Trusted Secure Accessing Protection Framework Based on Cloud-Channel-Device Cooperation

Yexia Cheng[1,2,3](✉), Yuejin Du[1,2,4](✉), Jin Peng[3](✉), Jun Fu[3],
and Baoxu Liu[1,2]

[1] Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, China
chengyexia@iie.ac.cn
[2] School of Cyber Security,
University of Chinese Academy of Sciences, Beijing, China
[3] Department of Security Technology,
China Mobile Research Institute, Beijing, China
pengjin@chinamobile.com
[4] Security Department, Alibaba Group, Beijing, China
yuejin.dyj@alibaba-inc.com

Abstract. With the rapid development of network technologies, such as mobile Internet, Internet of Things (IoT), secure accessing is becoming an important issue. Security protection framework based on cloud-channel-device cooperation is proposed in this paper to solve the issue. The trust base is introduced to channel-end to improve trust of secure accessing device. Then, the trust and security module are designed in the cloud-end. Meanwhile, access control based on connection tracking is adopted to reduce access latency. The framework can be used to construct an open, trusted, resilient network for secure accessing and provide security solutions for mobile office, IoT security, information security management and control, etc. The effectiveness of the framework has been proved by its application to the market.

Keywords: Secure accessing · Cloud-channel-device cooperation · Trust base · Protection framework · Secure connecting · Access control

1 Introduction

With the rapid development of network technologies, such as mobile Internet, Internet of Things (IoT), etc., people's working and life patterns have been changed. The mobile smart terminals are becoming increasingly popular and the mobile offices have grown year by year. Security is critical to these services. The global Internet of Things business has developed rapidly. The Internet of Things has got the trillion-dollar market and is in the stage of large-scale explosive growth. It is estimated that by 2020, the scale of the Internet of Things market is expected to exceed US$1.7 trillion; by 2020, the number of IoT devices will reach 38.5 billion, an increase of 285% from 13.4 billion in 2015, and everything is becoming connected step by step. However, there are

X. Yun et al. (Eds.): CNCERT 2018, CCIS 970, pp. 165–176, 2019.
https://doi.org/10.1007/978-981-13-6621-5_14

a lot of security problems for IoT devices. For example, 80% IoT devices have the risk of disclosure and abuse of privacy. 80% IoT devices allow using weak password. 60% IoT devices have vulnerability problems with web page of device management. 60% IoT devices can download upgrade packages and upgrade without using any password. Due to a large number of the IoT devices accessing to Internet or Intranet, some other security problems have been brought. For example, some new attack patterns will be launched by these IoT devices and they will become new threat to the enterprise. Among these security problems, whether the accessing is secure or not is one of the most important. To solve the problem, the secure accessing protection should be taken.

When it comes to secure accessing, the researchers have already taken some studies on it. And their specific research directions of secure accessing have been changing with the time. Scarfo focus on analysis of security risks and security threats of accessing [1]. Peng et al. propose differential deployment algorithm [2]. Li et al. point out analysis of security policy [3]. Zahadat et al. and Yeboah-Boateng propose framework construction and security suggestion for secure accessing [4, 5]. Hovav et al. focus on strengthening network management and strategies for mobile applications and devices [6]. Hong et al. focuses on architecture design for secure accessing [7]. Kumar et al. propose anonymous secure framework in connected smart home environments [8]. Park et al. point out the lightweight access security for IoT and cloud convergence [9]. Ranjbar et al. discuss about the secure and persistent connectivity [10]. Zhao talks about the node capture attacks and Kim designs a secure digital recording protection System with network connected devices [11, 12]. The overall trend of secure accessing research is turned to the concrete architecture and methods.

The related researches are from different directions of secure accessing. The trusted secure accessing hasn't been proposed yet and especially the trusted secure accessing protection method based on cloud-channel-device cooperation hasn't been proposed until now.

