2014 IEEE 17th International Conference on Computational Science and Engineering

Usable Security Mechanisms in Smart Building

Weihan Bo, Yiling Zhang, Xianbin Hong, Hanrong Sun, Xin Huang
Department of Computer Science and Software Engineering
Xi'an Jiaotong–Liverpool University
Suzhou, China

***Abstract*—Smart building becomes popular these years. It enables many interesting applications, for example, elderly monitoring and remote healthcare. Sensitive information protection in the smart building system is always required; security is thus one important component in such system. So far, many security mechanisms are proposed, however, the study on the balance of security and usability is still lacking. In this paper, we focus on usable security mechanisms in smart building. In particular, usable authentication mechanisms and usable data privacy protection methods are studied.**

Keywords—security;usability

I. INTRODUCTION

These years, smart building systems become popular. However, security is one main problem in such applications. For example, if attackers can login to a smart device, they can access private user data. This should be prevented.

In this paper, several authentication methods are studied. We identify some potential problems in current mechanisms, and investigate users' opinion about these methods. Also, a data storage mechanism is proposed and investigated. The main contributions are as follows.

- Survey on security requirements in smart building systems. We find that people do care about security in smart building. However, current mechanisms are still not satisfying.
- Survey on five authentication methods including a key logger prevention method designed based on [1]. We find that although pattern locker is preferred in general, alphanumeric passwords and other methods also have their advantages.
- Data protection method is proposed and investigated. Data slices are stored in different cloud suppliers, thus no single supplier can maliciously leak user data.

This paper is organized as follows. In Section 2, we introduce the smart building. In Section 3, we present survey results on security requirements. In Section 4, several authentication methods are described. In Section 5, a data protection method is proposed. In Section 6, a survey on previous security mechanisms are discussed. Finally, some conclusions are made in Section 7.

II. SMART BUIDING

In this section, an overview of the smart building is firstly given. After that a demo system is introduced.

A. Scenario Overview

The smart building system consists of four parts: smart devices, central controller, mobile controller and cloud (web server). Users can use their mobile controller to send commands to the central controller through wireless links; and the central controller transfers users' commands to target devices. Alternatively, users can use their mobile phone to send commands to the cloud, and the cloud transmits each command to their respective central controllers. The cloud can access central controllers for operation logs.

1) Smart Devices.

Smart devices can be a socket, freezer, television, and some other devices in the building. These devices are able to send or receive data from the central controller. Meanwhile, they can also control other device automatically.

2) Central Controller.

The central controller is used to directly control smart devices. Also, the cloud can send control commands to the central controller; and then it transmits different commands to smart devices.

3) Mobile Controller.

Mobile controller is a mobile phone application that is similar to a chatting software. Users can use this application to communicate with smart devices. They can send messages, for example 'Hello, freezer, close at 8:30 am', to the central controller.

4) Cloud.

Cloud has two main functions. Firstly, the cloud transmits commands from the mobile controller to the central controller. Secondly, the cloud is used to store data.

B. Use case

This use case is named as smart power genius. It can use mobile phone to remotely switch on or off appliances. This smart power genius use Raspberry Pi as the central controller, an Android application as the mobile controller, and a socket as the smart device. The mobile controller is shown in the left of Fig. 1, the smart device is shown in the right of Fig. 1, and the central controller is shown in Fig. 2.

978-1-4799-7981-3/14 $31.00 © 2014 IEEE
DOI 10.1109/CSE.2014.154

The design of this smart power genius is as follows. Firstly, mobile controller sends a string type variable to the central controller. The central controller analyzes the string, and then it sends different operation commands to the smart socket. The light can be switch on or off remotely.

A cloud is used to store operation logs. In addition, it helps users to control the smart socket even when users are not inside the building.

