© 2017 IJSRSET | Volume 3 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Securing NFC Againts Data Corruption and Eavesdropping Using Diffie Hellman

Darshankumar M Parmar, Prof. Bakul Panchal

Information Technology Department, L.D. College of Engineering, Ahmedabad, Gujarat, India

ABSTRACT

Now a day's smart phone have Near Field Communication (NFC), which can be used for transferring data, payment trough mobile gateway and automation. With this new contactless technology set to become an important part of our lives, people have some valid and understandable security concerns. NFC is inherently vulnerable to data corruption and eavesdropping attacks. In this research work, we are trying to make security data model in secure element of NFC. Our aim is securing against data corruption and eavesdropping using Daffier Hellman.

Keywords: NFC, Diffie Hallman Algorithm, Data Corruption and Eavesdropping

I. INTRODUCTION

There are a handful of technologies on the market today trying to get noticed and adopted in a mainstream way, some like QR codes have been able to do this, but others have not or their future remain unsure. For those still considering whether or not to use NFC technology for your marketing campaign, your payment systems, or whatever, below are five reasons why you should choose NFC [1].

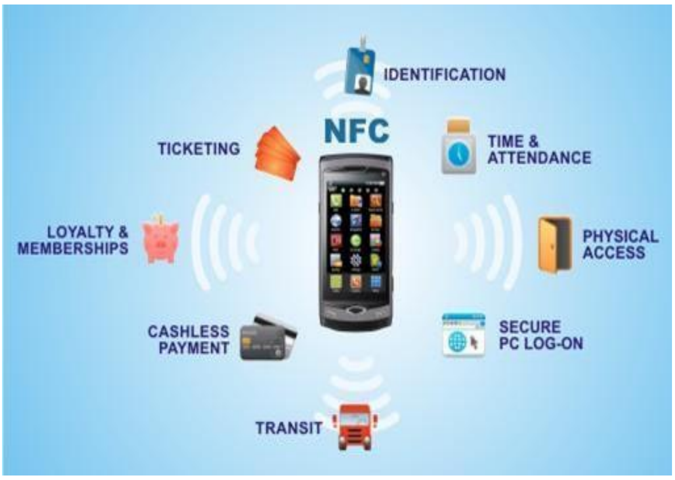


Figure 1. NFC Applications

1. Instinctive :

NFC requires almost no thought or effort on the part of the user unlike some other similar technologies like QR codes (which require the downloading of an app, the opening of the app and the scanning of a bar code). All the user needs to do is tap or wave their smart phone near the NFC tag and the transaction occurs. It is as simple as that. The easier it is for the user the more likely the technology will be used, and it doesn't get easier than NFC.

2. Multipurpose :

NFC can serve an incredible number of purposes and can be useful for almost any industry, or any need. For example, a company like Starbucks might, and indeed has in the past, used NFC as a system of payment. Another company might use the technology as a way to advertise on physical marketing material. Another company might use it as a way to provide additional value to their product, like a Museum using it to create an interactive experience with visitors. There are thousands, if not millions of ways NFC can be used, just figure out what is best for your company or organization and start using the technology for great results.

3. Secure :

The fact that NFC transmissions are such short range, varying anywhere from contact to a few centimeters ensures that the transaction will be private and secure. The technology also has built in capabilities to improve security if needed.

4. Interoperable :

This NFC technology is compatible with the many existing contactless card technologies that are already on the market, making adaption seamless in most cases.

5. Trend Payment :

NFC is already a well-known technology and the infrastructure already exists. Most smart phones already have NFC capabilities built in and the few that don't plan on seeing their next generation phones become NFC compatible. The momentum is towards NFC and it doesn't look to be slowing down. People are already familiar with the technology and as even more businesses and organization are beginning to use NFC the critical mass needed for full market adoption will not be far off.

II. PROBLEM STATEMENT

The main objective of this research work is how to make prevention of mobile payment in secure element NFC from data corruption and eavesdropping.