Our Contributions. From the perspective of secure accessing, security protection framework based on cloud-channel-device cooperation is proposed in this paper to solve the issue. The trust base is introduced to channel-end to improve trust of secure accessing device. Then, the trust and security module are designed in the cloud-end. Meanwhile, access control based on connection tracking is adopted to reduce access latency. The framework can be used to construct an open, trusted, resilient network for secure accessing and provide security solutions for mobile office, IoT security, information security management and control, etc. The effectiveness of the framework has been proved by its application to the market. There are three innovations and contributions. The first is the cloud-channel-device cooperated protection framework. The second is the trust design of secure accessing devices. The third one is the connection tracking based access control of secure accessing devices and cloud platform.

The rest of this paper is organized as follows. Section 2 introduces the cloud-channel-device cooperated protection framework of secure accessing and for each part of protection framework, the function components of security and trust are designed. Section 3 presents the trust base of secure accessing devices. Section 4 proposes the trust of secure cloud platform. Section 5 mainly specifies the access control based on connection tracking for secure accessing. And in Sect. 6, the implementation and market application are introduced. Finally, in Sect. 7 we draw the conclusion of this paper.

2 Cloud-Channel-Device Cooperated Protection Framework

2.1 Secure Accessing Protection Framework Based on Cloud-Channel-Device Cooperation

As for secure accessing, especially with the development of mobile Internet, the mobility and boundary ambiguity is becoming much more obvious, as well as the openness of the various services and capabilities. So the security threats may be in any node and any different paths or links. Just relying on a single technology or a single protection device can no longer meet the demands. Therefore an integrated, coordinated, systematic security protection framework is a prerequisite for secure accessing.

Hence, in order to get the secure accessing, we propose a cloud-channel-device cooperated protection framework. The protection framework is shown in Fig. 1.

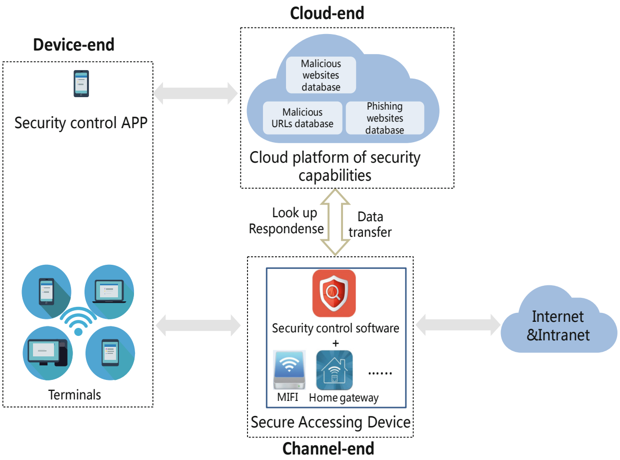


Fig. 1. Cloud-channel-device cooperated protection framework

We can see from Fig. 1 that there are three main parts of the protection framework, which are cloud-end, channel-end, device-end. As for cloud-end, it is the cloud platform of security capabilities. They can provide such realistic databases as malicious websites, malicious URLs, phishing websites, etc. As for channel-end, which is the channel between device to Internet or Intranet, there lies secure accessing devices. They can provide such functions as internet accessing, malicious website filtering, link selection, remote device monitoring, etc. The security control APP or software is used to manage the secure accessing device. As for device-end, it is terminal used by users, such as the smart phone, laptop and notebook. The security control APP will be installed in some terminals.

These three parts are cooperated with each other. The channel-end secure accessing device looks up the malicious websites, malicious URLs, phishing websites in the cloud-end. The cloud-end can transfer and exchange security data with the channel-end secure accessing device, by the operation of correspondence, etc. The channel-end secure accessing device also interacts with the device-end terminals. The websites data from device-end terminals can be extracted with the users' allowance and be compared with the data in the channel-end secure accessing device. The result will determine whether the access is secure or not. Besides, the device-end terminals with security control APP can also interact the control information with secure accessing device in channel-end.

Secure accessing protection framework based on cloud-channel-device cooperation can be used to construct an open, trusted, resilient network, which makes accessing secure and trusted. More specifically, the secure accessing protection framework can provide security solutions for information security management and control, mobile office and IoT security, etc.

