Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 28, S. 246-250, Kasım 2021

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 28, pp. 246-250, November 2021

Research Article

Security and Privacy Based NFC Wallet Design

Faruk Özkan[1], Ömer Aydın[2*]

[1*] Dokuz Eylül University, Faculty of Engineering, Computer Engineering, Izmir, Turkey, (ORCID:0000-0001-6665-2691), faruk.ozkan@ceng.deu.edu.tr, faruk.ozkan@onarfa.com

[2] Manisa Celal Bayar University, Faculty of Engineering, Electrical and Electronics Engineering, Manisa, Turkey, (ORCID: 0000-0002-7137-4881), omer.aydin@cbu.edu.tr

(1st International Conference on Applied Engineering and Natural Sciences ICAENS 2021, November 1-3, 2021)

(**DOI:** 10.31590/ejosat.995411)

ATIF/REFERENCE: Ozkan, F., Aydın, O. (2021). Security and Privacy Based NFC Wallet Design. *European Journal of Science and Technology*, (28), 246-250.

Abstract

With the Covid-19 pandemic, contactless and remote payment options have started to be used more widely. NFC technology is also used for contactless payment. In this study, it is aimed to create a payment system using NFC. The design of the payment system used a portable NFC, an Android phone with version 4.4 or higher, an NFC card, Firebase database from Google, and tokenization. We can define tokenization as generating a random string of text with your credit card number. First of all, the developed application must be downloaded and installed on the phone. With this application, the phone will act as a POS machine. Users can use the phone as a POS and make transactions using it. In this system, only a random text string will be visible in an unauthorized access to the database. In this way, security and confidentiality are provided in the system.

Keywords: NFC, Wallet, wireless connection, security, privacy.

Güvenlik ve Mahremiyet Tabanlı NFC Tasarımı

Öz

Covid-19 pandemisi ile birlikte temassız ve uzaktan ödeme seçenekleri daha yaygın olarak kullanılmaya başlamıştır. NFC teknolojisi de temassız ödeme için kullanılmaktadır. Bu çalışmada NFC kullanarak bir ödeme sistemi oluşturmak amaçlanmıştır. Ödeme sisteminin tasarımında taşınabilir bir NFC, 4.4 veya üzeri sürüme sahip bir Android telefon, NFC kartı, Google tarafından sunulan Firebase veritabanı ve simgeleştirme kullanılmıştır. Simgeleştirmeyi, kredi kartı numaranızla rastgele bir metin dizisi oluşturmak olarak tanımlayabiliriz. Öncelikle geliştirilen uygulamanın telefona indirilerek kurulması gerekmektedir. Bu uygulama ile telefon bir POS makinesi görevi görecektir. Kullanıcılar telefonu POS olarak kullanabilir ve bunu kullanarak işlem yapabilir. Bu sistemde, veritabanına izinsiz bir erişimde yalnızca rastgele bir metin dizisi görülebilecektir. Bu şekilde sistemde güvenlik ve gizlilik sağlanmaktadır.

Anahtar Kelimeler: NFC, Cüzdan, kablosuz bağlantı, güvenlik, gizlilik.

[*] Corresponding Author: omer.aydin@cbu.edu.tr

1. Introduction

NFC stands for "Near Field Communication". NFC is a wireless communication style with a working distance of about 10 cm. It can operate in several modes. The modes are determined by whether the device creates its Radio Frequency(RF) field or retrieve it from generated by others. The ones which create the RF field is called active (like phones) and they have a power supply. The other ones which retrieve the RF field from others are called passive devices (like student cards) and usually, they don't have a power supply. When two devices will communicate one device must be active but the second device can be both [1]. The best thing about NFC's is the passive NFC devices can work without power. It makes NFC easier to use in many ways like payment, bus tickets, connecting Wi-Fi, transferring data easily, entering places that need identification etc. You can use it to connect your phone with a car's radio when you enter the car or use it to share data with your friends like a location, a photo etc. Also, you can use it to enter places that need personal identification just by showing your NFC card to the reader. NFC is a very good way, especially in payment. In city busses or ferries, you can easily pay and pass even without waiting. Also, you can use NFC in restaurants or markets, while paying you can easily just use your NFC card and pay quickly just like in busses. It has some advantages over the Bluetooth. NFC consumes less power because of passive NFC devices that do not need a power source. Also, it is way faster than Bluetooth. When two NFC devices come near 10 cm to each other the data transfer begins and this makes NFC more usable. On other hand, there are phone applications that use NFC technology to pay without needing your credit card. After saving your credit card to the application you can pay everywhere that uses the contactless payment option by using your phone. You don't need your credit card anymore to make payments. In some secure applications, they use encryption and store the data on servers. It is too hard to break into transactions as a middle man because the application uses the session key to encrypt the data of your credit card and that means the hackers only have one shot to solve encryption and that does not seem possible. In our application, after entering your credit card details, they will be stored in the cloud by tokenized. While paying, your application will generate a session key and sends it to the cloud to match the card details then sends it to the bank to do the money transaction. As you can see above NFC technology is very useful and easy to use. It is fast and it is secure enough to make transactions.

