Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Editorial:

Security for cyberspace: challenges and opportunities

Jiang-xing WU[1], Jian-hua LI[†‡2], Xin-sheng JI[1]

[1]*National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China*

[2]*School of Cyber Security, Shanghai Jiao Tong University, Shanghai 200240, China*

[†]E-mail: lijh888@sjtu.edu.cn

https://doi.org/10.1631/FITEE.1840000

Nowadays, cyberspace has become the "fifth frontier" after the ocean, land, air, and space. With the globalization of information, cyberspace has never faced so many challenges, such as principle innovation, theory innovation, technology innovation, and application innovation. Thus, the transition from traditional cyberspace to new cyberspace is inevitable. In the future, cyberspace will have many important characteristics, such as openness, heterogeneity, mobility, dynamism, and security.

With the rapid development of information technologies, future cyberspace will have higher openness, dynamism, and flexibility. The realization of cyberspace security is particularly important and emergent. Compared with traditional network security, future cyberspace security has its particularity because of the following factors. First, the traditional static security methods based on known threat characteristics can no longer effectively defend against novel threats, such as 0-day attacks and advanced persistent threats (APT). Specifically, for backdoor threats, neither static defense nor dynamic defense, not even encryption technology, can do anything about it. By exploiting the concealed and complicated means, attackers could launch targeted attacks and persistent penetrations, presenting strong concealment, latent and long-term entanglement. Usually, the detection and isolation nature of passive defense technology are invalid for these unknown novel threats. Second, because future network is based on network programming and virtualization, it can provide programmable interfaces for network applications, and these interfaces will also provide opportunity for hackers to attack, making future networks face greater risks than traditional networks. Third, due to the incomplete collection of network traffic, state and semantic gap, vulnerability analysis is difficult. To achieve multi-level, multi-angle, and multi-function security threat assessment, security defense and awareness approaches are necessary.

Regarding the aforementioned challenges, novel and efficient security should be studied. First, security should be taken as the priority in the design of architecture, to avoid or reduce the threat of attacks from various unknown vulnerabilities or backdoors in hardware and software designs, to make the system immune to endogenous security. Second, dynamic defense architecture should be considered, which can provide adaptive security protection for cyberspace. Moreover, many advanced security technologies, such as novel cryptography, should be studied and used. Finally, novel networking, computing, and artificial intelligence can all benefit high-level security for future cyberspace.

In this context, the Chinese Academy of Engineering (CAE) organized a special issue of "Cyberspace Security" in *Frontiers of Information Technology and Electronic Engineering*. This special issue aims to promote advanced theory, technologies, and industry of cyberspace security. Seven papers are included in this special issue, by invitation or

‡ Corresponding author

contribution, including three survey papers and four research papers.

1 Scanning the special issue

Mimic defense is an endogenous security defense technology with generalized robust control capability based on architecture design. It is a promising and efficient security technology with defense capability against unknown novel threats (Jiang-xing WU's group). The cloud workflow, which makes full use of a mimic defense based dynamic heterogeneous redundant (DHR) robust task execution space, is much more capable of resisting unknown vulnerabilities and backdoor threats. Based on the diverse physical servers, hypervisors, and virtual machine operating systems, cloud workflow constructs heterogeneous redundant parallel task execution subspaces. The result of task execution is judged by a multi-mode decision mechanism, where the inconsistency found is used to determine whether the running task is being attacked. If any inconsistency appears, the environment of the compromised task execution will be cleaned. Moreover, feedback control mechanism will be adopted to perform dynamic reconstruction of the defense scenario, which would block the attack process and defend against attacks based on unknown backdoors effectively and ensure reliability and credibility of cloud workflow execution.

