Lock Access Control and Authorization using Smartphone Based on Bluetooth Communication

Ren Junn Hwang[1] , Bo-Cheng Chen[2] and Der-Ren Liao[3]
[1,2]Department of Computer Science and Information Engineering, Tamkang Uuiversity
151, Yingzhuan Rd., Tamsui Dist., New Taipei City 25137, Taiwan
[3]Advanced Engineering Division, Hua-chuang Automobile Information Technical Center Co., Ltd.
No.3, Sec. 3, Zhongxing Rd., Xindian City, New Taipei City 23144, Taiwan
E-mail: [1]victor@gms.tku.edu.tw, [2]602410036@s02.tku.edu.tw

Abstract: Most the mobile devices today are equipped with Bluetooth technology. Features such as low power consumption and medium-to-long transmission range make this technology important for the Internet of Things. This paper proposes an access and authority control scheme based on Bluetooth technology for personal or family usage. In this scheme, a smartphone equipped with Bluetooth acts as a personal trusted device, which can be used as a key device by its owner. The proposed scheme can be applied to the access and authority control of a door, vehicle, or special facility, whose lock is initialized and automatically authenticates the accessing device via Bluetooth without connecting to the server or the Internet. The accessing device is authorized for as long as the user wants to open the lock. The master-phone of the lock can authorize or revoke the disposable or time-limited access right to another phone to open the lock. The proposed scheme provides an efficient and flexible function for managing a varying set of users opening a lock. This scheme is secure as it is resistant to attacks such as replay attack, masquerade attack, modification of messages, man in the middle, and eavesdrop.

Keywords-- **Bluetooth, Access Control, Authority, Smart Phone**

1. Introduction

In the present generation of Internet of Things, life can be made more convenient through various communication and mobile devices. We need some type of access control in our daily life. For example, we need to unlock our apartments, cars, or special facilities. A traditional access control system consists of locked doors, keys that match the door locks, and a method to manage the key-door combinations. A facility owner must be able to control the keys for the locks. Locks are seen as the symbol of protecting property and privacy. The one who owns the key has the access to open the lock. Keys have, for centuries, played a central part in managing access rights to facilities. Physical keys are easy to use, but difficult to manage, especially for large institutions with a large and varying number of users and even worse when access rights to a facility keep changing over time. Traditionally, authorizing the access right of a lock to a person is to give him a copy of the owner's key, and to revoke the authority is to retrieve the key from that person. In this way, there are many situations that can make authority management uncontrollable. For example, the key can be copied or transferred to another person without permission. These cases are threats to security and privacy. Thus, the physical key system is inconvenient and difficult to manage. Therefore, this study uses a smartphone instead of a physical key. A smartphone equipped with Bluetooth acts as a personal trusted device, which can be used as the key device by its owner. However, the proposed scheme should be more secure and convenient than the physical key system.

The concept of using a smartphone as a virtual key has been commercialized by several vendors such as MVC-Data [1], Bluelon ApS [2], Flexipanel Ltd. [3], Steab AB [4], ECKey [5], and SOREX [6]. The techniques used by these vendors are based on establishing a Bluetooth connection between the lock and the smartphone and rely on the Bluetooth stack for security. [8, 9] However, the security might be compromised with some modification in the consumer hardware. [7] To manage a varying set of users, such systems require either the lock to be connected to the Internet, the server, or a manual entry from each user into each lock. Furthermore, none of the above studies consider the temporary authorization of some validation users, such as authorizing disposable or time-limited access rights to these users.

In this study, we design a secure connection technique between a smartphone and a lock. This usage of Bluetooth virtual keys makes this technique convenient and provides more security than physical keys. Moreover, when using Bluetooth for lock access control, the user needs not go through the unlocking process like that in other existing electronic keys, such as IC card keys with short-range communication technology. The lock will be initialized and automatically authenticate the mobile device via Bluetooth without needing to connect to the server or Internet, and is authorized for as long as the user wants to unlock the door.

