Smart Home Secure Authentication and Communication Method Based on Trusted Platform Module

Peng Wang

College of Automation, Chongqing University of Posts and Telecommunications, Chongqing 400065, China

poengwang@163.com

Abstract

With the rapid development of the internet of things, smart home technology as an important branch of its application field, becoming more and more popular in people's daily life.However, the existing smart home systems require using open network to remote monitoring and control household equipment, this makes smart home system kernel which carrys a lot of important information will face malicious intrusion from the external network, the communication data will transmit through an insecure channel between the external network and the home network at the same time. This paper presents a smart home secure authentication and communication method based on trusted platform module, by building trusted platform module and embedded SHA-1 hash algorithm to authenticate integrity of smart home system kernel, applying AES symmetric encryption algorithm realize monitoring and control information’s secure communication for smart home. Test results in the embedded smart home platform show that: this secure authentication and communication method can effectively discriminating reliability of system kernel, improve confidentiality of network transmission.

Keywords

Smart home; TPM; secure authentication; hash algorithm; AES encryption.

1. Introduction

Smart home as an important aspect of the internet of things, bring pleasant life to people with its convenient, efficient, safe home environment and favored by many consumers[1]. Smart home technology involves a number of disciplines include computer technology, communication technology and control technology etc. It uses the application of wireless sensor network in home space, realize the information perception and smart control for home environment[2]. A typical smart home system mainly includes remote terminal equipment, home server and several communication nodes(various home devices or sensor node). home server is the core of smart home system, the server can receives control commands(including local/remote control command, remote mobile phone commands and storage media,etc.) and send them to the corresponding home device, achieve smart control of home environment.

Smart home create a pleasure living environment for people, on account of its application environment is the aspect of personal privacy, therefore compared with public network, it requires higher secure protection[3]. Smart home is in the emerging development phase, it has not been guaranteed in the system security and network transmission security[4-5], these security risks make the system vulnerable to malicious intrusion and the control information easily monitored and tampered.

2. Current situation analysis

In recent years, the domestic and foreign research on smart home is mainly about how to build a smart home network solutions, most of the existing smart home model allows authorized users at any time, anywhere, via remote terminal device to manage their own home[6-7], but the process of information exchange within the family between the node and the remote terminal must go through an insecure channel[8], it will inevitably suffer from hackers and viruses' malicious attacks and harassment, the more smart and complex functions, the greater likelihood of attack for the smart home system.

So far, the research on the security of smart home system is still in the primary stage, existing research mostly concentrated in the hardware implementation, networking method and a remote control of smart home system[9-10]. The research and analysis about network security in smart home system is relatively few, the only relevant literature that can be retrieved is: literature [11] provides an anonymous authentication protocol based on third party to enhance the privacy protection of smart home system, but it's lack of specific application scenario and verification system; literature [12] proposed a smart home security surveillance system that combines multiple sensors, distributed processing and event-triggered monitoring , provide users with the function of home environment parameter monitoring, appliances control, alarm trigger, which application background is home security objectives, but it doesn't involve own security; literature [13] proposed a smart home secure control system based on dynamic authentication mechanism, involving the security of man-machine interaction but does not include transmission and control security, it's need password confirmation of text messages to control the lower machine, this is inconvenient. based on the security situation faced with the smart home system, trusted authentication and secure communication solutions are the important issues to study and solve at present.

3. Smart home secure system components

3.1 System framework

Complete smart home security system needs to achieve secure access from remote clients, effectively resist the illegal invasion from the external network, securely forward the user's control commands to the corresponding smart home node device to perform. This paper build smart home security system based on internet of things technology which shown in Fig.1. The system's main hardware includes remote client, embedded smart home server, trusted platform module, wireless sensor network nodes.