Fig. 1. The mobile controller and the smart device

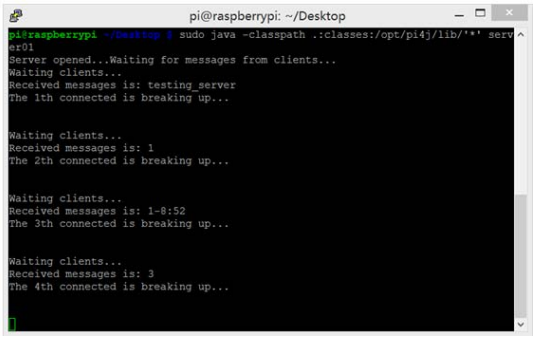

Fig. 2. The central controller

III. Survey on Security Requirements

In this section, a survey on security requirements is introduced.

A. Survey on the Attitude

A questionnaire is designed in order to study the attitude of candidates towards security mechanisms in the smart building. 43 people answered the questionnaire. 18 candidates are male, and 25 candidates are female. Most of them (41 candidates) are students.

The first question is about their attitude towards security. They are asked to rate the importance (from 1 to 5, and 5 is the most important) to four types of requirements: (1) easily setup, (2) high security, (3) remote control, and (4) easily managed. From Fig. 3, we can see that the average score of "high security" is 4.63. It is the highest score. Surprisingly, people even think that security is more important than "easily setup" and "easily managed".

The second question asks candidates whether or not a complicated configuration procedure of high security mechanism is acceptable. The result is shown in Fig. 4. 58% candidates think that complicated procedure is acceptable. 33% candidates think that they will choose less secure mechanisms that can be configured easily.

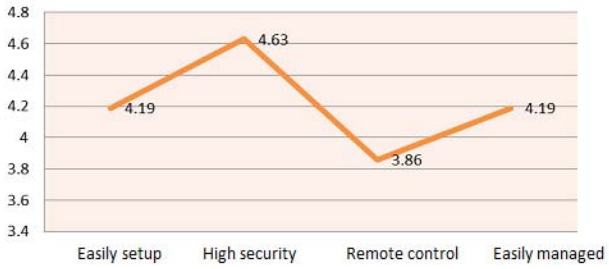

Fig. 3. Attitude invesitgation result I

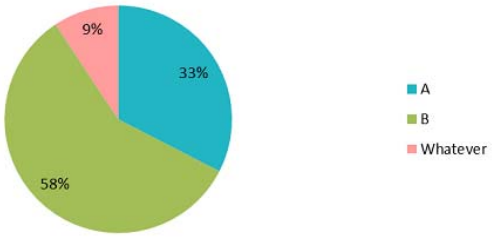

Fig. 4. Attitude invesitgation result II

B. Survey on Passwords

Since many current security mechanisms rely on passwords, a survey on passwords is done. 30 people answered the questionnaire. 12 candidates are male, and 18 candidates are female. Most of them are students.

As Fig. 5 shown, the security of users' password is worried due to the poor variety. Almost all participants applied lowercases and numbers in their passwords, with the exception of one student ignoring this question. Comparing with lowercases and numbers, the usage rate of capitals and symbols seems to be much lower. This means that the quality of passwords is not good.

Fig. 6 indicates the survey result of accounts and passwords reuse. More than half participants possess 6 accounts. However, the numbers of password decrease as the numbers of account increase. Most people have less than 6 passwords. It means that users' accounts tend to be attacked due to password reuse.

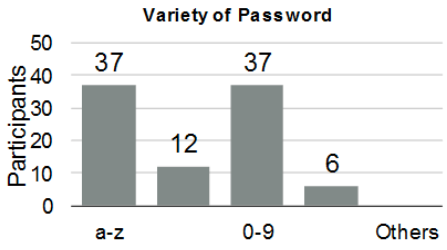

Fig. 5. Variety of passwords

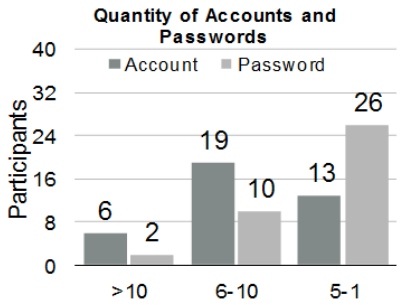

Fig. 6. Quantity of accounts and passwords

C. Survey on Data Storage

Another important issue is the security of data storage, especially the data stored on a cloud. One important reason is that the data may be private user information. However, many cloud computing suppliers store the data on the public cloud. Users may worry about the privacy protection of their data stored on the cloud.

