1: Reducing the e-security risk to Australia's national critical infrastructure
- Priority 2: Reducing the e-security risk to Australian Government information and communication systems
- Priority 3: Enhancing the protection of home users and SMEs from electronic attacks and fraud.

During the past few years ISI has slowly but surely developed a significant profile in Canberra with a variety of contracts with many of the different stakeholders. The consolidation of national security matters into a new Office of National Security within the Department of Prime Minister and Cabinet and a new Home Affairs portfolio continue the trend of consolidation and integration of the responsibilities for the protection of Australian citizens domestically.

All this is beneficial to ISI because we are moving from a highly fragmented market, with multiple stakeholders with relatively small budgets to deploy in finding solutions, toward a better coordinated national apparatus with significant resources to invest in the future.

new funded projects

- **Department of Prime Minister and Cabinet – National Security Science and Technology Unit (NSSTU), Research Support for Counter-Terrorism**
 1. **Dr Andrew Clark [FIT], Dr Jason Smith [FIT]** *Vulnerability Assessment for Web Services*, Total cash funding is \$222 500 from NSST and DSD over two years.
- **ARC Discovery**
 2. **Professor Bill Lane [LAW], Dr Adrian McCullagh [ISI]**, *A New Legal Framework for Identifying and Reporting Australian Data Breaches*, Total funding approved: \$358 445 for three years.
 3. **Professor Sridha Sridharan [BEE]**, *Robust Speaker Recognition with Reduced Utterance Duration and Intersession Variability*, Total funding approved: \$196 400 for three years.
- **Australian Indian Strategic Research Fund**

Collaboration between QUT, Indian Institute of Technology, Madras and Society for Electronic Transaction and Security, Madras, *Protecting Critical Infrastructure from Denial of Service Attacks: Tools, Technology and Policy* \$5.25M over three years

in this issue

- 3 **Resilience and Emergency Planning in Mega-cities – Issues and options**
Dr Paul Barnes
Advances in Face Biometrics
Professor Bill Caelli
- 4 **iPhone release may challenge Aus competition laws**
Dale Clapperton
- 5 **Fighting invisible intruders on wireless networks**
Dr Jason Smith
- 6 **Aggregating Government Information**
Dr Adrian McCullagh

isi diary

CONFERENCES

The ISI hosted the following conferences and workshops this year:

- The 4th Indo-Australian IT Security Conference (IACITS 2008) held in March at Pondicherry University, India.

VISITORS TO ISI

- Dr Matt Henricksen, Senior Research Fellow, Cryptology and Security Laboratory, Institute for Infocomm Research (I2R), Singapore.
- Professor Mike Burmester, Department of Computer Science, Florida State University, USA.
- Dr DongGook Park, Assistant Professor, School of Information and Communication Engineering, SunChon National University, Korea.

ISI KEYNOTE TALKS AT INTERNATIONAL CONFERENCES

- Barnes, P.H., (Keynote Presentation), ***Anticipating Vulnerabilities in Infrastructure(s)*** at the Australian Academy of Science sponsored *High Flyers Think Tank – Extreme Natural Hazards*, University of Melbourne, 30 October 2007.
- Barnes, P.H., (Invited Presentation), ***Uncertainties in Security and Risk Assessment: Issues for Infrastructure Design***, Transport Security Forum 08, Singapore, 14–15 May, 2008.

In April this year, ISI and two partner research institutions in India were successful in winning \$5.25 million for a three year project into *Protecting Infrastructure from Denial of Service Attacks: Tools, Technology and Policy*. The outcomes of this will be of direct interest to many of the government agencies mentioned above and we will endeavour to involve them as much as we can, so that our relationships continue to flourish and opportunities for follow-on work are captured here if possible. The kick-off meeting for this project is scheduled here at QUT for 7–8 August.

From a business development perspective, the ISI is already planning its' next large strategic bid for funding. This will certainly link with the priorities listed above, involve significant government agencies, and involve world-class researchers from a partner institution from the USA/UK. Watch this space for further information as this unfolds!



Professor Ed Dawson, Research Director

Professor Ed Dawson

After fifteen years from 1993–2007 of being Director and Research Director of the Information Security Research Centre and Information Security Institute I have retired from these positions. During this time our group at QUT has grown into one of the leading international research centres in information security. The formation of ISI in 2004 as a multidisciplinary research centre of expertise in information security has been a key development to the expansion of our research at QUT enabling us to investigate information security requirements from both a technical and legal/policy perspective. Our research student base has

grown to more than 80 students which is equal in size to any information security group on a worldwide basis. This includes numerous international students. We have expanded our project base both within Australia and overseas. During the past couple of years we have been involved in collaborative projects with both Australian and Queensland government departments as well as private industry partners such as SAP, IBM, and Motorola. International projects have been undertaken with partners in Japan, Spain, Korea, USA, UK, France, Austria, Singapore and India. It has been my great pleasure to be closely involved in these developments.