2. Proposed Scheme

The proposed scheme includes a server, a smartphone, and a lock. The smartphone and the lock are not trusted until they finish the registration process. The server is trusted and communicates with the smartphone through Wi-Fi or LTE. The smartphone communicates with the lock through Bluetooth. The communication channel between the two phones is Bluetooth. The lock and the server cannot communicate directly.

The identity of the server is S, which holds a public key PU_S and a private key PR_S for asymmetric encryption. Phone i is named P_i, which holds a public key PU_{Pi} and a private key PR_{Pi}. L is the identity of the lock, which generates a public key PU^B_L and a private key PR^B_L in the registration phase. The server stores the public key and

identity of each regisitered phone. The registered phone acts as a personal trusted device, which can be used as a key device for its owner. The authorized registered phone acts like a traditional key, which can open the lock via Bluetooth. The lock, which is an intergration of a traditional lock and Bluetooth, validates whether the connecting phone can open the lock.

The proposed scheme is divided into the Registration Phase, Authorization Phase, and Lock Opening Phase. The phone and lock should register at the server. The phone and lock authenticate each other with the server in the initial part of the Registration Phase, and then, generate secret parameters and a shared key. The phone directly registeres at the server, while the lock registers via its master-phone. The master-phone of a lock is a registered phone that initializes the lock. The master-phone provides temporary locking access to the other phone in the Authorization Phase; the authorized phone is named a vice-phone. The master-phone can also revoke the access right of the vice-phone. The Lock Opening Phase defines the process for a lock to validate the connecting phone that will open the lock.

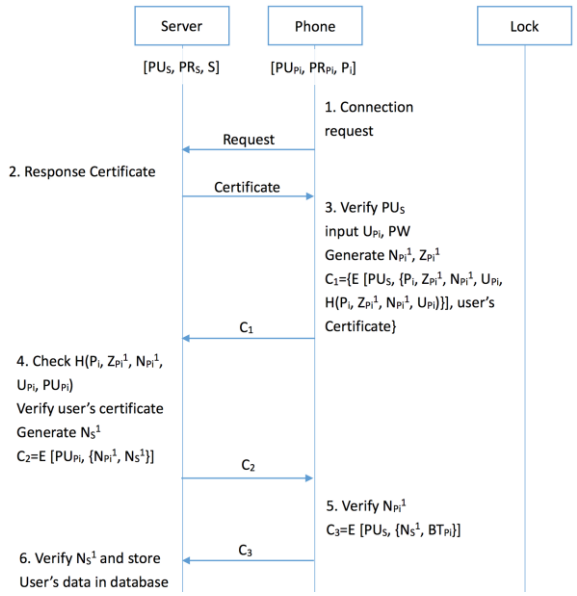

Figure 1. The process of the phone registers at Server

2. 1 Registration Phase

There are three types in the Registration Phase: The phone registers at the server, the phone connects to the lock, and the lock registers at the server through its master-phone.

The phone and the server authenticate each other and generate their shared secret parameters when the phone registers at the server. Figure 1 details the process of the phone registers at Server.

The registered phone can connect to a lock. The connection process is based on the Bluetooth Numeric Comparison Protocol. The registered phone is the master-phone of the lock. Both the connected lock and its master-phone share their link key after the Bluetooth connection has been successfully established.

The lock registers at the server by exchanging messages through the master-phone. The lock registers and server will mutual authenticate each other in this phase. The lock and the server share parameters after the registration process is completed. Figure 2 introduces the process of a lock registering at Server.