This study is about making an android application which can transfer money(data) with using the cloud system to other NFC device. In Google Pay [2], the first user adds a credit card to the application then google pay requests a token from the bank that the user adds its credit card. After that the application associates the card with a unique id and Google Pay encrypts the id, it becomes ready to use. While using an NFC reader, google pay sends the data of tokenized cards and a cryptogram. The network validates the cryptogram and matches the token with the real card number. In the end, acquiring bank and customer's bank solves the rest.

In the second section of this study, the studies carried out in the literature on this subject are given. In third section, the methods and materials used are presented. The proposed work is detailed in the fourth section. In last section, the conclusion and discussion are given. The goal in this study is making an application, that the user can make payment without using a POS machine but only using the mobile phone, securely.

2. Related Works

This article that written by Michelle Fisher and Rathin Guha is about making NFC transactions safe. There are two different parts to the security of transactions. The first one is phone safety. Before making transactions you need to enter your pin or make biometric authentication. Biometric security is safe enough to use your mobile NFC app. (In Germany, researchers tried to pass biometric authentication. They took their hand's photo and printed their hands on normal hands then covered with wax. After 2.500 attempts they finally passed the biometric security.) In this article, the mobile NFC payment app has some payment limitations that can be set by the user like, how much you can pay with this app or which payment types is allowed (Payment, bills, Transactions etc.). In the end, it probably won't be worth to pass someone's authentication after stealing their phone so it makes the app safe enough to use mobile application The second part is a transaction, in this part the app stores the data of the user not in the mobile phone but in the cloud (except coupons, balance or payment history etc.). In the transaction, the app generates a session key and it is a one-time key. After decrypting it the banks do the rest. As a result, in this project, there seems a problem that safety or speed. Making an authentication for every payment you do can be annoying also the fingerprint authentication on our phones can't be able to work from time to time and if it can't you must enter your pin code to make every transaction, in the end, it becomes nothing different from the normal credit card. But on the other hand not making every payment secure, can cause problems like taking money from you without even noticing [3].

This article written by Kent Griffin and Carl B. Stone is about making connections between two active NFC devices. In the article, PayPal has been used as a trusted server. In the app, after entering PayPal details of yours there will be a selection of send also user can change his/her funding source. After selecting the "send money" option first tap with another device will be shown on the screen of your mobile phone and will show the receiver, amount etc. after the second tap money will be sent to the second device and there will be confirmed via vibration or audio. This makes "unfortunate" transactions a bit harder. Also at the beginning, after your PayPal entered to the app an SMS will be sent to the PayPal user's mobile phone to provide theft. After selecting the "send money" option there will be also passcode protection. In the article there are two different ways of communicate, the first way is between two mobile devices that making money transaction between two credit card or debit account and it is called "open loop". The second is between a phone and a POS terminal and it is called "closed-loop". While paying to the POS terminal one tap will be enough to pay. In the article, there is nothing about transaction encryption like while transferring data between two mobile devices or POS how the sent data will be protected. Also, a four-number pin code is easy to solve and at the beginning, there can be SMS protection, not SMS notification. After entering the card details an SMS can be sent to the card owner's phone to make sure that the user is himself/herself. So by doing this stolen credit cards can't be entered into the app and used easily [4].

This article is written by Mohammad Khan is about a merchant payment system. In the merchant store, the customer can see the menu via an NFC device. NFC device directs the app to the link which the poster has. Then the customer selects what

to order from the menu and selects the "submit order" button to finish ordering. After that customer enters cards details or selects the card that has already been submitted to the app. In this system, NFC is used while getting the menu, not used while paying. There are several things about the system. First, the customer must have a mobile connection or the merchant must have public Wi-Fi. But if we think that public Wi-Fi is not secure enough to make money transactions and the customer can't have a mobile connection the system can fail easily. Also if the phone is stolen by a thief the app can be used to pay without authentication. Furthermore, the merchant can't know who ordered the menu because for example there is a coffee shop which has 20 customers inside and 3 of them has ordered different 3 coffees at the same time. The owner can't know who ordered the coffee because the system is only for seeing the menu and a payment. The system can be changed to a table-oriented NFC payment system which you order from a tablet that is integrated into the table and after selecting the order you pay the bill with the NFC tap that both the tablet and the phone has. The tablet will also have information about the sender table [5].

