A Design Solution to Security Simulation Platform for Intelligent Household

Hui Wang[1], Chengze Li[1*], Jing Yuan[1], Zhimin Wu[1].

{wh@cert.org.cn, lichengze@cert.org.cn, yuanjing@cert.org.cn, wuzhimin@cert.org.cn}

National Computer Network Emergency Response Technical

Team/Coordination Center of China, Beijing, 100029[1]

Abstract. Recently, with the rapid development of intelligent household, security issues have arisen. The design architectures adopted by intelligent household are usually significantly different, and the communication technique differs from others as well. So, the analysis technology involved for security purposes is very complex, and it is difficult for existing technique to effectively analyze the vulnerabilities of intelligent household. To tackle this problem, this paper presents a design solution of security of intelligent household, by achieving a simulation platform with universal applicability. In this paper, we study the monitoring methods for popular terminal equipment of smart home, including the system, mobile apps, communication methods, telematics service providers, and so on. Based on these methods, we implement a simulation platform, to recognize potential security issues of intelligent household. The establishment of the simulation platform provides a test environment for the research on the security technology of intelligent household.

Keywords: intelligent household, smart home, simulation, taint monitoring, security analysis.

1 Introduction

Smart Home is based on a common physical residential. It uses hardware of home equipment to wire and access networks to communication, applies security technology to enhancing the security performance and facilitates control by adding automatic control technology to upgrading family comfort. What's more, multimedia technologies are integrated into the home-life-related facilities, building an efficient, high-comfort and high-security home ecosystem that improve the quality of life [6].

With the development of Internet and other applications, smart home become increasingly intelligent and automatic, but at the same time security issues in smart home become even more prominent and urgent. The current smart home security threats are: self-halt of systems, intrusion of system, invasion of control terminals, and characteristics attacks [1].

There is a certain relationship between the highlighted security issues of intelligent household and security mechanism designed by smart home manufacturers. On one hand, technically speaking, manufacturers leave loopholes to smart home because they did not pay enough attention to it and erred in trusting the home network which expose products easily to debugging interface from the Internet.

MOBIMEDIA 2019, June 29-30, Weihai, People's Republic of China

DOI 10.4108/eai.29-6-2019.2282822

Simultaneously, negligence of safety management of intelligent router as the smart home system control center, which gives opportunity to hackers. On the other hand, this kind of negligence and misplaced trust also comes from the user. Hackers can easily figure out the password if a simple password is set, causing security vulnerabilities of intelligent household. In addition, unified safety standards of the smart home industry and fragmented nature of the major manufacturers leave a hidden danger to the intelligent home security.

At present, solutions to intelligent home security issues mainly focus on Intelligent Gateway [2]and physical networking applications [3][4], maintaining the safety of smart home system by node authentication, identity authentication and access control, data transmission security [4], the audit log [6], and other technologies. However, whether these security technologies for security vulnerabilities exposed is valid, and whether there are other unknown security risks, effective methods of testing and evaluation are in need. Furthermore, under the premise that testing and evaluating the effectiveness and performance in security mechanisms cannot destroy the actual device or system, a universal smart home security simulation platform should be established. By simulating for the physical security of the home environment, a variety of safety tests were carried out to discover security risks and vulnerabilities, and it can promote to study and put forward relevant security mechanisms to monitor and manage security situation of the smart home system.

The second part of this paper presents an overall design of the intelligent home security simulation platform, the third part elaborates implementation of the platform and its function, the fourth part makes a brief analysis of the simulation platform features, which has a guiding role in technical security system research and implementation of the current smart home.

2 An design solution for security simulation platform of intelligent household

Through the analysis of smart home security situation and current needs, the main function proposed is in the simulation of real smart home environment for facilitating testers to test existing home security system, including intelligent home security test, home monitoring system security test, home control system security test, etc. In this platform, testers get real-time data of interactive contents and internal logic situation of the measured target by monitoring systems to find potential existing vulnerabilities in smart home system and the attack, and finally make an assessment of them and made repair method.

