Safety risk analysis of Home Automation products

Hongqi Luo¹, Xia Liu²*, Po Wang ¹

¹ School of Artificial Intelligence, Beijing Technology and Business University, Beijing, China
² Quality Management Branch of China National Institute of standardization, Beijing, China

*Corresponding author’s e-mail: liuxia@cnis.ac.cn

Abstract. Home Automation can provide people with safe and comfortable living environment, but due to the defects of related equipment and support technology at different levels, the safety accidents of Home Automation products occur from time to time. By analyzing the composition of Home Automation system, the characteristics of each subsystem and the existing security risks, the risk relationship of each subsystem is analyzed. The risk research status of Home Automation products at home and abroad and the status of standard formulation and revision are compared, so as to provide support for the corresponding theoretical analysis and practical application.

1. Introduction
Home Automation is based on the residential platform, which uses the integrated wiring technology, network communication technology, and Safety prevention technology, automatic control technology and audio-visual technology[1]. Home Automation integrates the facilities related to home life, build an efficient management system of residential facilities and family schedule affairs. It can improve the safety, convenience, comfort and artistry of the home, and realize the environment of environmental protection and energy conservation[2]. Home Automation products are various, with an increasing trend year by year, covering intelligent security, intelligent lighting, intelligent background music, Home Automation appliances, intelligent security, intelligent environment monitoring and other aspects.

From home functions, it can be divided into home automation, home network, network appliances and information appliances. Home automation refers to the use of micro-processing electronic technology to integrate or control the home electronic and electrical products or systems[3]. Home network refers to the network system connecting PC, various peripherals and Internet in the family. It is a part of the home network. Network appliance is a new type of household appliance product which is designed and improved by using digital technology, network technology and intelligent control technology. Information home appliances are low price, easy to operate, practical and have the main functions of PC[4].

2. Technical characteristics and development trend of Home Automation products
With the implementation of integration technology, communication technology, interoperability and cabling standards, Home Automation network is constantly improving. It involves the operation and management of all intelligent furniture, equipment and systems in the home network, as well as the application of integration technology[5].
2.1. Technical features

2.1.1. Home gateway as the core part.
Home gateway is the core part of Home Automation LAN, which mainly completes the conversion and information sharing between different communication protocols in home internal network, and the data exchange function with external communication network. At the same time, the gateway is also responsible for the management and control of home intelligent devices.

2.1.2. Unified platform.
With computer technology, microelectronics technology and communication technology, home intelligent terminal integrates all functions of home intelligence, making Home Automation built on a unified platform. First of all, realize the data interaction between the home internal network and the external network; second, ensure that the instructions transmitted through the network are legal instructions, not the illegal invasion of "hackers". Therefore, the home intelligent terminal is not only the transportation hub of family information, but also the "protector" of information family.

2.1.3. External expansion module for interconnection with home appliances.
In order to realize the function of centralized control and remote control of household appliances, the home intelligent gateway controls household appliances or lighting equipment by means of external expansion module according to specific communication protocol through wired or wireless way.

2.1.4. Application of embedded system.
In the past, the vast majority of home intelligent terminals were controlled by single chip microcomputer. With the increase of new functions and the improvement of performance, the embedded operating system with network function and the control software program of single-chip microcomputer are adjusted to form a complete embedded system. Embedded technology is ubiquitous in Home Automation. Intelligent gateway is the core embedded device in Home Automation. The resource of home appliance control node is less than that of intelligent gateway. Embedded operating system is transplanted into intelligent gateway to manage the whole Home Automation system. Embedded devices used in Home Automation can cut and expand the hardware and software according to the needs of customers. It has high flexibility and avoids unnecessary redundancy.

2.2. Development trend

2.2.1. Environmental control and safety regulations.
The purpose of the construction of Home Automation is to provide people with a safe and comfortable living environment, but the current Home Automation system shows many shortcomings in this aspect, because the future development of Home Automation is bound to carry out the improvement work in this aspect, and this concept runs through all systems of home life, such as audio-visual equipment, temperature control For this aspect, we also need to complete the parallel task of remote control and centralized control to ensure that the whole home life reflects the characteristics of more humanization[6].