- NFC Security Risk :

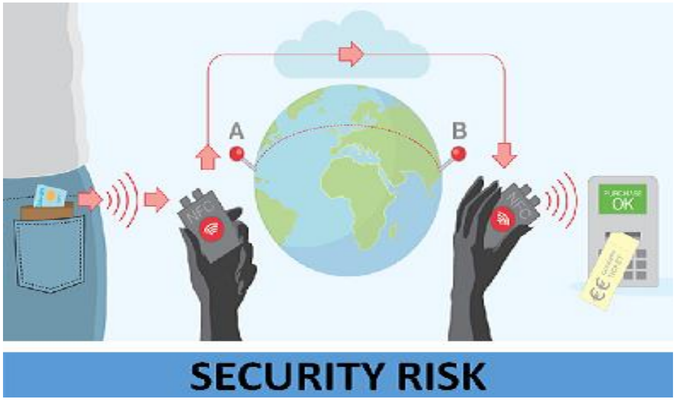


Figure 2. Security Risk

One of the most common concerns with NFC technology is that of eavesdropping. Eavesdropping occurs when a third party intercepts the signal sent between two devices. If that third party intercepted a data transmission between a smart phone and a credit card reader then, in theory, they would have access to that personal credit card information. They might also pick up other personal information passed between two smart phones.

- Eavesdropping :

Eavesdropping is when a criminal "listens in" on an NFC transaction. The criminal does not need to pick up every single signal to gather private information. Two methods can prevent eavesdropping. First there is the range of NFC itself. Since the devices must be fairly close to send signals, the criminal has a limited range to work in for intercepting signals. Then there are secure channels. When a secure channel is established, the information is encrypted and only an authorized device can decode it. NFC users should ensure the companies they do business with use secure channels [6].

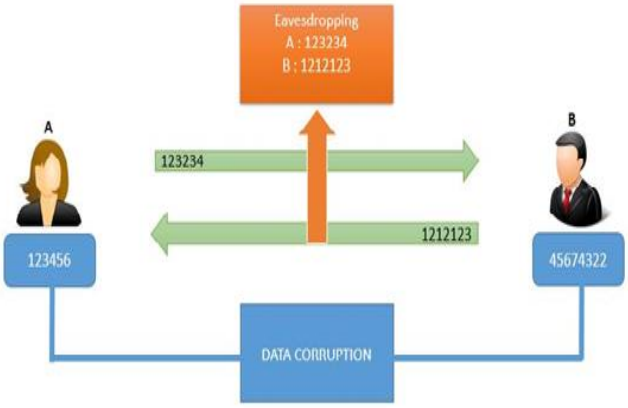


Figure 3. Data Corruption and Eavesdropping

- Data Corruption and Manipulation :

Data corruption and manipulation occur when a criminal manipulates the data being sent to a reader or interferes with the data being sent so it is corrupted and useless when it arrives. To prevent this, secure channels should be used for communication. Some NFC devices "listen" for data corruption attacks and prevent them before they have a chance to get up and running [6].

Another security concern is data manipulation or corruption. This occurs when a third party intercepts the signal being sent, alters it, and sends it on its way. The information the receiving party gets may be corrupt or modified. The attacker may or may not want to steal the information. In some cases, the attacker simply wants to prevent the correct information from getting through. This is often known as a denial of service attack [5]

NFC technology is valuable for the convenience it offers consumers. One person can access all their payment information and make purchases on several different credit or debit cards all with the wave of a smart phone. To protect users against these security risks, several measures have been taken. Users can also take their own precautions to protect their personal information [7].

