Information **2015**, *6*, 833-835; doi:10.3390/info6040833

OPEN ACCESS

information

ISSN 2078-2489

www.mdpi.com/journal/information

Editorial

A Summary of the Special Issue "Cybersecurity and Cryptography"

Qiong Huang [1,*] and Guomin Yang [2]

[1] College of Mathematics and Informatics, South China Agricultural University, 483 Wushan Rd, Tianhe, Guangzhou 510642, China

[2] School of Computing and Information Technology, University of Wollongong, Northfields Avenue, Wollongong, New South Wales 2522, Australia; E-Mail: gyang@uow.edu.au

* Author to whom correspondence should be addressed; E-Mail: csqhuang-c@my.cityu.edu.hk; Tel.: +86-20-85285389; Fax: +86-20-85285393.

Academic Editor: Willy Susilo

Received: 23 November 2015 / Accepted: 4 December 2015 / Published: 8 December 2015

Nowadays in the cyber world, massive amounts of data are being collected, transmitted, and stored by different organizations and individuals. As an important asset, data must be well protected in storage and during transmission. Data security is a crucial factor to the success of new information technologies and infrastructures, such as Cloud Computing and Big Data. This Special Issue includes seven research articles presenting new findings and technologies in the area of cybersecurity and cryptography.

The recent emergence of the targeted use of malware in cyber espionage urges a systematic review for better understanding its impact and mechanism. In the paper "The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism" [1], Wangen proposed a basic taxonomy to document major cyber espionage incidents, describing and comparing their impacts and their mechanisms. The proposed taxonomy provides not only a solid foundation of knowledge about the topic, but also a systematic way to document known and future attacks to facilitate research activities.

Radio Frequency Identification (RFID) technology is widely used in supply chain management. In the paper "Efficiency and Privacy Enhancement for a Track and Trace System of RFID-Based Supply Chains" [2], Chen *et al.* investigated the security and privacy issues in RFID-based track and trace systems. They first studied the relationship among three different security concepts proposed in the literature—namely privacy, path unlinkability, and tag unlinkability—and proved that privacy is equivalent to path unlinkability, and tag unlinkability implies privacy. Moreover, they proposed an efficient track and trace scheme named Tracker+, which incurs less computation and storage overhead, compared with other schemes of the same type proposed in the literature.

In another paper titled "Influences of Removable Devices on the Anti-Threat Model: Dynamic Analysis and Control Strategies" [3], Ma *et al.* also proposed a mathematical model to explore the influence of removable devices on the interaction dynamics between malicious worms and benign worms. The model takes two important network environment factors into consideration: benign worms and the influence of removable devices. The authors also demonstrated the effectiveness of their proposed model via simulations. Effective control strategies are also proposed in the paper to combat malicious worms.

Secret handshake is a very useful cryptographic primitive. In the paper "A Backward Unlinkable Secret Handshake Scheme with Revocation Support in the Standard Model" [4], Wen *et al.* proposed a novel secret handshake scheme with unlinkability, revocation and traceability. Moreover, their scheme also achieves backward unlinkability, which means the past transcripts of revoked members remain private. The proposed scheme is proven secure without random oracles.

In the paper "Analysis of Two-Worm Interaction Model in Heterogeneous M2M Network" [5], Ma *et al.* investigated complex interaction dynamics between benign worms and malicious worms in a heterogeneous M2M network. They analyzed and compared three-worm propagation models based on different immunization schemes, and conducted numerical simulations to verify their theoretical results. The results presented in this work enables the research community to further understand the spread of worms in heterogeneous M2M networks.

In the paper "Batch Attribute-Based Encryption for Secure Clouds" [6], Yang *et al.* proposed a novel batch attribute-based encryption (BABE) system for cloud storage. Inspired by the fact that the existing ABE systems only allow a data owner to perform encryption for receivers from a single organization, they proposed the BABE framework that allows the data owner to freely choose the receiving organizations and define separate attributes for the receivers of different organizations. The experimental results show that the proposed BABE scheme is more efficient than the existing ABE implementations, and hence is suitable for one-to-many organization-oriented sensitive data sharing in clouds.

In the paper "Cable Capacitance Attack against the KLJN Secure Key Exchange" [7], Chen *et al.* presented their findings on the cable capacitance attack against the Kirchhoff-law-Johnson-(like)-noise (KLJN) key exchange system. They used the industrial cable and circuit simulator LTSPICE to simulate practical realizations of the KLJN system and to evaluate the cable capacitance attack. Their simulation results also showed that privacy amplification and/or capacitor killer arrangements can effectively mitigate the attack.

Acknowledgements

We thank all the authors and reviewers of this Special Issue as well as the editorial staff of the MDPI *Information* Journal in making this Special Issue a success.

References

1. Wangen, G. The Role of Malware in Reported Cyber Espionage: A Review of the Impact and Mechanism. *Information* **2015**, *6*, 183–211.

2. Chen, X.; Zhu, Y.; Li, J.; Wen, Y.; Gong, Z. Efficiency and Privacy Enhancement for a Track and Trace System of RFID-Based Supply Chains. *Information* **2015**, *6*, 258–274.
3. Ma, J.; Chen, Z.; Wu, W.; Zheng, R.; Liu, J. Influences of Removable Devices on the Anti-Threat Model: Dynamic Analysis and Control Strategies. *Information* **2015**, *6*, 536–549.
4. Wen, Y.; Gong, Z.; Xu, L. A Backward Unlinkable Secret Handshake Scheme with Revocation Support in the Standard Model. *Information* **2015**, *6*, 576–591.
5. Ma, J.; Chen, Z.; Liu, J.; Zheng, R. Analysis of Two-Worm Interaction Model in Heterogeneous M2M Network. *Information* **2015**, *6*, 613–632.
6. Yang, C.; Sun, Y.; Wu, Q. Batch Attribute-Based Encryption for Secure Clouds. *Information* **2015**, *6*, 704–718.
7. Chen, H.-P.; Gonzalez, E.; Saez, Y.; Kish, L.B. Cable Capacitance Attack against the KLJN Secure Key Exchange. *Information* **2015**, *6*, 719–732.