International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 4, Issue 6, November - December 2015 ISSN 2278-6856

Security Analysis of NFC Technology Compared with other Mobile Wireless Technologies

Ahmed H. Ali[1], RehamAbdellatifAbouhogail[2], Ibrahim F. Tarrad[3] , Mohamed I. Youssef[4]

[1,2] Electrical Quantities Metrology Dept., National Institute for Standards, Egypt

[3,4] Electrical Engineering Department Al-Azhar University, Egypt

ABSTRACT

There are a many popular ways for mobile devices to connect wirelessly. This connectiongives users the ability to transfer data between two or more devices in additionto control a device remotely. Therefore, the security of such functions is insufficient for widespread use of these wireless technologies. However, in the near future,Near Field Communication (NFC) technology willbecome widespread for users, so its security weakness which can be dangerous to the privacy of the user's confidential information should be evaluated and handled accurately. The security issues of NFC are anactive area of research for the coming years. This paper gives a detailed comprehensive analysis of security with respect to NFC, Bluetooth and infrared.Finally, the paper puts the most important recommendations for future security improvement that can bedeveloped in NFC and other wireless technologies.

1. Introduction

Wireless communication is the transfer of information over a distance without the use ofconductors or cables. The distances of data transfer may be short in range of centimeters as in NFC applications or long in range of thousands or millions of kilometers as radio communications[1]. Also mobile wireless communications offer organizations and users many benefits such as portability and flexibility, increased productivity, and lower installation costs. Wireless technologies cover a broad range of differing capabilities oriented toward different uses and needs [2].

In just 25 years wireless technologies have changed the face of communications and have also changed the concept of network topology which has been applicable due to the relentless progress in silicon technology with higher integration, lower costs, more capabilities and technical advances in air interfaces i.e. higher efficiency for voice and data services, lower infrastructure capital costs [3].

The communications infrastructure necessary for the wireless environment is quite complex. Wireless devices are likely to remain at a disadvantage over their wired counterparts in terms of bandwidth. Limited bandwidth is a significant problem that requires organizations to rethink how users interact through a wireless device with an information system. An important issue is how to create efficient applications that can realistically work with current technology [4].

There are already a variety of mobile wireless technologies which can be used for mobile secured applications such as NFC, Bluetooth and others technologies. These wireless technologies are used in order to cover the needs of data wireless transfer from business and personal perspectives. In order to make these wireless applications that use those technologies work in a suitable way , the technology has to play a very important role where not only the used wireless communication, but other technologies has also to be used to make efficient and effective working of mobile applications [5].

The evolution of mobile phones that can be used anywhere as well as, the growing trend of their features and performances have triggered new serious security issues [6]. The security of wireless information is a very important technical issue in mobile systems. Users and organizations will want assurance that their mobile wireless communications and applications are not intercepted [4]. Users that set up mobile wireless connections must realize that there are no physical boundaries limiting their connections, and that people and devices outside the organization may have illegal access to their systems. Encryption technologies can also help, but will need to be made more efficient and more foolproof. The increased use of wireless devices for e-commerce and other sensitive applications make the issue of positive identity verification even more important yet more difficult to ensure[4].

As a result, security and privacy are very important elements for the success of mobile system and its applications specifically in payment area. As with any wireless technology, Mobile wireless technologies have several inherent security risks because access to any device is potentially open to anyone in the range of the device. Thus security is a huge concern for wireless applications [7].

However, mobile wireless technologies are inherent. Some of these risks are as those of wired risks; and some of them are produced by wireless connectivity; some are new. May be the most significant source of risks in wireless connections is that the technology's underlying communications environments[2]. The loss of confidentiality and integrity and the threat of service attacks are risks typically associated with wireless communications. Unauthorized subscribers may gain access to systems and information, corrupt the data, consume connection bandwidth, degrade connection performance, and launch attacks that prevent authorized users from accessing the information, or use agency resources to launch attacks on other connections channels[2].

The remaining part of this paper is organized as follows: in the next section, we make a briefoverview of mobile wireless technologies (NFC, Bluetooth and infrared). In section 3, we will focus on security analysis for NFC wireless technology .Then In section 4 we explains securityconcerns for Bluetooth and main recommendations to avoidattacks and threats and in Section 5 a brief definition for infrared security was presented and finally in section 6we present our concluding remarks.