In my new role as Professor Emeritus and Adjunct Professor in the ISI, I will be closely involved with future developments of our group. I will act as a senior advisor to the Business Director and Research Director of the ISI. I will be involved in leading and managing major projects. For a three year period commencing in July 2008 I will be leading the new project titled: *Protecting Critical Infrastructure from Denial of Service Attacks: Tools, Technology and Policy*. This is a collaborative project with the ISI and research groups in India, namely Indian Institute of Technology Madras and Society for Electronic Transactions and Security Madras. This project is funded under Australian-Indian Strategic Research Fund (AISRF). The aim of this project is to investigate technical and policy issues of distributed denial of service attacks which have become one of the major threats to individuals and corporate networks on a worldwide basis. The goal of this project is to develop techniques to detect and prevent such attacks.



resilience and emergency planning in mega-cities – issues and options



Dr Paul Barnes

New research is underway examining how Mega-cities coordinate and integrate crisis response planning. The work being carried out by ISI researcher Dr Paul Barnes will culminate in an edited book to be published by Edward Elgar (UK) in the first half of 2009. Central to work is a comparative assessment of the crisis planning activities and systems used in four mega-cities; New York, Paris,

London and Tokyo. Along with co-editor Professor Akira Nakamura from Tokyo's prestigious Meiji University, Dr Barnes will coordinate a group of specialist authors will examining each city.

The book will examine city-specific questions not clearly dealt with from a risk governance perspective – namely:

- 1) How should Mega-cities be governed to enable resilience?

- 2) How infrastructure, and the ICT integration evident within them, might be better re-designed/ designed to enhance resilience in face of disturbances and critical incidents
- 3) How might the public and private sector collaborate in implementing crisis and business continuity planning?
- 4) What differences in crisis planning capacities and capabilities exist between the selected Mega-cities?

The book will also include thematic issues such as:

- Failures and Disruptions in globally networked systems
- Governance and Public Administration in Mega-cities
- Security, Business Continuity and Crisis Planning.

A further issue is whether opportunities exist for anticipating the onset of such crises in Mega-cities by identifying 'precursor crisis signals' from background noise in socio-technical systems.

advances in face biometrics



Dr Clinton Fookes

As the world is placed under increasing pressure to secure its population and critical infrastructure, so too is the need to research and develop smart security solutions. Biometrics is one such field that has the potential to identify or authenticate an individual with much stronger certainty than traditional security solutions.

ISI researcher Dr Clinton Fookes said, 'Despite the enormous promise and potential capability of biometric technology, the uptake within industry and the community has not been as prolific as expected'. In addition to the challenges associated with practical implementation of biometrics such as interface and business process development, there are several problems associated with the actual biometric technology. This includes noise in the sensed data, intra-class variation, distinctiveness, non-universality and spoof attacks. The latter is particularly damaging as evidence of the ease of recreating a person's biometric, (especially a fingerprint), is becoming better known.

Further research is still required to advance the accuracy and robustness of biometric technology. The Image and Video Research Laboratory of ISI directed by Professor Sridha Sridharan is one such group leading the way, particularly within the area of facial biometrics. 'The uniqueness of face recognition technology that distinguishes it from the other cohort of biometrics is that is it completely unobtrusive and it is capable of operating in noisy crowded environments where other biometrics may fail'. 'It is also significantly harder to



spoof as the non-rigid nature of the face, expressions, and other features such as gaze can be built into the technology for 'liveness' detection'.

Dr Fookes said one of the group's aims is to further develop 3D face biometrics and multi-modal systems, and to research robust reconstruction methods that acquire accurate 3D models of a subjects face. Fortunately, face recognition in most scenarios (especially in surveillance) has the advantage of the availability of multiple images of a claimant's face in space and time. This enables the use of spatiotemporal information of the face in motion captured from video as well as images in space captured from different view points within a multi-camera network to obtain 3D information.

'The incorporation of this extra depth information eliminates many of the inherent problems associated with traditional 2D face recognition systems such as pose and illumination challenges. The temporal continuity and subject constancy contained in video can also help to provide a more robust representation of the face', Dr Fookes said.