2.2 Security and Trust Function Components for Secure Accessing Protection Framework

The architecture and security and trust function components for secure accessing protection framework are described in Fig. 2.

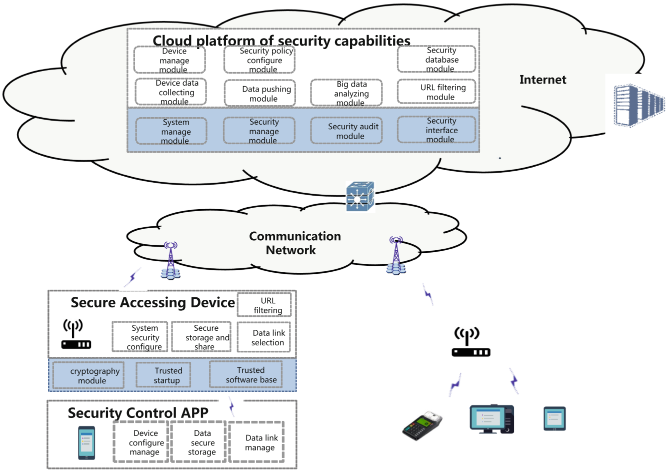


Fig. 2. Security and trust function components for secure accessing protection framework

According to the above Fig. 2, as for cloud-end, channel-end, device-end, we can get the components of security and trust for any one of the parts.

(1) **Cloud-end**
Cloud platform of security capabilities, it provides the security capabilities on the cloud and the ability of configuring the devices connected to the cloud platform of security capabilities, such as recognizing malicious websites and managing resources. The cloud platform of security capabilities can help secure connecting devices hold up the malicious URLs or phishing websites as well as real-time

querying the malicious URLs or phishing websites. The cloud platform of security capabilities provides the enterprise users with the user interface combining the functions of website blacklist configuring and user information maintenance, etc.

The security function components include device data collecting module, data pushing module, big data analyzing module, URL filtering module, device manage module, security policy configure module and security database module, etc.

The trust function components include system manage module, security manage module, security audit module and security interface module.

(2) **Channel-end**

Secure accessing device is a portable device with the security analysis and security filtering functions and meanwhile it is pre-configured with a SIM card. It is similar to the mobile WLAN hotspot device. The secure connecting device is used as a network access point for connecting to the Internet or the intranet of the enterprise. While accessing to the Internet, the secure accessing device will take advantage of various URL feature libraries on the cloud platform of security capabilities to check the user's accessing website or URL, and then hold up the malicious URL or phishing website. While connecting to the intranet of the enterprise, the secure connecting device will make use of various link selection modes to access to the intranet securely, such as APN, VPN, VPDN, etc.

The security function components include system security configure, secure storage and share, data link selection, URL filtering, etc.

The trust function components include cryptography module, trusted startup and trusted software base.

(3) **Device-end**

As for device-end, especially, the security control APP, users can easily manage security accessing devices through the security control APP. It can make sure the terminals are in secure environment to access.

The security function components include device configure manage, data secure storage, data link manage, etc.

3 Trust Base of Secure Accessing Devices

For the trusted base of secure accessing devices, we introduce Secure Element (SE) to support the establishment of trusted computing environment and provide the trusted base for secure services. Secure Element (SE) is described in detail as follows.

The Secure Element (SE) provides a miniature computing environment on a single chip, including CPU, ROM, EEPROM, RAM, and I/O interfaces, as well as cryptographic algorithm coprocessors and physical noise sources, etc. It can provide secure storage, secure computing, and cryptographic algorithm calculations for upper-layer software. Meanwhile, it provides with secure operating environment, random number generation capabilities, security protection and provides trusted computing capability as a trusted base.

The construction parts of the trusted base of secure accessing devices are shown in Fig. 3.