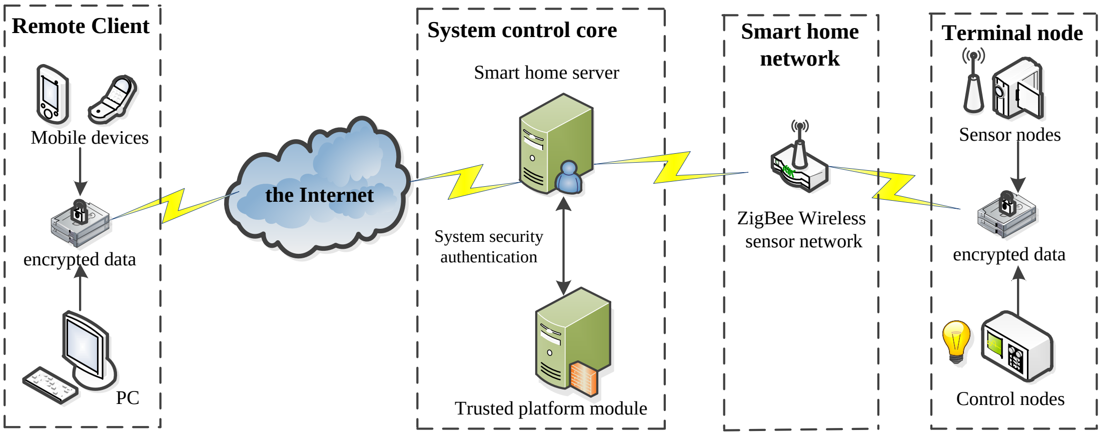


Fig.1 Diagram of smart home security system

3.2 Embedded server and remote client

Home server as the central device of smart home system, carrying smart home system kernel,it achieves information exchange and processing between internal and external network in smart home. This paper selects Samsung embedded processor S5PV210 as the main control unit of the smart home server, extended 512MB memory and nand flash, integrated DM9000 chip card and the corresponding peripheral circuit. Server integrated U-boot, embedded linux kernel, Yaffs2 file system as the operating system, transplant SQLite embedded database to provide users with access support. While using Qt/Embedded cross-platform user interface development technology to design interactive interface, connecting 7-inch LCD touch screen for user easily access and control locally.

Remote client selects Socket network process communication mechanism, achieve network communication based on TCP/IP protocol in Qt project, set the IP address and port number of access, by embedding the AES encryption algorithm to ensure the confidentiality of communications, finally, two executable files for embedded platforms and Windows platforms are generated by the cross-compiler environment.

3.3 TPM and smart home wireless sensor network

Trusted Platform Module(TPM) is a computing platform based on hardware security module,it's widely used in the computer and communications systems, it can improve overall system security and reliability. This paper applys the design of TPM, using STM32 chip as the core to build TPM of smart home, using SHA-1 hash algorithm to verify the integrity of home server's system kernel before its startup, realizing system-level security.

This paper selected CC2530 as the core unit of smart home wireless network node, applied ZigBee HA 1.2 protocol to form a star network, used Z-Stack protocol stack developed bidirectional communication program, ZigBee coordinator communicates with the server through the serial port, ZigBee terminal node communicates with the coordinator in the wireless manner. To making users can real-time monitoring, manage and control the home environment and home appliances, ZigBee terminal node connected sensors and home appliances, these sensors include: temperature and humidity sensors, gas sensors, light sensors and infrared sensors, etc. These appliances include: lighting, air conditioning, curtains and access control systems, etc.

4. Secure authentication of smart home system kernel

Smart home system as the core to achive the functions of communications, protocol conversion, security protection, it is the basis of all access and control functions. Once the smart home system was invaded by the rival, the smart home security will be meaningless, whether server database, home wireless node, or system key and so will be exposed in front of rivals, this will give great harm to smart home users' personal property and life. On the other hand, the hardware and software resources of smart home server are limited, it is difficult to perform complex processing.

