

## **Submission for E-Security Review 2008**

### **1. Introduction**

First I applaud this whole of government E-Security Review initiative being conducted by the Attorney General and the Minister for Broadband, Communications and the Digital Economy. Not only this Review is timely in the context of E-Security but also its comprehensive nature makes the scope of this initiative unique and hence the outcomes even more useful and their potential impact that much greater.

It is clear that the Internet is transforming the way we live and the recent decades have witnessed dramatic developments in information and communication technologies (ICT). Along with the phenomenal growth in technology enabled information economy has been a growth in computing technology related crimes. *These are posing not only significant technological challenges in the development and deployment of secure, trustworthy and dependable systems and services but also in the areas of policies – how to keep them up to-date and manage them, apply them across different business segments and jurisdictions as well as across international boundaries.* There is a clear need to build and maintain confidence on the infrastructures and systems among the different stakeholders such as ordinary end users, SME as well as corporate organizations. In this regard, the government has a critical role to play in developing research and education programs to address the emerging security challenges and helping to maintain an overall secure information infrastructure ecosystem for society and business. The security challenges we believe are multi-faceted involving technological, business as well as legal aspects. Hence there is a clear need for the new framework to explicitly address this multi-faceted nature of security.

### **2. E-Security Challenges**

It is not an overstatement to say that the information and communication technologies have become pervasive. We have been witnessing convergence of many technologies over the last several years. Though it has been talked about for many years now (since late 80s and early 90s), this is actually happening now and will continue to do in the future. We are seeing pervasive infrastructures involving wired (fixed), wireless, mobile, peer to peer networks, small devices from PDAs to embedded systems and smart phones to large scale grid computing and cluster computing systems, large scale distributed information systems and databases to distributed and mobile applications and services. These are changing the way the people work, behave and live their lives (cf. social networking and online businesses). Given these dramatic developments in technologies affecting our businesses and society, security issues have become even more significant. Here it is critical to note that *security itself is pervasive*. It is there in every part of the technology spectrum, be it hardware, operating systems, middleware, wired and wireless and mobile networks, databases, applications and users. It is in every business such as telecommunications, healthcare, transportation and environment management. It is this pervasive nature of security which makes the design of large scale secure systems and infrastructures highly complex. In terms of addressing these challenges, it is worth emphasizing that in order to secure a technology (e.g. database or broadband network), one should first understand the technology before we

can secure it. Though this may seem obvious but often security flaws are introduced due to this simple oversight. In turn, this has some important consequences in formulating the framework. For instance, if a system has multiple technologies, there is a need to understand and secure each of these technologies. Take for instance, even a simple PC which has hardware, operating system, middleware layer, applications and users, we need to look at security of each of these technologies.

This brings us to the next point. Major security technology challenges in the future (and even now) arise due to the *systems nature* (or even *systems of systems* in nature). No problems nowadays come in self-contained neat packages. Take for instance a healthcare system or a transportation system or a telecommunication system. These are all systems of systems with multiple technologies having different policies and different administrative authorities having jurisdictions. So there needs to be greater focus given to security in systems (or systems of systems) involving networks, distributed systems and applications as mentioned above. Incidentally this is equally important when it comes to evaluation and accreditation of secure systems (e.g. in the defense arena). There is a necessity to be able to evaluate and guarantee the security properties (or other otherwise) and provide assurance of a large scale system (that it will do what it claims to do and does not do anything else).

