Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 4, April 2014, pg.1272 – 1276

RESEARCH ARTICLE

MULTI LEVEL SECURITY ARCHITECTURE FOR NFC ENABLED CAR KEYS

Suman Chaudhary, Niharika Garg

Department of Computer Science**,** ITM University, Gurgaon**,** India

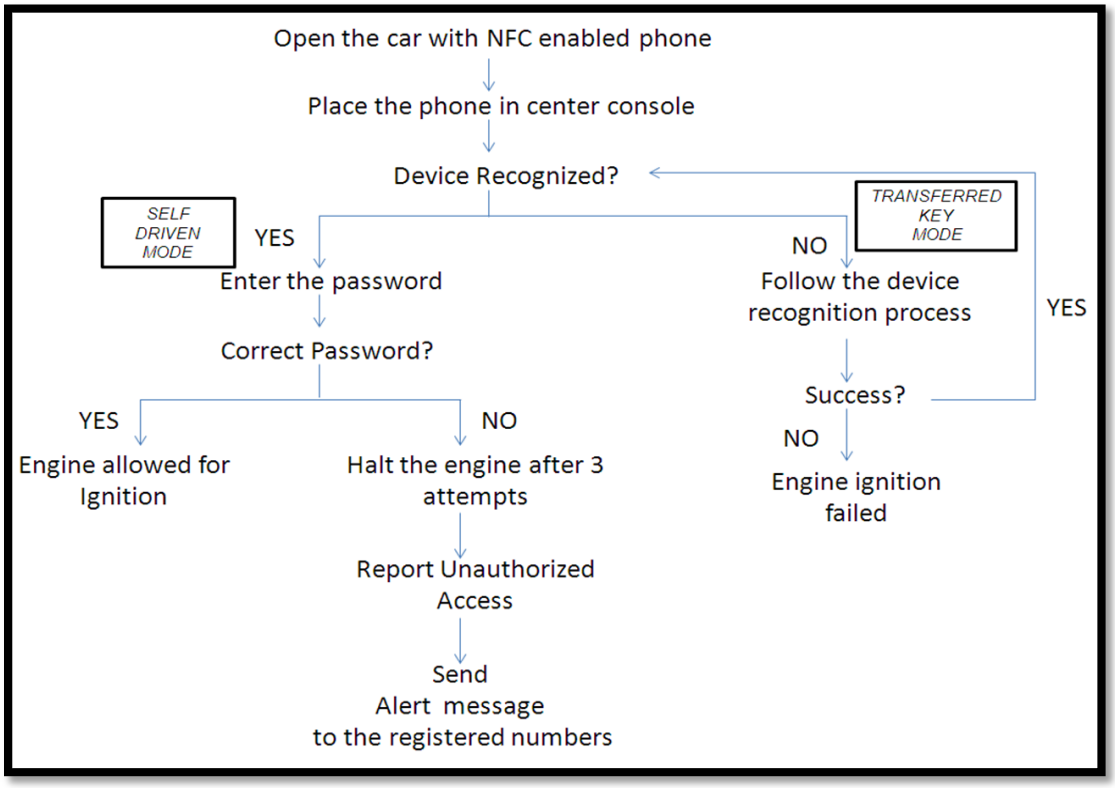
Abstract - NFC is incorporation of RFID in smartphones offering a large number of services which can make our lives simple. In this paper, we are going to discuss one such innovation known as 'NFC enabled car keys'. In future we will have cars which will facilitate keyless entry since the key will be present inside the phone and conferred to the car via NFC. It becomes necessary that such a system be secured by multiple authentication steps. The complete system is designed in a manner such that no single fact is sufficient enough for any adversary to drive away the car. Keys and code are distributed so as to make the system more secure. The key manager is involved in the scenario to ease the provision of transferring key Over-The-Air.

Keywords - NFC, Trusted Execution Environment (TrEE), Secure Element, Over-The-Air (OTA), Key Manager

I. NFC ENABLED CAR KEYS

An interesting technology which has surfaced lately and seems as a beneficial technique to support a better way of communication between a user and its surroundings is Near Field Communication (NFC). NFC unifies contactless discovery with interconnection technologies enabling wireless short range interaction between an NFC tag and device. Concept of introducing cars which support NFC enabled keys (using smart phones) is the latest in research and development domain [1]. Electronic access control key could offer multiple fascinating features such as Key Allocation Over-the-Air, reporting unauthorized access, Multi-level Authentication system for the safety of car.

i. Proposed Architecture



The Administrator will open the car using 'TAP AND GO' feature, sit inside the car and put his phone in the center console. As soon as the phone is placed in the center console, the procedure for device recognition is started.