In order to investigate this, a survey is done. 37 people answered the questionnaire. Most of them are students.

The result is introduced as follows. Around 89% users believe cloud computing suppliers will access their private data without permission. At the same time, around 68% users think that the suppliers will leak their data. Above survey shows users have a strong distrust to suppliers.

IV. Authentication Mechanism

In this section, we will study several authentication methods. The first one is password-based methods. The other one is WPS (Wi-Fi protected setup).

A. Authentication Using Password

Nowadays, many authentication methods in smart building rely on passwords. One example is WPA (Wi-Fi Protected Access) family: WPA and WPA2 [4, 5]. They adopt pre-shared key model. Users hold a password to access the wireless network.

Example passwords are alphanumeric passwords, graphical passwords [2], and pattern locks (point passwords). In addition, in this paper, we have developed another passwords named as *4-12 password* based on [1]. This method converts a 4-character password (e.g., Bluetooth PIN code) to a 12-character random string. The procedure of this method is listed as follows.

Step 1: The server firstly produces a 6*6 random matrix when client sends a request (Fig. 7). Each character in this matrix is generated randomly in range of 'A~Z', 'a~z', and '0~9'. Also, this matrix includes all characters of the password.

N	n	B	B	9	F
x	U	1	5	p	0
2	7	C	6	n	x
4	3	5	g	9	0
L	V	F	H	6	y
6	n	F	5	3	2

Fig. 7. Step 1

Step 2: Automatically, the server sends this random matrix to the client using SSL link. This matrix is divided into four parts by the client, and each section is a 3*3 matrix. A client can recognize these four parts shown in Fig. 8.

N	*n*	*B*
x	U	1
2	3	C

B	9	F
5	p	0
6	n	x

4	3	4
L	V	F
6	n	F

g	9	0
H	6	y
5	3	2

Fig. 8. Step 2

If the first character in the password is '0', the client should firstly input 2 or 4, because in Fig. 8 the second part and the fourth part include character '0'.

Step 3: Automatically, the 3*3 matrix is divided into 4 sections, and each section is a 2*2 matrix. If the client selects the part 2 in step 2, these four 2*2 matrices are as shown in Fig. 9.

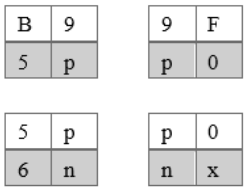

Fig. 9. Step 3

In Fig. 9, the second part and the fourth part include character '0', so the client can input '2' or '4'.

Step 4: Automatically, the 2*2 matrix is divided into 4 parts, and each part is a 1*1 matrix. If client selects the part 2 in step 3, four 1*1 matrices are shown in Fig. 10.

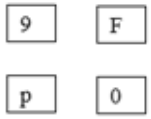

Fig. 10. Step 4

In figure 10, the fourth part includes character '0', so the client can input '4', and selects the fourth part in these four 1*1 matrices.

After client input 2-2-4, the system get the first character '0' in the password. Then, it goes back to step 1 three times for other 3 characters in the password. These 12 characters will send to the server with SSL links. Since matrices are generated randomly, thus key loggers cannot record the correct passwords anymore.

B. WPS

WPS [6,7] is another authentication method that can be used in the smart building system. WPS is a standard which assists users to setup their wireless network in an easier way. It provides two models: PIN model and WPS button model. It enables the user/device to join in the network by a convenient approach.

For the PIN model, the smart device should firstly generate a PIN locally by running a WPS configuration utility. Then the PIN should be filled into the router so that the verification is completed.

For the Button model, the (virtual) button on the router should firstly be pressed, and then the client device runs its local WPS configuration utility. A verification procedure runs until the router confirms the wireless connection.