Then there is the issue of dynamic nature of security threats (and security requirements) and the need to develop methods and effective mechanisms to counteract them. This changing nature of threats problem gets aggravated given the systems issue mentioned above. Dynamic nature of security threats can occur in any of the technologies mentioned above such as wireless security, 24/7 connected broadband security, web services security and peer to peer distributed application security. Furthermore it is not just the technology but also how they are being used by different people. For instance, security attacks happen due to the way users use the services and applications such as online banking and electronic patient records. There are different types of users such as individual ordinary home users to tech savvy users to SME to corporations to governments. Similarly attackers can range from individual hackers to hacker networks to corporate espionage to organized crime to state sponsored information warfare. So we have what I call “increasing threat velocity” with more and more vulnerabilities and attacks in different types of technologies in networked distributed systems, an evolving set of bad guys, attacks happening sooner and faster (with less and less grace period) and increasingly sophisticated attacks using easily available tools. This the environment we are dealing with and we need the framework to provide programs and initiatives, in the areas of research and development, educations and skills, policy and governance, partnership and collaboration, to address them. Hence we make the following recommendations.

### **Recommendation 1**

Given the dramatic developments in technology, recognizing that security is pervasive and the need to adopt a systems approach to address security challenges and to counteract the dynamic nature of threats, we make the following recommendation:

- *The framework develop and support programs that address e-security issues in systems, networks infrastructures and distributed applications and the development of policies for their secure management and deployment in different business segments and government agencies.*

- *Establish specific government programs and funds to support research activities in the E-Security areas mentioned below.*

In particular, we would like to suggest that this framework emphasize and support initiatives and programs that address the following specific areas below. These areas are in my view important not only from the point of view of technological trends, but also from the view point of protecting systems and infrastructures and maintaining Australia's competitive edge in the international context. These areas highlight the important emerging threats in the changing E-Security landscape and are significant from the point of view of R&D in E-Security in Australia.

### **Recommendation 1.1**

#### **Specific Emerging R&D Issues and Programs in E-Security for Australia**

- **Large Scale Secure Distributed Systems and Services:** With the developments in technology and communications over the next decades, the mobile distributed pervasive computing infrastructure could lead to billions of information appliances connected to wired and wireless infrastructure with numerous applications and huge number of users. We are not equipped to deal with large scales at present. We need to understand better how to design large scale secure systems and services and manage them in a dynamic environment. Topics include:
  - Dynamic policy based secure distributed systems and networked applications
  - Designing and building systems with desired properties such as security, trust and integrity
  - Distributed Identity and Privilege Management
  - Secure Service Oriented Architectures and Distributed Virtualization Systems
  - Secure Distributed Applications such as Internet Voting and E Commerce
- **Counteracting Epidemic-style Security Attacks Security Attacks and Intrusions:** There is a clear need to understand better, detect, monitor and develop techniques and mechanisms to counteract epidemic attacks such as DDoS, botnets, malware, virus, spam etc. in heterogeneous broadband network infrastructures.
  - Distributed Denial of Service Attacks, Phishing, Spam in wireless, mobile and IP networks
  - Protection of Critical Information Infrastructures and Applications
- **Mobile Software and Security in New Generation Networked Systems:** Movement of mobile code and content to achieve the deployment of services and applications as well as distributing content is becoming prevalent in the pervasive new generation networked computing environment. This raises a range of issues including protection and transfer of privileges and their attachment to content, protection of software and content over the network, and the secure management of privileges and their policies.
  - Security of mobile software in a network environment with malicious hosts
  - Security of mobile applications
- **Wireless Mobile Networks and Security:** Increasingly wireless mobile ad hoc networks and sensor networks are emerging as a new tier in the information network infrastructure ecosystem. Such networks poses some unique security challenges due to their decentralized management, limited

computational capability, dynamic network connectivity, ad hoc mobility and physical vulnerability and susceptibility of wireless communications.

