INDUSTRY AND COMMUNITY IMPACT – Vijay Varadharajan (in chronological order)

- **X.509** and **ISO Security Architecture 7498-2 Standards:** As part of my work at British Telecom, contributed to the development of major security standards X.509 and ISO Security Architecture 7498-2. Both these standards have been used in the industry in the development of many commercial security products over the last 30 years (1987-1988).
- **Secure Key Management and Encryption – Hewlett-Packard Security Products**: My work on encryption and secure key management integrated with smart cards in collaboration with Gemplus and implemented into HP Server products. Major customer for this secure server product was financial organizations such as SIA Banking Authority, Italy (1989-1990).
- **UK Security Evaluation Criteria**: One of 20 people in the UK invited to contribute to the development of Commercial Computer Security Evaluation Criteria (CCSC) (then called UK Green Book) as part of the UK Govt Dept of Trade and Industry initiative. This work subsequently formed part of the European Union Security Criteria (ITSEC) and currently forms part of Common Criteria (1989-1992).
- **Secure HP-UX Systems – Hewlett-Packard Security Products:** My work on formal modelling of security properties and their verification were used in the development of high assurance of HP Unix System products by the HP Federal Systems Organization. These products were evaluated at B1 level by the US Dept of Defence (1989-1991).
- **Open Software Foundation DCE Security:** My work on proxy and delegation protocols in inter-domain distributed system environment was adopted by Hewlett-Packard and Open Software Foundation in their product offerings of Distributed Computing Environment (DCE) platform (1989-1991).
- **Secure Bridge and Router – Hewlett-Packard Security Products:** My work on security mechanisms for local area and broadband networks were deployed in HP secure bridge and router products for LANs, SMDS and Frame Relay networks. My team and I were the first to design and demonstrate a complete secure LAN-MAN network system implementing the IEEE 802.10 security architecture between Bristol, UK and Palo Alto, USA (1989-1992). This work led also led to significant contributions to the development of IEEE 802.10 security standard. The financial impact was of the order of $100 to $200 million dollars of revenue for Hewlett-Packard (HP Roseville and Corvallis Network Divisions, USA).
- **Distributed Authorization – Hewlett-Packard Praesidium Security Products**: I was the Chief Architect of the Distributed Systems Security Research at Hewlett-Packard, which led to a major commercial security product on Distributed Authorization. My research work (1990-1994) led to the development of Hewlett-Packard Praesidium Authorization Server, which generated around a billion dollars in annual revenue for Hewlett-Packard for some 5 years (1995-2000). Major customers of Praesidium Authorization Server include Citicorp, Commerce Bank and Credit Bank. HP Praesidium won the Most Innovative Security Product Award, Security Magazine, London, 2000.
- **Creation of a New Hewlett-Packard Product Division:** As the Praesidium system drew on resources from multiple divisions in the HP organization (operating systems, networks, middleware, professional services and others), it cried out for the creation of a new program. With the support of the Senior Vice President, a new program called the Early Adopter Program was created in 1991 and the Praesidium Authorization System was developed with both HP, an external third party (Locus Software Systems, Los Angeles) and HP customer Citicorp. ***As the Praesidium product turned out to be highly successful, HP created a new product Division called Cooperative Computing Systems Division (CCSY) (1993)*** with all the associated functions such as development, marketing and sales, and employing around 100 people.
- **Audit Management Tool for Networked Systems – Hewlett-Packard Security Products:** My work on security mechanisms and management of networked Unix systems (called Sherlock) was integrated HP OpenView and HP Admin Centre and Operation Centre platform products. This work developed a secure agent and manager model and architecture enabling security auditing management of networked HP-Unix systems. Major customers include Proctor and Gamble Corporation (1992-1994). The financial impact was of the order of $100 million dollars of revenue for Hewlett-Packard (HP UX and Professional Services Organization, USA).
- **Telecom Network Authentication Centre – Hewlett-Packard Security Products:** My work on the design of authentication centre for mobile networks and secure inter-cell authentication protocols between home and visiting location authorities in 2G/3G networks were deployed into HP Authentication Centre (AuC) product. Major customers for HP AuC product included Italian Telecom (1991-1995), generating tens of millions of dollars for Hewlett-Packard.

- **Secure Mobile Appliance - Hewlett-Packard Security Products:** My work on secure remote authentication and dynamic key management protocol for mobile appliances (such as laptops) was patented by Hewlett-Packard in 1995. This patent has become more relevant in the recent times in the context of Covid-19.