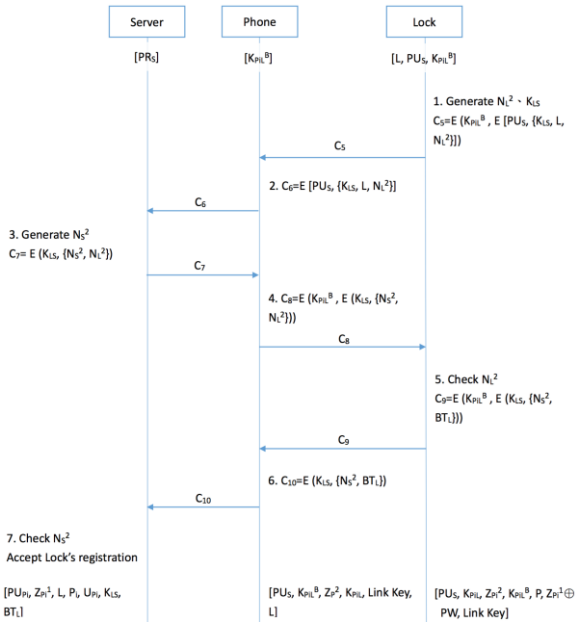

Figure 2. The process of a lock registering at Server

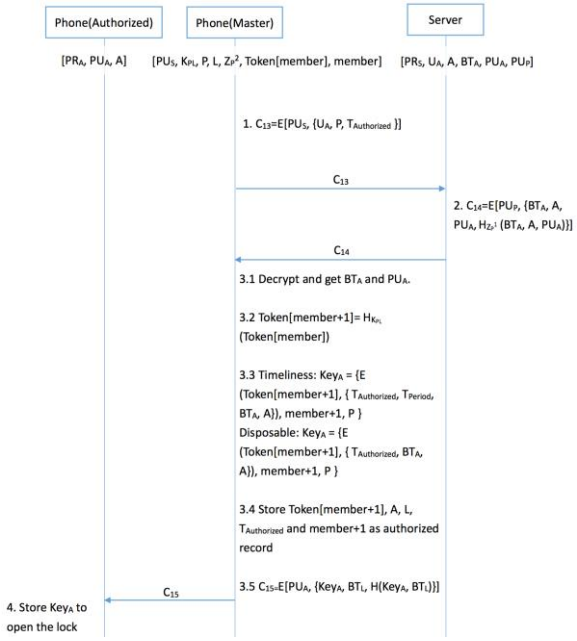

Figure 3. Authorization Phase

2. 2 Authorization Phase

In the Authorization Phase, the lock master-phone authorizes a registered phone to be a vice-phone or revokes the authorization of a vice-phone. The authorization of the vice-phone is divided into two types: disposable access right and time-limited access right. The vice-phone holding

the disposable access right can open the lock only once. Its access right gets disabled once the lock is opened. In contrast, the vice-phone holding the time-limited access right can open the lock within the authorized time interval. The vice-phone with a time-limited access right can open the lock multiple times until the deadline is reached. Figure 3 details the authorization process of the proposed Authorization Phase.

If for some reason, the master-phone has to revoke the authorization of the vice-phone. The revoked vice-phone cannot open the lock anymore.

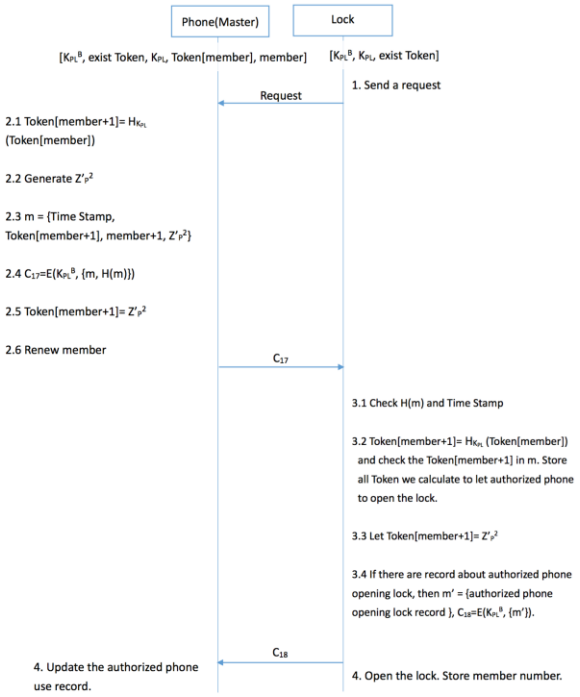

Figure 4. The process of Master-Phone opening Lock

2. 3 Lock Opening Phase

Another distinguishing feature of the proposed scheme is that the user who holds the master-phone or vice-phone can open the lock by just touching a specific area of the lock, and need not take out his smartphone. When a smartphone running the lock opening application in the backgroud is located in the Bluetooth communication range of a lock, the lock validates the neighboring smartphone without connecting to the server or Internet. The Lock Opening Phase considers three scenarios: Master-phone opens the lock, vice-phone with disposable access right opens the lock, and vice-phone with time-limited access right opens the lock.