- Securing dynamic mobile ad hoc networks and sensor networks
- Securing mobile applications and services over such mobile ad hoc and sensor networks
- ***Trusted Computing*** : Many of the security challenges proposed above form part of this and it is clear that without “trust” (whichever way one defines it), it would be difficult if not impossible to achieve security. Much depends upon developing models, mechanisms and tools to create and manage trust between unfamiliar entities over the Internet for enabling them to trade and interact in a secure manner. Hence under this banner, a range of topics need to be addressed from trusted operating systems to trusted applications to trusted networks to trusted hardware. Topics include:
  - Trusted Identity Management over the Internet
  - Trusted Platforms such as computers and mobile devices
  - Trust Enhanced Secure Peer to Peer Systems and Applications
  - Trust Management in Web Services and Online Communities
- ***Security and Risk Management in Future New Generation Information Architectures***: We are likely to see the growth in distributed virtual enterprises that are not only geographically separated but also dynamic, in the sense that they exist for a period of time and disband and reform again with different characteristics. There will be an increase in ad hoc peer to peer applications and new convergent networks. We will need to anticipate new threats in these emerging new generation networks and applications and analyse risks and develop security baselines and security policy management. For these distributed virtual organizations and new generation infrastructures and networks, we need to understand better the formulation of security policies, quantification of risks and their management as well as their implementation and monitoring.
  - Security baselines for New Generation Information Infrastructures and Networks
  - Security and Risk Management in Peer to Peer Applications and Virtual Enterprises

### **Information and Networked Systems Security Research, Macquarie University (INSS@MQ)**

At our Information and Networked Systems Security Research centre at Macquarie University (INSS@MQ), we carry out a range of research projects addressing several of the above challenges in Distributed System Security, Network Security, Wireless and Mobile Security, Secure Software, Trustworthy Computing, Secure Peer to Peer Applications and Virtual Enterprises, Secure ECommerce, Security Policies, Security Architectures, Formal Security Models and Analysis. (See [www.comp.mq.edu.au/research/inss](http://www.comp.mq.edu.au/research/inss)).

### **3. E-Security Education, Skills and Expertise**

In the context of the above technological challenges and their impact on the economy, it is critical for the framework to address the issue of E-Security education skills and expertise. In this context, it is important to note that it is in the systems areas (see above Section 2) where there is a shortage of expertise and lack of skills in the Australian scene. It is in these areas where there are significant challenges as mentioned above and where there are supply gap. Hence it is in these emerging systems and networks areas, the

research and education capacity needs to be increased (and NOT in the mathematical crypto-algorithm aspects).

### **Recommendation 2**

*Enhance the capacity and capability of Universities and Education Sector to educate, to do research and to train security professionals especially in the systems and networks areas mentioned above (cf. Section 2) where there are significant gaps and shortages in the Australian scene.*

*Develop schemes to increase these security skills and education in the market. Schemes should be designed both to attract and retain the pool of staff with the right expertise as well as increasing the number of people (e.g. students and employees) being educated and trained.*

**Specific measures for addressing Security Education and Training in Australia include the following:**

#### **Recommendation 2.1**

- *Develop schemes to support to Security Courses and Programs in the targeted areas by
  - *Providing funds to University (Depts/Schools/Groups) to develop appropriate information security and assurance programs targeted at aspects described in Section 2 above**
- *Increase the pool of suitably trained information security professionals by
  - *Providing financial support to University (Depts/Schools/Groups) in terms of scholarships for undergraduate, postgraduate and research students in information security and assurance**
- *Develop research programs in the areas mentioned above by
  - *Establishing government programs and funds to support information security research outlined in Section 2 above.*
  - *Offering partnership programs for academic staff and students to work with government agencies involved in security**
- *Attract and retain staff with security expertise in the education sector by
  - *Providing financial support to University (Depts/Schools/Groups) to recruit and retain staff with security expertise and skills in these areas**

#### **4. E-Security as a Key Mainstream Activity in Government Programs**

One of the unique aspects of security is that it permeates many parts of the economy be they telecommunications, finance, healthcare, education, defense or transportation and this will continue to increase in the future. Security has the potential to disrupt economies (and even potentially causing reduction in the sovereignty of countries). Given this pervasive nature, it is important that security considerations should form a core part of the decision making and governance of all parts of the government. Hence it is timely and appropriate to consider an overarching organization that can coordinate and oversee the critical security issues affecting the various agencies and departments in the

government. At the same time, there is a need to strengthen the units/branch within each of the government agencies which are responsible for security issues within that organization.