2. Overview of Mobile Wireless Technologies

In recent years, mobile wireless technology has given rise to a large number of available mobile tools and their applications are becoming more and more advancedsystems [8]. Therefore, many mobile applications use its wireless technology to communicate with otherdevices. Many mobile applications have equipped with wireless technology such as NFC, Bluetooth and others etc. This leads to a great possibility that the cellphone can control the user automatic needs[8].

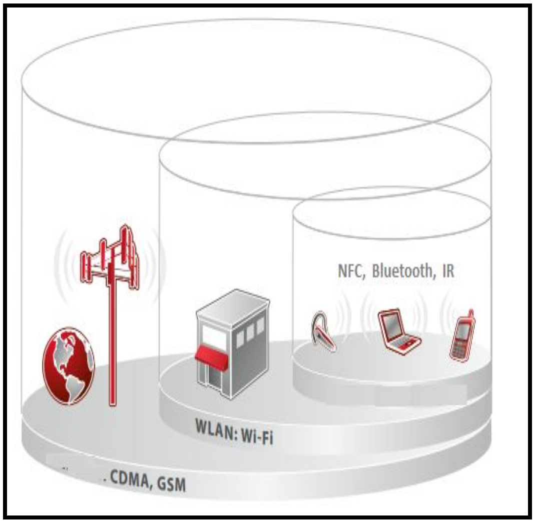

Figure 1: Mobile Wireless technologies.

3. Overview of Mobile Wireless Technologies Security Requirements

In the time being, wireless technologies suffer from many disadvantages, including security weaknesses and lack of locations management. Advancedresearch is also necessary to determine and evaluate the scalability of wireless technologies in terms of users, distance, and transactions. Before those technologies become widely used, many restrictions must be overcome. The future of wireless technologies is depending on how the technology and business issues are evaluated. Also one major issue would be the cost of services [9].

The security issues in mobile wireless system are onfidentiality, authentication, integrity, authorization, andnon-repudiation, below is the definition of each one [9].

a. **Confidentiality**: In mobile system no-one-else should find out what was a legal userdo during connectionand howitwas happened.
b. **Authentication**: each corresponding mobile user must be able to trust the identity claimed.
c. **Integrity**: the transmitteddata should not bemodified by others, knowingly orunknowingly.
d. **Authorization**: parties involved must be able to verify if everyone involved in a transmission process isallowed to make actions.
e. **Non-repudiation**: No one should be able to claim that the confidential data on his/herbehalf was made without their knowledge.

In the following sections, a detailed discussion for NFC and Bluetooth technologies are explained.Also,a brief introduction for Infrared technology is presented.

4. NFCOverview and Security Analysis

4.1 NFC overview

NFC stands for Near Field Communication. The specification details of NFC can be found in ISO 18092 [7]. The main characteristic of NFC is that it is a wireless communication technology with a working distance limited to about 10 cm. Short distance is one of specific characteristic of NFC if compared by all other technologies, among the latest technology NFC is the only technology which is developing at a faster rate and accepted worldwide [10]. Cellphones use NFC technology to pair with Bluetooth headsets, media players and speakers. The pairing of such devices with NFC is done with one tap with its NFC-enabled devices [10].

Also, NFC technology is an extension of several Radio Frequency Identification (RFID) proximity communication standards. It is basically a mixed between RFID standards and additional features are described in two new standards. The two main new features which added in the standards are peer-to-peer (P2P) connections between two active NFC mobiles and the emulation of a passive proximity RFID tag[11]. The NFC technology mainly focuses on contact-less smartcards that operate at a frequency of 13.56 MHzwith the introduction of several pervasive devices [11].

NFC can operate in many modes. The modes are determined whether a mobile phone creates its own Radio Signal (RF) field or whether a device retrieves the power from the RF field generated by another mobile phone[7]. In case of themobile device generates its own field it is called an active device, otherwise it is called a passive one. Active devices usually have a power supply; passive devices usually don't. When two devices communicate there are three different configurations are possible. Applicable configurations are listed intable 1. These configurations are important because the way data is transmitted depends on whether the transmitting device is in active or in passive mode[12].

Table 1: NFC Applicable Configuration

Device A	***Device B***	***Description***
Active	Active	When a device sends data it generates an RF field. When waiting for data a device does not generate an RF field. Thus, the RF field is alternately generated by Device A and Device B
Active	Passive	The RF field is generated by Device A only
Passive	Active	The RF field is generated by Device B only

In additional to the active and passive mode, there are two different roles for each deviceto play in NFC communication. NFC is based on a message and reply concept. This means one device (assumed its name is A) sends a message to another device (named B) and device B sends back a reply. It is not possible for device B to send data to device A without first receiving some message from device A, to which it could reply. The role of the device A which starts the data exchange is called initiator, the role of the other device is called target. The following table lists all possible combinations of this role with respect to the active or passive mode. Only the combination Initiator and Passive is not possible[12].