The Button model is a suitable way of authenticating devices that are not equipped with displays. After the setup procedure, devices can be paired by simply pressing a button.

V. DATA PROTECTION

In this section, we will study a data protection method based on data slicing.

Based on survey results in Section III (C), we believe that a cloud server should have the following characteristics. (1) The user knows where the data is stored and how the data is used. (2) Multiple cloud computing suppliers maintain data together but none of them could read all the data. [3,8]

Thus, we have designed a distributed private cloud computing model. In this model, the smart building company provides a cloud platform server, and each user has a private cloud on it (Fig. 11). There is a data manage system with a database on the private cloud that the user is its administrator. This database of each user is divided into multiple parts and each part has interfaces to communicate with others for exchanging data (Fig. 12). Then the user will have the right of choosing cloud computing suppliers. The duty of the cloud computing suppliers is to help users to translate data and maintain data. Operations on data should get the permission from the user and will be record in a log (Fig. 13).

Step of data processing is listed below.

The user sends the data processing request to the smart building cloud platform.

The platform sends the request to the data management system.

The data management system gets the request and analyzes which part of the data will be used.

The data management system generates permissions for the cloud computing suppliers who maintain part of the data.

The cloud computing suppliers read the data with permissions and combine data slices.

The data management system records the actions and generates a log (the user could read the log at any time).

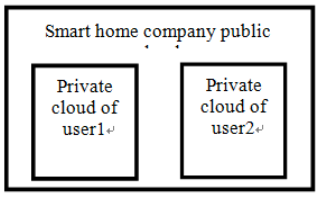

Fig. 11. Structure of the cloud

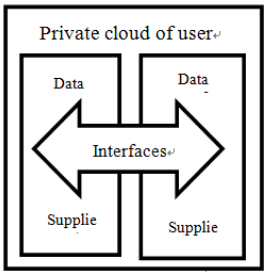

Fig. 12. Structure of one user's private cloud

Fig. 13. Data processing log

VI. Survey Results

A. Survey on Authentication Methods

In order to compare authentication methods described in Section IV, a survey is done. 16 questionnaire answers were collected. 7 candidates are male, and 9 candidates are female. Most of them (14) are college students.

Survey results are shown in Fig. 14, Fig. 15 and Fig. 16. Generally speaking, people think that pattern lock is the easiest way, but alphanumeric password gets the highest score regarding user preference.

However, if devices are different, general results are not always true. This can be more clearly seen in Fig 15. First of all, if the device is a computer, pattern lock is not a good method. Also, if the device is an embedded device with no displays, WPS with button pressing might be the best way.

The 4-12 password is one acceptable method, especially when computers are used as central controllers. Given that this method can prevent key logger based attacks, it is one useful security tool. In Fig. 16, we show the investigation result. Half of users will choose 4-12 password if it can prevent key logger.

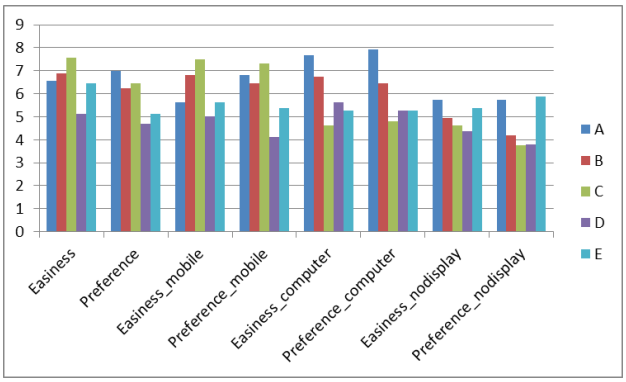

Fig. 14. Users opinions on authentication methods. Easiness indicates the easiness of using certain method; 1 is the most difficult method, and 10 is the most easy method. Preference means that if users like certain method. "_mobile" means that the device is a mobile phone. "_computer" means that the device is a computer. "_nodisplay" means that the device is a embeded device with no display. Method A is the alphanumeric password, B is the graphical password, C is the pattern lock, D is the 4-12 password, and E is the WPS using buttons.