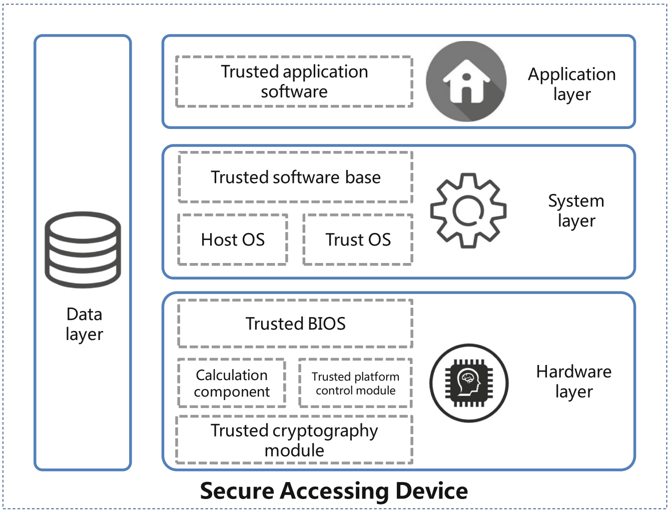


Fig. 3. Trusted base of secure accessing devices

In Fig. 3, the trusted base of secure accessing devices is constructed from four different layers, which are the hardware layer, system layer, application layer and data layer of the secure accessing devices. The specific construction parts are illustrated in below.

(1) **Hardware layer**
There are four trust modules in this layer, namely, trusted cryptography module, calculation component, trusted platform control module and trusted BIOS.

(2) **System layer**
In system layer, it is mainly based on Host OS, Trust OS, Trusted software base, etc.

(3) **Application layer**
The application layer is related to trusted application software.

(4) **Data layer**
The data layer is mainly about traditional security, which is the base insurance to trust part.

The secure accessing devices are designed with the strict security requirements of physical interface security, chip security, system privilege limitation, system update security, system security startup and system configuration security, etc. According to the requirements of different security level, the active trusted metrics and control of the equipment are introduced so as to ensure the security of the equipment fundamentally. Dived from the above four layers, the trust security requirements are listed as follows.

(1) **Hardware layer**
The trust security requirements of hardware layer include physical interface security and chip security. As for physical interface security, it includes debug interface security and peripheral interface security. As for chip security, it includes written protection security and trusted execution environment security.

(2) **System layer**
The trust security requirements of system layer include system authority restrictions, system update security, system configuration security, service configuration security and system security start. As for system authority restrictions, it includes multi-user authority control, remote connection authentication, application installation authorization and access control security. As for system update security, it includes OTA update security, firmware update security, version rollback mechanism and bug fixing ability. As for system configuration security, it includes important partition security, debug process authority restrictions and debug port control. As for service configuration security, it includes authorization minimization, application access control mechanism, data connection status and remote connection security. As for system security start, it includes integrity protection.

(3) **Application layer**
The trust security requirements of application layer include built-in application security, remote connection authentication, user's password security, multi-user access control, application update security, mobile client security, user's sensitive data security, data transmission security and login authentication mechanism.

(4) **Data layer**
The trust security requirements of data layer include data transmission, data storage, access control and log security. As for data transmission, it includes application and system sensitive data encryption. As for data storage, it includes user's privacy data encryption and application context sensitive data security. As for access control, it includes sensitive data isolation access control, third-party application access control and data isolation access control. As for log security, it includes web remote management, user's operation and alarm log management and log read authority control.

4 Trust of Secure Cloud Platform

The trust of secure cloud platform is constructed by deploying trusted computing platforms and establishing system-based platform protection measures. The following Fig. 4 shows the trust of secure cloud platform. All these designs guarantee the trust of secure cloud platform.

Accomplished with three layers' management, namely, system management, security management and audit management, we require the strict design of cloud platform of security capabilities, so as to build a trusted immune and active defense security protection.

