






Fundamental and applied research



Consultancy and audit



Commercialisation for the real world

In this age of the digital economy, reliance on information assets has never been greater. The Internet has delivered massive productivity windfalls to governments, business and communities alike. However, the full benefits of a digital economy are yet to be realised. The notion that information technology is now mature and fully commoditised, with little scope for innovation, sells future potential gains short.

Digital Forensics

The widespread adoption of new technologies such as Internet Protocol Version 6 (IPv6) and web services and the increasingly complex methods employed by those who would do us harm introduces new challenges for experts and law enforcers in bringing wrongdoers to justice. New tools and techniques are needed to support the role of computer forensic investigators who must analyse increasingly voluminous and complex corpora of digital evidence.

Identity Management

Identity management in a virtual world and the protection of vital national infrastructure, including telecommunications, web services, and control systems for water and electricity pose additional questions with the need for significant research investment.

Resilient Systems

Protecting information assets in a world that demands increased connectivity remains a challenge. Information technology has to deliver comparable trust and assurance attributes at the same level as those we are accustomed to in a non-virtual world. The design of information systems which are inherently more resilient, and which allow for graceful rather than catastrophic degradation, has become paramount.

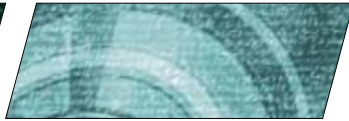
The Information Security Institute (ISI), a research institute within Queensland University of Technology (QUT), has grown into the largest university-based information assurance research concentration in Australia. The ISI is a collaborative undertaking of the Faculty of Built Environment and Engineering (BEE), the Faculty of Business (BUS), the Faculty of Science and Technology (FST), and the Faculty of Law (LAW). This consolidates expertise that QUT has developed in all aspects of information security over the past 20 years.

As a multidisciplinary institute, the ISI continues to build real solutions for government, business and the community by undertaking research in technology, legal, policy and governance issues related to information security. This multidisciplinary approach provides QUT with an opportunity to play a leading role in research in the area of safeguarding Australia, which has been identified by the Australian Research Council as one of the key areas of applied research for the nation.

The institute has developed a strong international presence with links with other universities and research bodies throughout Australia and in Asia, Europe, North America and Africa. During 2008 the ISI completed a national review on esecurity education and research for the Australian Government. Another example is the \$2.25 million awarded to QUT from the Commonwealth Department of Innovation Industry Science and Research Australia India Strategic Research Fund to research countermeasures for Distributed Denial of Services Attacks with the Indian Institute of Technology (IIT) Madras and the Society for Electronic Transactions Security.

The ISI's success in real-world research means that we can work with you to help you meet your specific business and service objectives. Our unique position provides access to an unparalleled range of expertise and experience to assist in solving the problems you face today and into the future.

Research groups



Cryptography

Leader: Dr Juan Gonzalez Nieto

Investigates the theoretical and applied areas of cryptography, with particular emphasis on the needs of banking and finance sectors, government requirements, gaming, manufacturing, insurance, utilities and allied industries globally and domestically.

EXPERTISE:

- Analysis and design of symmetric ciphers
- Analysis and design of public key algorithms
- Issues in global public key infrastructure (PKI)
- Proofs and specifications for cryptographic protocols
- Efficient software implementation
- Cryptographic protocols for control systems
- ID-based cryptography

Network Security and Digital Forensics

Leader: Associate Professor Andrew Clark

Identification of the best ways to architect, implement and manage secure information infrastructure in an environment that is increasingly interconnected and constantly evolving. Emerging business models that leverage new technologies and architectures present critical security challenges that demand innovative approaches to preventing, detecting, investigating, responding to and recovering from incidents.

EXPERTISE:

- Control systems
- Computer network vulnerability assessments
- Network and system event monitoring
- Web services and SOA security
- Incident response
- Fraud and misuse detection
- Cross-domain solutions
- Trusted computing
- Computer forensics

eBusiness and eGovernment

Leader: Professor Sharon Christensen

Information security is critical for the effective operation of commerce and governments in an electronic environment. This research examines and develops business models, appropriate policy responses, legislative, contractual and security frameworks and regimes to obtain the benefits of electronic commerce.

EXPERTISE:

- Secure electronic auctions
- Electronic contracting
- Electronic land dealing systems
- Electronic banking
- eTendering
- Secure electronic voting
- eLitigation – a 'best-practice' model
- Trusted information sharing networks (TISN)
- Electronic government information

Risk and Crisis Management

Leader: Dr Paul Barnes

The capacity to identify vulnerabilities within complex organisations, institutions and systems, followed by appropriate risk mitigation strategies, is an important part of effective management. This group's research focuses on examining and developing end-user capacities to enhance functional and organisational resilience.

EXPERTISE:

- Threat, vulnerability and risk analysis in the private and public sectors
- Business continuity planning and crisis management
- Resilience and interdependency modelling in critical infrastructure

Speech, Audio, Image and Video Technology

Leader: Professor Sridha Sridharan

Technologies are developed for biometric person identification, person tracking, human activity detection and intelligence gathering for audio and video surveillance applications. This includes the use of sensors to monitor, detect and identify persons; track their movements and activity; monitor conversations of suspects and signal processing techniques for extracting information and intelligence gathering.

