

## **Invited Keynote Speech one:**

### **Trust Enhanced Security**

**Professor Vijay Varadharajan**  
**Macquarie University, Australia**

#### Abstract

The notion of trust has been around for many decades (if not for centuries) in different disciplines in different disguises. In particular, the concept of trust has been studied extensively in various disciplines such as psychology, philosophy, economics, sociology as well as in technology. Yet we do not have a clear handle on this concept of trust which is increasingly becoming significant in our information economy and the Internet world. It is often quoted (and probably correctly) that trust is a key foundation stone of the information security world. In security, the concept of trusted systems has at least been around publicly for some 25 years and more recently “trustworthy computing” has taken a centre stage, with the launch of major initiatives in trustworthy computing by several major players in the information technology arena. In this talk, we will take a look at the concept of trust in the secure computing world and see some of the challenges and pitfalls involved. We will try to extract some fundamental issues in trust that could help in the design of secure systems in a pervasive computing environment. We will then introduce the notion of “trust enhanced security” and discuss how such a paradigm can be used to develop secure distributed systems and applications.

#### Short Biography

Vijay Varadharajan is the Microsoft Chair and Professor of Computing at Macquarie University. He is also the Director of Information and Networked System Security Research. Previous to this, he was the Foundation Chair Professor and Head of School of Computing and IT at UWS Nepean. Prior to taking up this appointment, he was responsible for Security Research at Corporate Hewlett-Packard Labs based at HP Labs Europe in Bristol, UK, for a number of years. He has published more than 260 papers in International Journals and Conferences and has co-authored and edited 8 books on Security, Networks and Distributed Systems. His current research interests are in distributed system security, network security, mobile agent security, trusted computing and secure peer to peer applications. He is on the Editorial Board of several journals including the ACM Transactions on Information System Security and The International Journal of Information Security (Springer). He has been a member of the Board of Advisors in Trusted Computing Platform Association (TCPA) (USA) and is on the Microsoft Trustworthy Computing Advisory Board (USA). He has held several invited Visiting Professorships including INRIA Research Labs (France), British Telecom Labs (UK), Chinese Academy of Sciences, Institute of Mathematical Sciences (NUS, Singapore), Indian Institute of Sciences as well as Visiting Senior Research Scientist at Microsoft Research Cambridge, UK. 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.

## **Invited Keynote Speech Two:**

### **Scalable Authentication Techniques Compatible With Modern Multimedia Coding Standards**

**Professor Robert H. Deng**  
**Singapore Management University, Singapore**

#### Abstract

Modern multimedia coding standards, such as JPEG2000 and MPEG-4, are scalable, i.e., they are designed for "encoding once and decoding many times" i.e., they support extraction of sub-code streams with different resolutions, qualities and regions-of-interest (ROIs), all from the same compressed code stream. This functionality allows applications to manipulate or disclose only the required sub-code stream for any target users based on their privileges, device capabilities or network bandwidth. Authentication of multimedia content is indispensable in certain applications, such as government, finance, health care and law. In this talk, we present scalable authentication schemes for JPEG2000 and MPEG-4 code streams which are fully compatible with the core part of the standards. The authentication schemes possess the so called "sign once, verify many ways" property - allowing users to verify the authenticity and integrity of any transcoded sub-code streams extracted from a single code-stream protected with a single digital signature. In addition, by integrating seamlessly cryptographic techniques and erasure correction coding, the authentication scheme for MPEG-4 achieves high probability of successful authentication for code streams transmitted over lossy networks.

#### Short Biography

Robert H. Deng received his B.Eng from National University of Defense Technology, China, his MSc and PhD from the Illinois Institute of Technology, USA. He has been with the Singapore Management University since 2004, and is currently Professor, Associate Dean for Faculty & Research, and Director of SIS Research Center, School of Information Systems. Prior to this, he was Principal Scientist and Manager of Infocomm Security Department, Institute for Infocomm Research, Singapore. He has 26 patents and more than 200 technical publications in international conferences and journals in the areas of computer networks, network security and information security. He served as general chair, program committee chair and member of numerous international conferences. He received the University Outstanding Researcher Award from the National University of Singapore in 1999 and the Lee Kuan Yew Fellow for Research Excellence from the Singapore Management University in 2006.