Therefore, the intelligent home security simulation platform should achieve the following functional goals:

(1) Can simulate home network environment;

(2) Can monitor smart home control systems, data interaction and internal logic situation of smart home in real time;

(3) Can provide specialized system interface, let various types of existing smart home system components fast access to the platform, and carry out safety testing.

Based on the functional objectives of intelligent home security simulation platform, a design scheme of smart home security simulation platform is presented. As shown in **Figure 1**, the smart home security simulation platform is divided into three subsystems: data monitoring subsystem, simulation subsystem, and security detection subsystem.

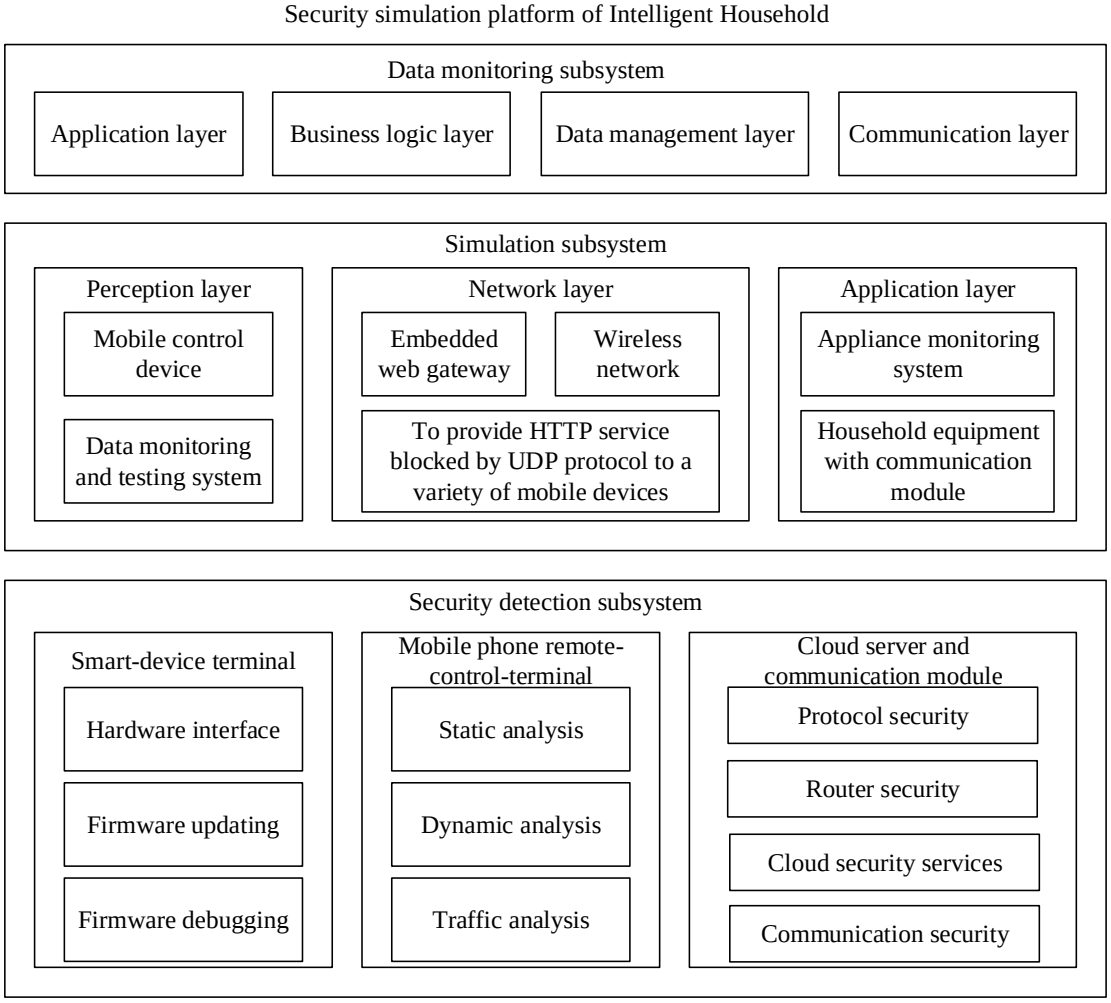

Fig. 1. The overall architecture of Intelligent home security simulation platform.