The master-phone connects to the lock and they share a link key in the Registration Phase. Figure 4 shows the process of the master-phone opening the lock.

The master-phone generates the witness key, Key_A, for the authorized vice-phone with a disposable access right in the Authorization Phase. Vice-phone A opens the lock by providing Key_A, Bluetooth address BT_A, and identity. Figure 5 details the process of lock opening by the vice-phone with a disposable access right. The vice-phone with a disposable access right can open the lock only once.

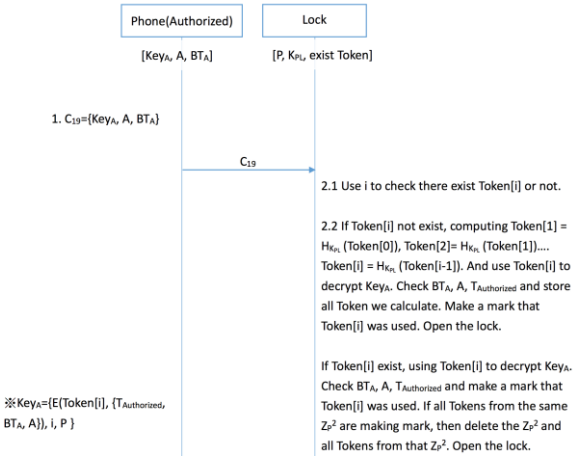

Figure 5. The process of Vice-phone with a disposable access right opening Lock

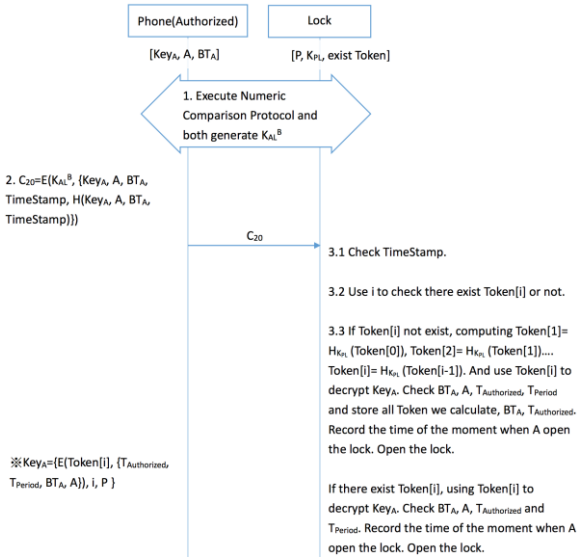

Figure 6. The process of the Vice-Phone with time-limit access right opening Lock at first time

The master-phone generates the witness key, Key_A, for the authorized vice-phone with a time-limited access right in the Authorization Phase. The witness keys of the time-limited access right and the disposable access right are different. There are two cases where the vice-phone, with a time-limited access right, opens the lock. In the first case, the vice-phone opens the lock for the first time, which includes the connection process. Figure 6 introduces the process of Vice-Phone with time-limit access right opening the lock at first time. The lock records some information corresponding to the vice-phone, which opens the lock for the first time. The vice-phone does not perform the connection process again when it opens the lock for the second time. The process of opening the lock for the second time is faster than that for the first time. The vice-phone with a time-limited access right can open the lock multiple times until the deadline is reached. Figure 7 details the

process of Vice-Phone with time-limit access right opening the lock after the first time.

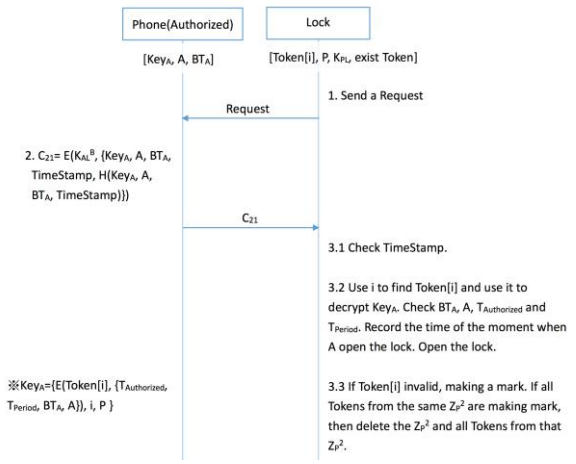

Figure 7. The process of Vice-Phone with time-limit access right opening the lock after the first time.