EXPERTISE:

- Speaker verification and identification
- Multi-camera video surveillance
- Multi-microphone audio surveillance
- Face verification and identification
- Multi-biometric systems
- Person tracking in a crowd and activity detection
- Biometric policy
- Biometric smart cards
- Perimeter protection

Governance, Law and Policy

Leader: Professor Bill Lane

Effective governance of information and related infrastructure is essential for corporate survival and critical to the protection of national information infrastructures. Current management and contingency planning practices related to information protection are unregulated and have the potential to impact significantly on national infrastructure. This raises questions about the effectiveness of technical, legal and regulatory infrastructures in blending the needs of both the private and government sectors meeting these requirements.

EXPERTISE:

- Policy frameworks for national infrastructure governance
- Legal frameworks for protection of NCIP
- Competition policy and regulation
- Privacy law and policy
- Technology governance
- Information security standards
- Privacy and FOI issues

Case studies

International collaborators

Department of Innovation, Industry, Science and Research (DIISR): Critical Infrastructure from Denial of Service Attacks: Tools, Technology and Policy

Collaborative project funded by Australia-India Strategic Research Fund (AISRF)

This is a joint three-year project with the IIT Madras and the Society for Electronic Transactions and Security. Based on the complementary expertise of researchers from India and Australia, this project has two aims:

- to understand the growing problem of Denial of Service (DoS) attacks on critical infrastructure and develop smart and proactive solutions
- to develop a distributed test bed across India and Australia to better understand the DoS imperatives in practice.

Researchers: Professor Ed Dawson (FST), Associate Professor Andrew Clark (FST), Professor Colin Boyd (FST), Professor Mark Looi (FST), Professor George Mohay (FST), Professor Bill Caelli (FST), Dr Husmukh Morarji (FST), Dr Jason Smith (FST), Professor Sharon Christensen (LAW), Professor William Duncan (LAW).

Domestic collaborators

Airports of the Future Pilot Project

A collaborative project in conjunction with Australian Federal Government, Brisbane Airport Corporation

This project examines outbound passenger facilitation in selected Australian international airports. Business processes, human-systems interfaces, security surveillance technologies and business continuity planning (with links to transport security planning) are being analysed in this initial study as part of a larger four-year research project.

The project is jointly funded by QUT, members of the Australian aviation industry and partners from the Australian Government.

Researchers: Dr Paul Barnes (BUS), Dr Clinton Fookes (BEE), Professor Sridha Sridharan (BEE).

Queensland Government Security Framework for Geospatial Data across Federated Data Repositories

Funded by the Queensland Government as part of the CRC for Smart Services

This multidisciplinary project focuses on the development of a risk, legal and security framework to protect geospatial data across multiple autonomous data repositories. Each repository has its own security infrastructure that operates independently of any other repository. The investigation analyses and develops security mechanisms for three authentication and authorisation technologies, as well as the development of a risk framework and legal framework. The project has produced significant findings that will impact upon all interdependent organisational structures irrespective of the type of information that has been collected and retained. Digital archiving, business continuity planning and privacy are just three areas that have been extensively explored.

Researchers: Dr Adrian McCullagh (ISI), Professor Sharon Christensen (LAW), Professor William Duncan (LAW), Professor William Lane (LAW), Professor Ed Dawson (FST), Dr Paul Barnes (BUS), Dr Leonie Simpson (FST), Dr Tony Sahama (FST).

ARC Discovery Grant: Technical and Legal Models for Virtual Info-Sharing Networks (VISN) for CIP

Funded by Australian Research Council

The protection of 'critical Infrastructure' (CI) such as electricity and water is a major issue for governments. In some areas more than 90 per cent of CI is privately owned, so protection depends on cooperation between industry and government. Info-Sharing Networks (ISNs) are one protective strategy. ISNs usually involve face-to-face data exchange arrangements between industry members. The aim of this project is to investigate the technical and legal issues arising from a new form of ISN structure involving a secure electronic/virtual community for the exchange of sensitive information.

Researchers: Professor Ed Dawson (FST), Professor Stephen Corones (LAW), Professor Bill Lane (LAW), Dr Adrian McCullagh (ISI), Dr Ernest Foo (FST).

ARC Discovery Grant: Voice Recognition Technology

Funded by Australian Research Council

This Australian Research Council-funded research aims to discover techniques which effectively model the unique characteristics of a speaker's voice with small amounts of speech data, in the presence of impairments and independent of the spoken language and text. The project hopes to achieve an order of magnitude reduction in the error rate, to enable widespread use of the technology in commercial as well as forensic speaker identification applications including voice-based tracking of terrorist activity.

Researcher: Professor Sridha Sridharan (BEE).

ARC Discovery Grant: Cryptographic Protocols – Proofs and Designs

Funded by Australian Research Council

Formal security proofs are usually expected for any newly designed cryptographic protocols. However, there are still many unanswered questions regarding how best to model such protocols, especially in situations with special requirements or restrictions. This project addresses some of the fundamental questions about security proofs and models for authentication and key exchange. As well as designing new models and protocols, the outcomes will improve understanding of how different formal models are related.