The data monitoring subsystem is responsible for monitoring intelligent home data monitoring, displaying the results, and launching the study from extracting features, data mining and analysis. It was divided into the application layer, business logic layer, data management and communication layer, and achieves data monitoring and analysis capabilities in combination with them. The simulation subsystem is responsible for realizing the smart home system simulation, and providing access interface to various smart-home-related equipment. The access interface is used to establish various experimental operating environments of smart home devices. The simulation covers the functions of the application layer, the network layer and the perception layer. The security detection subsystem is mainly responsible for security detecting various intelligent home equipment, including verifying Smart Home related known security issues, exploring new security risks related to smart home, and at the same time studying the patch upgrade approach, extensively involving security detection of intelligent terminal equipment, mobile remote control terminal, the cloud server and communication module.

Based on the function architecture of the platform, the program can solve the following four security issues about the smart home system:

(1) To verify the security vulnerabilities of smart home, analyze its generation mechanism, and proposed prevention methods.

(2) To explore the possible existence or unknown security risks of intelligent home, then proposed

security methods;

(3) To guide a research about related technologies of intelligent home security, and build a smart home security system;

(4) To monitor the security situation in the whole intelligent home network, and form the security posture analysis of the whole network security intelligent home.

3 Realization scheme of intelligent home security simulation platform

This section describes the specific implementation method and design content of intelligent home security simulation platform.

3.1 Data Monitoring Subsystem Design

Operating data monitoring subsystem uses ALDC four-system-designed structure. Its main duty is to operate as a center of the entire test platform, and can remote control other nodes to send a test message to test the smart home node (such as the control center) and collect its data memory and control figure through the testing platform network, to some extent, automate analyze and present to the testers.

Operating data monitoring subsystem is divided into four layers: application layer, business logic layer, data management layer and communication layer. The layers' function designed as follows:

(1)Application layer

Interaction level with testers. In addition to obtain operational information about the test officer, it will also show the results on the external large screen. Application layer provides a variety of automation applications, such as automatic target detection system, automated analysis of returned data, and generation reports of results.

(2)Business logic layer

Logical core of data monitoring operating platform, provides basic logic operations for the upper application and management of the underlying database.

(3)Management layer

Manage multiple databases, including knowing weak database, commonly using test script library, as well as the data in the near future of the home environment, facilitating the testing and system cross-match to find weak spots.

(4)Communication layer

Bearer of information exchanges between the test platform network and the target control center

3.2 Simulation Subsystem Design

1. The architecture design of simulation subsystem

Simulation subsystem is divided into three layers: perception layer, network layer and application layer.

The perception layer is equipped with a wireless communication module of furniture and equipment to achieve a comprehensive perception of family environment. It can return smart home situation and home environment information immediately to control center by home appliance monitoring module and accept the scheduler from control center for controlling of intelligent furniture.

The network layer in the core platform first need to simulate the user service interface in intelligent home control center, which by means of a virtual machine. the interface is usually presented in the form of Website. Control Center lets user interface's web runs on its own server and published on the Internet, then legal or authorized user through some authentication information logs in the Web

Interface and operation. The control center via RS232 serial ports links home appliances monitoring module, receives the return information of home appliances monitoring module to achieve control. It supports a variety of network communication modes, can access the Internet through a wired network, and also contains GPRS module to make wireless communication. Besides the control center via the USB interface mode accesses surveillance cameras to monitor the overall family environment.

The application layer provides good interaction. Users can adopt their mobile devices that equipped with a variety of web browsers to visit above sites, so to realize the management and control of smart home system. Furthermore, testers can test the smart home environment through data monitoring system.