This article is written by Darin William Smith, Rashid Skaf, James Pautler is about communications between devices. An active device waiting for connection from time to time like per 5 seconds it looks for a passive or an active device to connect. This article gives an example from a public network. When an active device gets a signal from another the device connects to the network and it can share videos, books etc. on the network. Actually, it uses NFC to connect to public Wi-Fi. Also with the NFC connection, the app can control the other stuff like home lights, windows etc. that can connect to public Wi-Fi. While connecting device gets a unique token for safety and uses encryption. For extra security and recognition while connecting user also enters unique information about himself like password, username or phone number. But this security system does not seem enough to prevent hackers [6].

This article is written by Jae Park, Karen Luk, Michael Connolly, Sogol Malekzadeh, John Skovron, Matthias Baer, Monica Gonzalez, Jonathan Aroner is about making easy contact with each other by using NFC devices. When two people want to know each other they just bump their phones and share the information only they want. The information they give each other goes to the server and the server tells what they have in common like food habits, the movies they like or the places they like to go and sends these common things each phone to make connections between people. There seems a little security issue that they sent their interest to the server without encrypting the information. We can't know how much will it affect their lives because the information what they send only information that they want [7].

This article is written by Kyoungmin Cho, Ayoung Hyung, Hyonmi Choi, Yunju Jeon is about an NFC payment app that can perform also without power. When you have to pay via NFC, the POS terminal sends a Bluetooth signal to check the battery of the phone. If it is enough to open the light application, the phone reboots. If that is not enough, there will be an IC card in the phone that holds the default card's information which you select as default. Whether the transaction fails or not the POS terminal sends a notification to the phone. There are also options about what to do while the power off in app like work with a light app always or work with an IC card [8]. This is for LG company.

This article is written by John Cronin and Seth Melvin Cronin is about storing NFC payments that we do. The payments store on our phones. The GPS coordinates, time, amount and vendor information stores on our phones. Also, you can add a photo of what you buy. There is a map that shows what, when and where you buy things. In app there are settings about NFC payments like weekly maximum, disabling NFC payment at some stores or maximum one-time payment with NFC. Storing the information on our phone can cause security issues [9].

Security and privacy are both very important issues for payment and communication so payment systems have to be secure and provide privacy. For mobile phones, IoT and lightweight devices so many security mechanisms or challenges are created and investigated in the literature [10-20].

3. Materials

In this project, we need an android device whose version is must be later 4.4 KitKat. Also, we need a cloud system in order to process the transaction and an encryption system. We used some materials to propose our study. In this section, these materials will be given. Android Studio [21], NFC Compatible Phone, Amazon Web Services [22], Tokenization will be investigated in subtitles below.

3.1. Android Studio

Android Studio was announced by Google in the Google I/O event in 2013[23]. Android Studio is a program that you can build android apps for mobile phones. In Android Studio I will use Java coding language. Android Studio has an emulator to test every step of your coding in an emulated mobile phone and it is easy to use because it has a tool to design your app.

3.2. NFC Compatible Phone

To use the NFC Payment application, we need an NFC compatible version of android or IOS phones. If the phone is not compatible the payment app can't be used.

3.3. Amazon Web Services

Amazon Web Services will be used to store data in servers. The details of the card will be stored tokenized in servers of AWS. A free version of AWS will be used in this application.

3.4. Tokenization

Tokenization is a kind of encryption. The credit card details of the customer will be tokenized. The numbers will change and will store as tokenized in the server. Only the service provider will have the details and will hold them in a different and stronger server.

3. Proposed Work

First of all, there is always a probability to lose your phone. Google Pay needs an authentication but when your phone is in someone else's hands, there is always a way to pass those authentications. If you use public Wi-Fi connection while entering your card details, there can be an intruder who can take your card details from your phone but this is not a special problem for the pay applications. Public Wi-Fi connections are not secure. Simply attackers can hack the phone that uses the application and get access to information but again this is not special for the pay applications. Anyone can use the apps securely but the problem is

the phone's security. Because cracking the transactions are harder than getting access to the phone. Knowing this, we will focus only on transaction security in our work.

In the algorithm, the goal is to create an application that works as a POS machine but there are some security issues to prevent. In the beginning, we need to write the amount we are going to receive. After that, the user can simply show the card to the application and it is done. You can see an example of a simple transaction in Fig 1.

