International Journal of Internet of Things 2017, 6(2): 67-70
DOI: 10.5923/j.ijit.20170602.12

Smart Key: Secure Door Lock System using NFC Enabled Smartphone

Menezes Allwyn Bonaventure, Priyadarshini S., Priyanka, Sindhu Nayak*, Ushadevi A.

Department of Computer Science, St Joseph Engineering College, Mangalore, India

Abstract Smartphones have become very popular and versatile devices. An emerging trend is the integration of smart phones into security systems and applications, particularly access control systems to unlock doors. Smartphone based security solutions promise to greatly enhance the user's experience by providing advanced features far beyond the conventional dedicated tokens/transponders. The generic security architecture protects the electronic access tokens on the smartphone and provides advanced features such as context-aware access policies, remote issuing, and revocation of access rights and their delegation to other users. Various approaches to instantiating the security architecture based on different hardware-based trusted execution environments and elaborate on their security properties are discussed here. The door lock system is implemented based on the latest Android-based NFC-enabled smartphone.

Keywords Nearfield Communication, Mobile Security, Access Control

1. Introduction

Today, smartphones are high-performance platforms providing a wide range of features and have become an integral part of daily life. The increasing computing and storage capabilities, the vast number and variety of apps available on app stores and new communication interfaces, such as Near Field Communication (NFC), provide many deployment possibilities for smartphones, including electronic ticketing, payment and access control. In this context, an emerging trend is the integration of smartphones into modern automotive systems and applications such as access control to lock and unlock and also configure the system. In particular, the NFC interface is well-suited for such applications due to its short nominal communication range (of a few centimeters) providing basic assurance of the user's physical proximity. In this paper, the focus is on smartphone-based NFC-enabled door lock systems. An electronic door lock is an anti-theft device that prevents an unknown person from entering the house unless the corresponding access token is (physically) present and authenticated. Currently, this access token is a transponder (i.e., an NFC chip) embedded into the NFC smartphone.

They do not require users to obtain a physical transponder but allow them to use their smartphone to remotely obtain electronic door lock access. Moreover, access rights can be delegated to other users, revoked or bound to specific policies. Despite the mentioned advantages for users, the core challenge concerns the security aspects of smartphone based door lock systems.

Smartphones are complex devices and appealing targets of attacks (e.g., by malware), especially when they are used in security-critical applications. The traditional locks used in practice are closed and proprietary systems and suffer from various security vulnerabilities. The reasons are conceptual protocol design flaws as well as the deployment of insecure or weak cryptographic schemes. On the other hand, a commercial smartphone-based NFC enabled door lock systems have been introduced recently, but without providing technical details or information on their security properties.

Goal and contribution: An open smartphone-based lock system architecture and the underlying security framework, which provides enhanced functional and security features and overcomes the security issues of the conventional door lock systems. In particular, the contribution is as follows:

Framework for smartphone-based door lock systems: Framework considers the functional and security requirements on the protocols and the system architecture of a smartphone based solution under realistic adversary models.

Evaluation of existing security hardware: This paper evaluates and discuss various instantiations of security architecture using different approaches to establishing trusted execution environments on smartphones. It discusses which security guarantees can be provided by these instantiations, under which assumptions, and how some of these assumptions can be fulfilled by leveraging the features of security hardware currently available on recent

* Corresponding author:
sindhunayak1995@gmail.com (Sindhu Nayak)
Published online at http://journal.sapub.org/ijit

smartphones.

Implementation: It shows show that it is feasible to implement a secure NFC-enabled and smartphone based door lock system. In particular, the paper discusses the conditions for the secure integration of enhanced features such as delegation under a strong but realistic adversary model, where the adversary has full control over the software on the smartphone platform. Hereby, it takes the technical limitations of currently available security hardware for smartphones into account.

