

iACiTS

Third Indo-Australian Conference on Information Technology Security

9-10 July, 2007

**Queensland University of Technology (QUT)
Brisbane, Queensland, Australia**

eServices-eSecurity: The Growing Challenge for Critical National Infrastructure

The third *Indo-Australian Conference on Information Technology Security*, will bring together leaders from both countries to examine these vital factors, from legal frameworks to security technology, particularly from a national policy development perspective.



Australian Government

Australian Education International



isi

Information Security Institute

CONTENTS

	Page No
Welcome Message from Australian High Commissioner to India	i
Message from Counsellor (Education, Science & Training), Australian High Commission, New Dehli	ii
Co-Chairs Biographies	1
Prof E Dawson	2
Professor S V Raghavan	2
Opening Adressee Abstracts and Biographies	3
Hon Mike Ahern	4
Professor Simon Kaplan	4
Speaker Abstracts and Biographies	5
India:	
Suganya Annadurai	6
Dr C Chellappan	6
Dr S Dhekne	7
Ms Ratnaboli Ghorai Dinda	8
Dr Krishnan Ganapathy	9
Professor S Kuppuswami	10
Professor S F Raghavan	11
Mr Srinivasan Ramakrishnan	13
Mr S S Sarma	14
Dr. M S Vijayaraghavan	14
Australia:	17
Mr Paul Ashley	18
Mr Simon Bartlett	18
Mr Vishnu Bhat	19
Professor Peter Croll	20
Mr Richard Czumak	20
Mr Grae Meyer-Gleaves	21
Dr John Harrison	22
Dr Adrian McCullagh	22
Mr Chris Marsden	23
Mr Walter Williams	24
Professor Vijay Varadharajan	24
Appendix:	26
• Australian Scholarships	27
• Overview Australia–India Strategic Research Fund	28



Message from the Australian High Commissioner to India

It's with much pleasure that I extend a warm welcome to all the participants of this conference on IT Security, both from India and Australia. I was pleased to participate in the opening of the previous Conference in Chennai, India in January 2005, hosted by IIT Madras. Subsequently, during the visit to India of the Australian Prime Minister, Hon. John Howard MP, two Memoranda of Understanding were signed in his presence during his visit to the campus of IIT Madras, to strengthen institutional linkages for collaboration in research cooperation in IT Security. The Agreements involved IIT Madras and the Society for Electronic Transmission and Security (SETS) together with the Queensland University of Technology. I am confident that the current conference will offer an excellent opportunity to the participants to deliberate further on this important theme.

Worldwide, operations and management of critical infrastructure as well as the physical security and wellbeing of people are increasingly becoming dependent on Information Communications Technology. Correct and reliable functioning of computer systems has become critical for today globalized world. As applications of information security technologies become ever more pervasive, issues pertaining to their deployment and operation are becoming increasingly important. I'm glad that Australia and India are intensifying on-going research cooperation to address such issues arising from the increasing interdependency of our critical network information systems.

I wish the Queensland University of Technology, as host of this important meeting, and the participants of the Conference every success in strengthening these new links. The relationship between Australia and India is growing stronger by the day and this engagement of research communities in India and Australia concerned with IT security is a most welcome contribution.

John McCarthy
Australian High Commissioner to India.

22 June 2007

**Australian Education International
Department of Education, Science and Training
Government of Australia**

Education and research are striking aspects of the India-Australia relationship. The past 12 months saw close to 40,000 enrolments by Indian students studying in Australian schools, colleges, institutes and Universities. Australian Education International, AEI, within the Australian Government's Department of Education, Science and Training has responsibilities for the generic promotion of this education market, the policy and government-to-government relationships and facilitating the strengthening of links between education institutions in Australia with their counterparts in India. These linkages are increasing by the month as are collaborative research ventures and exchanges of staff and students.

The education and research relationship between India and Australia has been growing steadily for some time and is now poised to reach new levels through the availability of additional funding and opportunities for collaborative research and exchange of researchers. These opportunities emerged from the visit by the Australian Prime Minister, John Howard MP to India in March 2006. Firstly, I bring to your attention the considerable expansion in the Australian Scholarship Scheme and, secondly, the establishment of the Australia India Strategic Research Fund. Details of both of these programs are given in the following pages.

As part of AEI's strategy to strengthen and enrich the education and research relationship between Australia and India, we have sought to profile Australia's excellence in research and innovation through a series of seminars and workshops in topical areas of priority. One theme of these has been research, development and innovation in the field of IT Security. This meeting in Brisbane is the third in this series of IT Security Workshops, with the previous two having been held at IIT Madras in Chennai, India.

AEI is pleased to provide funding to support the hosting of this meeting and the participation by some of the Indian delegates. I thank the Queensland University of Technology and the Organising Committee for their hospitality and hard work in making this meeting possible.

I extend to all the delegates my best wishes for a stimulating meeting and discussions and exchanges that will lead to further collaboration in this important field.

Professor John Webb, OAM
Counsellor (Education, Science and Training)
Australian High Commission
New Delhi,
India

John.webb@aei.gov.au

CO-CHAIRS BIOGRAPHIES

Professor Ed Dawson

e.dawson@qut.edu.au

Professor Ed Dawson is the Research Director of the Information Security Institute (ISI), and Professor of Cryptology and Its Applications at Queensland University of Technology (QUT) in Australia. He has research interests in all aspects of cryptology especially related to the design and analysis of encryption algorithms and their application to e-commerce and secure communications. He has published over 200 research papers on various aspects of cryptology. Professor Dawson was a member of the Board of Directors of the International Association of Cryptology Research.

Professor S V Raghavan

Given in section: "Speaker Abstracts and Biographies" – page 12

OPENING ADRESSEES BIOGRAPHIES

Hon Mike Ahern

Former Queensland Premier, the Hon Mike Ahern, was a member of the Australian Department of Industry, Technology and Communications Ministerial Council for three years. While Minister for Industry, Small Business and Technology, Mr Ahern developed the first technology strategy for Queensland. He was Queensland's first technology Minister. Mr Ahern was also formerly Primary Industries Minister and a member of the Australian Fisheries Council, Minister for Health and Environment and State Treasurer.

He was educated at Downlands College, Toowoomba and then attended the University of Queensland where he was awarded a Bachelor of Agricultural Science degree in 1963.

Mr Ahern has been appointed a Special Representative by the Queensland Government to promote Trade and Investment with Africa, the Middle East and India. He is also Chairman of Australia Petroleum Pty Ltd; Chairman of the Indue Group of Companies; Director of Brisbane Markets Ltd; Member of the Board of Governors of the ATSE Clunies Ross Foundation; Chair of the Consultative Committee of the Queensland Centre for Advanced Technology; Chairman of Directors of McIntosh Financial Planning Pty Ltd; Chair of the Australian Liver Foundation; Chair of the Family Care Friendly Society; and Chair of Family Care Medical Services, the largest Medical Deputising Service in Australia.

For his services to the state's development, the Queensland University of Technology awarded Mr. Ahern an honorary doctorate.

Professor Simon Kaplan

*Executive Dean, Faculty of Information Technology
Queensland University of Technology
Email:*

Simon Kaplan is Professor of Computer Science and Executive Dean of the Faculty of Information Technology at the Queensland University of Technology. Prior to this, he was Head of the School of Information Technology and Electrical Engineering at the University of Queensland. He holds B.Sc (Hons) (first class) and Ph.D. degrees in Computer Science, both from the University of Cape Town. He has over 25 years of industry and research experience in information technology.