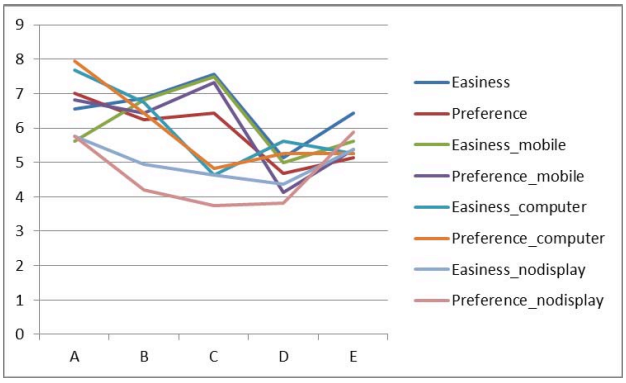

Fig. 15. Users opinions on authentication methods II. Method A is the alphanumeric password, B is the graphical password, C is the pattern lock, D is the 4-12 password, and E is the WPS using buttons.

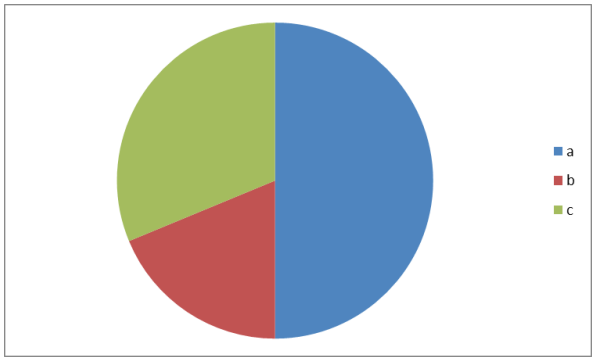

Fig. 16. Users opinions on 4-12 password. a means they will use it; b means they will not; and c means that they have no idea.

B. Survey on Data Protection Mechanism

In order to find out users' opinions on our proposed data protection mechanism (Section V), a survey is done. 38 answers were collected. 30 users choose "trust" or "strongly trust", which is nearly 79%. Note that, this percentage is 32% before our mechanism is employed.

VII. Conclusion

In this paper, usable security mechanisms are discussed. First of all, security requirements are investigated. Also, several authentication methods are described and investigated. In addition, a data protection mechanism is also proposed and investigated.

In the next stage, more security mechanisms will be studied from the standpoint of usability. The balance of security and usability is still a very interesting issue.

References

[1] Ito et al., "Input Password Only with Four Keys, Three Times," in Symposium On Usable Privacy and Security (SOUPS 2014), Menlo Park, CA, July. 9-11, 2014.

[2] S. Wiedenbeck et al., "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice," in Symposium On Usable Privacy and Security (SOUPS 2005), Pittsburgh, PA, July. 6-8, 2005.

[3] W. Jansen, T. Grance, "Guidelines on Security and Privacy in Public Cloud Computing" [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-144/SP800-144.pdf

[4] (2014, Nov. 10). HTG Explains: The Difference Between WEP, WPA, and WPA2 Wireless Encryption (and Why It Matters) [Online]. Available: http://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/

[5] (2014, Nov. 7). Configuring WPA-PSK and WPA2-PSK Wireless Security [Online]. Available: http://documentation.netgear.com/wgr614v9/enu/202-10308-01/WGR614v9-04-07.html

[6] (2014, Nov. 7). Using PIN Entry to Add a WPS Client [Online]. Available: http://documentation.netgear.com/dg834g/enu/202-10363-01/DG834Gv5_RM_29Jun-04-11.html

[7] (2014, Nov. 7). Using a WPS Button to Add a WPS Client [Online]. Available: http://documentation.netgear.com/dg834g/enu/202-10363-01/DG834Gv5_RM_29Jun-04-10.html

[8] National Institute of Standards and Technology, NIST Cloud Computing Program [online]. Available: http://www.nist.gov/itl/cloud/