2. The sub module design of simulation subsystem

Control Center is the core of intelligent home, which receives user's operation and monitors the underlying device. It can access the home network simulation environment in different ways, and communicate with intelligent home node in home environment through family's dashboard module.

Data Monitoring and Testing System are the central modules of the test platform, also are the main operating system of testers. As a platform that observes smart home real-time data, analyze the contents to find a suspected weakness, it controls all testing process in a simulated environment, and monitor the behavior and data of all the smart nodes under family environment.

Finally, the communication module is a bridge to complete the communication between intelligent home appliances and control system. Legitimate users' phone after connecting the internet can access the Internet cloud server, through users it can connect the smart home control system that has already registered, get home information and publish home command. Or in case of near-field communication, users can directly access to the nearest authorized smart home control systems.

(1) Design and Simulation of Smart Home Control Center

i) Hardware design of smart home control center

Intelligent home control center is simulated by installing a virtual machine in PC and other devices, involves the hardware design, the following describe hardware design of other modules:

-- Applications control module uses ARM＋AVR as the corn, communicates with the control center by serial ports. In the smart home system, home applications control panel is connected to common serial ports, and network communication module connecting to Bluetooth serial ports. Furthermore, the sensor interface circuit takes advantages of photoelectric coupling chip's sensitivity to sensors' output, outputs level signals to the SCM Interface connected. Then SCM collects alarm signals and makes appropriate treatments.

-- Video monitoring module is connected to ARM + AVR experiment box through the USB interface.

-- Network communication module which corresponding to the smart home communication mode is divided into three modules. Wherein the GSM communication part connects to and communicates with the experiment box via RS-232 serial port. The wireless communication section can use the home Wi-Fi service as long as catching an external wireless card, and the wired communication part needs access home network switches and gateways.

ii) Hardware design of smart home control center

-- Core logic server: The core server is to run the user interface operation Web, which usually is an embedded system. Furthermore, it can use Tomcat + Apache way to build a website server in Windows Server 2003, and do basic security configuration of Tomcat by operations like turning off the server port, adding firewall and shielding directory files which are automatically listed, so to enhance

its security level. Website design uses the hierarchical design, stratifies corresponding function from top to bottom in application layer, business logic layer, network layer and sensing layer.

-- Control panel of furniture: Control panel through smart home monitor, home sensor and core server, packages received information by means of the protocol stack, sends and receives furniture control signals and unload information of home sensor. For this purpose, design and implementation seamless integration between STP/SP protocol and TCP/IP protocol, so compatible with existing network communications, and communicate ordinary TCP/IP networks with intelligent home node.

(2) Cloud server simulation

It uses ALDC four-layer system. Users apply for services by accessing to the application layer of cloud through the mobile terminal. The Cloud authenticates users' identities and then jumps to the users' own home control centers. Users select specific services and transmit them to cloud servers. Then cloud server authenticates control security and forwards control information. Finally, the results will be returned to the terminal to display to the users after cloud services finishing the work.

Communication layer: It mainly completes the service of exchanging information with smart home center and user mobile terminal, including service application, information interaction as well as download and upload service outcome data and terminal information.

Data management layer: It manages the database in the cloud platform system. It can call the interactive services of the communication layer to collect smart-home and user data and send result data of services. It can also be called to provide and manage data for logical operation of services by the business module logic layer.

Business module logic layer: It completes the core module of cloud service. The service module of the application layer is split into several logic modules to realize the reuse of the service.

Application layer: It is the layer of interacting with users, and it can provide a variety of services. After receiving users' requests, it calls the corresponding business logic module and combines the results to present issues to users.

(3) Smart-home node network communication simulation

i) ZigBee

Generally, smart furniture and smart home nodes have ZigBee transceiver and driver. If not, it will be easy to install the above part. There are connection serial ports of the ZigBee transceiver module on the home control panel. A home control panel can communicate with other smart-home nodes through ZigBee and receive the sensing information of smart home and send controlling signals.

ii) family Wi-Fi

The smart home network which is simulated in the test platform is built with reference to large family network. Usually the control center is connected to the Internet via the home Wi-Fi network. Home Wi-Fi network requires comprehensive coverage, strong penetration to ensure the control center network smooth. Therefore, we will build a multiple access-node family Wi-Fi network to adapt to a variety of terrain family environments and experimental environments.