Before switching to an academic career Simon was the principal designer and implementer of a range of Enterprise Resource Planning Tools built in Cape Town, South Africa that were widely deployed in South Africa and abroad. Aimed at the SME market, these systems were often the first IT systems installed in many companies, and covered general ledger, debtors, creditors, stock, payroll and related applications. Building these systems in a world before PCs and Windows often required construction of an entire support infrastructure, including database, networking and graphics support to underpin the development of the ERP applications. These codes were subsequently ported to Unix and remained in commercial use until well into the 1990s.

Simon has extensive experience as an expert witness in a range of patent and contractual disputes relating to a wide range of aspects of Information Technology.

Simon is the author of over 100 research papers, and has served on the editorial boards of ACM Transactions on Information Systems, Collaborative Computing, and the CSCW Journal. He has also served as chair or program committee member for numerous ACM, IEEE and international conferences.

SPEAKER ABSTRACTS AND BIOGRAPHIES

India

Suganya Annadurai

*Society for Electronic Transactions and Security (SETS)
Chennai*

Abstract:

Risks in Information Service Access via Mobile Devices

Not provided

Bio:

BioSuganya Annadurai holds a Masters degree in VLSI Design from SASTRA University, Tamilnadu, India. She is currently working as Senior Research Associate at Society for Electronic Transactions and Security (SETS), Chennai, India, an Information Security research organization. Her research interests include analysis and design aspects of cryptographic hash functions and efficient hardware realisation of secure communication systems. She has published papers in reputed journals.

Dr C Chellappan , ME, Ph.D ,

*Professor of Computer Science & Engg
Anna University, Chennai-600 025. INDIA
Email: drcc@annauniv.edu*

Abstract

E-Services: The need for higher levels of trust by populace

Web based services, also termed as E-services are either stand-alone or use other web services for performing their tasks. E-services are federated, composite, and autonomous. To conduct a business task, an e-service undertakes a conversation that spans across multiple e-services, which is often asynchronous and asymmetric.

It is the inevitable model in the world with the issues that websites of e-services frequently lack the social presence of the physical services and is critical in the creation of trust. Trust itself is a major issue affecting the phenomenal growth rate of e-services, according to industry sources and recent academic studies. As a central issue of modern e-services, trust has to be tackled not only during the development phases but also in operation and maintenance phases.

The trust is viewed as a two-way thing; the e-service must validate the user and, equally, it must present an identity and trust credentials allowing the user to believe it can deliver the service.

The trust is conceptualized into a framework consisting of constructs derived from related domain areas like management, sociology, economics, politics, science, psychology. The higher level views of trust are trusting intention, trusting behavior, trusting beliefs, system trust, dispositional trust, and situational decision. These general concepts are refined into notions like feelings of security, vulnerability, honesty, situational normality, belief in-person, or trust stance.

The e-services building process encapsulates Service-Oriented Architecture (SOA) to address issues of authentication, access control, encryption, non-repudiation, and authorization.

Keywords: e-service, Trust, SOA, Web Services, Belief, Security, Social presence

Bio:

Dr C Chellappan ME, Ph.D has more than 27 years of teaching and research experience. He did his undergraduate at PSG College of Technology, Coimbatore and his Post graduate in ME in Computer science and Engineering at College of engineering , Guindy, and Ph.D in computer science at Anna university, Chennai, India. He has joined as Associate lecturer at College of Engg. and occupied various positions as Assistant Professor and Professor. He has published more than 50 research papers at national and international conferences and visited many countries like USA, Canada, China, Singapore. He is guiding a number of research scholars in area network security, distributed/mobile computing and soft computing. He was the Director, Ramanujan Computing Centre, Anna university for three years since 2002. He is a expert member in computer purchases and software developments for TamilNadu State Government departments. He is the coordinator for the collaborative research project on 'Smart and secure Environment'.

Dr P S Dhekne

Associate Director

Bhadha Atomic Research Center (BARC)

Numbai, India

Abstract :***National Information and Computation Grid***

Advances in computational technology continue to transform Science and Technology research, practice, and allied education. Users in many disciplines have begun revolutionizing their fields by using digital information, computers, digital data, and networks to replace and extend their traditional efforts. Furthermore, Information processing activities, such as data base indexing and financial modeling, emails, data mining via search engines through Internet etc. are becoming more computationally and I/O intensive and require high performance computing facilities. As a result, adequate computing & networking capabilities have become a crucial resource at premiere research universities like IIT's, national libraries and R & D laboratories.

The development of upcoming Grid technology for handling Terabytes amount of experimental data, requiring hundreds of TeraFlops of computing stands out as unique technology. The Grids allow integration of all resources available in all collaborating places via high-speed Internet-2 similar to an electric Grid. This is not just connecting computers around the world but it is a technology where one needs to deal with the problem of connecting heterogeneous systems, data security & connecting them at high speed so that they break the barrier of distance and many other issues. By integrating these distributed Environment using low cost Internet based technology, now it has become possible to provide supercomputing power in the hands of individual users that until now could only dream of affording such power without having to make an exorbitant capital investment. This World Wide Grid Technology driven by High Energy Researchers at the moment would surely reach out from high-energy physics to e-governance and then in medical, geophysics, and weather thus forming a very important National Information backbone.

Over the years since Independence, India has built up a tremendous S&T platform, backed by a growing industrial base. It is therefore natural that we make a huge contribution in solving this complex problem and make Internet computing and data handling a reality. This presentation will describe various Grid initiatives in India, its development, current status and the tools developed with brief description of various applications benefited from this Grid technology.

Bio:

Shri P.S.Dhekne after graduating in Physics from University of Pune with first class and B.E. with Distinction from University of Pune during 1970, joined ECIL, Hyderabad training school in computer discipline & served in many DAE institutions including ECIL, TIFR, VECC and BARC. He has ably shouldered the responsibility as an Officer-In-Charge, Computer Centre, BARC and then as head Computer Division, BARC. Currently he is holding charge as Associate Director Electronics & Instrumentation Group at BARC.

His major contributions include those of design and development of various models of **ANUPAM parallel processing systems**. He was also actively involved in the design and development of high-resolution (5120x4096) wall-size **tiled display panel** using commercially available multiple LCD's (4x4) interfaced with a parallel cluster for large volume data visualization purpose, which is first of its kind in the country. He made innovative use of clustering approach as a low cost alternative to many IT solutions in computing such as Web Farms, Computing Farms, Load Balancing Cluster, High Availability Cluster, HPC Cluster, High-end Graphics and Grid Computing. He also made significant contributions in information security and security surveillance area.

He is an India representative at CERN (the European Laboratory for Particle Physics), Geneva as leading person to develop Grid software for Large Hydron Collider (LHC) Computing Grid (LCG) as per DAE-CERN agreement to provide software worth of 7.5 MCHF. He is a member & India representative for C-RRB and Grid Deployment Board for LCG project at CERN. He has done pioneering work in developing BARC-Computing *Grid and DAE grid*. He is also closely associated with European EU-India Grid and India's Garuda Grid.

Shri Dhekne has published more than 40-refereed papers on International & National Journals/Symposiums. He is a winner of the Indian Nuclear Society Award INS-2001, presented by Honorable Prime Minister of India on Thursday 30th Oct 2002 for his pioneering work in development of parallel processing computer series ANUPAM. He was also elected as fellow of National Academy of Engineers (FNAE) in 2002. Currently he has been awarded distinguish professor award from National Academy of Engineering.