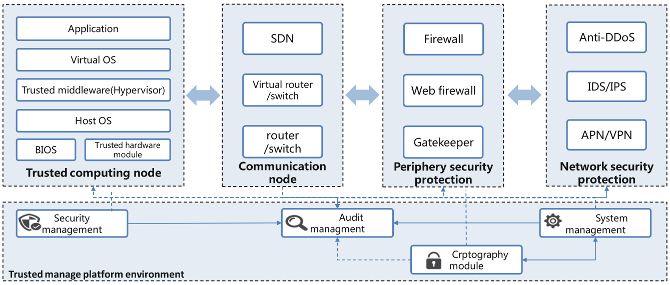


Fig. 4. Trust of secure cloud platform

5 Access Control Based on Connection Tracking for Secure Accessing

The access control based on connection tracking for secure accessing can realize application access and application queries in parallel and at the same time, it can reduce the access latency and user perception.

The method is as follows, which can also be seen in Fig. 5. Firstly, the application access traffic and extract the key feature information of the request message are analyzed. Secondly, the key feature information to query the security attributes of the traffic in the cloud platform of security capabilities is used while forwarding the request message. Thirdly, through connection tracking technology, the application access request and response message are associated. Finally, according to the lookup result from the cloud platform of security capabilities, the insecure response messages are intercepted.

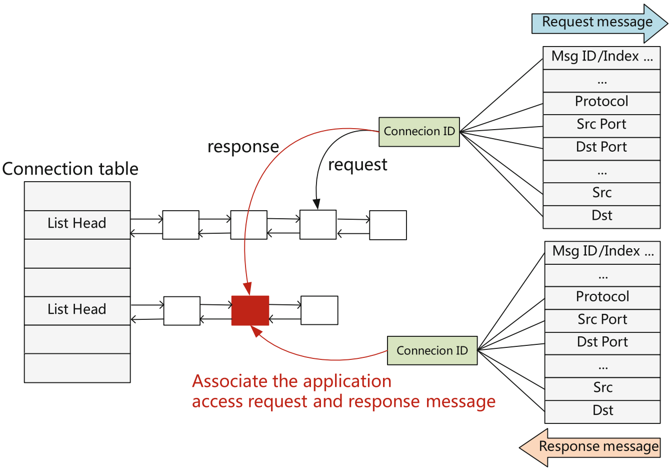


Fig. 5. Access control based on connection tracking for secure accessing

The comparison of our method based on connection tracking with other method is shown in Fig. 6. Our method can realize application access and application queries in parallel, while other methods are sequent, which is first making request, then accessing. The access latency of our method is much less than other methods.

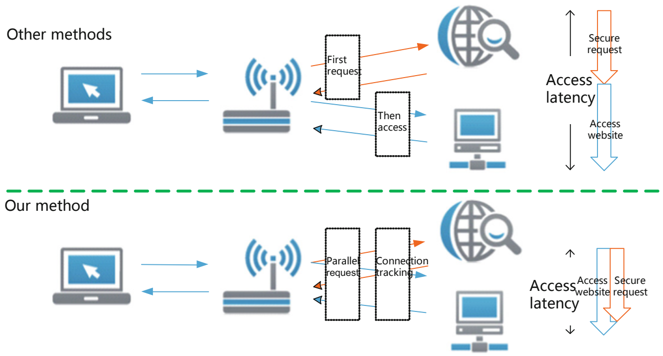


Fig. 6. Comparison of our method with other methods

6 Implementation and Market Application

The security protection framework proposed in this paper has been implemented and practically applied to the market.

What's more, the implemented system has already been tested by a third party testing agency, which showed a good test result. The query response time of the cloud platform of security capabilities is less than 200 ms. The accuracy is more than 99.9%. Concerning to the secure accessing device, when 30 terminals simultaneously access to Internet by the same secure accessing device, the latency is less than 500 ms and the system operates stably. The test results prove that the system meets the performance requirements of the existing network operation.

Compared with other relevant existing methods and systems, our framework and system has many more advantages in the analysis of performance indicators, function indicators and even in the scene parts. Specifically speaking, it is as follows.

