ISSN: 2321-7782 (Online)
e-ISJN: A4372-3114
Impact Factor: 7.327

Volume 7, Issue 3, March 2019

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Near Field Communication security threats & secure passive communication based on "BUZZ"tag

Jignesh Patel[1]
Department of Computer Science,
Hemchandracharya North Gujarat University,
Raj-Mahel Road, Patan-384265, Gujarat, – India

Dr. A. R. Patel[2]
Florida Polytechnic University,
Florida – USA

Abstract: ***Near Field Communication (NFC) has been fast growing technology since last few years. A tight integration of such technology with mobile phones has given a tremendous opportunity to the world. It is a close range induction based technology. In this paper I would like to explore more about this technology threats and what can be the possible outcome to stay away from threats. All these threat are based on passive communication.***

Key Words: RFID, Near-field communication, RFID tag.

I. INTRODUCTION

Near Field Communication (NFC) is a consumer-oriented wireless technology exploitation magnetic fields and induction to communicate over a distance of centimeters at low information measure. It's backed by the NFC Forum, consisting of over a hundred and sixty members as well as trade heavy-weights like Samsung, Sony and NXP. They push and certify integration of NFC technology in fashionable client physical science like smart phones and in operation systems like golem and Windows eight. Current applications embody payment and ticketing by simply waving your phone, the setup of Bluetooth or Wi-Fi connections between devices by touching them along and embedding of knowledge or device configurations in passive entities, thus referred to as NFC tags. [1]

Figure-1- Mobile writing into tag or reading from tag.

The NFC technology might be terribly effective in varied areas. The most applications which will profit from its introduction are:

- Payment through mobile devices like Smartphone and tablets.
- Electronic identity.
- Electronic ticketing for transportation.

- Integration of credit cards in mobile devices.
- Data transfer among any types of devices such as mobile phones and media players.
- P2P data transfer link between wireless devices.
- Loyalty and couponing/targeted marketing/location-based services
- Device pairing
- Healthcare/patient monitoring
- Gaming
- Access control/security patrols/inventory control (tags and readers)

NFC enabled devices will operate in 2 modes as active mode and passive mode. Passive mode is accountable for achieving vital power savings and lengthening the dear battery time. Devices operative in active mode will pro-vide all the facility required for communication with passive devices through their internally generated RF field.

COMMUNICATION MODES

As per NFCIP (NFC Interface and Protocol), there are two communication modes,

- Active NFC mode: In active NFC mode, both the originator and the target are using their own generated RF field to enable the communication (peer to peer).
- Passive NFC mode: In passive NFC mode, the target answers to an originator command in a load modulation scheme. The originator generates the RF field.

OPERATING MODES

- Reader/Writer mode: In the reader/writer mode (figure 1), NFC devices can read and write data from/to NFC tags and smart cards.
- Card Emulation mode: In the card emulation mode (figure 2), NFC device acts as an RFID card and other NFC devices can read data from this NFC device. Stored information in the NFC device is used for further.

Figure-2. Card emulation Mode

- Peer-to-Peer mode: In the peer-to-peer mode (figure 3), two devices can exchange data at link-level. This mode is standardized on the ISO/IEC 18092 (formerly ECMA 340) standard, and allows data speed up to 424 Kbit/sec.

Figure-3. Peer to peer mode

II. COMMUNICATION BASED THREATS

This mode is additionally referred to as a card emulation mode. This NFC mode allows mobile device homeowners to form a contactless business action, within the same approach sensible cards also known as smart cards, area unit used nowadays. This mode of operation allows mobile devices to be used for identification, payment and access management applications.

NFC devices conjointly act as smart card (ISO 14443) and contain a secure smartcard chip also referred as a Secure Element (SE) that operates in card emulation mode. The SE is associated to the NFC controller for contactless payments. Using such mechanism NFC device can be used for purchasing goods as well.

Eavesdropping

Because NFC could be a wireless communication interface it's obvious that eavesdropping is a vital issue. Once 2 devices communicate via NFC they use RF waves to speak to every alternative. Associate wrongdoer will after all use associate antenna to additionally receive the transmitted signals. Either by experimenting or by literature analysis the wrongdoer will have the desired data on a way to extract the transmitted knowledge out of the received RF signal. Additionally the instrumentality needed to receive the RF signal moreover because the instrumentality to decipher the RF signal should be assumed to be obtainable to associate wrongdoer as there's no special instrumentality necessary

The NFC communication is sometimes done between 2 devices in close up proximity. This suggests they're less than ten cm (typically less) off from one another. The most question is however near associate offender has to be to be able to retrieve a usable RF signal. Sadly, there's no correct answer to the current question. The rationale for that's the massive range of parameters that confirm the solution.