Project	Research Team	Funding Sources	Contact
Multi-modal Face Biometrics	Dr Clinton Fookes Dr George Mamic Professor Sridha Sridharan Associate Professor Vinod Chandran	Australian Research Council, National Security Science and Technology Unit, US Office of Naval Research	Dr Clinton Fookes +617 3138 2458 c.fookes@qut.edu.au

iPhone release may challenge Aus competition laws



Dale Clapperton

The release of Apple's iPhone in Australia this year could be illegal under this country's competition laws, say Queensland University of Technology law researchers.

QUT law researcher Dale Clapperton said Apple had released the iPhone (a mobile phone, iPod and Internet-connected computer in one) in June 2007 with an exclusive agreement with giant US telco AT&T to provide mobile coverage.

'US iPhone buyers are required to sign a two-year mobile contract with AT&T before the iPhone will operate,' Mr Clapperton said.

'Despite there being at least two class actions in the US against Apple alleging violations of antitrust and consumer protection laws, Apple has released the iPhone in Germany, France and the UK with exclusive agreements with mobile carriers.'

However, Mr Clapperton said that if Apple used this strategy in Australia it could come up against our third-line forcing laws which would make the strategy of forcing consumers to do business with another organisation illegal.

'Australia's competition laws may be uniquely suited to preventing this type of anti-competitive technological tying because they prohibit third-line forcing per se.'

This position is explored in an article, published in the *QUT Law and Justice Journal* this month by Mr Clapperton and QUT's Professor Stephen Coronos, analysing the implications of the technological locking of the Apple iPhone under Australia's competition laws.

'US financial analysts have calculated that AT&T is paying Apple a US\$18-a-month 'commission' per iPhone customer which, of course, is ultimately paid by the customer,' Mr Clapperton said.

'The digital locking of the iPhone forces consumers to use the mobile carrier nominated by Apple so that over the two-year contract term, the consumer would probably pay more in secret commissions to Apple than they paid for the iPhone in the first place.'

Mr Clapperton said Apple's plans for releasing the iPhone in Australia had not yet been publicly announced but if its US marketing strategy were adopted in Australia, it would likely be prohibited by the *Trade Practices Act 1974 (TPA)* provision dealing with third-line forcing.

'This law will greatly simplify the task of seeking redress for such behaviour through the courts and could prove a deterrent for exclusive release of the iPhone with one carrier,' Mr Clapperton said.

Inside QUT, 25 February, 2008



awards and achievements

- **Professor Ed Dawson**
 - Professor Emeritus [QUT]
 - Elected Vice-President of International Association of Cryptologic Research (2008–2010)
- **Dr Andrew Clark [FIT] and Dr Clinton Fookes [BEE]** recipients of the 2008 Vice-Chancellor's Performance Awards
- **Dr Jason Smith [FIT]** recipient of the 2007 Dean's Outstanding Doctoral Thesis Award.

new appointments

Gleb Sechenov,
Laboratory Manager

fighting invisible intruders on wireless networks



Dr Jason Smith

How can you detect a theft when there is no shattered glass, busted locks or missing objects? That's the question wireless computer network users now have an answer to thanks to Queensland University of Technology research.

The study has created groundbreaking systems for detecting the invisible intruders on wireless local area networks that threaten businesses and government agencies.

QUT Information Security Institute co-researcher Dr Jason Smith said he and a colleague had invented an effective system to detect unwanted presence on wireless networks.

'Unlike a building, there are no clearly defined boundaries to wireless networks. The perimeter of a network is defined by the quality of the receiving antenna,' Dr Smith said.

'Intruders can easily gain access to wireless networks by either eavesdropping on unencrypted networks or actively hijacking computer sessions when a legitimate user logged onto the network leaves the connection.'

Dr Smith said the system was a window into an invisible world that let network administrators see whether unexpected or undesirable things had occurred on their networks.

'We've created a series of monitoring techniques that when used together can effectively watch for both attackers and configuration mistakes in devices on the network,' he said.

'The monitor is independent of the network, yet uses information accumulated by the network. This makes the system cheap and easy for businesses to incorporate.

'The strength of the signal travelling in a wireless network and the round trip time of the signal are both monitored because they will change if an intruder enters the network.

'Separately monitoring the signal and round trip time is unreliable, but correlating them against each other makes the system accurate.'

Dr Smith said when an intruder was detected a number of steps could then be taken.

'Depending on how sensitive the network is, armed security guards could be deployed, or the wireless network may be turned off. The security protection might alter to avert the intrusion or the intruder may simply be monitored to see what they get up to,' he said.