Outline: The paper presents the framework for smartphone based door lock system systems, an overview of related work in Section 2 and the proposed system in Section 3. The security requirements are defined in section 4 and the implementation and evaluation of solution in Section 5. Finally, conclude in Section 6. References are presented in Section 7.

2. Related Work

In this section, existing door lock system systems in practice and in literature are discussed. Further, it gives an overview of related work regarding access control with smartphones.

NFC-based Door lock system: NXP Semiconductors presented the prototype of an NFC-based door lock system. The security of this approach relies on the secure element of the smartphone. However, it is unclear how this secure element is instantiated and whether this approach requires new phones with special security hardware.

Transponder-based Door lock system: Lemke et al present a system model and requirement analysis for electronic door lock system systems that use dedicated hardware tokens. The proposed model does not capture advanced use cases such as delegation and thus cannot be applied to the system.

Delegable Access Control with Smartphones: The work is along the lines of the Smart Token system by Dmitrienko et al. which enables NFC-enabled smartphones to maintain electronic access control tokens that can be delegated to other users. Specifically, the project adapt the protocols of the Smart Token scheme to the door lock system use case and provide a tool-based security verification of these protocols.

3. Proposed System

A. System Model

The system model is depicted in Figure 1 and involves a Security Technician, a Home, an owner, and a user.

The technician produces lock equipped with door lock system, which are electronic control units that prevent unauthorized users from starting the house. Moreover, Technician also represents service stations authorized by the Interior Designer. An owner is a private person who received an electronic access control token T_O from Technician. The token is securely deployed and stored on the mobile platform of Owner. A guest user is a person who is authorized by Owner to use. This can be a friend or a family member of the owner. The authorization is given by means of issuing a delegated access control token which grants the User access to the home.

Figure 2 shows the operational flow chart of the proposed system. The setup is powered up and initializations of modules are done. The owner of the house sends a message to a person of NFC mobile holder and to the door. When a person taps NFC mobile on NFC reader which are installed on the door, it compares SMS data with data received from NFC mobile when it matches the door unlocks.