Therefore, in order to guarantee the security of smart home system kernel, this paper realized the the main function of TPM on the STM32 platform, which communicate with smart home server via RS232 and embedded SHA-1 hash algorithm to validate the integrity of the server system kernel. SHA-1 is a one-way cryptography, it can make any length of plaintext turn into fixed-length message digest by calculating and transforming, once the original information is changed, the digest will change a lot, this divergence can effectively detect data's integrity

In the secure authentication of smart home system, before server starts, TPM get the U-Boot and kernel which stored in server's nand flash by turn, after SHA-1 hashing algorithm generated a message digest and compared with the correct digest which stored in the TPM, only when comparison results is the same, TPM send signal to allow the server loading the kernel, the identification process of home sever is shown in Fig.2.

1)TPM sent authentication signal to the home server, the server received the signal and find the memory address of the U-Boot.

uboot = (*void* *)*CONFIG_SYS_TEXT_BASE*

Server judged the size of the U-Boot and send the U-Boot image to TPM through RS232 serial port.

memcpy(*buffer_uboot*+*buffer_len_uboot*,*buffer_TPM*,*nread*)

2)After TPM received the U-Boot, it used SHA-1 to calculate and generated message digest in the buffer,this digest will be compared with the correct digest.

$$if\ (uboot\_sha1 == uboot\_Message\_Digest)$$

uboot_Message_Digest represented the correct digest stored in the TPM。 If the comparison results is the same, TPM send signal to allow the server loading the U-Boot.

$$board\_init\_in\_ram(uboot\ )$$

3)When the U-Boot was authenticated and loaded successfully, TPM continue to use the same steps to authenticate kernel, the process is similar to the U-Boot. If any of these steps authenticated unsuccessfully, TPM will issue a warning signal. Finally the output results will be displayed through SecureCRT, the authentication process of home server system shown in Fig.3.

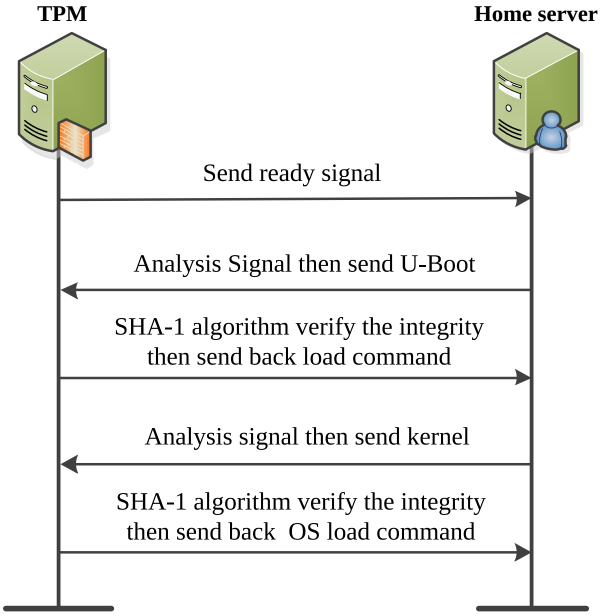
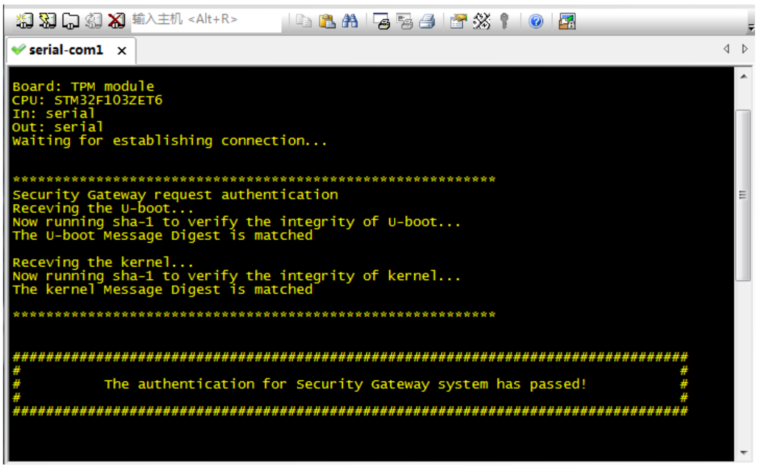

TPM
Home server
Send ready signal
Analysis Signal then send U-Boot
SHA-1 algorithm verify the integrity then send back load command
Analysis signal then send kernel
SHA-1 algorithm verify the integrity then send back OS load command