Ms. Ratnaboli Ghorai Dinda

Senior Technical Director, Cyber Security Division

National Informatics Center

Email: ratnaboli@nic.in

Abstract :

Government Services : Systems Security and Information Assurance Challenges

Information Assurance aims at providing the means and mechanisms for the protection of information and information systems. The overall assurance methodology involves risk assessment, risk management, countermeasures and technology solutions, compliance and audits, and incidents responses. The objective is to protect information systems, detect breaches, and react to incidents.

Information technologies provide enormous opportunities for government to transform its services into digital form. E-governance has exponentially increased the number of services, technologies, and individuals that have access to sensitive information. The National e-Governance Plan of the Indian Government seeks to lay the foundation and provide the impetus for long-term growth of e-Governance within the country. The plan seeks to create the right governance and institutional mechanisms, set up the core infrastructure and policies and implement a number of Mission Mode Projects.

National Informatics Centre plays a major role in the governments' initiative towards e-Governance. Services such as passport, land records, treasury, transport etc. disseminate volumes of data to a large citizen base. Protecting such vital information and systems, including legacy systems that have usually not been subjected to information security life cycle is one of the greatest challenges facing the Government. The most crucial element here is to address the security concerns at each level of the government's information infrastructure for safeguarding the data belonging to government and citizens. With the help of suitable Information Assurance practices, this goal can be met.

Bio:

Ms. Ratnaboli Ghorai Dinda has been working with the National Informatics Centre under the Ministry of Communications and Information Technology of the Government of India. She has a Masters degree in Computer Applications from the University of Delhi.

She has been working in the area of Information Security for the past 7 years. Her current responsibilities include architecting a framework for information assurance through security

audit services for applications, secure coding methodologies, security awareness building and creating a secure hosting environment. She has also worked in messaging services, roll out the Certification Authority for NIC (NIC-CA) and PKI integration of applications.

Dr Krishnan Ganapathy

Head, Apollo Telemedicine Networking Foundation

Chennai, India

E mail: drkganapathy@gmail.com

Abstract

Telehealth in India from a national perspective: Security and other issues

Telehealth will eventually become an integral part of the Indian healthcare delivery system . With 800 million Indians living in suburban and rural India, speaking different languages, of different educational and socio economic status, with varied access to modern *ICT*, creating a uniform national infrastructure is not just a challenge, it can be a nightmare. Following the west is not the solution. Customised, need based, culture sensitive solutions are necessary. However we do not have to rewrite the past or piggy back. We can leap frog. This paper will reflect not only the author's 7 year experience overseeing 19,000 teleconsults but also summarise the emerging Indian e Health scenario Technological challenges have been many. Some have been overcome, others have been bypassed many remain to be addressed. As a member of the Ministry of Health's National Task Force and the Planning Commission's working group on Telemedicine, the author will review the recommendations made, including the creation of a National Telemedicine Grid. Various issues ranging from the use of different types of connectivity, standardization of hardware and software, legal frameworks and security technology will be discussed. The paper will illustrate how e Health in India will soon be a reality. Issues like licensure, credentialing, standards, quality control mechanisms and authentication will be highlighted A solution however is not a solution unless it is cost effective, universally accepted and applicable. Regulatory bodies should take into account the wide diversity cultural, social and economic factors. Social, ethical and legal solutions can never ever keep up with technology. Litigation is not usually in the vocabulary of the average Indian patient. A policy of "wait and watch" may therefore be better, than taking pre-emptive measures Immediate imposition of stringent global e security measures in suburban and rural India may be counterproductive .

Bio:

Dr Krishnan Ganapathy, M.S. (Neuro), M.N.A.M.S. (Neuro) FACS, FICS, Ph.D.

- *President, Neurological Society of India, 2006*
- *Senior Consultant Neurosurgeon & Head, Division of Stereotactic Radiosurgery, Apollo Hospitals,*
- *Sr. Vice President & Head, Apollo Telemedicine Network Foundation.*
- *Adjunct Professor, IIT & ANNA UNIVERSITY, Chennai*
- *Secretary, Neurological Society of India 1996 - 2002*
- *Secretary General – Asian Australasian Society of Neurological Surgery 1999- 2007*
- *Honorary Consultant and Advisor in Neurosurgery Armed Forces Medical Services, 2001-04*
- *Examiner & Inspector, National Board of Examinations, Ministry of Health, Govt. of India*
- *Overseas External Examiner for Universiti Sains Malaysia – first and only neurosurgeon from India.*
- *Member Editorial Board - Journal of Clinical Neuroscience (Australia) and South African Journal of Neurosciences and Pan Arab Journal of Neurosurgery*
- *Member, National Task Force on Telemedicine, India & Member, Working Group - Sub- Committee on Health Informatics including Telemedicine, Planning Commission.*
- *Member Expert Group for setting up Telemedicine in SAARC countries.*
- *Founder Member, (Joint Secretary and Treasurer) Telemedicine Society of India.*
- *International lecturer, World Federation of Neurosurgical Societies, Post Graduate Education Course*

1. Certified in Biomedical Communication and Bioinformatics.
2. Course director – Certificate course on Telehealth Technology Anna University, MGR Medical University .
3. Chairman, Organising Committee 3rd National Conference of Telemedicine Society of India & 12th IsfTeH international conference November 2007
4. Have published about 50 papers in regional/ national/ international journals on telemedicine and given almost a 120 talks at regional/ national/ international forums on telemedicine
5. 32 years of extensive teaching, clinical and operative experience at the Institute of Neurology, Madras Medical College, Stanley Medical College, Apollo Hospitals and Sundaram Medical Foundation Madras
6. *First Neurosurgeon in India to get a Ph.D. in Neuroimaging (1990).*
7. Presented about 195 papers in National Conferences and 45 in International Conferences.
8. Published about 165 scientific papers and several chapters in books besides about 45 articles in India's leading daily newspaper " The Hindu" and about 20 in national magazines.
9. Awarded the International College of Surgeons visiting professorship (Indian Section) in 1993 and Kamarakar Oration 1999.
10. Charter member and member Executive committee, Asian Society of Stereotactic and Functional Neurosurgery.
11. Charter member of the Indian Society of Stereotactic and Functional Neurosurgery.
12. Formerly Associate Editor, Neurology India and Associate editor of the CME Programme, Neurological Society of India. Formerly Co-Convenor CME programme NSI and Co-Editor Progress in Clinical Neurosciences. Member Editorial Advisory board and referee– "Neurology India"
13. Guide and supervisor for the Ph.D in Dr. MGR Medical University, Chennai, M. Phil – Madurai Kamaraj University, M.Phil BITS, PILANI, MA hospital administration Stuart University Australia.

S. Kuppuswami

*Professor of Computer Science & Director of Studies
Pondicherry University, India*

Abstract:

Service Oriented Architecture- An Upcoming Wave

Modern enterprises face hard restrictions and requirements than it was a decade ago due to the progress of globalization and world economy developments. Business and the business user's requirements are too dynamic on one end and at the other end the current IT infrastructure does not have the agility to keep up with the changing business objectives and thus places limitations on Business.

Service Orientation (SO) has now evolved as the enterprise technology solution that promises the agility and flexibility the business users have been looking for by leveraging the integration process through composition of the services spanning multiple enterprises. SO is an aspect which finds its origin from human organization in which we often make use of available services. The same analogy can also be used in software development wherein we think about business outcomes as a set of "composed" services instead of monolithic applications.