3. Security Discussion

The proposed scheme can resist certain attacks. Due to the page length limitations, these attacks are briefly defined as follows:

Replay attack: An adversary copies a legitimate message and replays it later.

Masquerade attack: This attack usually includes one of the other forms of attack. For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an unauthorized smartphone to obtain the access right by impersonating an authorized smartphone to open the lock.

Modification of messages: Some portion of a legitimate message is altered, or delayed or reordered, to produce an unauthorized effect.

Man in the middle: An adversary intercepts messages, and then, either relays the intercepted message or substitutes it with another message.

Eavesdrop: An adversary learns the contents of the transmitted message. This assists the attacker in performing another attack.

4. Conclusions

This paper proposes a secure connection technique between a smartphone and a lock. The person who holds the authorized smartphone can open the lock embedded in a facility. This technique is convenient because of the use of Bluetooth virtual keys and provides more security and efficiency than physical keys. Moreover, an advantage of using Bluetooth for lock access control is that the user does not need to go through the unlock process, such as that in the other existing electronic keys. Besides, the lock is initialized and automatically authenticates the smartphone via Bluetooth technology, which is authorized as long as the user wants to open the lock. The lock authenticates the smartphone without needing to connect to the server or Internet. In the proposed scheme, the master-phone is the manager of the lock, which initializes and connects the lock in the Registration Phase. The master-phone can authorize or revoke the disposable access right or time-limited access right given to a phone for opening the lock. The master-phone manages a varying set of users to open the lock efficiently and flexibly. The proposed scheme is secure and resistant to attacks such as replay attack, masquerade attack, modification of messages, man in the middle, and eavesdrop. Thus, this study provides a secure, elastic, and efficient technique to access control a lock.

Acknowledgement

This work was partially supported by the Ministry of Economic Affairs, Taiwan, under the Grants No. 105-EC-17-A-02-I2-0001.

References

[1] MVC-Data ApS. (2012, January 11th) Wireless Bluetooth access control. [Online]. Available: http://www.mvc-data.com/Home.html

[2] BlueLon. (2011, May 24th) BlueAccess BAL-100-BL. [Online]. Available: http: //www.bluelon.com/ index.php?id=248

[3] FlexiPanel. (2007, March 1st) BlueLock - Access control triggered by Bluetooth on your mobile phone. [Online]. Available: http://www.flexipanel.com/Docs/ BlueLock%20DS377%20Cover.pdf

[4] Steab AB. (2012, January 11th) Blue Step. [Online]. Available: http://steab.se/2bluestep.html

[5] ECKey. (2011, May 24th) ECKey - turn your phone into a key! [Online]. Available: http://www.eckey.com

[6] SOREX - Wireless Solutions GmbH. (2012, January 11th) SOREX wireless products. [Online]. Available: http://www.sorex-austria.com/overview wireless.html

[7] E. R. Wognsen, H. S. Karlsen, M. Calverley, and M. N. Follin. (2016, March 20th) A proposal for a secure relay protocol for door access control. Student report at Aalborg University. [Online]. Available: http://sw8.lmz.dk/report.pdf

[8]Erik Ramsgaard Wognsen, Henrik Søndberg Karlsen, Marcus Calverley, Mikkel Normann Follin, Bent Thomsen, H Huttel, "A secure relay protocol for door access control," *Proceedings of the Xii Brazilian Symposium on Information and Computer System Security*, 2012.

[9]T. Y. Teck, P. Sebastian and V. Asirvadam, "Card Emulator for Door Access Using Android Platform," *Proceedings of the IEEE International Conference on Control System, Computing and Engineering*, pp.397-402, 2013.