Fig.2 The identification process of home sever



```
Board: TPM module
CPU: STM32F103ZET6
In: serial
Out: serial
Waiting for establishing connection...


**********************************************************
Security Gateway request authentication
Receving the U-boot...
Now running sha-1 to verify the integrity of U-boot...
The U-boot Message Digest is matched

Receving the kernel...
Now running sha-1 to verify the integrity of kernel...
The kernel Message Digest is matched

**********************************************************


#################################################################################
#                                                                               #
#          The authentication for Security Gateway system has passed!           #
#                                                                               #
#################################################################################
```

Fig.3 TPM trusted authentication mechanism

5. Secure communication of smart home system

When the users login the smart home system via the remote client and send control instructions to the smart home devices. However, if the control instructions transmit in an untrusted network with the form of plaintext, it could be easily monitor, access and tampering by enemies.So it is necessary to introduce secure communications mechanism to the smart home system, to ensure that there is no plaintext in the process of communication and potect the security of information transfer.

This paper uses the AES encryption algorithm to realize the smart home system’s secure communications. The AES encryption algorithm is one of the most popular algorithm of symmetric cryptosystems, it integrated the security performance, efficiency, realizability and flexibility together, and low memory requirement, it can resist strong and real time attacks. The AES encryption algorithm is an iterative block cipher, its block length is 128 bits, and allow three different key length: 128bits, 192bits and 256bits, the corresponding iterative rounds are 10, 12 and 14. The AES algorithm encryption process as shown in Fig.4.

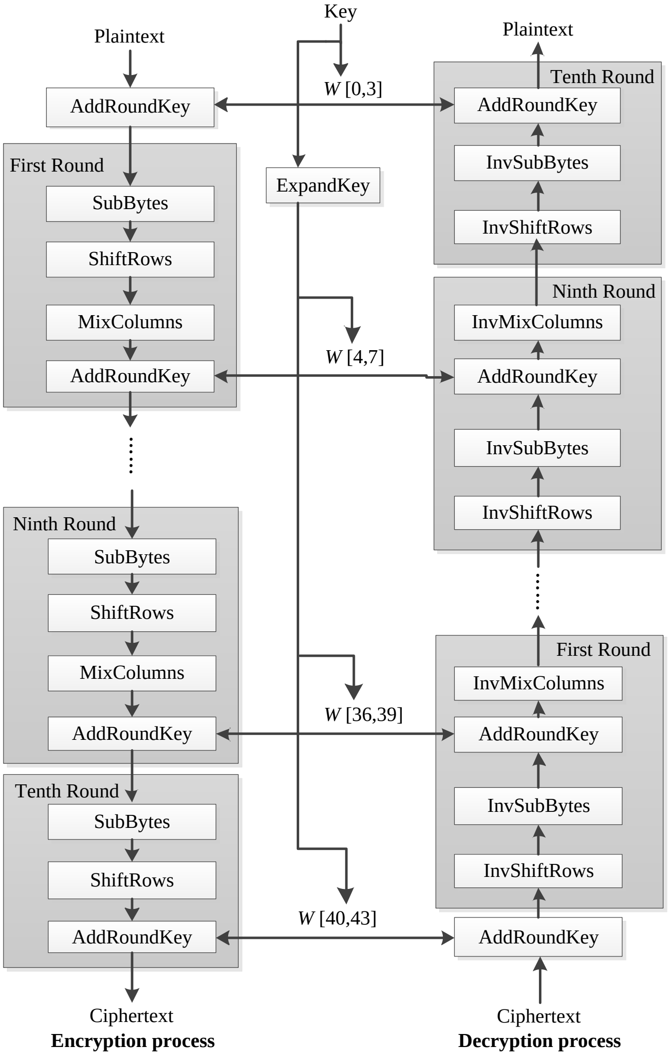


Fig.4 AES encryption and decryption process

Each round of the AES algorithm uses substitution and confusion to dispose the whole data block, process made up of 4 different stages.