Different design paradigms exist for distributed solution logic. What distinguishes SO is the manner in which it carries out the separation of concerns and how it shapes the individual units of solution logic. Applying SO, to a meaningful extent, results in solution logic. That can be safely classified as "service-oriented" and units that qualify as "services." Solutions like CORBA and DCOM have some features of SO but the reality of ownership boundaries is truly reflected in SO whereas the former try to implement *transparent* distributed systems; *ownership* is the essence of SO.

The SOA concept is based on an architectural style that defines an interaction model between three primary parties: the *service provider*, who publishes a service description and provides the implementation for the service, a *service consumer*, who can either use the uniform resource identifier (URI) for the service description directly or can find the service description

in a service registry and bind and invoke the service. The *service broker* provides and maintains the service registry. In essence, SOA abstracts away the details of implementation through the use of a common Interface specification or service.

Basically in an SOA approach, only what needs to be changed is changed in response to requested service improvements. To realize business agility in a heterogeneous environment, SOA transforms an organization.

Bank is taken as an example, which offers various financial services such as online banking, bill payments, etc., and these financial services are accessible through variety of channels – branch offices, ATMs, telephony, call centers, fax, e-mails, & Internet, to name a few. We provide a Service Oriented Computing Model for E-Banking in order to explain the above said SOA concepts.

Bio:

Professor S. Kuppuswami received his Bachelor's and Master's degrees in Electronic Engineering from University of Madras in 1975 and 1977 respectively. He also received Doctorate Degree in Engineering (Computer Science) from University of Rennes I, France in 1986.

He has worked as a Computer Science faculty in Anna University, University of Rennes I, Pondicherry Engineering College before joining Pondicherry University. Currently he is holding the position of Director of Studies, Educational Innovations and Rural Reconstruction in Pondicherry University.

He is responsible for establishing departments and initiating new courses. He has published more than 60 research papers in various journals and conferences in the areas of Software Engineering.

His areas of research interests include Software Engineering, Agent Technology, Multilingual Computing and Network Management.

Professor S V Raghavan

*Network Systems Laboratory
Department of Computer Science and Engineering
Indian Institute of Technology Madras
Chennai 600036 INDIA
svr@cs.iitm.ernet.in*

Abstract

Next Generation ICT Security Functionality

Next generation ICT Security Functionality raises several scenarios that matter; ICT infrastructure, utilities infrastructure, business safety and continuity, governance, reliability and safety; above all – user confidence in systems. As a consequence, several issues surface - policy, procedures, technology, design, impact on the nation and beyond, and trusted systems, to list a few. Besides, there are several perceptions; attacks, vulnerabilities and threat – that too dynamic. In such a backdrop, sensing, avoidance, and mitigation of possible large scale attacks such as DoS necessitate the need for using trusted computing base along with trusted transactions. Thus transforming the current Internet and preparing for future leads naturally to networks that are IPv6+MPLS+VPN+IS+Privacy+IA. Can they scale? Are they reliable? Are they dependable?

While the expectations are high, one should acknowledge that the current Internet is a great success but fragile for critical infrastructure applications. We need to leave the syntactic approach of the present and adopt a semantic approach – where *we secure the information that is exchanged*. At the same time the solution one proposes should be computationally efficient using building blocks that are based on proven cryptographic techniques and protocols that are usable in a variety of situations.

The primary areas that need attention when we take a “fresh approach” are Identity Management, Secure Routing, Secure Name Resolution, and perhaps support for end-host security as well. Use of novel crypto techniques that can “fight” DoS attacks, use of cryptography within a well defined economic model for interactions by non-adversarial but selfish users, cryptographic protection of forensic data from tampering, and distributed alternatives to PKI models are a few opportunities available for the (visionary and elitist) designer of tomorrow’s Internet. Perhaps such an Internet will provide secure foundation to critical infrastructure applications as well.

As a first step, the talk will present our current research in “doing away with” IP addressing and introduce a paradigm shift in identity (address), routing, name resolution, and mobility. Instead of assigning an address (static or dynamic), we propose assuming an address – an approach that takes an integrated view of the addressing, routing, and mobility problem in one go. We explain in some detail Protocol

Bio:

Professor S V Raghavan is a gifted teacher, noted orator, voracious reader, avid writer, able administrator, active researcher, talented professional, and a team worker. Professor Raghavan is a Founder Member of Ernet (Education and Research Network) Project, which was jointly funded by Government of India and United Nations Development Program and was involved in the Design, Development, and Technology Adaptation. Professor Raghavan was instrumental in establishing MoUs with University of Maryland, College Park, University of Vienna, Austria, and Queensland University of Technology, Australia for R&D cooperation. Presently he is chairing the National Expert Committee for establishing a multi-gigabit network for Indian Science, Technology, Research, and higher education.

Professor Raghavan is the General Co-Chair of the Indo-Australian Conference on IT Security IACITS Series held in India and Australia. He Represents India in the International Federation for Information Processing, TC-6 on Data Communication. He participated in the Ministerial delegation that visited Sofia, Bulgaria in February 2004 to explore ties in the areas of Information Technology.

He was the Chair of the Department of Computer Science and Engineering at IIT Madras during 1995-1998 and was Dean (Planning) during 2003-2005.

He is the recipient of Silver Core Award of International Federation for Information Processing, IFIP, Geneva, and Elected Governor of International Council for Computer Communication, USA. Recently, he was awarded the Outstanding Alumnus award, MIT Alumni Association, Anna University, India.

Professor Raghavan is the Founder – Director of the most modern Network Systems Laboratory (NSL) in India. NSL is created with comprehensive facilities for promoting Experimental Computer Science and Engineering. His current research interests include System architecture, design and analysis, Mobile Ad-hoc Networks, Mobile agents, Next Generation Internet design, Information System Security, Wireless Sensor Networks, National Information Infrastructure Protection, and Electronic Commerce.

Professor S V Raghavan is a gifted teacher, noted orator, voracious reader, avid writer, able administrator, active researcher, talented professional, and a team worker. Professor Raghavan is a Founder Member of Ernet (Education and Research Network) Project, which was jointly funded by Government of India and United Nations Development Program and was involved in the Design, Development, and Technology Adaptation. Professor Raghavan was instrumental in establishing MoUs with University of Maryland, College Park, University of Vienna, Austria, and Queensland University of Technology, Australia for R&D cooperation. Presently he is chairing the National Expert Committee for establishing a multi-gigabit network for Indian Science, Technology, Research, and higher education.

Professor Raghavan is the General Co-Chair of the Indo-Australian Conference on IT Security IACITS Series held in India and Australia. He Represents India in the International Federation for Information Processing, TC-6 on Data Communication. He participated in the Ministerial delegation that visited Sofia, Bulgaria in February 2004 to explore ties in the areas of Information Technology.

He was the Chair of the Department of Computer Science and Engineering at IIT Madras during 1995-1998 and was Dean (Planning) during 2003-2005.

He is the recipient of Silver Core Award of International Federation for Information Processing, IFIP, Geneva, and Elected Governor of International Council for Computer Communication, USA. Recently, he was awarded the Outstanding Alumnus award, MIT Alumni Association, Anna University, India.

Professor Raghavan is the Founder – Director of the most modern Network Systems Laboratory (NSL) in India. NSL is created with comprehensive facilities for promoting Experimental Computer Science and Engineering. His current research interests include System architecture, design and analysis, Mobile Ad-hoc Networks, Mobile agents, Next Generation Internet design, Information System Security, Wireless Sensor Networks, National Information Infrastructure Protection, and Electronic Commerce.