'Another application is to use the monitoring to search for security vulnerabilities in devices legitimately connected to the network. When a compromising security configuration is detected, the mistake could be corrected.'

Dr Smith said he created the system with PhD researcher Rupinder Gill, who was now employed by a wireless network vendor in the US to create security products.

He said the valuable commodity at greatest risk on local area networks was information

Inside QUT, 29 November, 2007



aggregating government information



Dr Adrian McCullagh

This project is in collaboration with the Smart Internet Technology (April, 2006 to June, 2008) and Smart Services CRC (July, 2008 to July 2009).

The development of a secure yet open access regime for a federated environment involving information spread across multiple Queensland Government agencies has

been the research task undertaken by a group of researchers with the Information Security Institute. The research involves the development of appropriate security frameworks which can benefit the Queensland Government in its ability to commercialise the aggregation of geo-spatial information that is presently spread across multiple government agencies. The project within the Government is known as the Information Queensland (IQ) Project and it is lead by its director Mr Gary Shaw. Mr Shaw and his team within the Department of Natural Resources and Water have been a great help to the ISI researchers.

The researchers comprise members from three faculties namely the Faculty of Business led by Dr Paul Barnes, the Faculty of Information Technology led by Professor Ed Dawson and the Faculty of Law led by Professor Sharon Christiansen. Dr McCullagh is the overall project leader. Each faculty has been able to bring their relevant expertise to ensure that a holistic solution can be attained. Each faculty has been able to contribute their particular perspective in deriving a solution that is hoped will stand the test of time.

The foremost position for the IQ security project is that any solution must not in any way compromise the security of each agency's information repository. Each agency has developed their own security framework. The risks involved for each agency can be different and as such there is no single security framework that will necessarily cover the field. With this in mind the IQ security project researchers have had to develop a number of position papers and solution sets to assist each government agency in participating in the aggregation of their geospatial information.

The IQ security Project is now entering its third phase. Phase one of the project resulted in the development of a substantial report that covered the requirements needed to provide a secure access to information repositories that are federated.

Phase two produced a set of Information Security Management Guidelines that addressed the following key issues arising out of the IQ project:

- Legal liability which has been completed as part of the research project.
- Recordkeeping and retention which requires further investigation; and
- Privacy which also involves further investigation.

Phase three will now involve the last two areas which it is hoped will be completed by June 2009. This project has been successful due to the collaboration of both the government personnel involved and the dedication and commitment of the researchers involved who have each contributed to a holistic solution which can only ensure that this is the smart state.

Project	Research Team Leaders	Funding Sources	Contact
Legal and technical security framework across multi-agency information repositories: Information Queensland Project	Dr Adrian McCullagh (ISI) Professor Ed Dawson (FIT) Dr Paul Barnes (BUS) Professor Sharon Christensen (LAW)	Smart Internet Technology CRC (April 2006–June 2008) Smart Services CRC (July 2008–July 2009) Queensland Government	Dr Adrian McCullagh +617 3138 9554 a.mccullagh@qut.edu.au

completions

Masters by Research

- Dominika Zerba (BUS) **Critical Impediments to the Effective Implementation of Business Continuity Management (BCM) Initiatives at the Brisbane Airport Corporation.** Supervisor: Dr Paul Barnes (Principal)
- Michael McGreevy (BEE), **Statistical Language Modelling for Large Vocabulary Speech Recognition.** Supervisors: Professor Sridha Sridharan (Principal), Dr Michael Mason (Associate)

PhD

- Ken Wong (FIT), **Application of Finite Field Computation to Cryptology: Extension Field Arithmetic in Public Key Systems and Algebraic Attacks on Stream Ciphers.** Supervisors: Professor Ed Dawson (Principal), Dr Gary Carter (Associate)

- Brendan Baker (BEE), **Speaker Verification Incorporating High-Level Linguistic Features:** Professor Sridha Sridharan (Principal), Dr Michael Mason (Associate), Dr Robert Vogt (Associate)
- Frank Chi-Hao Lin (BEE), **Super-Resolution ImageProcessing With Application to Face Recognition** Associate Professor Vinod Chandran (Principal): Professor Sridha Sridharan (Associate), Dr Clinton Fookes (Associate)
- David Dean (BEE), **Synchronous HMMs for Audio-visual Speech Processing,** Professor Sridha Sridharan (Principal), Associate Professor Vinod Chandran (Associate)
- Patrick Lucey (BEE), **Lipreading Across Multiple Views,** Professor Sridha Sridharan (Principal), Associate Professor Vinod Chandran (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