2.2.2. Application of new technology and new field.
In the future development process of Home Automation, in order to adapt to the development situation at that time, it is bound to integrate with new technologies that have not been combined with it. The development of new communication technologies such as IPv6 will play an important role in promoting it. The control of Home Automation will trigger a new trend in the development of IT industry. After the improvement of Home Automation system, it can be applied in the commercial atmosphere, so as to broaden its application scope. This situation will make the market of Home Automation expand in a large range.
2.2.3. Combined with smart grid.
In our country, the construction of smart grid has its fundamental demand. It will provide all kinds of intelligent facilities services for the whole residence. In the process of power services, it can also form a penetration effect on the network of Home Automation. If users of smart grid are also enjoying the services of Home Automation, their demand is that they can establish an effective relationship between the two Close communication can coordinate all kinds of information of the combination of Home Automation and smart grid, and then carry out the actual effective management.

3. Quality and safety status of Home Automation products
At present, Home Automation security research is mainly divided into platform security, device security and communication security. Platform security research mainly focuses on identity authentication and access control scheme design, and finds security problems in new scenarios such as device linkage and intelligent speaker. Communication security research mainly focuses on protocol vulnerability mining and network traffic analysis[7]. Device security research mainly focuses on device firmware vulnerability mining and device side channel analysis.

3.1. Platform security
The platform connects all kinds of Home Automation devices and services. The security problem of the platform will bring serious threat to the Home Automation ecology of manufacturers, and will affect all devices and end users under the platform, so the platform is the focus of Home Automation security research. The security problems of the platform mainly exist in the following aspects: Home Automation user authentication, Home Automation device access control, device linkage security and smart speaker security.

3.2. Equipment safety
There are many kinds of Home Automation devices, and the number of smart device security vulnerabilities is also very alarming and serious. It not only enables attackers to control devices locally or remotely, steal user privacy data, but also threatens personal and property security. According to the state Internet Emergency Response Center (CNCERT) released "China's Internet network security situation in 2019", in 2019, the number of security vulnerabilities included in the national information security vulnerability sharing platform (cnvd) reached a record high, with a year-on-year growth of 14.0%, a total of 16193. At present, there are more than 15 malware families active on smart devices, including Mirai, gafgyt, dofloo, tsunami, Hajime, mrblack, etc. These malicious programs usually invade and control intelligent devices through loopholes, brute force cracking and other ways. There are a lot of security threats and risks after the network intelligent devices are controlled by intrusion, including the leakage of user information and device data, the control and destruction of hardware devices, being used for DDoS attacks or other malicious attacks, attacking routers and other network devices to steal users' online data, etc. In 2019, CNCERT will capture about 3.241 million malware samples of smart devices. There are about 27800 IP addresses in the service end, most of which are located abroad (accounting for 79.9%), and the number of IP addresses of suspected infected smart devices in China is about 2038000 (up 31.8% on a year-on-year basis).

3.3. Communication security
Communication protocol security is the basis of user sensitive information transmission protection. Finding the security problem of communication protocol has always been the focus of network security research. In the research of Home Automation security, researchers mainly focus on the security issues in the configuration and implementation of popular ZigBee, Bluetooth and other protocols, as well as common Mqtt, COAP and other application layer protocols[5].

Network traffic analysis is an important method of computer information security research. It takes the network traffic generated by a group of devices as input and the information related to these devices, users, applications or traffic itself as output. By analyzing the network traffic of Home Automation
system and understanding the relationship between network traffic characteristics and device behavior, we can evaluate the security status of Home Automation system, control the privacy leakage of Home Automation devices, alleviate the security threat of Home Automation system, and manage the security of Home Automation system at the network layer.