Mr Srinivasan Ramakrishnan

*Director General, Centre for Development of Advanced Computing
Pune University Campus, Ganeshkhind Road
Pune 411007, India
Email: ramki@cdac.in*

Abstract:

Management of large scale Terabyte Store Information servers

World over the threats against integrity and confidentiality of stored data is the primary concern. Organizations are struggling to cope with the management of unprecedented data growth, regulatory requirements for data archival along with the ever increasing new data hungry applications. The dramatic rise in the volume of data is set to continue and expected to put more strain on management and security of large storage servers, demanding strategies and plans for more efficient utilization and management of storage. Besides, managing these Storage contribute to one of the most expensive manpower costs. Also, the explosive growth of data combined with the demands like ubiquitous secured access to information all the time mean no end to the rising complexity of storage management.

According to IDC, in 2006, worldwide disk storage systems accounted for 3 million terabytes of data. In 2009, that number is estimated to grow to more than 10 million terabytes. Much of this data is sensitive, and a challenge exists to protect it, even when it is at rest inside the organization: whether on backup tapes, CDs, other physical media, or proliferated across thousands of servers, desktops, and laptops.

World over, threats against integrity and confidentiality of stored data is primary concern. As such, along with the challenges of managing such data, organizations now need to put in security policies in place that meet requirements specific to business critical applications and data protection. Since the risks are enormous, an organization has to keep evolving and relying on its ability to safeguard the data, regardless of where it is.

Apart from highlighting the various challenges faced by the organizations in handling large volumes of data, this presentation brings out the various dimensions of secure management of such large scale storage including heterogeneous technology adoption and management, data protection at various levels of storage, content management along with secure access. The presentation also brings in some case studies from India about the practices followed in large IT organizations and mission critical applications.

Bio:

Srinivasan Ramakrishnan is currently Director General of Centre for Development of Advanced Computing (C-DAC). C-DAC has been a pioneer in High Performance Computing with its PARAM series of Supercomputers and is today complementing it with its recent initiative on national grid computing called "GARUDA". Besides, it is continuing its leadership role in Indian Language Computing through products, technologies, tools and research programs – often through collaborative efforts. Other areas of focus include software

technologies with special thrust on Open Source Software, Health Informatics, Cyber Security, delivery of solutions in various sectors, Electronics Technology and associated products and Flagship Training programs targeted at Industrial needs.

Prior to his current assignment, he has handled a variety of portfolios including Founder & National Project Director of ERNET, [the National Academic and Research Network - a collaborative effort of five IITs, IISc, former NCST and DIT (former DoE)]; Director of National Centre for Software Technology; Founder Director of Media Lab Asia (MLA); National Y2K coordinator; Head of Education, Research & Technology Division, Head of Software Development Division, Head of Communications, Convergence and Broadband Technology group – among others – in the Department of IT, Ministry of Communications and IT.

Shri Ramakrishnan has earlier been in industry as design engineer, Avionics Design Bureau, HAL, Hyderabad.

He holds a B.Tech and M.Tech degree from IIT Madras. He has been Vice President and Governor of International Council for Computer Communications and member of IEEE, IETE and Internet Society.

Mr S S Sarma

Scientist

Department of Information Technology, Gol

Abstract:

Security in Banking and Finance – Indian Experience

Not provided

Bio:

Mr. Sarma is currently looking after activities of CERT-In relating to Computer security Incidents such as Phishing, Malware propagation etc ,tracking of malicious code, Botnets, analysis of vulnerabilities and exploits, artifact analysis, Vulnerability Assessment and Penetration Testing. He has over seven years of experience in Information Security. He has overall experience of 17 years in the area computer communications and broadcasting.

He is a CISSP (from ISC2, USA) and a Certified Ethical Hacker from EC Council, USA. He received training in Information Security and Computer Forensics at CERT/CC, Carnegie Mellon University.

He holds a Bachelors degree in Electronics & Communication Engineering.

Dr. M. S. Vijayaraghavan

MSV, SETS and SVR, IIT M

Abstract:

Critical Infrastructure of a Nation

Our Nation's critical infrastructures consist of the physical and cyber assets of public and private institutions in several sectors: information and telecommunications, banking and finance, government, defense, industrial base, energy, agriculture, food, water, public health, emergency services, transportation, chemicals and hazardous materials, and postal and shipping. Cyberspace is the nervous system of these infrastructures—the control system of our country. Cyberspace comprises hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security. Unfortunately, recent events have highlighted the existence of cyberspace vulnerabilities and the fact that malicious actors seek to exploit them.

Protecting infrastructures in the Information Age raises new and difficult issues. Our Nation depends on the stable, consistent operation of our critical infrastructures for our way of life, our well-being, and our security. These critical infrastructures include, but are not limited to, telecommunications, energy banking and finance, transportation, water systems, and emergency services, both government and private. Cyberspace is becoming the nervous system of these infrastructures—the control system of our country. Unfortunately, recent events have highlighted the existence of cyberspace vulnerabilities and the fact that malicious actors seek to exploit them. Fast and resolute mitigating action is needed to avoid future national disaster. Recently, a terrorist organization had shut down the electrical power grid of USA for six hours. The same can happen with our country, might be in a different manner. Recent advances in computer hardware, software, and communications technologies have made these infrastructures highly automated and capable. But while technological advances have promoted greater efficiency and improved service, they have also made these infrastructures potentially more vulnerable to disruption or incapacitation by a wide range of physical or computer-based ("cyber") threats. And the infrastructures are much more interdependent than in the past, with the result that the debilitation or destruction of one could have cascading destructive effects on others.

Finally, some of these infrastructures are owned and operated by private industry. This means that guarding against infrastructure threats requires an unprecedented degree of cooperation and information sharing between the government and private sector. In addition to protecting today's infrastructure it is important to evolve the infrastructure in new directions to meet new technological challenges and provide new functionalities such as in oil/chemical plants/nuclear power generation, highway systems, medical devices. A key characteristic of critical infrastructures is the need to be able to operate through attacks. Despite significant progress in intrusion detection and protection using firewalls, VPNs and other technology solutions, current systems continue to be unable to operate through attacks. New approaches to tolerating attacks include the use of diversity, redundancy, decentralization, detection and repair of damage. Further, long term research on biological models of tolerating attacks may shed light on the development of these schemes. Due to the global nature of information networks, attacks can be launched from anywhere in the world, and discovering the origin of attacks remains a major difficulty, if, indeed, they are detected at all. In this report we analyze various issues related to need of establishing Critical Infrastructure Protection Centre in India.

Bio:

Dr. Vijayaraghavan did his Masters in Materials Science and Ph.D. in Opto-Magnetic memory development from Indian Institute of Technology, Madras.

He joined DRDO in early seventies and established ab initio an hybrid microelectronics facility while he was in Defence Electronics Research Lab [DLRL], Hyderabad till 1994. Institution of Electronics & Telecommunication Engineers (IETE) awarded the Bapu Seetharam Gold Medal to Dr. Vijayaraghavan and his team for the best R&D effort in the country in the field of Electronics & Telecommunication, in 1993.

After a long stint in DLRL, Dr. Vijayaraghavan moved over to DRDO Headquarters to work with then Scientific Advisor to Defense Minister Dr. Abdul Kalam, as Director (Technology Interface) in order to network institutions and engage in conceptual planning to prepare DRDO in the age of liberalization. During this period he was convener of the team that brought out a document. This document was later evolved into India Millennium Missions 2020 by Dr.Kalam to transform India into a developed nation by the year 2020.