Table 2: Possible Combination of NFC Roles

	Initiator	**Target**
Active	Possible	Possible
Passive	Not Possible	Possible

Furthermore, it should be mentioned that NFC communication is not limited to a pair of two devices. In fact, one initiator device can talk to multiple target devices. In this case, all target devices are enabled at the same time. But before sending a message, the initiator device must select a receiving device. The message must then be ignored by all non-selected target devices. Only the selected target device is allowed to answer to the re-ceived data. Therefore, it is not possible to send data to more than one device at the same time [12].

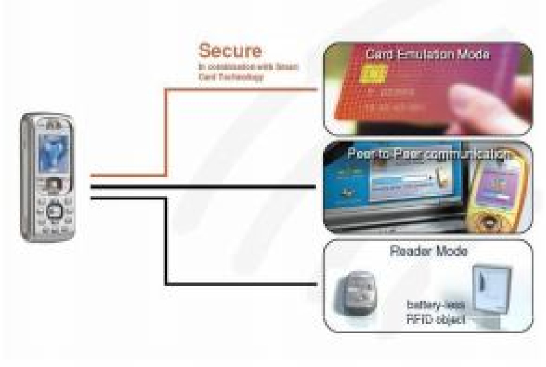
Secure
In combination with Smart Card Technology
Card Emulation Mode
Peer-to-Peer communication
Reader Mode
battery-less RFID object

Figure 2: NFC modes

4.2 NFC Security Attacks and Recommendations

Due to contactless reading and identification of transponders of NFC without a line of sight, privacy as other security concerns go hand in hand with NFC technology. As the standardization of integrating NFC into mobile devices is still ongoing, there is a chance that security and privacy issues are well considered. Hence, we analyze devices and technology as far as possible toprovide a comprehensive discussionabout the main issues related toNFC [13].

By using a shorter communication range and special communication protocols, NFC should be able to overcome security problems, different types of attacks can be executed on the way NFC compliant devices connections as listed below[14]:

1-Eavesdropping: Eavesdropping is the most occurred attack on wireless communications. using an antenna and analysis tool an attacker can listen to any confidential information being sent between mobile devices[14] . Due to the close distance in additional to low power RF field of communicating for NFC devices, it can be stated that NFC communications are hardlyvulnerable to eavesdroppingif compared with other mobile technologies.

2- Data Modification:an attacker needs more advanced and harmful attacks. Attackermay betry to modify the transferring data. NFC is protectedagainst attacker's data modification by manyscenarios. By using 106k Baud in active mode it gets impossible for an attacker to modify all the data transmitted via the RF link. Also, NFC devices can check the RF field while transmitting data and when an attack is detected,the device will stop sending more data.

As shown in figure 3, attacker (Eve) will listen to the communication channel between devices (Alice and Bob) and try to modify the data which is transmitted via the NFC channels. In the simplest case, the attacker needs to disturb the communication such that the target device is not able to get the data sent by the initiator device.[15].

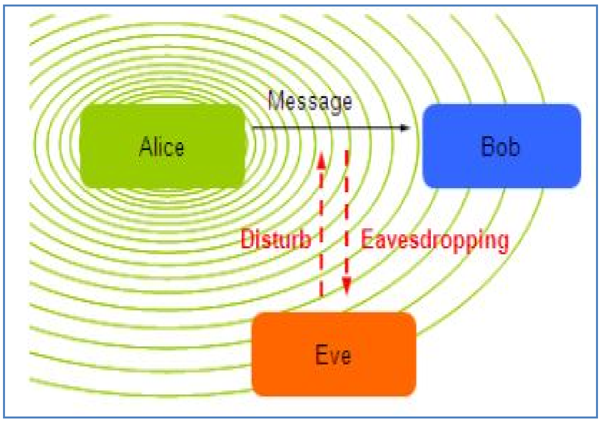

Figure 3: Eavesdropping and Data Modification Threats

3-Data Corruption:Instead of just listening an attacker can also try to modify the data which is transmitted via the NFC connection channel for example attackerneeds to disturb the communication such that the receiver is not able to understand the data sent by the other device.

Avoiding Data corruption can be achieved by transmitting valid frequencies of the data spectrum at a correct time. [12].