When a NFC device is causation data in active mode, eavesdropping will be wrapped to a distance of regarding ten meters, whereas once the causation device is in passive mode, this distance is considerably reduced to regarding one meter.

Data Corruption

Instead of simply listening, a wrongdoer may also try and modify the info that is transmitted via the NFC interface. Within the simplest case the wrongdoer simply desires to disturb the communication such the receiver isn't able to perceive the info sent by the opposite device.

Data corruption may be achieved by transmittal valid frequencies of the info spectrum at an accurate time. The proper time may be calculated if the wrongdoer includes a smart understanding of the used modulation theme and secret writing. This attack isn't too difficult; however it doesn't enable the wrongdoer to influence the particular data. It’s essentially a Denial of Service attack.

Data Modification

In data modification the wrongdoer needs the receiving device to really receive some valid, however manipulated information. This can be terribly completely different from simply data corruption.

The feasibleness of this attack extremely depends on the applied strength of the modulation. This can be as a result of the decryption of the signal is completely different for 100 percent and 10 percent modulation.

Data Insertion

This means that the wrongdoer inserts messages into the information exchange between 2 devices. However this can be solely doable, just in case the respondent device desires a awfully while to answer. The wrongdoer may then send his data before the valid receiver. The insertion are going to be fortunate, only, if the inserted data is transmitted, before the initial device starts with the answer. If each data streams overlap, the information is going to be corrupted.

Man-In-Middle Attack

In the classical Man-in-the-Middle Attack, 2 parties that need to speak to every alternative, referred to as 'X' and 'Y', area unit tricked into a 3 party spoken communication by associate offender 'E'. this is often shown in Figure 4.

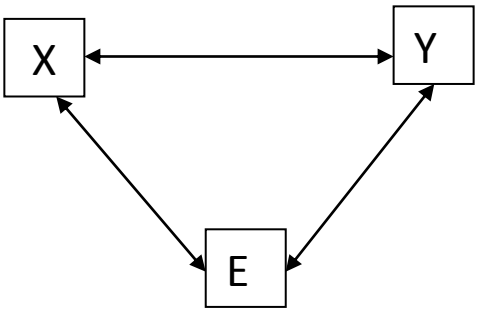

Figure-4 Man in Middle

X and Y should not bear in mind of the actual fact that they're not speech one another, however that they're each causing and receiving information from E. Such a setup is that the classical threat in unauthenticated key agreement protocols like Diffie-Hellmann protocol. X and Y need to agree on a secret key, that they then use for a secure channel. However, as E is within the middle, it's attainable for E to determine a key with X and another key with B. once X and Y later use their key to secure information, E is ready to listen in on the communication and additionally to control information being transferred.

How would that work once the link between X associates degreed Y is an NFC link?

We claim that it's much impracticable to mount a Man-in-the-Middle attack in an exceedingly real-world situation in NFC [8] [4]. Man-in-the-Middle attacks are practically impossible as either initiator or target is able to detect additional fields by a third party as mentioned before.

Relay Attack

A relay attack is dead by sitting within the middle of 2 human action parties and easily "relaying" requests and responses effectively creating oneself invisible to either party (figure 5). Relay attacks exist already for RFID systems and are formed to figure with regular NFC phones by simply putting in specific items of software system.

Figure 5: representation of a relay attack using a contactless smartcard, 2 NFC equipped phones and a reader terminal.

A wrongdoer would need 2 phones to act as proxies connected to every alternative with a high-speed link like Bluetooth. One proxy device interfaces with the NFC token or device of a victim functioning as a proxy-reader. It forwards all messages over the high-speed link to the second proxy device imitating a NFC token to interface with the particular NFC reader, acting as proxy-token. Relaying even permits circumventing dynamic authentication on newer NFC card models as mistreatment the relay link introduces solely little delays still accepted by current card readers. This attack considerations any ISO/IEC 14443 implementing contactless system, many, not NFC, of that square measure wide in use just like the antecedently mentioned NXP MIFARE merchandise. Attainable countermeasures embody aborting the communication if trip times or the situation of the pairing device aren't evidently.

III. KEY AGREEMENT BASED PROTOCOL

Besides the quality key agreement mechanism, it's conjointly attainable to implement associate NFC specific key agreement.