From the perspective of performance indicators, compared with other methods and systems, our system can have more terminals involved in concurrent intervention, up to 30, while other systems can only reach up to 15. As for network latency, the network latency of our system is lower, less than 500 ms, while other systems reach up to 1000 ms. Concerning to the query response time of the cloud platform of security capabilities, our query response speed is faster, response time is shorter, less than 200 ms, while the query response time of other systems can generally reach up to 500 ms, sometimes even 1000 ms. For malicious URL detection accuracy, our system accuracy is greater than 99.9%, while the detection accuracy of other systems may only be 85–95%.

From the perspective of functional indicators, the functions of our system are more abundant than other methods and systems. In addition to network accessing and network routing functions of other systems, our system has link selection functions, security filtering functions, encrypted communication functions, and secure storage functions, etc.

From the perspective of scene, compared with other methods and systems, our system has mobile office security access, IoT security access, industry terminal security access, and home gateway security access scenarios, which is much more than other systems.

The following Figs. 7, 8 and 9 are the practical application figures. Figure 7 displays cloud-end platform of security capabilities. Figure 8 displays channel-end secure accessing devices. Figure 9 displays device-end security control APP.

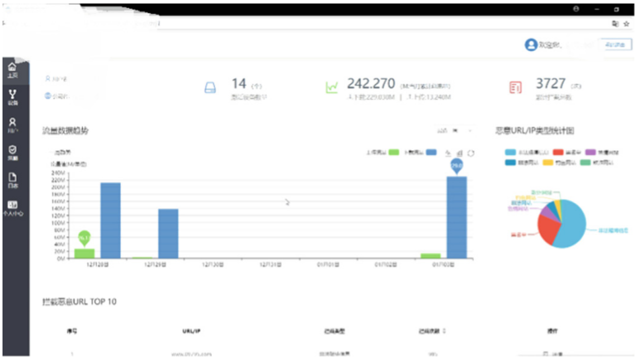
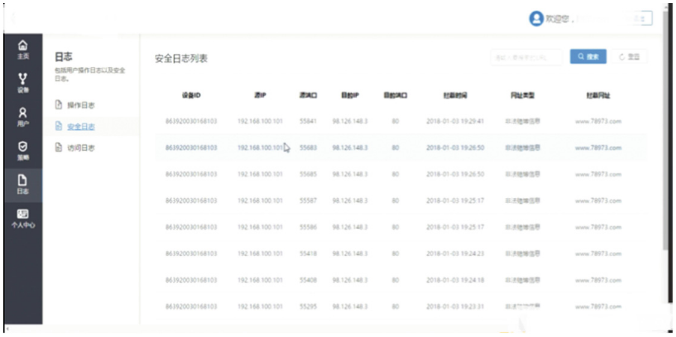


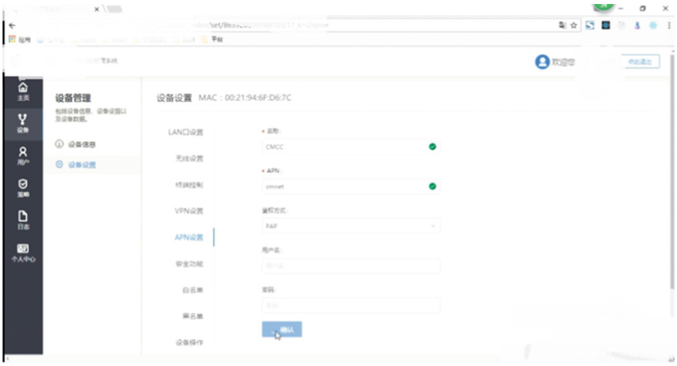
Fig. 7. Display of cloud-end cloud platform of security capabilities



安全日志列表

设备ID	源IP	源端口	目的IP	目的端口	拦截时间	网址类型	拦截网址
863920030168103	192.168.100.101	55841	98.126.148.3	80	2018-01-03 19:29:41	[illegible]	www.78973.com
863920030168103	192.168.100.101	55683	98.126.148.3	80	2018-01-03 19:26:50	[illegible]	www.78973.com
863920030168103	192.168.100.101	55685	98.126.148.3	80	2018-01-03 19:26:50	[illegible]	www.78973.com
863920030168103	192.168.100.101	55587	98.126.148.3	80	2018-01-03 19:25:17	[illegible]	www.78973.com
863920030168103	192.168.100.101	55586	98.126.148.3	80	2018-01-03 19:25:17	[illegible]	www.78973.com
863920030168103	192.168.100.101	55418	98.126.148.3	80	2018-01-03 19:24:23	[illegible]	www.78973.com
863920030168103	192.168.100.101	55408	98.126.148.3	80	2018-01-03 19:24:18	[illegible]	www.78973.com
863920030168103	192.168.100.101	55295	98.126.148.3	80	2018-01-03 19:23:31	[illegible]	www.78973.com