As Adviser, in the Office of the Principal Scientific Adviser [PSA] to the Government of India between 2000-2002, Dr. Vijayaraghavan has initiated a number of national programmes. He was involved intensely with the preparation of the report on Information Security that lead to the birth of India's first Public-Private- Partnership Institution - Society for Electronics Transaction & Security (SETS). Dr.Vijayaraghavan is the founder Executive Director of SETS. At SETS, he lead a team that successfully designed the robust Secrecy System. The President of India Dr.A P J Abdul Kalam presented this system design to ECIL at Rashtrapathi Bhawan on 22nd June 2005.

He is the member of the Information Security Technology Development Board [ISTDB] of the Ministry of Information Technology, Government of India representing SETS. He is also a member of the NASSCOM's National Advisory Board on Information Security and Assurance.

Dr.Vijayaraghavan was extensively involved as a member and also in the preparation of the report 'India as Knowledge Superpower – Strategy for transformation' of the national task force on Knowledge Society constituted by the Prime Minister under the chairmanship of the Deputy Chairman, Union Planning Commission.

He is piloting a unique mission on higher technical education called REACH (Relevance and Excellence in Achieving new heights in educational institutions) for Department of Science & Technology, Government of India. He received the prestigious Seva Rathna Award by The Centenarian Trust, Chennai for his outstanding contributions in the area of Education.

In 2002, Dr. Vijayaraghavan took over as the Chief Executive Officer of the autonomous society SITAR that manufactures VLSI/ASIC devices. Dr.Vijayaraghavan and his team has achieved a milestone by getting ISO 9001-2000 certification for fab. by STQC in 2005.

In 2004, Dr.Vijayaraghavan was appointed by Government of India as a Director of Reserve Bank of India's Bharatiya Reserve Bank Note Mudran Private Limited [BRBNMPL] which is RBI's currency security press operating at Mysore and Salboni, West Bengal.

Dr.Vijayaraghavan has published a number of technical papers in peer-reviewed journals, has guided students for Ph.D and M.Tech degrees and has been Ph.D examiner for a number of Universities/Institutions.

SPEAKER ABSTRACTS AND BIOGRAPHIES

Australia

Dr Paul Ashley

Lead Architect, SOA Advance Technologies
IBM Australia
Email: pashley@au1.ibm.com

Abstract:

Securing Service Oriented Architectures

When experienced security professionals begin to work on Service Oriented Architecture (SOA) based projects, they are typically unaware of what is ahead of them. SOA projects are different from many other types of projects, and the security issues faced are quite unique. To help provide security architects world wide with a framework for securing SOAs, early in 2007 IBM released a redbook titled "Understanding SOA Security Design and Implementation". This redbook outlined an SOA security model describing different security aspects of SOAs and some implementation examples. The presentation will review the IBM SOA security model, and also present by practical example, the security issues faced by the author when securing a number of large SOA security projects world wide.

Bio:

Dr Ashley is Lead Architect for the SOA Advanced Technology Team in Australia/New Zealand, the IBM Software Group worldwide SOA team. In that role, he is supporting the Asia-Pacific South region and his responsibilities include technical responsibility for SOA engagements and contributing to thought leadership in the region. His background covers activities including consulting, solution architecture, application development, systems integration, and information security. He is a regular speaker at industry and academic conferences and publishes regularly.

Dr Ashley has 17 years of Information Technology and Communications experience. His PhD is in Information Security. He has written a book titled Intranet Security, authored an IBM redbook titled Understanding SOA Security Design and Implementation and has written numerous technical papers. He has also filed many patents and received awards at IBM for patent filing and authorship.

Paul works closely with a number of universities being an IBM University Ambassador. He is a member of two university industry advisory boards, guest lectures in security at two universities and supervises postgraduate students. In 2006 he was recognized world wide by IBM for his university contributions.

He also leads the Australia and New Zealand Software Engineering Community within IBM and is a member of the ANZ technical experts council.

Mr Simon Bartlett

BE(Hons), BSc, FIEAust, FAICD, FATSE, CPEng,

Abstract:

Control Systems for Widely Dispersed Electricity Infrastructure

Powerlink Queensland owns and operates the high voltage transmission network throughout Queensland which extends more than 1700 km from Cairns in the north to the NSW border. This includes more than 1200 km of high voltage transmission lines connecting some 100 substations.

The power system is monitored and controlled from a single state wide control centre. The protection and control of this transmission network requires a dedicated high speed telecommunications network and extensive protection and control systems.

This presentation will give an overview of Powerlink's protection and control systems including the choice of technology and requirements to protect this critical infrastructure.

Bio:

Simon Bartlett has 35 years of experience in the Australian, European and North American power generation and transmission industries.

Simon is Powerlink's Chief Operating Officer, responsible for ensuring that the Queensland's electricity transmission network meets Queensland growing needs reliably and efficiently.

This includes the planning, design and construction of more than \$2,600 million of new transmission lines and substations over the next five years. Simon is also responsible for the asset management, operation and maintenance of 12,000 km of transmission lines and 100 substations valued at some \$4 billion, extending from Cairns to the New South Wales border.

Simon is also a Director on the Board of ElectraNet, the privatised South Australian Transmission Business that is 41% owned by Powerlink.

Mr Vishnu Bhat

Chief Operating Officer

Infosys Australia

Email: VishnuGB@infosys.com

Abstract:

Enhancing Security in National Payment Systems

" The world is changing. The world is flattening. Influenced by a few factors – Opening of Emerging Economies, Shifts in global demographics, Ubiquity of Technology and Accountability regulations. What does it mean to do business in this flattening world and address key security concerns ? "

Bio:

Vishnu joined Infosys as a software engineer early in 1993 after working and teaching in the Instrumentation Technology Industry. He quickly progressed to the role of architect for various open systems projects before moving on to manage large complex projects for key Infosys clients around the globe. Vishnu anchored key client relationships in California before assuming responsibility for Infosys' Canada Delivery Operations in 2002 and 2003. Vishnu moved to Australia early 2004 to take over as the Chief Operating Officer for Infosys Australia. He is responsible for all of Infosys Australia's delivery operations including customer delivery, consulting, quality assurance, processes and technology.

Professor Peter R Croll, PhD, FACS, FBCS CITP, CEng.
Faculty of Information Technology
Queensland University of Technology
Email: p.croll@qut.edu.au

Abstract:

Privacy and Security in National e-Health Systems

With the fast developing movement towards e-services in the healthcare sector worldwide there is a need to urgently consider the emerging Privacy and Security issues. Many countries are at a turning point where concerns regarding privacy legislation, standardization and implementation constraints are converging at the same time as the planned introduction of unified electronic healthcare records. Consideration of all aspects of these concerns has taken on an urgent impetus. These developments have acted as a catalyst to launch national symposiums, large-scale projects and government initiatives to move towards promoting some unified solutions to address an area which is proving to be both complex and emotive. The concerns of Privacy and Security are much wider than just the Electronic Health Record as the ubiquitous nature of today's technology also has implications for telehealth, smart homes and assistive technologies, tracking and locating devices, prescription monitoring, healthcare asset management, etc. Evidence has shown that too restrictive an approach to cater for privacy is already raising concerns for the future of medical research studies reliant on secondary use of health data, whereas too much reliance on commodity software solutions is causing a backlash over security concerns. This talk will identify the key privacy and security issues that need to be researched to ensure e-health acceptance which is deemed necessary before widespread adoption at the national level.