Artificial intelligence (AI) is one of the fastest growing branches of computer sciences, and offers a feasible way to achieve cyber security and resolve the aforementioned challenges. When AI meets cyber security, such cross-disciplinary studies focus on two aspects. AI technologies, such as deep learning, can be introduced into cyber security to construct smart models to implement malware classification, intrusion detection, and threat intelligence sensing. Moreover, AI models need specific cyber security defense and protection technologies to combat adversarial machine learning, preserve privacy in machine learning, secure federated learning, etc. The intersection of AI and cyber security was discussed by Jian-hua LI.

Bankcard enrollment on mobile device, being the first step of mobile transactions, has become the first target of fraud attempt. Hong-feng CHAI's group introduced several traditional machine learning algorithms, and finally chose the improved gradient boosting decision tree (GBDT) algorithm software library for a real system, which is XGBoost. Their work expands multiple features based on analysis of the enrollment behavior, and they plan to add historical transactions in their future work. The results and framework are adopted and absorbed into the new design of a mobile payment fraud detection system within the Chinese payment processor.

The Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) supported by the National Institute of Standards and Technology (NIST) is an ongoing project calling for submissions of authenticated encryption (AE) schemes. The competition itself aims at enhancing both the design of AE schemes and related analyses. Kui REN's group introduced the requirements of the proposed design and the progress of the candidate screening in the CAESAR competition. Then, the candidate AE schemes in the final round are classified according to their design structures and encryption modes. Next, comprehensive performance and security evaluation are conducted on these candidates, and research trends for the future are discussed.

Software-defined networking (SDN) is one of the most popular and promising technologies. In SDN, the high-level strategy is deployed by proprietary equipment, which is used to guide data forwarding of the network equipment; this can reduce many complicated functions of the network equipment and improve the flexibility and operability of the implementation. However, this novel networking technology faces many challenges in terms of architecture and security. Shen WANG's group offered a comprehensive review of the state-of-the-art research on novel advances of programmable SDN, to highlight what has been investigated and what needs to be addressed, particularly, in terms of architecture and security.

The current boom in Internet of Things (IoT) is changing daily life in many ways, from wearable devices to connected vehicles and smart cities. Kaoru OTA and Mian-xiong DONG's group proposed a Byzantine fault-tolerant networking method and two resource allocation strategies for IoT fog computing. The aim is to build a secure fog network called

"SIoTFog" to resist Byzantine faults and improve the efficiency of transmitting and processing IoT big data. Two cases are considered, one with a single Byzantine fault and the other with multiple faults, to compare their performances when facing different degrees of risk.

With the development of fog computing, the need has arisen to delegate private set intersection (PSI) on outsourced datasets to the fog. However, the existing PSI schemes are based on either fully homomorphic encryption (FHE) or pairing computation. Fu-cai ZHOU's group proposed a novel primitive called "faster fog-aided private set intersection with integrity preserving," where the fog conducts delegated intersection operations over encrypted data without the decryption capacity.

2 Future work

Cyberspace security faces a lot of challenges and opportunities. In the future, some new topics should be paid more attention. First, human-factor security is an interdisciplinary topic, which can fetch up the shortcomings of current security technologies. Second, intrusion-tolerant cryptography is an important issue for new networks, such as 5G/6G. Third, the applications of cyberspace security technologies should be extended to a lot of new areas.

Prof. Jiang-xing WU was born in 1953 in Jiaxing, Zhejiang, China, academician of Chinese Academy of Engineering, a well-known expert in communication and information systems, computer and network technology in China. He developed the first digital telephone SPC exchange of China. He is the principal investigator and chief designer of mimic defense theory and technology. As the director of the National Digital Switching System Engineering & Technological R&D Center, his current research interests include the next generation information network theory and technology, and mimic defense technology.

Prof. Jian-hua LI is the dean of School of Cyber Security, Shanghai Jiao Tong University, China. He is also the director of the National Engineering Laboratory for Information Content Analysis Technology. He is the vice president of the Association of Cyber Security Association of China, vice chairman of the Advisory Committee of Information Security Teaching in the Higher Education Ministry of Education of China.

Prof. Xin-sheng JI is the chief engineer of the National Digital Switching System Engineering & Technological R&D Center.