Guest Editorial: Special Issue on Cyber Security Protections and Applications*

Xiaofeng Chen[†] State Key Laboratory of Integrated Service Networks (ISN) Xidian University, Xi'an, P.R.China xfchen@xidian.edu.cn

Willy Susilo Centre for Computer and Information Security Research (CCISR) School of Computer Science and Software Engineering University of Wollongong, Australia wsusilo@uow.edu.au

Nowadays, the Internet has become increasingly ubiquitous that supports many aspects of our lives. People and our societies have become increasingly dependent on the Internet for personal or professional uses, either for business or leisure. Despite all of the diverse advantages and benefits offered by the Internet, it also has become a common channel for communication and data transmission. Nevertheless, with the rapid development of network, many new challenges have been encountered and arising. In particular, a major issue is the security and privacy. Furthermore, the problem of privacy protection and any information leakage prevention becomes more severe, with some serious implications. These challenges come from the fact that the network may be compromised or controlled by malware or adversaries. Malware or adversary that targets the operating system is usually intended to collect sensitive information illegally. Clearly, these information security threats to vital national infrastructures and the risks of using these insecure services span from some serious financial loss to invasions of our privacy. Therefore, keeping the information safe and hence, the development of techniques for ensuring the security of data during transmission is an emerging and important problem in our society. To ensure a safe and prosperous human society and a good performance for network applications, information protection methods should be considered. Therefore, it is essential that we have effective techniques and tools to design and evaluate secure systems and demonstrate that they meet their security requirements.

This special issue on "Cyber Security Protections and Applications" attempts to highlight some of the latest research addressing those challenges. It collects a series of papers on the important topics, More specifically:

• The first paper, "Reconciling Malicious and Accidental Risk in Cyber Security" by Pieters et al. [1], proposes a new approach for Cyber risk analysis that combines frequentist and adversarial approaches to risk in a single framework. Although there are risk assessment methods that deal with strategic attackers, these do not provide expected frequencies as outputs, making it impossible to integrate those in existing (safety) risk management practices. To overcome this problem,

Journal of Internet Services and Information Security (JISIS), volume: 4, number: 2, pp. 1-3

^{*}This work is supported by the National Natural Science Foundation of China (Nos. 61272455), China 111 Project (No. B08038), and the Australian Reserach Council Future Fellowship (FT0991397).

[†]Corresponding author: Tel: +86-29-88204749

the authors extend the FAIR framework to enable integration of safety and security risk assessments. And this approach constitutes an innovative way to quantify expected attack frequencies as a component of (information) security metrics for investment decisions.

- The paper of Ye et al. [2], entitled "Dynamic Model for Anonymity Measurement Base on Information Entropy" proposes a dynamic model based on information entropy. The measurement and comparisons of anonymity system is very important to evaluate the security of system with large amounts of data transmitting on networks. There are many technical solutions to protect the identifiable information of senders and receivers in various applications and services. But for each scheme, the anonymous security is different, and there are some insecure anonymous protocols. While the model proposed in this paper can measure the system anonymity according to the different attack capabilities of adversaries and the model can be widely used for the anonymity measurement and the anonymity competitions of different systems.
- The paper of Fujinoki et al., "Fail-Safe Security Architecture to Prevent Privacy Leaks from Ecommerce Servers" [3], focuses on the protection against the customer private information leaks. Nowadays, privacy leaks from e-commerce servers are a serious problem. Furthermore, frequent leaks of E-commerce customers' privacy have impacted to acceptance of e-commerce applications. To solve this problem , the authors propose a secure network architecture, called Fail-Safe Security Architecture (FSSA) that protects customers' privacy information not only from external attackers, but also from internal attackers (insiders) at the same time it satisfies the legal requirements.
- The paper of Sakamoto et al. [4], entitled "DroidTrack: Tracking and Visualizing Information Diffusion for Preventing Information Leakage on Android", proposes DroidTrack, a method for tracking and visualizing the diffusion of sensitive information and preventing its leakage on an Android device. Following the rapid proliferation of smartphones, Android has emerged as a popular smartphone operating system. However, an app can hijack administrative privileges by exploiting vulnerabilities in the Android OS, and thus send out illegally collected sensitive information. In this paper, the authors have evaluated AP and compared the information diffusion path which generated by DroidTrack with the operation of the example AP.
- The final paper by Li et al. [5] on "Key Policy Attribute-based Proxy Re-encryption and RCCA Secure Scheme" presents a KP-AB-PRE scheme, in which the cloud server can function as the proxy and deal with the ABE ciphertext directly. Recently, cloud computing is a promising computing paradigm. However, as the decryption algorithm of attribute-based encryption need a lot of computations, with the help of cloud server, a lot of attribute-based encryption schemes are designed for practical applications in cloud computing. In this paper, the authors use matrix access structure to realize the key policy. And the secret key size, encryption, and decryption time scales linearly with the complexity of the access formula.

We believe that the papers included in this special issue illustrate some of the important issues investigated at the research of internet security and technology. We are happy and privileged to have been offered the opportunity to guest-edit this special issue of *Journal of Internet Services and Information Security (JISIS)*.

With the Editor-in Chief, Dr. Ilsun You, we wish to extend our special thanks to all authors, reviewers and editorial members for their invaluable contributions, without which this special issue would not have been possible.

References

- [1] W. Pieters, Z. Lukszo, D. Hadžiosmanović, and J. van den Berg. Reconciling malicious and accidental risk in cyber security. *Journal of Internet Services and Information Security (JISIS)*, 4(2):4–26, May 2014.
- [2] J. Ye, Y. Ding, X. Xiong, and S. Wu. Dynamic model for anonymity measurement base on information entropy. *Journal of Internet Services and Information Security (JISIS)*, 4(2):27–37, May 2014.
- [3] H. Fujinoki, C. A. Chelmecki, and D. M. Henry. Fail-safe security architecture to prevent privacy leaks from e-commerce servers. *Journal of Internet Services and Information Security (JISIS)*, 4(2):38–54, May 2014.
- [4] S. Sakamoto, K. Okuda, R. Nakatsuka, and T. Yamauchi. Droidtrack: Tracking and visualizing information diffusion for preventing information leakage on android. *Journal of Internet Services and Information Security* (*JISIS*), 4(2):55–69, May 2014.
- [5] K. Li, J. Wang, Y. Zhang, and H. Ma. Key policy attribute-based proxy re-encryption and rcca secure scheme. *Journal of Internet Services and Information Security (JISIS)*, 4(2):70–82, May 2014.

Author Biography



Xiaofeng Chen received his B.S. and M.S. on Mathematics in Northwest University, China. He got his Ph.D degree in Cryptography from Xidian University at 2003. Currently, he works at Xidian University as a professor. His research interests include applied cryptography and cloud computing security. He has published over 100 research papers in refereed international conferences and journals. His work has been cited more than 1800 times at Google Scholar. He has served as the program/general chair or program committee member in over 20 international conferences.



Willy Susilo received a Ph.D. in Computer Science from University of Wollongong, Australia. He is a Professor at the School of Computer Science and Software Engineering and the director of Centre for Computer and Information Security Research (CCISR) at the University of Wollongong. He is currently holding the prestigious ARC Future Fellow awarded by the Australian Research Council (ARC). His main research interests include cryptography and information security. His main contribution is in the area of digital signature schemes. He has served as a program committee

member in dozens of international conferences. He has published numerous publications in the area of digital signature schemes and encryption schemes.