Bio:

Peter Croll is a Professor of Software Engineering in the Faculty of Information Technology at QUT, Brisbane. He has recently completed a fellowship with government's research body, CSIRO in support of their National Flagship on Preventative Health to investigate the privacy and security risks associated with electronic health data integration. At QUT, he directs the e-health research group focusing on risk and trust management of health information systems. His previous roles have included the directorships of an ICT research institute and an IT research centre, head of school of IT and Computer Science and an academy director. He is currently a Fellow of both the Australian and the British Computer Societies, a Chartered Engineer, a Chartered IT Professional, a Board Director of the Health Informatics Society of Australia (HISA) Ltd. and the Research Director for the QSHI consortium which focuses on Agedcare ICT. He chairs the national forums HIPS and ehPASS which focus on Health Informatics Privacy and Security.

Mr Richard Czumak

Acting Director, National Information Infrastructure
Critical Infrastructure Protection Branch
Attorney-General's Department
Email: Richard.Czumak@ag.gov.au

Abstract

Australia's Critical Infrastructure Protection Branch Activities

Critical Infrastructure Protection is one element of National Security. Security of the National Information Infrastructure is a key element of Critical Infrastructure Protection. Within Australia the E-Security National Agenda (ESNA) provides a means to achieve this security.

The ESNA was established in 2001 to create a secure, trusted electronic operating environment for both the public and private sectors. It encompasses the main tenets of the Australian approach to E-Security. These are to take a holistic approach, to manage risk and to build security into the infrastructure.

The Attorney-General's Department leads the implementation of ESNA initiatives. This is a "Whole-of-Government" activity with specific agencies focusing their program delivery on

areas in one of three broad segments. The segments are; Government, Industry, Small Business and Home Users.

Funding for ESNA activities has grown steadily since 2000. Some unique capabilities have been developed in this time. Critical Infrastructure Protection Modelling and Analysis (CIPMA) and Computer Network Vulnerability Assessment (CNVA) are two of these.

A review of the ESNA was completed in 2006. It acknowledged continuing change in the online environment, the increasing sophistication of electronic threats and the need for a holistic approach to address these challenges. Additional funding was allocated in the 2007 Federal Budget for the implementation of a range of measures identified in the recommendations of the ESNA review.

Within the Attorney-General's Department this has resulted in the progress of three key initiatives in addition to the ongoing work of Critical Infrastructure Protection Branch. These are an expansion of the Government Computer Emergency Response Team (GovCERT.au), the development of a cyber exercise capability and examination of the feasibility of establishing a business centre for sharing IT security information.

Bio:

Richard is the Assistant Director, National Information Infrastructure, in the Critical Infrastructure Protection Branch of the Australian Attorney-General's Department. In this role he is responsible for the development and implementation of policy related to the Information Infrastructure that underpins national Critical Infrastructure.

He has a background in fixed and mobile Telecommunications and has also been involved with aspects of Electronic Warfare. Richard gained experience in these areas through service ashore and at sea in the Royal Australian Navy. This was followed by work in these fields as a civilian employee with the Australian Department of Defence.

He has also spent time working in state government in the Queensland Department of Primary Industries. This was primarily with the Rural Industry Business Services area of the Department. Through his work in Primary Industries he gained experience with Industry-Government relations and the management of consultancies and Industry-Government partnerships.

Richard received a Bachelor of Information Technology with a major in Computer Software Development from the University of Southern Queensland in 2001. During his service with the Royal Australian Navy he was awarded an Associate Diploma in Telecommunications. More recently he has completed the Government sponsored Public Sector Management Program. Successful completion of the program was marked by the award of a Graduate Certificate in Public Sector Leadership from Griffith University.

Mr Grae Meyer-Gleaves

Information and Communication Technology (ICT) Services

Data #3

Email: Grae.Meyer-Gleaves@data3.com.au

Abstract:

Next Generation Security Management and Optimisation

Managing and optimisation of information security infrastructure is a challenge for all organisations. There are more than seven layers to the OSI model in the real world and your organisation will not realise benefits without investment in all layers.

In this presentation, Grae will explore some of the information security management issues faced by organisations in the past, present and into potentially in the future. Grae will expose some of the next generation solutions and talk about how organisations could leverage some expected benefits.

Bio:

Grae Meyer-Gleaves is an information security professional with skills in management, consulting, architecture and engineering. He began his career in information security whilst working as part of specialist unit which installed and maintained the Australian Defence Force secure communications network for Queensland.

Grae has an extensive background in managing, designing, installing, architecting and implementing secure information systems. He has worked in a number of different industry sectors including defence, banking and finance, government, mining and retail. He has been working in ICT for well over a decade. Grae has previously managed the Data#3 security practice in Queensland and is now a service delivery manager. He also holds a number of certifications, including the CISSP.

Dr John Harrison

iDivision

Brisbane City Council

Email: John.Harrison@brisbane.qld.gov.au

Abstract:

Information Security Management in the Public Service

This presentation addresses information security issues confronting those in the public service. A range of practical security issues that confront larger organisations are raised, and very briefly discussed, from a local government perspective. Some of these issues include ICT architecture, security product vendors, threats, governance and disaster recovery. Suggestions are offered as to how to better manage information security delivery in the context of rapid technological change, growing citizen and business expectations, and the dynamically changing threat environment.

Bio:

John is currently responsible for ICT risk and security management across Brisbane City Council. Prior to BCC, he provided ICT risk, security and SOX compliance advice to two large US corporations, namely the Las Vegas Sands (NYSE:LVS) and Ameristar Casinos (NASDAQ:ASCA). He also served as Deputy Director of the Center for Cybersecurity Research at the University of Nevada (USA).

In previous lives John was a system architect for a Silicon Valley company that developed network-based scheduling, distribution and billing systems for digital advertising networks. He led the development of an information system reengineering product for Oracle Corporation and conducted computer science research at the University of Queensland. John holds a PhD in Computer Science from Arizona State University (USA) and is currently pursuing the Juris Doctor degree at the TC Beirne School of Law (Qld).

Dr Adrian McCullagh

Special Counsel

Phillips Fox, Lawyers

Email: a.mccullagh@qut.edu.au

Abstract:

Electronic Government Commercialisation of Information in a Federated System

Governments globally have for the last 20 years been slowly migrating the delivery of many of their services to an electronic service delivery model. This process has been relatively slow in coming principally due to certain restrictions such as PC deployment and telecommunication speed. With the advancement of broadband deployment many governments are now being forced to accelerate their e-government strategies which has in turn caused these governments to re-evaluate the type of information they need to deliver to

their respective citizens, the security frameworks required and the archiving structure to preserve the information that has been delivered electronically. This has also resulted in the development of legal frameworks to manage the resultant liability that can arise from the publication of information.

Bio:

Adrian McCullagh has degrees in Computer Science and Law and has a PhD in IT Security. He has written a number of academic referred papers that have been published in the United States, United Kingdom and Australia. His principal research interests are digital signature technology, digital rights management and conflicts of trust from a legal social perspective. His most recent publication is in the Oxford International Journal for Law and Technology in the area of identity theft which is becoming a global issue in the 21st century.

Mr Chris Marsden

*Director, Critical Infrastructure Security
Security Branch
Department of Communications, IT and Arts (DICTA)
Email: Chris.Marsden@dcita.gov.au*

Abstract:

E-Security: Safeguarding National Information Systems

Australia's National Information Systems are an important subset of the national critical infrastructure. They consist of the electronic systems and infrastructure that underpin critical services such as telecommunications, transport and distribution, energy and utilities and banking and finance. The security of these systems is a priority for the Australian Government.