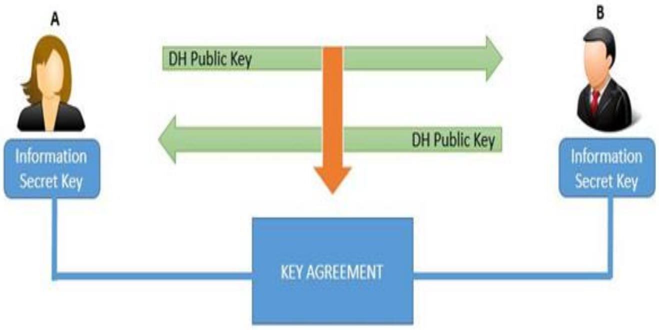
III. RELATED WORK AND LITERATURE SURVEY

No	Paper Title	Publication Journal and publication year	Method	Research Gap
1	NFC Mobile Payments, Are we ready for them?	IEEE, 2016	**Survey , Analysis and Comparison**	NFC mobile payments to see daylight in the world markets, and further ensure a brighter payment future for consumers and stakeholders
2	NFC Devices: Security and Privacy	IEEE, 2008	**Classification Security and Privacy depend on Use cases**	technological aspects of NFC to provided security and privacy we should know the use cases, Assumptions, Components and Trust Levels, Assets to be protected and Threats
3	A Near Field Communication security model based on OSI reference model	IEEE, 2015	**Based on OSI Layer**	In this paper NFC security model is set up based on the OSI reference model, almost all of the OSI Layer reference for NFC protocol design and security analyses.
4	Analysis and Optimization to an NFC Security Authentication Algorithm Based on Hash Functions	IEEE, 2014	**Hash Functions**	This paper has proposed an authentication algorithm without the aid of third-party certification platform and based on Hash function entirely, compared to other schemes with the aid of third-party certification platforms, its power consumption and costs are much lower.
5	Protecting NFC Data Exchange against Eavesdropping with Encryption Record Type Definition	IEEE, 2016	**Encryption Record Type Definition**	In this paper they designed and implemented a lightweight confidentiality middleware based on the proposed ERTD to protect the users from accessing the malicious or spoofed URIs in NFC tags.

IV. PROPOSED SOLUTION

A. Preventing Security Risks with NFC

NFC technology is valuable for the convenience it offers consumers. One person can access all their payment information and make purchases on several different credit or debit cards all with the wave of a smart phone. To protect users against these security risks, several measures have been taken. Users can also take their own precautions to protect their personal information [7].



First, the design of NFC discourages security issues. While they can still occur, it is typically more challenging to steal credit card information through this type of data transfer. The person stealing the info would need to be very close to the smart phone sending it since the signal does not carry very far. Secure channels are used for sending sensitive information, making them hard to access. In the event that a hacker did make it past these security measures to steal the information, the information itself is encrypted. Encryptions prove very difficult to crack and the information would likely be useless to the hacker.

V. CONCLUSION

We are trying to optimize data interference, corruption and eavesdropping on NFC security using Diffie Hellman Algorithm. Diffie Hellman is a key exchange protocol. It is an interactive protocol with the aim that two parties can compute a common secret which can then be used to derive a secret key typically used for some symmetric encryption scheme.

VI. REFERENCES

[1]. Boyle, T. (2013, September 6). 5 reasons you should use nfc. Retrieved November 21, 2016, from Qfuse Blog - QR Code, NFC, and Mobile Marketing News: http://qfuse.com/blog/5-reasons-you-should-use-nfc/

[2]. Rampton, J. (2016, June 14). The evolution of the mobile payment. Retrieved November 13, 2016, from techcrunch.com/2016/06: https://techcrunch.com/2016/06/17/the-evolution-of-the-mobile-payment/

[3]. Fan, W., Huang, W., Zhang, Z., Wang, Y., & Sun, D. (2015). A Near Field Communication (NFC) security model based on OSI reference model. IEEE Computer Society, 1324-1328

[4]. Hameed, S., Jamali, U. M., & Samad, A. (2016). Protecting NFC Data Exchange against Eavesdropping with Encryption Record Type Definition. Network Operations and Management Journal, 577-583.

[5]. Madlmayr, G., Langer, J., Kantner, C., & Scharinger, J. (2008). NFC Devices: Security and Privacy. IEEE Computer Society, 642-647

[6]. Roland, M. (2015). Security Issues in Mobile NFC Devices. Switzerland: Springer.

[7]. Sajid , O., & Haddara, M. (2016). NFC Mobile Payments, Are we ready for them? SAI Computing Journal, 961-967.

[8]. Zhuang, Z. J., Zhang, J., & Geng, W. D. (2014). Analysis and Optimization to an NFC Security Authentication Algorithm Based on Hash Functions. Wireless Communication and Sensor Network Journal, 240-245.