### **Recommendation 3**

*This recommendation has 2 parts in terms of organization structure to support E-Security activities and programs in the government.*

- *Establish an overarching organization at the highest level in the government with the responsibility to oversee, coordinate and align the E-Security priorities across various agencies and departments in the government. Such an organization will also have the ability to be more proactive and respond better when it comes to dynamic changes in the security threats.*
- *Strengthen the individual security units and branches within each of the government agencies which are responsible for security issues within that agency and empower them to work cooperatively with the overarching organization proposed above.*
- *Create an external advisory board (to the government) with representatives from various external stakeholder organizations, especially with people who have expertise and experience in the emerging security technology areas outlined above in Section 2. Past experience indicates such an external advisory board is highly valuable in anticipating emerging issues and helping to determine strategic priorities.*

### **5. E-Security and Partnerships**

Given the dynamic nature of security threats and the need to develop up to date security countermeasures, partnerships between industry, academia and government are critical. In particular, in Australia, there is a clear need to enhance and develop government programs that encourages both research and development as well as education partnerships between industry and academia leading to relevant security solutions (e.g. such as those identified in Section 2) and educational courses and degrees in system and network security (as mentioned in Section 3). In this regard, programs such as the Research Support against Counter Terrorism (administered by the Dept of PMC) as well as the Infosec programs of the DSD are deserve support and expansion. We have participated in both these programs over the recent years (in projects such as denial of service attacks and networked system security) and found them to be highly productive and relevant, focusing on the types of problems that really need to be addressed in the security space. I would strongly recommend the continuation and further enhancement of such programs which are highly beneficial to the government agencies as well as to the industry and user community at large. In this context, I would also encourage establishment of programs and mechanisms that would enable agencies such as DSTO, DBCDE and AG to nurture partnerships with both academia and industry. The setting up of the overarching organization in Recommendation 3 with membership from a range of government agencies will be highly beneficial to develop such partnerships. The global nature of security issues makes international collaboration and cooperation particularly significant.

At our Information and Networked Systems Security Research centre at Macquarie University (INSS@MQ), we have research collaboration and partnership with a range of industrial and academic institutions such as Microsoft (US, Asia, UK, Australia), Hewlett-Packard (US), INRIA/LORIA Research Labs (France), British Prof. Vijay Varadharajan

Telecom Labs (UK), Indian Inst of Science and Technology (India), Chinese Academy of Sciences (China) and Infocom Research (Singapore), Defense Signals Directorate and the Dept of PMC (Australia).

#### **Recommendation 4**

*Develop specific government initiatives and programs that establish and enhance research and development programs in the area of new generation networked systems and broadband security*

- *between government agencies and academia in Australia  
(e.g. establish specific research partnership programs enabling collaboration between government agencies and academia in targeted areas in security)*
- *between industry and academia in Australia  
(e.g. provide research funds to academia and industry to form joint projects in relevant targeted areas in security mentioned above)*
- *between Australian academic institutions and international institutions  
(e.g. provide support for Australian academic institutions to participate in EU 7<sup>th</sup> Framework and OECD Programmes)*

#### **Concluding Remarks**

We are thankful to the Dept of the Attorney General and the Dept of Minister for Broadband, Communications and the Digital Economy for giving us the opportunity to provide inputs to this important E-Security Review.

We hope that our comments and recommendations will be of some help to the Review Committee in its deliberations.

Looking forward to hearing the outcomes of the Review in due course

Best Regards

Vijay Varadharajan FIEE, FACS, FIEAust, FBCS, FIMA

Professor and Microsoft Chair in Innovation in Computing  
Director of Information and Networked Systems Security Research (INSS)  
Dept of Computing, Macquarie University, Australia

Email: [vijay@ics.mq.edu.au](mailto:vijay@ics.mq.edu.au)

Tel: +61 2 9850 9534

Fax: +61 2 9850 9511