3.3 Security monitoring subsystem

The technical architecture of Internet of things (IoT) technology applications which is represented by smart home can be divided into cloud server, device terminal and mobile phone terminal. The implementation process of IoT technology is mainly: 1) mobile phone downloads remote control App; 2) communicates with cloud server; 3) cloud forwards control instruction to device terminal. It controls a smart device in the network in any environment that can access to the Internet.

Intelligent home security detection module set information point of data interaction as an attack

surface according to the flow of information data. Information point can be divided into smart-device firmware, App remote control terminal and Cloud server. Each information point has the process of data storage, data interaction and data controlling. This section will decide whether there is a security risk through the analysis of interactive data, authentication, transmission encryption and access control. It will also do safety detection from the aspects of the intelligent terminal equipment, remote app, and cloud server to reduce the occurrence of security problems.

1.Smart-device terminal security detection

Smart-device terminal is the main part of the smart home. Currently, the mainstream Smart-device terminals have common security risks. It can be mainly from the following three parts to carry out safety testing:

(1) Hardware interface security detection

The hardware interface is used for debugging the design, program burning, and diagnostic testing. 80% of the hardware on the device are reserved for debugging interfaces. Through these interfaces, attackers can get the details of the implementation details, and then use the understanding of these information, remotely effect more and more types of equipment.

(2) Firmware upgrading security detection

Firmware upgrade issues include: upgrading package source, downloading and transmitting, whether version and content are safe, whether the data of the update file is sensitive and whether the implementation of the update operation is complete. These problems can all allow an attacker to get, unzip, analyze, tamper firmware, and finally record to the device leading to persistent effect.

(3) Debug command interface in firmware

The debug command interface in the Internet of things is used in factory tests and the development and debugging. Based on the understanding of protocols, attackers can encapsulate the corresponding call interface and remotely operate equipment. Therefore, we need to do security detection on debug interface services.

2. Mobile phone's remote-control-terminal security detection

It is an important guarantee for the safety of smart home to use remote control application of mobile phone to do security detection on smart home system. Protection of App and the corresponding system is the core issue of smart home security. This project adopts the method of static analysis and dynamic analysis to carry on the security test and the vulnerable analysis of the application program and the system.

(1) Static analysis

Static analysis of the application software program is a code analysis, including preprocessing, decryption, reversion, and flow analysis. According to the data flow, control flow, semantic and other information in the program, it is matched with the specific software security rule based to finding out the potential security vulnerabilities in the code. In addition, static source code security testing is also a very useful method.

(2) dynamic analysis

Dynamic analysis implements client's applications dynamically, constructs fuzz test cases, runs monitor agent, captures key behaviors at running time, and carries out safety detection and analysis. Dynamic analysis mainly uses the dynamic tracking technology. Dynamic tracking technology is divided into dynamic debugging technique and dynamic taint tracking technology.

(3) Software database structure security detection

Software database's file security detection analyzes and detects the potential vulnerabilities in the

local database of mobile phone software through Password invasion, privilege upgrade, vulnerability invasion, SQL injection, steal backup and other means of attack. It is an integral part of the remote control of App detection.

3. Cloud server and communication module security detection

Communication between smart homes is usually required to support one or more communication modes at the same time. It can choose different communication modes according to different applications and data priority. These communications mean there are all kinds of traditional security risks, vulnerable to various types of attacks by hackers. We intend to carry out security detection from the smart home directly connects to protocol analysis, intelligent router, the cloud server, and communication between them.

(1) Protocol analysis security detection

Study protocol reverse parsing refers to using the idea of reverse analysis, analyzing format the target network application protocol used, simulating protocol and analyzing defects, etc. The specific approach is to combine static analysis with dynamic debugging technology based on network analysis tools. By analyzing the communication protocol of smart home, it can be more efficient to detect the overall security of the system.