4-Data Insertion: This means that the attacker inserts messages into the data exchange between two devices. But this is only possible, in case the answering device needs a very long time to reply. In this case, the attacker can send his data before the initiator to the target device. The insertion will be applied to the channel, only, if the inserted data can be transmitted, before the original device begins the answer. [12].

From the previous discussion, we can conclude that there are three possible countermeasures. One is that the answering device answers with no delay. In this case, the attacker cannot be faster than the correct device. The attacker can be as fast as the correct device, but if two devices answer at the same time no correct data is received. The second possible countermeasure is listening by the answering device to the channel during the time, it is open and the staring point of the transmission. The device could then detect an attacker, who wants to insert data. The third option again is a secure channel between the two devices.

5-Man-in-the-middle: In MITM attacks, two parties are tricked into thinking they are communicating securely with each other, while the attacker actually sits in between them, communicating with both. The attacker gets messages from one device and then sets up a new communication channel with the second device. Then, he catches the reply of the second device and sends his own response to the first device. [14].As already it is practically impossible to do a Man-in-the-Middle-Attack on an NFC link. The recommendation is to use active-passive communication mode which the RF field is always generated by one of the valid parties. So, if the active party listen to the RF field while sending data will be able to detect any disturbances caused by a potential attackerwhich will be considered a good solution.

Also, establishing a secure channel between two NFC devices is clearly the best approach to protect againsteavesdropping, data modification attack, and enhance the inherent protection of NFC against Man-in-the-Middle-Attacks. A standard key agreement protocol based on RSA or Elliptic Curves could be applied to establish a shared secret between two devices. The shared secret can then be used to derive a symmetric key like Data Encryption Standard (3DES) or Advanced Encryption Standard (AES), which is then used for the secure channel providing confidentiality, integrity, and authenticity of the transmitted data. Various modes of operation for 3DES and AES could be used for such a secure channel [15].

Compared with the common mobile phone, the most important component in NFC phone is the Secure Element(SE), which is an integrated circuit can provide some secure functions such as encryption, digital signature and secure storage, and so on. SE is connected with the NFC Controller for proximity transactions, and the host controller is able to exchange data with the SE[16]. The physical link between SE and the NFC controller has not yet been defined. All privacy data and valuable data are stored on SE[16].

To eliminate or alleviate the security threats of NFC based phone NFC systems, the mitigation plan can be made from two aspects: technique and usage. Technical solutions are based on some security mechanisms used in all the different components of the NFC system. While the usages emphasize the matters and security rules to which users should pay more attention in the data transmission. The following subsection gives the threats mitigation plan from two aspects,technical and usage recommendationswhich described as below.

1-Technical Security Recommendations Prospective

The technical solution of NFC threats mitigations depends on the components that will be mentionedbelow:

A-Secure mechanisms for Secure Element (SE)

- Access control mechanism for SE, such as to restrict the numbers of PIN or password trials, and set a life-cycle and a fixed number of operations that can be performed for each user authentication.
- The mechanism of cryptographic keys recovery, but it should not be able to recover data which the user has invalidated.
- Confidential data should be stored encrypted.
- The data transmission records should have time stamp to prevent the replay or substitution attack.
- Detect the integrity of NFC hardware, especially the main modules of NFC, and support the bilateral authentication between SE and baseband chip.
- Forbid loading or even downloading the software without signatures using NFC applications.

B- Security mechanism for baseband chip

Detect the integrity and authenticity of applications running in NFC phone:

- Prevent the hijacking of PIN.
- Set a specific secure domain for each application, and restrict accessing other application’s private data.
- The sensitive data that handled by the application should avoid being extracted the secret information on this data, even if the memory is dumped.
- Bilateral authentication with SE.

C- Secure mechanisms for NFC chip:To avoid being read arbitrarily the ID or tag in NFC chip by other NFC device, NFC chip should support the function of turning on and off the NFC module.

2-Usages Security Recommendations Prospective

The usage solutions of NFC threats mitigations dependon the components that will be mentioned below:

A-Security Awareness to users

Some security awareness should be trained to users who use the NFC phone in offline payment. It includes that the user should know how to correctly use their NFC phone, how to spot potential attacks and deal with the threats latent in NFC phone, how to prevent their phone from being stolen, lost or damaged, and how to keep their PIN or password secret, and set a secure password for your phone.

B- Secure guard of operating system and applications

- The right using of phone operating system and applications to avoid download malicious software;
- Installing updated anti-virus and firewall software programs.