①SubBytes: use a S box to instead the byte of the block.

②ShiftRows: Through the cyclic shift operation in row to complete replacement.

③MixColumns: use the properties of arithmetic on domain GF(2^8) to complete replacement, its formula shown in (1).

$$s'(x) = c(x) \cdot s(x) \bmod (x^4 + 1) \tag{1}$$

And $c(x) = \{03\} \cdot x^3 + \{01\} \cdot x^2 + \{01\} \cdot x + \{02\}$, $s(x)$ means SubBytes, x means bytes, shown in a matrix as(2).

$$\begin{bmatrix} s'_{0,c} \\ s'_{1,c} \\ s'_{2,c} \\ s'_{3,c} \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \begin{bmatrix} s_{0,c} \\ s_{1,c} \\ s_{2,c} \\ s_{3,c} \end{bmatrix} \tag{2}$$

④AddRoundKey: Using the current block and one part of the expansion key to bitwise xor. Decryption process is the reverse of encryption, SubBytes, ShiftRows and MixColumns are should do inverse transformation. They are called InvSubBytes, InvShiftRows, InvMixColumns.

This paper created a new AES function and add the AES algorithm to it in a Qt project:

QStringWidget :: *AES_Encrypt* (*QString cmd*);

QStringWidget :: *AES_Decrypt* (*QString cmd*);

These two codes respectively calls encrypt and decrypt function of AES algorithm, *cmd* is the control instruction waiting for of encrypting and decrypting.

Aes->InitializePrivateKey(16,**p&Key*$_n$);

This code completed the initialization process of AES key, the parameter 16 means the length of the key is 256 bits (2^{16}), *Key*$_n$ is the user preset key.

memcpy(*mingwen,cmd.toAscii*(),*size*);

*cmd.*toAscii() means the length of plaintext string is size should be hexadecimal output.

aes->OnAesEncrypt(*mingwen,size, C*$_n$);

This means we use the AES algorithm in this project to encrypt the plaintext and output the cipher C_n. The decryption process is similar to the encryption process, it's the inverse transformation of each other.

6. Security performance test of system

The introduction of the smart home system security communication mechanism is bound to led the time delay in data processing and instruction execution in system. This paper tested the time delay in the process of instruction forwarding before and after we used the encrypted communication. We send home node an encryption control instruction by using the remote client every fixed time, we recorded the current time T_c when sending the instruction, after the home node received the instruction and executed, then returned it back, when the client received the return instructions again we record the current time T_n, so a single instruction forwarding time delay is calculated as equation(3), δ is the time when the data transfer in the network(it related to the length of different instructions, the value here is $6*10^{-6}$s), R means the times of instruction back and forth(the value here is 4).

$$T_{c,n} = \frac{T_c - T_n - \delta}{R} \tag{3}$$

In order to reduce the network fluctuation and the effects of abnormal transmission in test, to make the test data is more close to the real situation, this paper carried out 1000 times repeated tests according to the above methods and calculated the control instruction's average forward delay rate by using equation(4), the rate is named P_a, and $T'_{c,n}$ means the instruction time delay before encrypt, M is the repeated test times.

$$P_a = \frac{\sum_{k=1}^{M} (T_{c,n} - T'_{c,n})}{M \times T'_{c,n}} \tag{4}$$

After joining the encryption communication mechanism, the system instruction forwarding delay rate is only 5.31% higher than before, and the hash distribution of the delay rate as shown in Fig.5. So we can see that the encryption communication mechanism we build could improve the security of the smart home system and it has not much impact on overall system performance by its algorithm cost.