- **Co-founded the Australasian Conference on Information Security and Privacy (ACISP)** – 1996: I was one of the co-founders of the successful ACISP in 1996 with Professors Seberry, Caelli and Pieprzyk. ACISP is in its 25th year in 2020 and is still going strong.
- **Distributed Denial of Service (DDoS) Attacks:** My work on Distributed Denial of Service attacks (2001-2003) proposed novel and practical techniques for counteracting DDoS attacks on the Internet. Our team was the first to demonstrate these techniques in a practical Internet environment in 2003-2004 and were shown to be more efficient than others known at the time. Locally this work attracted attention in the Australian media in The Australian, The Sydney Morning Herald and the Financial Review during 2003-2005.
- **Established Joint Microsoft NICTA Research Centre in Trustworthy Computing (2004-2006)**: As Microsoft Chair Professor, conceived the idea of establishing a Microsoft Research Centre in Security and Trustworthy Computing at Sydney, Australia. Worked with Microsoft Australia, Microsoft Research Cambridge, UK, Microsoft Redmond, US and Microsoft Research Asia, Beijing to develop the Research Centre. Established the joint Microsoft NICTA Research Centre in Trustworthy Computing with $1M support from Microsoft and an equal amount of funding from NICTA. Board Member and Director of Microsoft NICTA Research Centre (April 2005 - Dec 2006).
- **Mobile Ad hoc Networks (MANET) Security**: The Defence Science Technology Organization (DSTO) Australia found our comprehensive framework to securing MANETs to be significantly valuable for their MANET operations after a thorough evaluation in 2006-07. Our multi-dimensional MANET security framework achieved detection/reaction to security attacks, a dynamic fellowship and reputation-based trust model, and prevention and enforcement of secure MANET routing with dynamic decentralised key management.
- **Web Services Authorization Architecture**: The work on authorization for service-oriented architectures led to the development of web services authorization architecture (WSAA) layer on top of the web services security layer. The WSAA layer provided the flexibility for supporting multiple types of authorization policies and mechanisms. WSAA was integrated with Microsoft's .NET environment and was used to demonstrate a comprehensive solution to securing electronic patient records in a distributed system (2003-2006). The technologies providing conditional and joint authorization were transferred to Microsoft ACL Manager Product Group. Was awarded Microsoft Trustworthy Computing Award for this work (2006).
- **Trust Enhanced Security Paradigm**: Coined the notion of “trust enhanced security" referring using trust model to enhance the quality of secure decision making, such as an authorization decision or a routing decision. In particular, the trust model captured both hard trust characteristics (such as certificates and credentials) and soft trust characteristics (such as reputation and social trust parameters). Our work demonstrated how such a hybrid trust model can improve the security evaluation decisions in different contexts such as mobile agents (at the application level), mobile network ad hoc routing (at the network level), and computing platforms (at the system level). This new paradigm and its applications formed the basis for several keynotes in international conferences and industry forums during 2005-2010.
- **TrustLite Architecture:** Our work on the design of lightweight trusted security architecture, TrustLite, was patented by Intel Corporation and being used in their low-cost embedded system products (2010-2014).
- **Cloud Data Security**: The work on Role Based Encryption (RBE) enabling policy driven access to encrypted electronic health patient records in the cloud received the Runner Up EUREKA Prize *for Outstanding Science in Safeguarding Australia in 2013.* The RBE theoretical framework also obtained the prestigious Wilkes Award 2011 from The Computer Journal, UK (named after Sir Maurice Wilkes, Cambridge University).
- **Founded Optus-Macquarie Cyber Security Hub (Sept 2014 – June 2016)**: Conceived and founded the Cyber Security Institute/Hub at MQ – Sept 2014. Worked to bring together aspects of Cyber Security from Computing and Information Technology (Faculty of Science and Engineering), Business Risk Management (Faculty of Business and Economics) and Policing and Counterterrorism (Faculty of Arts) – May 2015 to Nov 2015. Obtained the support of Senior Execs at Singtel/Optus in Cyber Security Strategy Nov 2014 – Feb 2015. Presentation to University Executive of the Cyber Security Hub initiative and obtained their support - Nov 2015. Worked to establish the Cyber Security Hub – 27 May 2016 (with $5M from Optus and an equal amount from Macquarie University)
- **Software Defined Networks (SDN) Security**: Our work on policy-based security architecture for Software-Defined Networks was selected by the IEEE Signal Processing Society’s as Top 25 downloaded articles in 2018-2019 in the *IEEE Transactions on Information Forensics and Security* on IEEE *Xplore®*.