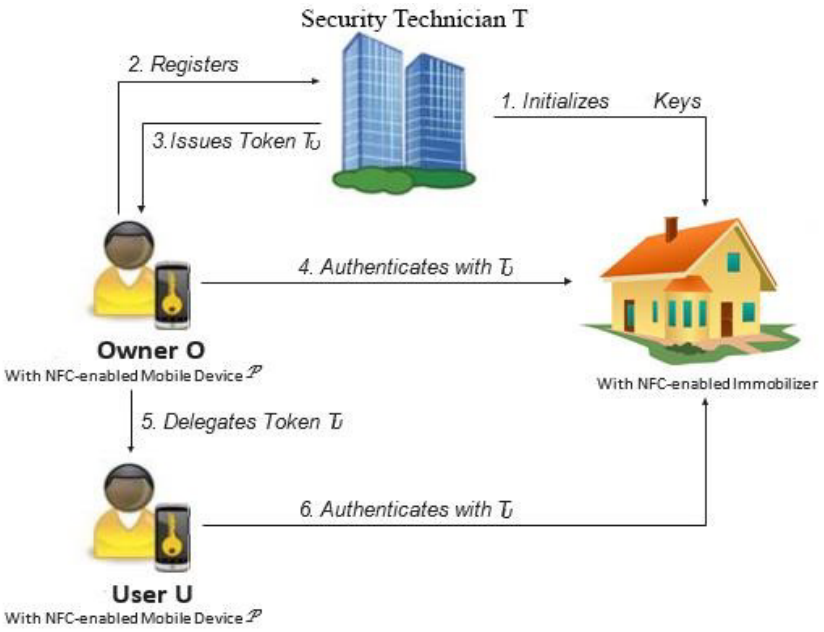

Figure 1. System Model

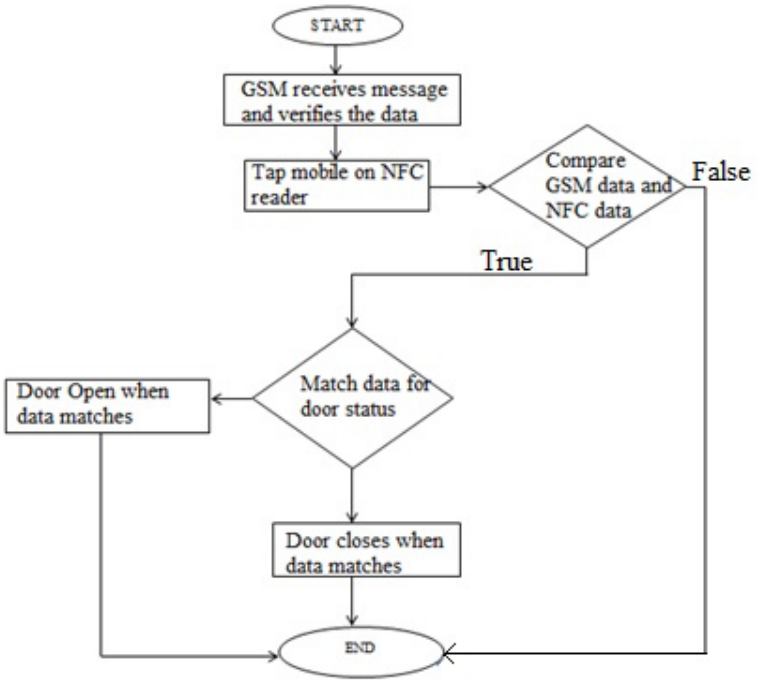

Figure 2. Operational Flowchart

B. Objectives

As in traditional door lock systems, the main objective is to prevent unauthorized access:

Access control: Only authorized entities, namely Owner authorized by Technician and User authorized by Own, should be able to unlock the door. Further, the performance, i.e., the time needed for authentication is a significant usability aspect, which is essential for a positive user experience:

Performance: Authentication of Owner or User to Door should be performed within an unnoticeable time interval. Moreover, the compatibility to existing smartphones is important to ensure the applicability of the solution in practice:

Compatibility: An important requirement is a compatibility with commodity mobile platforms. The door system should be compatible with existing hardware and require no or only minor changes to the mobile operating system. A smartphone-based door system should enable new appealing features, such as the remote issuing and revocation of electronic tokens, remote replacement of electronic keys in case of loss or theft of the mobile device, or provide mechanisms to ensure access revocation of former owners in case of House re-sell.

Remote issuing: The Security Technician should be able to remotely (e.g., via the Internet) issue and deploy the electronic access token to the Owner.

Remote revocation: Technician should be able to remotely revoke access tokens issued. Moreover, revocation of the token by Technician should automatically revoke all delegated tokens issued by Owner. Some other desirable enhanced features include token delegation and support for context-aware access policies:

Delegation: An Owner should be able to securely delegate her access rights to a third party User.

Policy-based access control: An owner should be able to restrict access to delegated users are based on contextual information such as time and location. Off-the-shelf smartphone platforms and security hardware can be used to achieve objectives. However, due to the technical constraints of available security hardware and the limitations posed by some security hardware manufacturers, objectives Delegation, and Policy-based access control cannot be realized with the currently available commodity hardware.

4. Security Requirements

Protocol-specific requirements:

The main security objective of a door lock system is the secure authentication of the owner (or the delegated user) to the door lock system.

Platform-specific requirements:

Mobile platforms typically host a mobile operating system that can potentially be compromised and expose all secrets stored on the platform. Hence, to achieve the objective, the security-sensitive data used in the underlying protocols must be protected against untrusted code. Therefore, it defines the following security requirements on the underlying mobile platform:

Secure storage: Security-sensitive data should not be accessible by untrusted software components while stored on the platform.