4.3 NFC CryptographyTools and Security Protocols

The NFC-SEC is a series of NFC security standards that specify cryptographic mechanisms using the Elliptic Curve Diffie-Hellman (ECDH) protocol for key agreement and the AES algorithm forsecurity and data encryption and integrity. NFC standardused to establish a secure communication channel between two NFCdevices that do not share any common secret prior to their communication over a non-secure and public medium. Table 3 presents a summary of the security topics provided by these standards [17].

Table 3: Summary of Provided Security topics

Protocol	**Protocol Topics**
NFC-SEC	Eavesdropping, Data Modification
NFC-SEC-01	Shared Secret Service (SSE) - Elliptic Curve Diffie-Hellman (ECDH) KeyExchange (192 bit) - Key derivation and confirmation (AES 128 bit)Secure Channel Service (SCH) - - Data encryption (AES 128 bit) - -Data integrity (AES 128 bit)

4.3.1 Overview of NFC Elliptic Curve Diffie-Hellman scheme

Elliptic Curve Diffie-Hellman scheme (ECDH) is the most used security protocol when two different devices is communicating using the NFC standard [18]. ECDH is one of the key agreement schemes protocols which its main objective is to establish a secure wireless connection over an insecure channel as shown in Figure 4. ECDH is designed to provide many security goals which depends on the NFC applicationfunctions include key authentication, key authentication and known-key security [18].

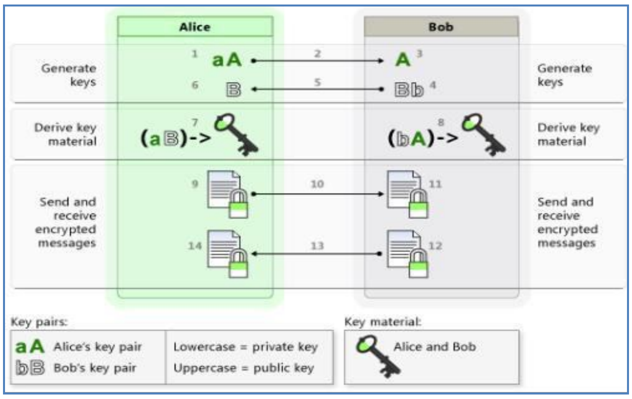

Figure 4: How ECDH works

ECDH keyagreement protocol used to enable two users to create a sharedsecret agreement. The ECDH protocol depends on twopublic parameters: p and g. Parameter p is a large primenumber, and parameter g is an integer which is less than p.These two parameters are exchanged over a non-secureline. After both Alice and Bob receive the two publicparameters, they select private integers. Alice chooses parameter a,and Bob chooses b. These values are referred to asprivate keys. Alice and Bob then create public keys byusing the public parameters and their private keys. Aliceuses (g^a) mod p, and Bob uses (g^b) mod p. Theseare asymmetric keys because they do not match. Aliceand Bob exchange these public keys and use them tocompute their shared secret agreement. ECDHmathematics guarantees that both Alice and Bob willcompute the same shared secret agreement, althoughthey do not know each other's private keys. ECDH is described in Figure 5[19]:

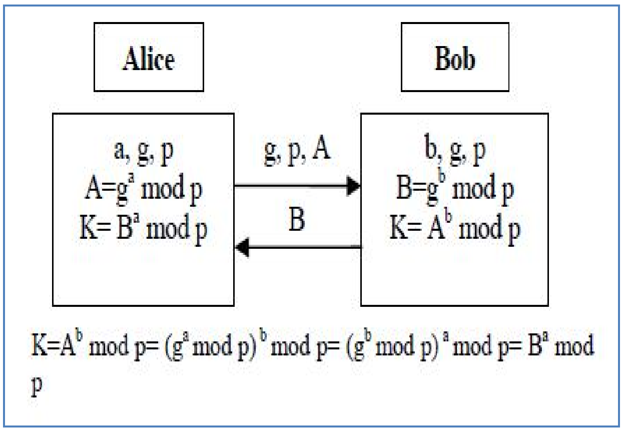

Figure 5: ECDH Protocol

5. Bluetooth Security Analysis

5.1 Bluetooth overview

Bluetooth SIG (Bluetooth Special Interest Group) was established in 1998. It developsBluetooth technology and brings new Bluetooth enabled devices to the market. Bluetooth version 1.0 was found in 1999.[17].Bluetooth is a wireless technology for short distance wireless data transmission and two-way voice transfer with data rates up to 3 Mb/s. Bluetooth also operates at 2.4 GHz frequency Bluetooth used to connect any kind of Bluetooth enabled device to another one. The range of Bluetooth communication distance is from 10 to 100 meters indoors [20].

