Hindawi
Security and Communication Networks
Volume 2018, Article ID 5313980, 1 page
https://doi.org/10.1155/2018/5313980

Editorial

Cyberspace Security for Future Internet

Dafang Zhang,[1] Guojun Wang,[2] Xin Wang,[3] Zhengyu Li,[4] and Wenjia Li[5]

[1] *Hunan University, Changsha 410082, China*
[2] *Guangzhou University, Guangzhou 510006, China*
[3] *Stony Brook University, Stony Brook, NY 11794-2350, USA*
[4] *Institute of Computing Technology (ICT), Chinese Academy of Sciences (CAS), Beijing 100190, China*
[5] *New York Institute of Technology, New York, 10023, USA*

Correspondence should be addressed to Dafang Zhang; liyanbiao@ict.ac.cn

Received 10 July 2018; Accepted 10 July 2018; Published 5 August 2018

Cyberspace is the most popular environment for information exchange whose security suffers from ever-increasing challenges with the rapid development of the Internet. This issue published 7 latest contributions on cyberspace security for future Internet.

Due to the fast advance of mobile technologies and mobile applications, smartphones, especially Android devices, are widely used in our daily life, which are threatened greatly by attacks. Therefore, malware analysis on Android platform is in urgent demand. Regarding drawbacks of existing static and dynamic analysis approaches, a new framework is introduced here, which can better satisfy the demand for actual use. In addition to malware detection, privacy is another big concern. For example, mobile devices are always equipped with numerous sensors, which may reveal sensitive information when correlated with other data or sources. How to protect user privacy or identify privacy risks exposed by applications? Some novel user deanonymization approaches and user fingerprinting in Android are introduced. Besides, location-based services (LBSs) become more and more popular in mobile Internet, such as map directions, restaurant recommendations, and taxi reservations. Regarding the privacy of personal location information, an efficient and privacy-preserving multiuser query scheme is presented for cloud-based LBSs.

Access control, on the other hand, also plays a very important role in cyberspace security. Regarding the absence of a flexible exceptional approval mechanism in attribute-based access control (ABAC), a feasible fuzzy-extended ABAC technique is presented, which improves the flexibility in urgent exceptional authorizations and thereby improves the resource usability and business timeliness. In the field of satellite communication, existing centralized authentication protocols for MEO/GEO satellite networks cannot accommodate LEO satellite networks with frequent user connection switching. Combining identity-based encryption and the block-chain technology, a fast and efficient access verification protocol is introduced.

New architectures and new computing technologies bring in both opportunities and challenges in cyberspace security. In Small Object Networks with IPv6, the process of Duplicate Address Detection is subject to many attacks. In view of this, a new algorithm to optimize the security in IPv6-DAD is presented. With quantum computers, cyberspace security has become the most critical issue in the Internet in near future. So, characteristics of the quantum cryptography and how to use it in future Internet are analyzed.

Dafang Zhang
Guojun Wang
Xin Wang
Zhengyu Li
Wenjia Li