The changing nature of the online environment has led to the Australian Government reviewing its e-security policy framework, the E-Security National Agenda, and supporting the efforts of critical infrastructure owners and operators to adequately secure their assets through the Trusted Information Sharing Network (TISN).

Strong business-government collaboration, cooperative arrangements with industry, law enforcement, the education of home users and small business about e-security issues, international collaboration and research and development are all important steps being taken to secure Australia's national information systems.

Bio:

Chris Marsden is currently the Director of the Critical Infrastructure Security Section within the Security Branch of the Department of Communications, Information Technology and the Arts. He has been in this role since the beginning of April 2006. Previously, Chris had 11 years in senior management roles within the ATO dealing with the integrity of the Tax File Number database and high risk refunds.

In his current role, Chris provides the secretariat and project management support to two Advisory Groups within the Australian Government's Trusted Information Sharing Network. These groups are the Communications Sector Infrastructure Assurance Advisory Group and the IT Security Expert Advisory Group. Under the latter, Chris' section provides the Secretariat to the SCADA Community of Interest which recently completed a series of workshops in five capital cities earlier this month.

In early May 2007, Chris led the Australian participation at the Idaho National Laboratories' International SCADA Workshop in Idaho Falls

Mr Walter Williams
Chief Risk Officer, Risk Unit
Queensland Rail
Email: Walter.Williams@qr.com.au

Abstract:
Security Issues in Queensland Rail

With ever growing cities being so dependant on efficient transport networks for moving people and freight the dedicated information technology networks used by transport operators have become a critical point of failure in managing both day to day operations and crisis response.

Walter's presentation will provide an overview of surface transport security issues in the context of information technology security and then review some of the corporate strategies and practices for security, emergency management, and business continuity management that assist QR's managers to fully carry out their responsibility to protect QR's tangible and intangible assets against compromise on a national basis as part of QR's total asset management policy.

Bio:
Walter joined Queensland Rail (QR) in January 2002 after 30 years in both the public and private sectors in Australia and overseas. Walter's career specialities are security, business continuity and emergency management, and he has held senior and executive management positions in diverse organisations such as Australia Post, the Office of The Ombudsman, the Defence Department and the Family Court of Australia.

Prior to joining QR Walter was the Security and Safety Director Asia Pacific Region for a large multi-national company and worked in places as far apart as New York, USA; Tokyo, Japan; and Bangalore, India.

Walter is a graduate of the Officer Cadet School, Portsea, and Mitchell College, and holds a number of undergraduate and postgraduate qualifications in both security management and risk management.

Walter is an Associate Fellow of the Risk Management Institution of Australasia and across the broader rail industry he chairs the national Rail Trusted Information Sharing Network, the Australasian Railway Association Security Working Group, and was recently elected as Vice Chairman of the Security Commission of the International Union for Passenger Transport (the UITP) based in Brussels.

Professor Vijay Varadharajan
Microsoft Chair for Innovation in Computing
Macquarie University
Email: vijay@ics.mq.edu.au

Abstract:
Security in Mobile Systems

Security issues play a significant role in the pervasive mobile distributed computing environment, where useful information and services being delivered to users using mobile software agents and large scale distributed applications over wired and wireless networks using a range of mobile devices. In this talk, we will address some of the security challenges posed in a mobile distributed environment and then describe an approach to developing a trust enhanced secure mobile agent based software systems. We will discuss the design choices and describe security architecture and show it has been used to develop secure distributed applications.

Bio:

Vijay Varadharajan is the Microsoft Chair and Professor of Computing at Macquarie University, and he is also the Director of Information and Networked System Security Research. He is the Australian Delegate at the IFIP Technical Committee on Security and is the Chair of the ACS Security Committee. He sits on several editorial boards of International Journals and advisory boards of several companies, including Microsoft Trustworthy Computing Academic Advisory Board (TCAAB). He is a Fellow of the British Computer Society (FBCS), a Fellow of the IEE (FIEE), a Fellow of the IMA (FIMA), a Fellow of the Australian Institute of Engineers (FIEAust), and a Fellow of the Australian Computer Society (FACS).

APPENDICIES

Australian Scholarships

The Australian Government offers a variety of awards that can support research studies and exchanges, faculty exchanges and professional development under the Australia Scholarships Program. With respect to research collaboration and exchanges between India and Australia, the Leaderships Awards (administered by the Australian Government's Agency, AusAID and the Endeavour Awards (administered by the Department of Education, Science and Training, DEST)are particularly relevant.

The website is:

www.australianscholarships.gov.au

The Endeavour Programme is an Australian government initiative, bringing together under one umbrella all of the Department of Education, Science and Training's international scholarships. The objective is to establish the Endeavour awards as a prestigious scholarship programme that showcase the excellence of Australia's education and research sector. The awards will enable scholars and professionals to undertake study, research or professional development in Australia and allow Australians to do the same abroad. This latter aspect is noteworthy, since the Awards enable Australian to come to India for research and related professional activities. These Awards offer new opportunities for fully-funded exchange visits that can do much for stimulating research cooperation between research groups in Australia and India. The Endeavour website lists the awards for India:

http://www.endeavour.dest.gov.au/awards_by_country/for_internationals/for_asian_applicants/

Of particular interest to the research communities are the Endeavour Postgraduate Awards, Research Fellowships and Executive Awards,. The applications for these are submitted on-line to DEST in Canberra.

The Endeavour Postgraduate Awards provide full financial support for international students for up to 3 years to undertake a postgraduate qualification at a Masters or PhD level either by coursework or research in any field of study in Australia

The Endeavour Research Fellowships enable top rate Indian researchers to carry out short-term (4-6 months) postgraduate or post-doctoral research in Australia in any field of study, and for Australians to do the same in India

The Endeavour Executive Awards allow high achieving professionals from India in government, business, and industry or education sector to undertake a professional development opportunity for up to 4 months at a counterpart institution/organisation in Australia, and for Australians to do the same in India.

Australia-India Strategic Research Fund Overview

The Australian Government in conjunction with the Government of India has established the **Australia-India Strategic Research Fund** for scientific and technological cooperation with a commitment of \$20 million over 5 years from Australia and with matching funding from India. The **Australia-India Strategic Research Fund** is jointly managed by the Australian Government's Department of Education, Science and Training (DEST) and the Indian Government's Department of Science and Technology (DST) and the Department of Biotechnology (DBT). The funding will be provided over five years commencing in FY 2006/07 for collaborative research activities between Australia and India through the AISRF.

The AISRF comprises three components:

1. Indo-Australian Science & Technology Fund
2. Indo-Australian Biotechnology Fund
3. Targeted Allocations

The Indo-Australian Science & Technology Fund and the Indo-Australian Biotechnology Fund provide funding support for collaborative research activities and workshops.

Targeted Allocations promotes effective research collaboration by providing a vehicle for the Australian Government to establish strategic links and relationships with Indian counterparts.

The Indo-Australian Science & Technology Fund is a bilateral fund and applicants must apply for funding to support collaboration between Australian and Indian partners. Each Australian applicant must have an Indian 'partner' and each partner must submit an application to their respective government. Australian applicants must apply to the DEST and Indians to DST/DBT respectively.

For further details please visit us on <https://sciencegrants.dest.gov.au/aisrf>

Or

Contact

Ms Shweta Datt
Science Specialist
Australian High Commission
1/50 G, Shantipath,
Chanakyapuri
New Delhi – 110021
Tel : +91 11 41494312
Fax : +91 11 26873172
E-mail : shweta.datt@aei.gov.au