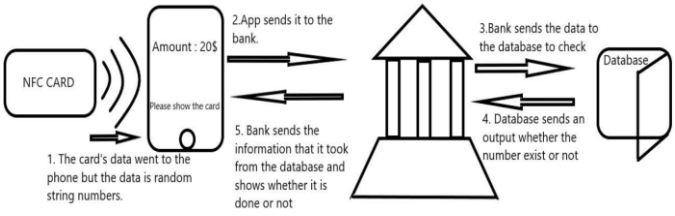

Figure 1. A simple transaction scenario

Here we can see that the application sends a tokenized string number to the issuer bank. Then the bank takes a response from the database whether the card exists or not and gives a response back depending on the database's record. The key in this algorithm is that we use tokenized strings to prevent hackers. Tokenization creates a random string that is going to act like a user's credit card number. The real card number is stored in the bank's database. There is an attack-type that tokenization prevents. The eavesdropping attack, in this type of attack, the attacker tries to take information while the transaction is happening. The attacker steals the card details then copies them. But with tokenization, the attacker has nothing because the only thing that the attacker will get is going to be random string numbers that is useless without the bank's approval. Here we can see an example of a transaction in Fig 2.

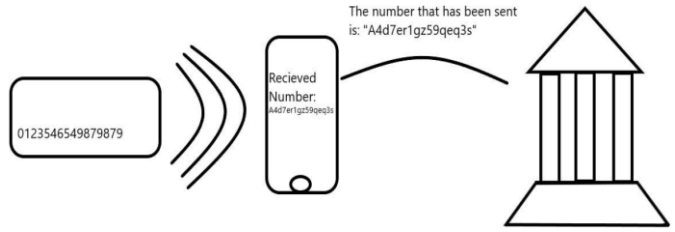

Figure 2. Example of a transaction

In the simulator, we have a database that acts like a bank's database. It stores the user credit card details and responses whether the tokenized number exists or not. After making a payment, the card's tokenized number changes so replay attacks can be prevented. Also if there is a middle man which tries to steal card details, he won't be able to because the number she/he gets is just a random string that is useless.

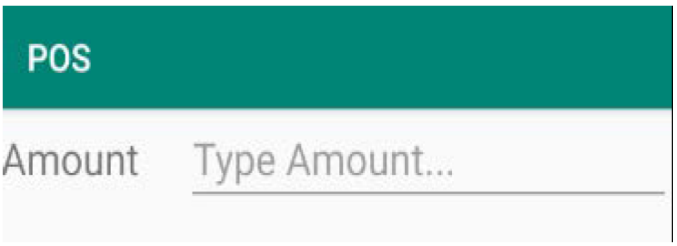

Figure 3. Screenshot of the amount

The POS payment screen on the mobile phone is designed as shown in Fig 3. The transaction is carried out by entering the amount of payment to be made in this field. At the same time, Fig 4 shows the operations of the last system by the NFC card side.

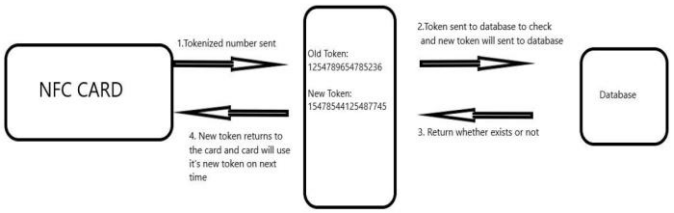

Figure 4. end system from card's side

After a payment, new token will be created and will be changed in the database also will be sent to the card. The card is going to use the new token to make payment. In this way, the payment process will be carried out securely.

4. Conclusions and Recommendations

In this study, a payment system has been tried to be designed by considering the advantages of NFC. As is known, security in payment systems is of great importance. These are the dangers that attackers can capture, change or use payment information for different purposes. It is of great importance to design a system that will operate smoothly against these dangers. On the other hand, there are important advantages of using an NFC-enabled mobile phone for payment transactions. For this reason, in this study, it has been tried to perform a secure payment transaction through an application developed on a mobile phone. In future studies, the coding process of this application will be completed and different IOS and so on. can be made to work in different environments.

5. Acknowledge

We would like to thank Dokuz Eylül University Computer Engineering Department for their support.

References

[1] Haselsteiner, E., & Breitfuß, K. (2006, July). Security in near field communication (NFC). In Workshop on RFID security (Vol. 517, No. 517, p. 517).