4. Analysis of the safety risk of Home Automation products

4.1. Product safety risk relationship

In general, all kinds of electronic equipment in Home Automation widely use electronic devices and software. In addition to the safety risks caused by the problems of material, structure design, software and hardware failure of the equipment, functional security and network security risks caused by equipment interconnection and interoperability, remote network operation, etc. if these risks are not properly evaluated and handled, they will be set up The standby transmission to the user, make it in a dangerous state, even cause personal and property damage. Under the network conditions, the local security problems and network security problems interact with each other. As shown in Figure 1, the main security threats and possible security risks faced by Home Automation products are briefly described. Among them, the risks in equipment security and functional security mainly come from the equipment body, which will directly affect the personal property security of users; the threat of network security mainly comes from the network, which will bring direct data leakage and property loss to users, and indirectly affect the personal property security of users[1]. For non network devices, there is no network working scene, and there is no security threat as described on the right side of Figure 1.

![Figure 1 security threats and possible risks of Home Automation products](image)

4.2. Comparative analysis of domestic and foreign standards

Since the world's first intelligent building appeared in the United States in 1984, the United States, Canada, Europe, Australia, Southeast Asia and other economically developed countries have put forward a variety of Home Automation solutions. Home Automation has been widely used in the United States, Germany, Singapore, Japan and other countries[8].

| Analogy content   | Foreign developed countries                                                                 | Domestic                                                                 |
|------------------|---------------------------------------------------------------------------------------------|--------------------------------------------------------------------------|
| Industry development | It develops early and has a large scale; It has large consumer groups, wide application fields, high quality, strong sense of science and technology, and wide audience. | It starts late and has low market access; The ability of independent research and development is weak; Compared with traditional home furnishings, the degree of acceptance is not high; Rapid development and great market potential. |

Table 1  Comparison of domestic and foreign standards
By comparison (shown in Table 1), it can be seen that the Home Automation industry in major developed countries has entered an advanced stage. Relying on laws and regulations, market access, product safety, quality and performance and other factors, foreign consumers pay more attention to their own privacy, data security, high quality and high standards when purchasing Home Automation products, so as to truly meet their own requirements for Home Automation. However, the development of Home Automation industry in China is relatively late, just after the initial stage, and the audience is relatively small.

5. Conclusion
Home Automation can improve people's living environment. In the future development process, it will continue to adapt to the development situation at that time, integrate new technologies, continuously develop and improve in all aspects, broaden its application scope, and need to solve all kinds of security risks according to the development situation. It can solve all kinds of problems from the aspects of cloud protection, device terminal protection, communication protocol protection, etc., design a secure identity authentication, authentication and access control mechanism. It can solve firmware reinforcement and confusion processing. It is useful to standardize the development and test process to prevent known vulnerabilities. It can take necessary measures to resist side channel attacks and use security chips to avoid meltdown and SPECT Re and other vulnerabilities. It can also use encryption algorithm with high security strength to encrypt transmission data and use mature communication protocol with high security strength. Home Automation can strengthen the authentication process to ensure that the transmission data and user privacy content are not obtained by the third party, and add random numbers, time stamps and other ways to resist replay attacks. Only by continuously reducing the security risk in the process of Home Automation development, can the Home Automation industry get rapid development.

Acknowledgments
Project is supported by National Key R&D Program of China (2017YFF0207200).

References
[1] Liu Jia. Research and design of Home Automation security protocol based on ECC and embedded [D]. Chengdu: University of Electronic Science and technology, 2017.
[2] http://field.10jqka.com.cn/20191028/c614690363.shtml
[3] https://baike.baidu.com/item/%E6%99%BA%E8%83%BD%E5%AE%B6%E5%B1%85/686345?fr=aladdin
[4] http://www.tiansongdata.com/data/1032-cn.html
[5] Li xiaopro, ansa, Wang Liwei, wenxinyu, Zhou Dong. Overview of Home Automation development and key technologies [j]. Measurement and control technology, 2018,37 (11): 1-4+15
[6] Zhang Wei, Hu XiongQiang, Wang Mingqian, Ren Kang. A design of intelligent home system based on Internet of things [j]. Information technology, 2019 (03): 48-51
[7] Deng Yun, Li Chaoqing, Cheng Xiaohui. Design of intelligent home remote wireless monitoring system based on Internet of things [J]. Computer application, 2017,37 (01): 159-165

[8] Hu Xiangdong, Han Kaimin, Xu Hongru. Security design and verification of Home Automation Internet of things [J]. Journal of Chongqing University of Posts and Telecommunications, 2014,26 (02): 171-176