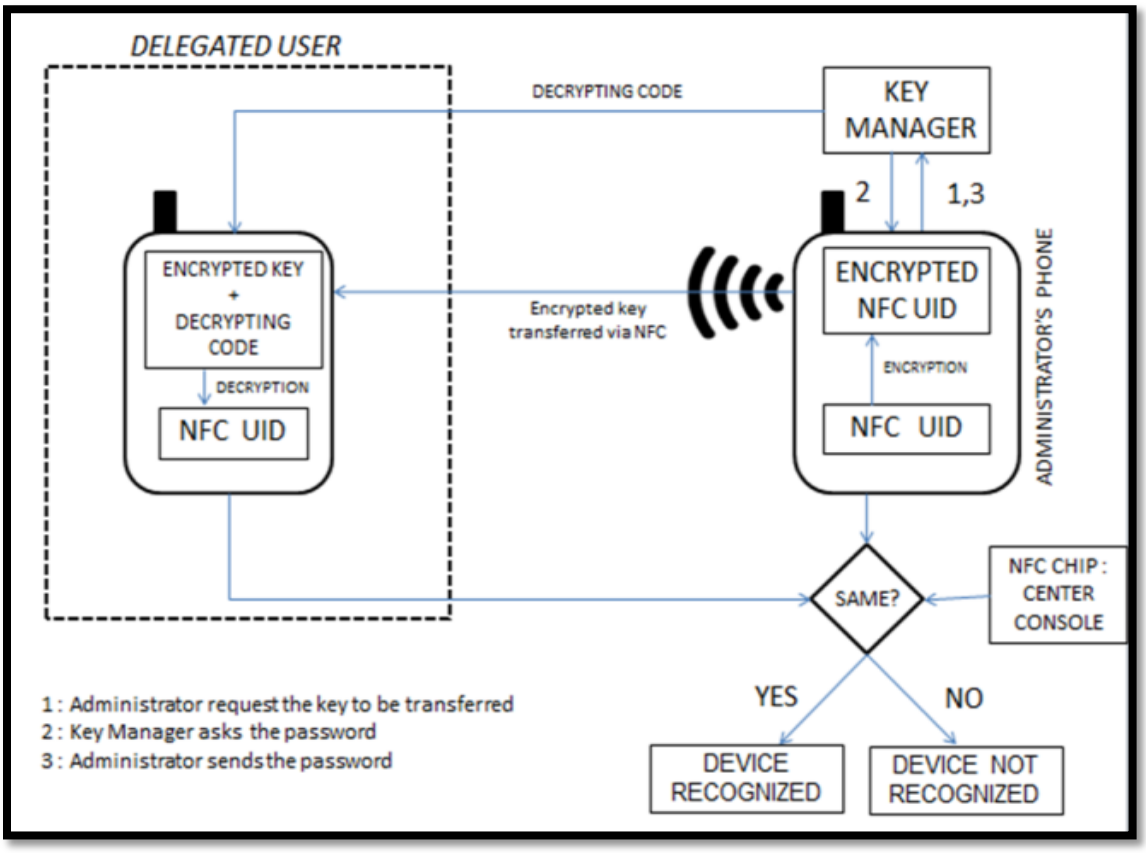
- If the device is recognized.

The circuit for engine ignition is initialized. Here placing the phone in center console acts the same as putting the key in the existing cars. However, the phone will still ask for password which has to be entered by the administrator. If three times the wrong password is entered the alert message is sent to the registered numbers. The registered numbers could be those which the administrator has listed with the network operator. The additional password shall prove to be valuable in case the phone is stolen.

II. KEY TRANSMISSION

When the key has to be entrusted to some other user, multiple steps are followed to ensure that the security of the system becomes stronger. In the delegated mode, the Encrypted code (E_c) is transferred via NFC from the administrator's phone to the delegated user. The E_c proves to be gibberish unless decrypted. The Decrypting Code (D_k) is needed to make the garbage value useful which resides at the server (Key Manager). The D_k can only be received if the administrator contacts the Key Manager and asks to deliver the D_k to the particular mobile number. Consequently, the E_c is decrypted and matched with the chip in Center console NFC chip. If the two strings match, the device is recognized with the respect to the chip in Center console and the car becomes ready for driving.

The main aim of designing such a system is to block the adversary from being able to validate himself to the key manager which could be made possible due to distribution of keys and codes.



System becomes more secure because of the distribution of keys and code [2].

a. Server: The decrypting code lies with key manager. [Inherence Factor]

b. Phone: The unique NFC chip ID resides in the phone. [Possession Factor]

C. User: The manual password has to be entered by the user. [Knowledge Factor]

At no point the adversary would be possess all the credentials required to access the car.