Fig. 8. Display of channel-end secure accessing devices



设备设置 MAC：00:21:94:6F:D6:7C

* 名称：CMCC

* APN：cmnet

鉴权方式：PAP

用户名：

密码：

Fig. 9. Display of device-end security control APP

7 Conclusion

In this paper, security protection framework based on cloud-channel-device cooperation is proposed in this paper to solve the issue. The trust base is introduced to channel-end to improve trust of secure accessing device. Then, the trust and security module are designed in the cloud-end. Meanwhile, access control based on connection tracking is adopted to reduce access latency. The framework can be used to construct an open, trusted, resilient network for secure accessing and provide security solutions for mobile office, IoT security, information security management and control, etc. The security protection framework has been implemented and tested by a third party testing agency, the result shows that the proposed framework has better performance compared to other methods. At present, the framework has been practically applied to the market and the results show that it is useful and effective. It will be applied to operators, enterprises and government departments on a large scale.

Acknowledgement. This work is supported by the National Natural Science Foundation of China (No. 61702508 and No. 61602470) and Strategic Priority Research Program of Chinese Academy of Sciences. This work is also supported by Key Laboratory of Network Assessment Technology at Chinese Academy of Sciences and Beijing Key Laboratory of Network Security and Protection Technology.

References

1. Scarfo, A.: New security perspectives around BYOD. In: BWCCA 2012, pp. 446–451 (2012)
2. Peng, W., Li, F., Han, K.J., Zou, X., Wu, J.: T-dominance: prioritized defense deployment for BYOD security. In: CNS 2013, pp. 37–45 (2013)
3. Li, F., Huang, C.T., Huang, J., Peng, W.: Feedback-based smartphone strategic sampling for BYOD security. In: ICCCN 2014, pp. 1–8 (2014)
4. Zahadat, N., Blessner, P., Blackburn, T., Olson, B.A.: BYOD security engineering: a framework and its analysis. Comput. Secur. **55**, 81–99 (2015)

5. Yeboah-Boateng, E.O., Boaten, F.E.: Bring-Your-Own-Device (BYOD): an evaluation of associated risks to corporate information security. CoRR abs/1609.01821 (2016)
6. Hovav, A., Putri, F.F.: This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. Pervasive Mob. Comput. **32**, 35–49 (2016)
7. Hong, S., Baykov, R., Xu, L., Nadimpalli, S., Gu, G.: Towards SDN-defined programmable BYOD (Bring Your Own Device) security. In: NDSS (2016)
8. Kumar, P., Braeken, A., Gurtov, A., Iinatti, J., Ha, P.H.: Anonymous secure framework in connected smart home environments. IEEE Trans. Inf. Forensics Secur. **12**(4), 968–979 (2017)
9. Park, J., Kwon, H., Kang, N.: IoT-Cloud collaboration to establish a secure connection for lightweight devices. Wireless Netw. **23**(3), 681–692 (2017)
10. Ranjbar, A., Komu, M., Salmela, P., Aura, T.: SynAPTIC: Secure And Persistent connecTIvity for Containers. In: CCGrid 2017, pp. 262–267 (2017)
11. Zhao, J.: On resilience and connectivity of secure wireless sensor networks under node capture attacks. IEEE Trans. Inf. Forensics Secur. **12**(3), 557–571 (2017)
12. Kim, H.: Design of a secure digital recording protection system with network connected devices. In: AINA Workshops 2017, pp. 375–378 (2017)