Researchers: Professor Colin Boyd (FST), Dr Juan Gonzalez Nieto (FST).

ARC Linkage Grant: Integrated Financial Fraud Detection in Enterprise Applications:

Funded by Australian Research Council and SAP Resources

A significant problem with enterprise resource planning systems (ERP) is fraudulent behaviour by employees using these systems for activities such as invoicing and salary payments. This collaborative three-year project with SAP Research aims to develop automated processes to identify unusual patterns that may indicate fraudulent behaviour.

Researchers: Professor George Mohay (FST), Associate Professor Andrew Clark (FST), Professor Benno Torgler (BUS).

Key researchers



BUSINESS DIRECTOR

Mr Eric Hall
eric.hall@qut.edu.au
General Manager and Director of Business Development



RESEARCH DIRECTOR

Professor Colin Boyd
c.boyd@qut.edu.au
Research Expertise:
• Design and analysis of cryptographic protocols

DEPUTY DIRECTORS

Faculty of Science and Technology



Associate Professor Andrew Clark – FST

a.clark@qut.edu.au
Research Expertise
• Network security and intrusion detection
• Digital forensics
• Control systems security
• Web services security

Faculty of Built Environment and Engineering



Professor Sridha Sridharan

s.sridharan@qut.edu.au
Research Expertise
• Biometric person authentication and surveillance using speech and image technologies

Faculty of Business



Dr Paul Barnes

p.barnes@qut.edu.au
Research Expertise:
• Business continuity planning
• Crisis and risk management

Faculty of Law



Professor Sharon Christensen

s.christensen@qut.edu.au
Research Expertise:
• Electronic contracting
• Liability aspects of electronic information
• Electronic property transactions

EMERITUS PROFESSORS



Emeritus Professor Bill Caelli – FST

w.caelli@qut.edu.au
Research Expertise
• Trusted systems
• Information security policy



Emeritus Professor Ed Dawson – FST

e.dawson@qut.edu.au
Research Expertise:
• All aspects of cryptology, especially those concerned with the design and analysis of encryption algorithms
• The application of cryptology to ecommerce and secure communications



KEY RESEARCHERS

Dr Gary Carter – FST
g.carter@qut.edu.au
Research Expertise:
• Design and analysis of encryption algorithms



Associate Professor Vinod Chandran – BEE

v.chandran@qut.edu.au
Research Expertise:
• Biometric person authentication and surveillance using speech and image technologies



Professor Stephen Coronos – LAW

s.coronos@qut.edu.au
Research Expertise:
• Competition law
• Legal implications of information exchange arrangements



Professor Bill Duncan – LAW

w.duncan@qut.edu.au
Research Expertise:
• Legal aspects of electronic conveyancing
• Electronic contracting liability for electronic information



Professor Colin Fidge – FST

c.fidge@qut.edu.au
Research Expertise:
• High-integrity software engineering
• Information security evaluation of communications devices
• Formalisms for modeling and analysing complex systems



Dr Ernest Foo – FST

e.foo@qut.edu.au
Research Expertise:
• Design and analysis of cryptographic protocols
• Network security



Dr Clinton Fookes – BEE

c.fookes@qut.edu.au
Research Expertise:
• Image and video technology
• Biometrics
• Intelligence surveillance



Dr Juan Gonzalez Nieto – FST

j.gonzalezniето@qut.edu.au
Research Expertise:
• Design and analysis of cryptographic protocols



Professor Bill Lane – LAW

wb.lane@qut.edu.au
Research Expertise:
• Information access regimes
• FOI
• Privacy law

Key researchers



Professor Mark Looi – FST

m.looi@qut.edu.au

Research Expertise:

- Network security, particularly in the areas of the security of smart cards, wireless systems and mobile networks



Professor George Mohay – FST

g.mohay@qut.edu.au

Research Expertise:

- Intrusion detection
- Computer forensics



Dr Jason Reid – FST

jf.reid@qut.edu.au

Research Expertise:

- Trusted computing
- Access control in distributed systems
- Privacy compliance



Dr Leonie Simpson – FST

lr.simpson@qut.edu.au

Research Expertise:

- Design and analysis of symmetric ciphers



Dr Jason Smith – FST

j4.smith@qut.edu.au

Research Expertise:

- Industrial control system security
- Vulnerability assessments
- Incident response



Professor Benno Torgler – BUS

benno.torgler@qut.edu.au

Research Expertise:

- Public policy
- Economics



Dr Robbie Vogt – BEE

r.vogt@qut.edu.au

Research Expertise:

- Speech technology
- Speaker verification
- Audio data mining



Contact

Information Security Institute is located at the Queensland University of Technology
GPO Box 2434, (126 Margaret Street),
Brisbane, QLD 4001 Australia

International

Phone +61 7 3138 9572 Fax +61 7 3221 2384

For more information

please email us at info@isi.qut.edu.au
or visit our website at www.isi.qut.edu.au

CRICOS No. 00213J ABN: 83 791 724622

a university for the **real world**[®]