Isolation: The system components operating on security-sensitive data must be trusted and isolated from the untrusted

components. Further, it has to be ensured that the security sensitive operations, such as authentication and delegation, are triggered by the user rather than by malware. Moreover, advanced use cases, such as delegation and policy-based access control, rely on security-critical user inputs, such as passwords and user-defined access-control policies. Hence, for these use cases it needs an additional security requirement:

Secure user interface: The user (the owner or the user) should be able to securely communicate with the trusted components.

5. Implementation

An NFC reader/writer is connected to an Arduino which reads the details of the user from the NFC smartphone. The Arduino then checks if the d is an owner d or a guest d. If it is a guest d, it verifies it with the code provided to the GSM module. For this and the previous condition, if the NFC smart d code matches with the required data. It will send a signal to the servo motor to rotate to either locked or unlocked state. When the servo motor is in the locked state, a red LED will be on and the LCD screen will display that the door is locked, and when the servo motor is in the unlocked state the green LED will be on and the LCD screen will show that the door is unlocked. Android provides an adaptive app framework that allows you to provide unique resources for different device configurations. For example, you can create different XML layout files for different screen sizes and the system determines which layout to apply based on the current device's screen size. You can query the availability of device features at runtime.

Owner sends a message to a person having NFC mobile, Message is received by the person. The message will have the key and person need to take his mobile to NFC reader which is on the door. A person needs to enter the key in the android application and tap on the NFC reader. Based on the key door can be opened or closed.

Performance Evaluation: The performance of the implementation of the authentication protocol running between the smartphone and the door lock system is evaluated. For this purpose, we made the following measurements: the time required to start the authentication mechanism and to get the challenge from the door lock system after the NFC connection has been established, the time required by the phone to send the response to the door lock system. The time required by the door lock system to verify the phone's response, and the time required for the complete authentication protocol.

6. Conclusions

Unlike the conventional, closed and proprietary door lock systems that suffer from various vulnerabilities, this open approach allows the independent evaluation of the solution by the research community. The framework consists of a set of secure protocols and a security architecture for the mobile platform. The security of the underlying protocols using automated formal verification tools is analyzed. Moreover, the paper analyses the security of the architecture and discuss which objectives can be achieved using off-the shelf secure hardware for mobile platforms. The paper shows that available hardware allows remote issuing and remote revocation of electronic tokens, which cannot be achieved with classical (transponder-based) door lock system systems. Further, the project outline approaches to achieve more advanced security features, such as secure delegation and context-aware access control.

REFERENCES

[1] Hussain Ahmed AL-OFEISHAT, "Near Field Communication", IJCSNC International Journal of Computer Science and Network Security, vol.12, no.2, Feburary 2012.

[2] Roy Want, "Near Field Communication", IEEE Pervasive Computing, vol.10, no.3, July-September 2011.

[3] Sungbum Kim, Taeyong Yang, Dongwork Kim, "Critical Success Factors of Convergency Technology Commercialization:Near Field Communication", Technology and Society Magazine IEEE, vol.32, pp 21-28, ISSN 0278-0097.

[4] Stephen Tang, Beeling Tok, Hanneghan, "Passive Indoor Positioning System (PIPS) using Near Field Communication", Development of E-System Engineering 2015 International Conference on 13-14 december 2015, pp 150-155, 2015.

[5] Karan Katiyar, Harsh Gupta, Abhishek Gupta, "Integrating contactless Near Field Communication and context-aware systems: Improved Internet-of-Things and cyberphysical system", Confluence The Next Generation Information Technology Summit (Confluence) 2014 5th International Conference, pp. 365-372, 2014.

[6] Pei-Lee. Teh, Pervaiz K. Ahmed, Soon-Nyean. Cheong, Alan H.S. Chan, Wen-Jiun. Yap, "Knowing what a user likes: Mobiquitous home with NFC smartphone", Industrial Engineering and Engineering Management (IEEM) 2013 IEEE International Conference on, pp. 121-125, 2013.