Using Bluetooth a securedcommunication channel between two devices called 'pairing' are established by exchanging shared secret codes referred to as PIN. An initiator device called 'master' device has the option of pairing with up to seven target devices called 'slaves' devices establishing a network called a piconet[21].User can transmit any type of files e.g. photos from the mobile phone devices with a camera to his computer which can resend it to configured printer using Bluetooth technology. All of that can be done without cables as illustrated in Figure 4.

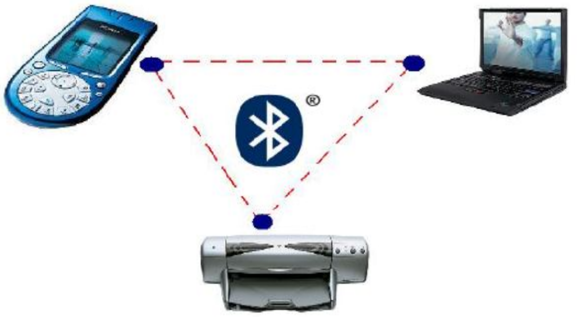

Figure 4: Bluetooth usage scenarios

Bluetooth wireless technology embedded with many mobile phones,computers, cameras, laptops was accepted as a replacement of cables to enableinformation sharing/exchanging among devices. Also it can be used for web connectivity, online gaming and many more.However, any time a user is transmitting or receivingdata, he can befaced spammers, hackers and attackers[8].

5.2 Bluetooth Security Analysis

Security topic has a major role in the uses of Bluetooth technology. The Bluetooth SIG has delivered much effort in order to let Bluetooth a secured technology. Many security measures have been developed at different protocol levels, the basic Bluetooth security setting depends on the user's Bluetooth device, who take a decision about the discoverability and connection options. Generally, Bluetooth discoverability and connection options are classifiedas three operation modes which are as follows[21]:

• **BluetoothPrivate Mode**: The device is hidden and cannot be detected. A connection will be established only if the Bluetooth device address (BD_ADDR) of the device is known to the prospective master device.

• **Bluetooth Silent Mode**: The device will never connect to other device. It just monitors the Bluetooth traffic.

• **Bluetooth Public Modes**: The device can be discovered and connected to any other devicein this case; it is called adiscoverable device.

In addition to above mentioned operations modes, there are also different Bluetooth security modes that a device canimplement. These security modes are listed below[18].

• **BluetoothNon-secure:** The Bluetooth device isn't initiating any security measures**.**

• **Bluetooth Service-level enforced security mode:** Bluetooth devices can establish a non-secureAsynchronous Connection-Less (ACL). Security procedures are initiated after a Logical Link Control and Adaptation Protocol (L2CAP) connection oriented orL2CAP connection-less channel request is made.

•**BluetoothLink-level enforced security mode:** Security mechanism are initiated when an ACLlink is established and before any channel request called.

• Bluetooth **Service-level enforced security mode (SSP):** This mode is similar to mode Service-level enforced security mode, but Bluetooth devices using secure simple pairing (SSP).

Bluetooth technology security includes three major areas which areauthentication, authorization and encryption. Authentication always used for confirming the validity of the identity of one piconetmember to another. After authentication success and depends on the valid identity of the user a determinationof the client's authorization levelevaluated. The Encryption is used for encoding the data being sent between Bluetooth devices in the method that eavesdroppers cannotget its contents[20].

Bluetooth devices always begin their connection with the same PIN number that is used for generating several 128-bit. Each two paired devices can have a different PIN code for providing trusted connection channel [20].

Bluetooth wireless technology has many vulnerabilities issues due to the following reasons [22]:

- Encryption is an optional action
- Users sometimes use weak PINs whichcan be guessed by attackers.
- Bluetooth uses unit keys are insecure
- Weak protection of integrity
- Different quality of random number generator.

Now by seeing these vulnerabilities how many of you start thinking that why we have chosen the same PIN for connecting to each and every other device. The following additional aspects should also be considered [22]:

- Mobile devices are exposed to a higher risk of theft than stationary devices.
- All that is needed to use a Bluetooth device is for the device to authenticate itself; normally the user does not have to authenticate himself to the device. When a mobile , paired devices go missing, unauthorized third parties will thus normally be able to use them immediately.
- Bluetooth device addresses can be manipulated with suitable equipment (flash memory).
- Again, in ad hoc networks there exists a danger that computer viruses and Trojan horses could spread.