[2] Michael, S. (2018). Google is combining Android Pay and Google Wallet under one brand: Google Pay. PCWorld. https://www.pcworld.com/article/3246290/google-pay.html

[3] Fisher, M., & Guha, R. (2016). Mobile communication device near field communication (NFC) transactions. U.S. Patent

No. 9,378,493. Washington, DC: U.S. Patent and Trademark Office.
[4] Griffin, K., & Stone, C. B. (2017). Two step near field communication transactions. U.S. Patent No. 9,558,485. Washington, DC: U.S. Patent and Trademark Office.
[5] Khan, M. (2017). Methods, systems, and computer readable media for facilitating in-store or near-store ordering and payment of goods and services through a single-tap of a near field communication (NFC) device. U.S. Patent No. 9,536,243. Washington, DC: U.S. Patent and Trademark Office.
[6] Smith, D. W., Skaf, R., & Pautler, J. (2017). Processing near field communications between active/passive devices and a control system. U.S. Patent No. 9,793,962. Washington, DC: U.S. Patent and Trademark Office.
[7] Park, J., Luk, K., Connolly, M., Malekzadeh, S., Skovron, J., Baer, M., ... & Aroner, J. (2016). Sharing of information common to two mobile device users over a near-field communication (NFC) link. U.S. Patent No. 9,264,104. Washington, DC: U.S. Patent and Trademark Office.
[8] Cho, K., Hyung, A., Choi, H., & Jeon, Y. (2017). Mobile terminal and method of performing NFC payment using the mobile terminal. U.S. Patent No. 9,697,515. Washington, DC: U.S. Patent and Trademark Office.
[9] Cronin, J., & Cronin, S. M. (2019). Securing nfc-based payment. U.S. Patent Application No. 16/271,677.
[10] Çepik, H., Aydın, Ö., & Dalkılıç, G. (2021). Security Vulnerability Assessment of Google Home Connection with an Internet of Things Device. In Multidisciplinary Digital Publishing Institute Proceedings (Vol. 74, No. 1, p. 1).
[11] Wang, Y., Hahn, C., & Sutrave, K. (2016, February). Mobile payment security, threats, and challenges. In 2016 second international conference on mobile and secure services (MobiSecServ) (pp. 1-5). IEEE.4.
[12] Cabuk, U. C., Aydin, Ö., & Dalkiliç, G. (2017). A random number generator for lightweight authentication protocols: xorshiftR+. Turkish Journal of Electrical Engineering & Computer Sciences, 25(6), 4818-4828.
[13] Xiao, L., Wan, X., Lu, X., Zhang, Y., & Wu, D. (2018). IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?. IEEE Signal Processing Magazine, 35(5), 41-49.
[14] Liu, Z., Ma, J., Weng, J., Huang, F., Wu, Y., Wei, L., & Li, Y. (2021). LPPTE: A lightweight privacy-preserving trust evaluation scheme for facilitating distributed data fusion in cooperative vehicular safety applications. Information Fusion, 73, 144-156.
[15] Wang, Z., Lin, Y., Zhuo, Z., Gu, J., & Yang, T. (2021). GNFCVulFinder: NDEF Vulnerability Discovering for NFC-Enabled Smart Mobile Devices Based on Fuzzing. Security and Communication Networks, 2021.
[16] Yakut, S., Şeker, Ö., Batur, E., & Dalkılıç, G. (2019, October). Blockchain platform for Internet of Things. In 2019 Innovations in Intelligent Systems and Applications Conference (ASYU) (pp. 1-6). IEEE.
[17] Li, S., Zhao, S., Min, G., Qi, L., & Liu, G. (2021). Lightweight privacy-preserving scheme using homomorphic encryption in industrial Internet of Things. IEEE Internet of Things Journal.
[18] Lu, H. J., & Liu, D. (2021). An improved NFC device authentication protocol. Plos one, 16(8), e0256367.
[19] Aydin, Ö., Dalkiliç, G., & Kösemen, C. (2020). A novel grouping proof authentication protocol for lightweight devices: GPAPXR+. Turkish Journal of Electrical Engineering & Computer Sciences, 28(5), 3036-3051.
[20] Vishwakarma, P. P., Tripathy, A. K., & Vemuru, S. (2021). Cryptanalysis of Near Field Communication Based Authentication Protocol for Mobile Payment System. Wireless Personal Communications, 1-21.
[21] Hagos, T. (2018). Android studio. In Learn Android Studio 3 (pp. 5-17). Apress, Berkeley, CA.
[22] Cloud, A. E. C. (2011). Amazon web services. Retrieved November, 9(2011), 2011.
[23] Huysman, M. (2013). Everything announced at the Google I/O 2013 keynote in one handy list. TNW-The Financial Times. https://thenextweb.com/news/everything-announced-at-the-google-io-2013-keynote-in-one-handy-list