(2) Intelligent router security detection

With the development of the Internet of things, more and more smart home products launch intelligent routers. These smart routers have brought many convenient functions, but also own some security characteristics which the traditional router does not have. These characteristics are mainly concentrated in the back door of the router and firmware update. Therefore, it is necessary to carry out the security detection. The encryption algorithm security detection is the most necessary and important.

(3) Smart-home cloud services security detection

This module can be specifically studied from the smart home cloud services perception layer, application layer and key management. The Cloud services perception layer detects the security of smart home system by obtaining external information. The Application layer carries out external detection in view of the security problems existing in the smart home system. Key management includes key distribution, key and identity binding, key generation, key maintenance and revocation.

(4) Security issues in devices, cloud, and mobile applications

Tampering and eavesdropping of smart-home communication links can lead to hijack, sensitive information**'s** disclosure and unauthorized access. Security issues in devices, cloud, and mobile applications include: if it is authenticated between equipment and server, if it is able to resist the middle attack between equipment and server, if the channel encrypted and if there is a replay attack.

4 Characteristics analysis of smart home security simulation platform

In this paper, a universal intelligent home security simulation platform is built with the analysis of the characteristics of smart home and security needs. The platform has two advantages: (1) it contains the mainstream smart home terminal devices, mainstream smart home communication methods, and a variety of monitoring means; (2) it covers a variety of detection and analysis methods for smart home security problems and security risks.

5 Conclusion

This paper presents a smart home security simulation platform. It implements the smart home environment simulation configuration and security monitor through data monitor, simulation and security detection. It meets requirements of the experimental study of existing safety problems. At the

same time, it meets the various tests of possible security vulnerabilities. It will help further study of the relevant issues of smart home, as well as protect the healthy and steady development of the smart home industry.

Acknowledgments

This work was supported in part by the National Key R&D Program of China under Grant 2018YFC0806900.

Reference

[1] Lou, Y., Bai, Y.: Smart Home Security Issues [J]. Computer CD Software and Applications, 2014(13):178-179.

[2] Forrest, S.: Security Will Be the Primary Challenge for the Development of Intelligent Home Gateway. Electronics Today, 2016(1):34-35.

[3] Wang, X.B.: Analysis of the Security of Smart Home Networking[J]. Modern Business, 2015(8):28-29.

[4] Luo, H., Yang, J.: Discussion on Intelligent Home Security in the IoT[J]. Information and Computer, 2015(21):76-78.

[5] Yin, J., Yuan, J., Yu, J.B.: Review of Smart Home System [EB/OL]. Beijing: Chinese Science and Technology Papers Online. [2012-04-28].

[6] Zhu, H.X., Liu, Y.H., Song, Y.: Research and Design of Smart Home Security System[J]. Journal of Beijing Polytechnic College, 2015(14(2)):9-12.

Hui Wang, received the Ph.D. degree in Computer Science and Technology from Harbin Institute of Technology, Harbin, China. He is currently an security engineer of National Computer Network Emergency Response Technical Team/Coordination Center of China. His research includes network security and Internet of things, mathematical modeling on networks.

Chengze Li, received the Ph.D. degree in information security at Beijing University of Posts and Telecommunications, China. He is currently an security engineer of National Computer Network Emergency Response Technical Team/Coordination Center of China. His research interest lies at the intersection of program analysis, privacy and security analysis of mobile systems and Internet of things.

Jing Yuan, (b. June 18, 1983) received her Ph.D. degree (2014) from Department of Automation, Tsinghua University, China. Now she works in National Computer Network Emergency Response Technical Team/Coordination Center of China. Her research interests include network security, malicious program analysis and IoT security.

Zhimin Wu, received his Ph.D. degree in computer science and engineering from Nanyang technological University, Singapore. Currently he is a security engineer in National Computer Network Emergency Response Technical Team/Coordination Center of China. His research interests are related to the interaction of software engineering, cybersecurity and internet of things