Also, Bluetooth secured channel depends on users, below are recommendations for Bluetooth application users [22]:

1. Did not accept all unknown pairing requests.
2. Disable Bluetooth when not needed.
3. When using pairing key, user have to use complex and none guessable PIN keys.
4. Keep your device updated by firmware and latest update of Bluetooth software's.
5. User's device should have an updated version of good antivirus.
6. Away device should be in hidden mode (none discoverable).
7. Comply with all applicable directives, policies, regulations, and guidance.
8. User has to use encryption before connecting Bluetooth devices.
9. Keep devices as close together as possible when Bluetooth links are active.

10. Maintain physical control of devices at all times. Remove lost or stolen devices from paired device lists.

6. Infrared Wireless Technology

6.1 Infrared Overview

The Infrared Data Association (IrDA) is a nonprofit organization. Its goal is to develop specifications for infrared wireless communication. The IrDA version 1.0 specification was released in 1994. It was implemented for cheap and reliable short range wireless connections providing data rates up to 115.2 kb/s[20]. Infrared Mobile Communications (IrMC) is a standard for interoperability between mobile communication devices, was also released in 1997. Advanced Infrared Medium Access Control (AIrMAC) standard was released in 1999 for providing Advanced Infrared Wireless systems[20].

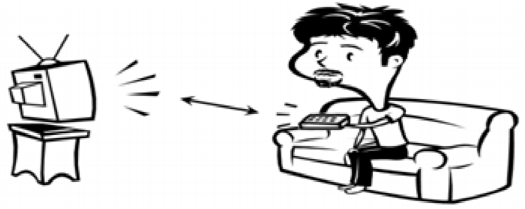

Figure 5: IrDA line of sight connections

The technology of IrDA wireless local area network is one branch of the IEEE802.II protocol's access network technology. As a medium for short-range or indoor communication, infrared radiation offers several significant advantages over radio. Infrared emitters and detector capable of high-speed operation are available at low cost. The Infrared spectral region offers a virtually unlimited bandwidth that is unregulated worldwide [5].

Today, the IrDA is the widely spread wireless transmission standard. IrDA is a half-duplex wireless technology. IrDA Data is suitable for high speed short range, line of sight and point-to-point cordless data [5].

6.2 infrared security analysis

IrDA does not provide any link-level security[20], which means that no authentication norauthorization is used by IrDA, also alldata is sent unencrypted. This means that authentication, authorization and encryption should be implemented by user at software application level [19].

By the way,IrDA supports only Point-to-Point connections, and works only in case of line-of-sight between two IrDA devices. Also, IrDA communicationrange is only up to 2 meters [20].In spite of IrDA's limited communication range, it is doable to eavesdrop on a IrDA connection by detecting reflected infrared-light and filtering out the surrounding ambient noise[20].

7 Conclusion

This paper presenteda detailed analysis formobile NFC wireless technology security compared by Bluetooth and infrared ones. A list of security issues for eachtechnologywas listed in additional to research recommendations for each one. Regarding NFC and IrDA by itself cannot provide protection against eavesdropping or data modifications. The proper way for handling this issue is to develop asoftware solution to achieve the user required security level.

Also, NFC technology can operates in three modes with different security levels, the top security level of NFC application can be achieved by using secure connections over NFC using secure element SE. But for Bluetooth, there are an authentication and authorization mechanisms for devices paring.

However, forNFC technology it is hardly to be eavesdropped due to its short range connection supports and low RF power used but it can be happen for Bluetooth due to its long range and high power of its radio frequency.For Bluetooth, user has to follow the same action to avoid attackers. As updating mobile operating system and Bluetooth software versions in additional to installing antivirus and do not enabling Bluetooth when it's not needed.Table 4 containsthe main results of the security analysis for NFC andBluetooth.

Table4: Summary of the Security Analysis Comparison between NFC and Bluetooth

	NFC	Bluetooth
Eavesdropping	Hardly to be eavesdropped due to short distance between two devices and low power of RF signal and for	Easy to be eavesdropped Due to long distance between the two devices and high power of RF signal, needs special handling
MAN-in-the-middle	Hardly to be done in case of using Active-passive Additional action needs to be done as mention in section 4.1.b	Easy to be done because the two devices are in active modes and sending data, needs special handling
Data Modifications	Hardly to be done in case of using 106K bit rate	Easy to be done due to long distance between devices , needs special handling
Secure Element	Supported and recommended to be used for secure communications	Not supported

References

[1] MuditRatanaBhalla, AnandVardhanBhalla "Generations of Mobile Wireless Technology:A Survey", International Journal of Computer Applications Volume 5– No.4, August 2010.