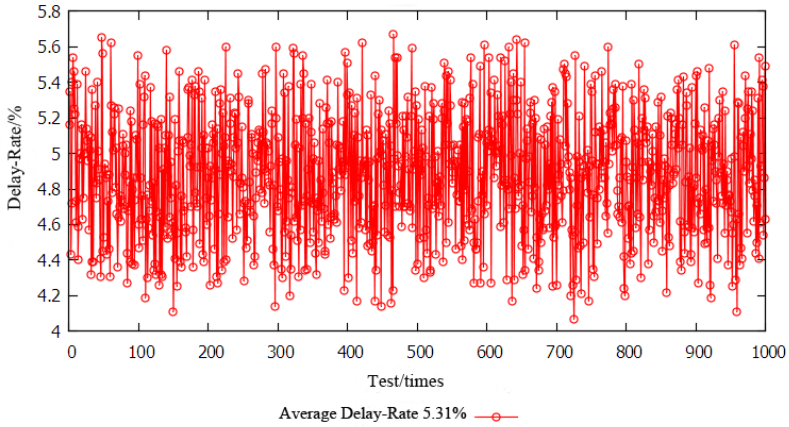


Fig.5 Delay effect of secure communication mechanism on system

7. Conclusion

The Internet of things is the third wave of information industry of the world after the computer and the Internet, it will create a new era of connecting everything and also bring the new solutions and opportunities to the smart home fields. But the lack of security in the current smart home system will hinder the development of smart home technology and its market popularization.

In this paper, by constructing trusted platform module in the smart home system and embedded hash algorithm to implement secure authentication of the system kernel to make the it is reliable. At the same time, we built the secure communication mechanism based on the AES encryption algorithm in the system to improve the confidentiality of network information transmission. The test results in the embedded platform of smart home show that the secure authentication and communication mode we design in this paper can meet the requirements in the smart home system. It helps the system to improve its ability of resist the illegal invasion to guarantee it in a safe and reliable run.

Acknowledgements

Natural Science Foundation.

References

[1] Gubbi J, Buyya R, Marusic S, et al. Internet of Things (IoT): A vision, architectural elements, and future directions[J]. Future Generation Computer Systems, 2013, 29(7):1645-1660.

[2] Man S, Yang H X, Peng Y, et al. Design of embedded wireless smart home gateway based on ARM9[J]. Journal of Computer Applications,2010, 9 (9):2541-2544.

[3] Wu W Z, Li W L. Smart home system based on ARM and ZigBee[J]. Computer Engineering and Design, 2011, 32(6): 1987-1990.

[4] Hou W Y, Wei Y H, Pang Z Q. Design and implementation of the gateway for smart home and its web control software[J]. Process Automation Instrumentation, 2015,5(5):64-67.

[5] Furfari F, Girolami M, Lenzi S, et al. A service-oriented Zigbee gateway for smart environments[J]. Journal of Ambient Intelligence and Smart Environments, 2014, 6(6): 691-705.

[6] Ni Y, Miao F, Liu J, et al. Implementation of wireless gateway for smart home[J]. Communications & Network, 2013, 5(1):16-20.

[7] Zhang W H, Tan W, Chen Y P. The IOT gateway design based on the embedded web server[J]. Journal of Sichuan University(Natural Science Edition),2013, 5(5):962-966.

[8] Mowad M A E L, Fathy A, Hafez A. Smart home automated control system using android application and microcontroller[J]. International Journal of Scientific & Engineering Research, 2014, 5(5): 935-939.
[9] Gao P, Zheng C, Ren Q M, et al. Design of monitoring network of smart home system based on ARM and Zigbee[J]. Computer Measurement & Control, 2014, 22(010): 3206-3209.
[10] Gong Q, Li G, Pang Y. Design and implementation of smart home system based on Zigbee technology[J]. International Journal of Smart Home, 2014, 8(6): 143-156.
[11] Alcaide A, Palomar E, Montero C J, Ribagorda A. Anonymous authentication for privacy-preserving IOT target-driven applications[J]. Computers and Security, Vol.37,No.9, 2013 : 111-123.
[12] Zhu X J, Ying Y P, Ying S D, Feng Z L. Smart home monitoring system based on ZigBee and WLAN design [J]. Journal of telecom science, 2009 (6) : 45 -50.
[13] Deng B W, Li C. Time sequence to encrypt the design and implementation of smart home control system security [J]. Journal of electronics world, 2012 (9) : 33-35.