The transfer of key over the network via Key Manager is facilitated by OTA. Over-The-Air (OTA) is a technology based on Client-Server architecture which can be used to provision the delegated user mode [3]. It updates any changes required directly into SIM, in our case the decrypting key is directly sent to the SIM and executed automatically.

III. SECURE HARDWARE

To realize the given features, NFC must be present inside the phone. There are two possible ways to embed NFC in mobile [4]:

a. NFC chip incorporated into mobile device with the suitable antenna.
b. NFC application incorporated into the SIM

Second option is more suitable for the case discussed above [2].

i. UICC

NFC enabled SIM is a totally new concept in the mobile telephony system. The specialized new generation SIM is known as UICC (Universal Integrated Circuit Chip). It is the most Secure Element (SE) possible in the mobile phone devices ensuring the security and integrity of personal data. A secure element (SE) is a non-corruptible platform ideal for safely hosting applications and their secret and encrypted data (e.g. key management) in accordance with the conventions and safety requirements established by a set of well-recognized trusted authorities [5]. While several applications are stored and executed in the same device it is necessary to place them in a secure environment. The presence of the secure element is necessary to implement value added services such as authentication and password management. One of the three forms in which secure element could be incorporated is the SIM called UICC.

i. Trusted Execution Environment

To make the application environment safer, we rely on Trusted Execution Environment (TrEE) which is a secure zone in the main processor of any smartphone [6]. The sensitive data is stored, executed and safeguarded in a trusted setting. It is disconnected by hardware from the main operating system ensuring the secure storage of sensitive data and execution of trusted applications. It safeguards the integrity and privacy of key resources, such as the service provider assets and user interface. It also handles and executes trusted applications developed by device manufacturers as well as third party applications as demanded by people. Together the Secure Element and the TrEE make the smartphone safer for the critical applications. Also execution of application in the TrEE ensures the following:

- Code integrity
- Code access control
- Code isolation
- Confidentiality of user credentials

IV. OTA SERVICES

The Over-The-Air (OTA) services facilitate secure remote management of the user credentials ensuring that the data remains updated consistently. OTA platform becomes functional due to the establishment of mobile based IP infrastructure and is implemented on client server architecture. In the NFC enabled car keys system, OTA services play a major role enabling the transfer of keys from the administrator to the delegated user. Here the key manager acts as the Server and the administrator acts as the client. UICC based OTA users and key managers along with the mobile network operator would be able to maintain a quality of service as it is possible to allocate software and hardware for NFC and Key management activities [7].

V. SECURITY CONCERNS

- NFC is just an interaction medium based in the physical layer. Whatever security has to be provided will be added above the physical layer in the form of encryption. The key string could be eavesdropped easily if it is not encrypted. The code to decrypt the key string lies inside secure element. Moreover, the execution of the application takes place in the Trusted Execution Environment.
- In the case where mobile phone is stolen with the intent of stealing the car, it is not possible for the adversary to drive away the car since the password has to be entered manually when the phone is placed in the center console.
- It is also not possible to corrupt the key as it lies inside the SE and executed inside the TrEE.

VI. CONCLUSIONS

While the technology is advancing, NFC would be implemented into everyday objects making our lives easier and convenient. Similarly incorporating NFC into car keys is a wonderful concept but a very secure architecture is needed to realize the idea. Therefore it is essential to involve various entities in the system such as Key Manager and authentication from the device and user. The credentials too are stored in a secure environment present inside the smartphone. Further development in OTA services will make it easier to handle and transmit keys.

REFERENCES

[1]http://www.nfcworld.com/2013/01/08/321777/hyundai-shows-off-nfc-car-key-concept/
[2]http://en.wikipedia.org/wiki/Multi-factor_authentication
[3] Sirpa Nordlund, Venyon "Secure Over-The-Air Services in NFC Ecosystems", NFC Applications Conference Hagenberg March 20th, 2007.
[4] Lishoy Francis, Gerhard Hancke, Keith Mayes and Konstantinos Markantonakis, "Potential Misuse of NFC Enabled Mobile Phones with Embedded Security Elements as Contactless Attack Platforms", Institute of Electrical and Electronics Engineers, 2009.
[5] "Global Platform's Proposition for NFC Mobile:
Secure Element Management and Messaging", White Paper April 2009.
[6] Roland van Rijswijk-Deij, and Erik Poll "Using Trusted Execution Environments in Two-factor Authentication: comparing approaches".
[7] "The OTA Platform in the World of LTE", Giesecke & Devrient.

