TRUSTED COMPUTING AND INFORMATION SECURITY

ZHANG Huanguo **MU Yi**

With the rapid development of the information industry and the widespread use of information technology, information security has become a major concern in our society. In the information society, in addition to being a part of human society and the physical world, all persons are considered to belong to the information space. It is generally accepted that safety and reliability in human society are closely related to the security and trust associated with the information space. To ensure a safe, harmonious, prosperous and progressive human society, we must ensure that there exist security and trust in both the human society and information space simultaneously.

To ensure security and trust in the information space, there needs to be an integrated approach to implementing cryptography, network security, information system security, content security and other security technologies. Trusted computing is an effective system security technology that has been rapidly developing in recent years, and which has been widely used.

The Internet of Things, Big Data and Cloud Computing are hot topics in the current information field. The Internet of Things promotes the informatization of society by connecting the social space with physical space. Then, Big Data is generated in the information society. Also, the processing of Big Data relies on Cloud Computing. All of these systems require Trusted Computing and other information security technologies to ensure that security and trust are maintained.

To show the latest research results of information security and trusted computing in China, and to promote technological progress in these fields, *China Communications* publishes this Feature Topic in Trusted Computing and Information Security which contains following five papers.

The first paper, "*Protocol for Trusted Channel Based on Portable Trusted Module*", was written by ZHANG Dawei and HAN Zhen, et al. This paper deals with the security of web-based electronic transactions. It proposes the concept of the "Portable Trusted Module", and introduces the remote attestation mechanism of trusted computing into the TLS handshake protocol, which can establish a trusted channel between two points in a network. This channel is robust to a variety of malicious attacks and ensures the security of electronic transactions. Experiments show that this technical solution is suitable for E-commerce applications.

Kernel hooks are a kind of important data in operating systems. If such data are tampered with, the behaviour of an operating system will change. Many successful malicious attacks have resulted from the hacking of systems involving modifying the kernel hooks. The previous protection schemes of kernel hooks have some disadvantages. The paper, "*OPKH: A Lightweight Online Approach to Protecting Kernel Hooks in Kernel Modules*", which was written by TIAN Donghai, LI Xuanya, et al., proposes a kind of on-the-fly hook protection system based on virtualization technology. Some experiments show that this system can effectively protect the dynamic hooks with minimal performance overhead.

The third paper, "*Model for Software Behaviour Detection Based on Process Algebra and System Call*", was written by SHEN Limin, WANG Tao and MA Chuan. As some existing detection models have the disadvantages of being unpredictable and imprecise, this paper proposes a model for software Behaviour Detection based on Process Algebra and system calls (BDPA). Experiments demonstrate that the BDPA model has better precision and efficiency than traditional methods.

Signcryption is an important cryptographic scheme which combines the signature and encryption schemes. Previously developed signcryption schemes are mostly based on elliptic curve bilinear pairings. QI Yanfeng, TANG Chunming, et al. proposes a certificateless proxy identity-based signcryption scheme without bilinear pairings in their paper titled "*Certificateless Proxy Identity-Based Signcryption Scheme Without Bilinear Pairings*", which is both efficient and secure.

The fifth paper, "*Accurate Classification of P2P Traffic by Clustering Flows*", was written by HE Jie, YANG Yuexiang, et al. This paper addresses the problem regarding the accurate classification of P2P traffic. The authors propose a novel approach to accurately classifying P2P traffic at a fine-grained level, which solely depends on the counting of some special flows during small time windows. Experimental results show that their approach correctly classifies P2P applications with an average true positive rate of above 98% and a negligible false positive of about 0.01%.

Finally, we would like to thank all of the authors for their submissions to this special section; and we are also grateful to the anonymous reviewers for the timely responses and their valuable comments to improve the quality of the articles. We believe that this special section will further stimulate the research interests in this significant research area of trusted computing and information security.

Biographies

ZHANG Huanguo, was born in June, 1945, Professor and Ph.D. supervisor of Computer School in Wuhan University, China. He graduated from Xidian University, China in 1970. He is a Senior Researcher of China Computer Federation (CCF). At present he holds the professional post of adviser of Didactic Committee of Information Security Major of Ministry of Education of China and director of Chinese Association for Cryptologic Research. His research interests include information security, cryptography, trusted computing, cloud computing, fault tolerance and computer application. He has published over 100 research papers and 2 academic lucubrations, i.e. Introduction to Evolutionary Cryptosystem and Trusted Computing. As a leading specialist, he created the first major of "information security" as undergraduate, graduate, doctor and postdoctoral program in China. He also proposed the idea of evolutionary cryptosystem and the method to design and analyse automatically cipher based on the idea of evolutionary cryptosystem and met with practical success. By cooperating with some corporations, Prof. ZHANG developed the first "Trusted Platform Module (TPM)" and "Trusted Computer" in China, which have been used widely; and he developed the "Trusted Platform of Cloud Computing System" in China. He also developed the first "Trusted PDA" and "Software System for Testing and Evaluating of Trusted Computer" in China.

MU Yi, received his Ph.D. degree from the Australian National University, Australia in 1994. He currently is a full Professor, Head of School of Computer Science and Software Engineering and the Co-Director of Centre for Computer and Information Security Research at University of Wollongong, Australia. Prior to joining University of Wollongong, he was a Senior Lecturer in the Department of Computing, Macquarie University, Australia. He also worked in the Department of Computing, University of Western Sydney, Australia as a Lecturer. He has been with the University of Wollongong since 2003. His current research interests include cryptography, network security and computer security. His researches have been funded by Australian Research Council, National Natural Science Foundation of China and other government and industrial organisations. Professor MU is the Editor-in-Chief of International Journal of Applied Cryptography and serves as associate editor for nine other international journals. He is a senior member of the IEEE and a member of the International Association for Cryptologic Research (IACR).