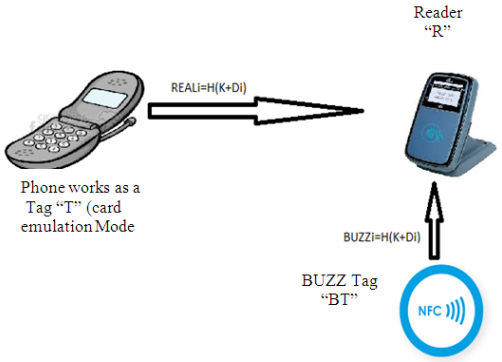

Figure-6 Suggested BUZZ tag based key agreement protocol

Establishing a secure channel between 2 NFC devices is clearly the most effective approach to safeguard against eavesdropping and any reasonably data modification attack.

Because of the inherent guard of NFC against Man-in-the-Middle-Attacks it's rather trouble-free and effortless to setup a secure channel. A standard key agreement protocol like Diffie-Hellmann supported RSA or Elliptic Curves may well be applied to determine a shared secret between 2 devices. As a result of Man-in-the-Middle is not any threat, the quality, unauthenticated version of Diffie-Hellman works utterly.

The solution, which we are going to talk here consist of two tags, which sends codes as similar to CSMA mechanism.

In the beginning we also assume that reader 'R' already shared a secret key 'K' with BUZZ tag. This key is used by BUZZ tag with some pseudo random function to generate codes.

This protocol is based on *n* rounds. We describe round 'j' as follow. In following term 'R' denotes Reader, BUZZ tag which creates noise termed as 'BT' and original tag (in our case cell phone, which emulated card mode) termed as 'T'.

Card Reader 'R' broadcast arbitrary pattern 'Di'.

1. BUZZ tag 'BT' answers with some random arbitrary code BUZZi, which is a combination generated from a pseudo-random function Di and secret key 'K' i.e. 'BUZZi=hash(K , Di)'. Now this sequence of string feels random to a wrongdoer. Reader can easily manipulate that string because reader is having BUZZ tag key in advance so can understand it.
2. Our original data coming from NFC device, working as a tag 'T' in our case reply in same manner as BUZZ tag replies, which is called as REALi.
3. After receiving BUZZi and REALi , reader 'R' will find out false string BUZZi using "hash(k , Di)" but wrongdoer cannot understand random code BUZZi and real code REALi that's why he/she will ignores it.

NOTE: Step No 2 & 3 execution should take place randomly at every round or else wrongdoer can identify which data coming from which tag. Same we can implement using CSMA concept. After receiving Di, tag 'T' and 'BT' will start a timer with random value from 0 to *t, where t is one round duration.* Reply sends by a tag first whose timer expires first.

After finishing of *n* rounds, 'R' and 'T' share *n* codes. Now they could generate a secret key, 'S' as S = REAL1 + REAL2 + REAL3 …..REAL*n*.

This mechanism can be created more critical for wrongdoer by adding more BUZZ tags in to the system.

IV. Conclusion

We bestowed typical an inventory of threats has been derived and addressed. NFC by itself cannot give guard against eavesdropping or information modifications. The sole answer to realize this is often the creation of a secure channel over NFC.

This could be done simply, as a result of the NFC link isn't at risk of the Man-in the-Middle attack. We tend to introduced a NFC specific key agreement mechanism, that provides low-cost and quick secure key agreement.

References

1. NFC - Possibilities and Risks by Uwe Trottmann Betreuer: Matthias Wachs,Seminar Future Internet WS2012.
2. NFC Forum: www.nfc-forum.org.
3. NFC World: www.nfcworld.com.
4. Security in Near Field Communication (NFC)
5. Strengths and Weaknesses by Ernst Haselsteiner and Klemens Breitfuß, Philips SemiconductorsMikronweg 1, 8101 Gratkorn, Austria
6. C. Castelluccia and G. Avoine, (2006). Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags, Proceedings of CARDIS, LNCS 3928, 289-299.
7. E.Y. Choi, S.M. Lee, and D.H. Lee. (2005).Efficient RFID authentication protocol for ubiquitous computing environment. In Proc. Of SECUBIQ'05, LNCS.
8. Gowtham Mamidisetti, P.N.S.L.Sravani, P.Anusha, Mnfc-Operation Modes and Risks, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-3, Issue-5, November 2013.
9. Dan Balaban: London Oyster Card Chief: NFC Not Ready for Fast-Paced Fare Payment, NFC Times, May 30, 2012, http://nfctimes.com/news/london-oyster-card-chief-nfc-not-ready-fast-paced-fare-payment.