[2] Tom Karygiannis, Les Owens "Wireless Network Security", Special Publication , Computer Security Division Information Technology Laboratory,National Institute of Standards and Technology, November 2002.

[3] Nandini Deb, TusharSaxena , HimanshuGoyal "A Comparative Study of Security Attacks in Bluetooth, Wi-fi and Wimax", Amity University, Amity Institute of Telecom Engineering & Management, 2010.

[4] Peter Tarasewich, Robert C. Nickerson, Merrill Warkentin "Wireless/Mobile e-commerce:

Technologies, Applications, and Issues", Seventh Americas Conference on Information Systems, 2001.

[5] Ahmed H. Ali, RehamAbdellatifAbouhogail, Ibrahim F. Tarrad , Mohamed I. Youssef" Assessment and Comparison of Commonly used Wireless Technologies from Mobile payment Systems Perspective", International Journal of Software Engineering and Its Applications Vol.8, 2014.

[6] Najimammari, Mohamed ghallali, Anasabou el kalam, Norelislam el hami, Abdellahaitouahman, Bouabid el ouahidi" Mobile Security: Security Mechanisms and Protection of Mobile Applications", Journal of Theoretical and Applied Information Technology Vol.70 No.2, 2014.

[7] KiyanaZolfaghar, ShahriarMohammadi" Securing Bluetooth-based Payment System using Honeypot", Innovations in Information Technology, International Conference, 2009.

[8] SaliyahKahar, RizaSulaiman,AntonSatriaPrabuwono, NahdatulAkma Ahmad and Mohammad Ashri Abu Hassan. "A Review of Wireless Technology Usage for Mobile Robot Controller", International Conference on System Engineering and Modeling ,Singapore, 2012.

[9] Upkarvarshney, "Mobile and Wireless Information Systems: Applications, Networks, and Research Problems", Communications of the Association for Information Systems, 2003.

[10] Ajay Mohandas, Khoshrav Doctor, ShubhamJayawant, MohitPattni, and Asst Prof. Era Johri "NFC vs Bluetooth", International Journal of Multidisciplinary and Scientific Emerging Research , 2014.

[11] RoelVerdult, Franc¸oisKooman "Practical attacks on NFC enabled cell phones", Third International Workshop on Near Field Communication , 2011.

[12] Ernst Haselsteiner and KlemensBreitfu" Security in Near Field Communication (NFC)", Philips Semiconductors, Printed handout of Workshop on RFID Security RFIDSec 06, July 2006.

[13] Gerald Madlmayr, Josef Langer," NFC Devices: Security and Privacy", The Third International Conference on Availability, Reliability and Security, 2008.

[14] Gauthier Van Damme and KarelWouters, "Practical Experiences with NFC Security on Mobile Phones", Belgium, 2008 .

[15] Mohamed Mostafa Abd Allah "Strengths and Weaknesses of Near FieldCommunication (NFC)Technology", Global Journal of Computer Science and Technology Volume 11 Issue Version 1.0 March 2011.

[16] Fan Jia, Yong Liu, Li Zhang "Threat Modeling for offline NFC Payments", Journal of Convergence Information Technology(JCIT) Volume8, Number4,Feb 2013.

[17] Wang Rui , Wong Cheng Teck and Wang Jue "Near Field Communication (NFC) Security", The Projects for CS2107 (Introduction to Information and System Security), Singapore, July 2013.

[18] Chan Yik Cheung "Cryptography and Protocols used in NFC", The Projects for CS2107 (Introduction to Information and System Security), Singapore, July 2013.

[19] Md. ArifulAlam and Mohammad Ibrahim Khan "Security Enhancement of Pairing and Authentication Process of Bluetooth" IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.6, June 2010.

[20] Keijo M.J. Haataja "Security in Bluetooth, WLAN and IrDA:a comparison", Report A/2006/1 university of kuopioDepartment of Computer Science, 2006.

[21] Nateq Be-NazirIbnMinar and Mohammed Tarique "bluetooth security threats and solutions: a survey", International Journal of Distributed and Parallel Systems (IJDPS) Vol.3, No.1, January 2012.

[22] Ajay Sharma "Bluetooth Security Issues, Threats And Consequences", Proceedings of 2nd National Conference on Challenges & Opportunities in Information Technology (COIT-2008)RIMT-IET, MandiGobindgarh. March 29, 2008.