ABSTRACT

Near Field Communication is a short-range communication channel that is one of the most promising technologies around. One of the purposes for this technology is to simplify first-time connections to other wireless technologies, like Wi-Fi and Bluetooth. In this thesis we will incorporate Near Field Communication in an 802.11 network for a hotel. We will show how this technology will be used in a scenario like this, where guests will get easily access to the hotels wireless network through their personal devices. NFC will be used for initiation, authentication and exchange of configuration settings. With this new technology incorporated, a threat analysis and risk assessment will be performed. This is to acknowledge what needs to be protected in terms of assets and points of attacks. We will set some requirements for the system to make it even more secure and propose some solutions for implementation to improve protection of our assets.

PREFACE

This thesis fulfills the requirements for the master's degree in Information and Communication Technology (ICT) at the University of Agder (UoA), Faculty of Engineering and Science in Grimstad, Norway. The thesis project has a workload of 30 ECTS, and concludes a two-year 120 ECTS master's programme.

First of all we would like to thank our internal supervisor professor Frank Reichert for excellent supervision and guidance throughout the project period. We also appreciate the help from PhD Geir Køien and professor Vladimir Oleshchuk, with relevant questions along the way.

Grimstad, September 2008

_____	_____
Rune Magnussen	Sølve Oppheim

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

AP	Access Point
Bluetooth	Industrial specification for wireless personal area network
BSS	Basic Service Set
Credentials	A data structure issued by a registrar to en enrollee, allow the latter to gain access to the network
DHCP	Dynamic Host Configuration Protocol – is a protocol used by networked devices (clients) to obtain the necessary parameters for operation in an Internet Protocol network.
DDoS	Distributed Denial of Service
DoS	Denial of Service
EAP	Extensible Authentication Protocol
EAPOL	Extensible Authentication Protocol over LAN
EAPOW	Extensible Authentication Protocol over Wireless
ECMA	Industry association dedicated to the standardization of Information and Communication Technology and Consumer Electronic
ECMA340	Near Field Communication Interface and Protocol - 1 (NFCIP-1) by ECMA
ECMA352	Near Field Communication Interface and Protocol - 2 (NFCIP-2) by ECMA
Enrollee	A device seeking to join a WLAN domain
ESSID	Extended Service Set ID
ETSI	European Telecommunication Standards Institute
ETSI TS 102 190	Near Field Communication Interface and Protocol -1 (NFCIP-1) by ETSI
ETSI TS 102 312	Near Field Communication Interface and Protocol -2 (NFCIP-2) by ETSI
IEEE	Institute of Electrical and Electronics Engineers
ISM	Industrial, Scientific and Medical radio bands
ISO	International Standards Organization
ISO14443	Standard for proximity card, also described as smart card
ISO18092	Near Field Communication Interface and Protocol -1 (NFCIP-1) by ISO
ISO21481	Near Field Communication Interface and Protocol -2 (NFCIP-2) by ISO
LAN	Local Area Network
MAC	Media Access Control, Message Authentication Code, a MAC address refers to a physical address on a interface
MIC	Message Integrity Code
MitM	Man-in-the-Middle
NAT	Network Address Translation - is the process of modifying network address information in datagram packet headers, to remap a given address space into another address space.
NFC	Near Field Communication
NFCIP-1	Specification of the interface and protocol to NFC
NFCIP-2	Specification of the mechanism to detect and select communication mode in NFC
Personal device	A device a person usually bring along everywhere, e.g. a mobile phone
PDA	Personal Digital Assistant (a handheld computer)
Phillips MIFARE	Contactless integrated circuit technology developed by NXP\Phillips
Proximity card	A generic name for contactless integrated circuit devices
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
Registrar	An entity with the authority to issue and revoke Domain
RF	Radio Frequency
RFID	Radio Frequency Identification Device
SDD	Single Device Detection
Sony Felicia	Contactless integrated circuit technology developed by Sony

SSID	Service Set Identifier
SYN	Synchronize sequence Number
Tag	A small unit with a small amount of memory available
TLS	Transport Layer Security
Transferjet	Industrial specification for wireless personal area network
USB	Universal Serial Bus
Vicinity device	A device close to another (e.g. two NFC devices)
WLAN	A Wi-Fi network (Wireless Local Area Network)
WPS	Wi-Fi Protected Setup
Wi-Fi Connection	Wireless network connection, e.g 802.11g, also described as WLAN
802.11(g)	Wireless network specification

THESIS DEFINITION

Security in NFC with Wi-Fi Protected Setup as use case

Near Field Communication (NFC) is a high frequency wireless communication technology used for short range communication. The underlying magnetic field induction technology restricts the range of the communication to a decimeter. NFC operates in the unlicensed and globally available ISM band of 13.56MHz. The data rates within the distances can be up to 424 Kbps depending on the coding schemes implemented and modulation techniques used. Similar technologies for short range communication include Bluetooth and TransferJet (Sony).

NFC, being a relatively new technology, has not identified and addressed all possible security issues. A challenge will be to identify and examine security risks for NFC, which we will address in our thesis. We will take an in-depth look at security through relevant protocols and technologies, and then present our findings regarding security risks in NFC.

A relevant use case is where wireless network settings and keys are exchanged securely for enabling users to connect to a secured Wi-Fi access point using Wi-Fi Protected Setup (WPS). In this use case we will use NFC to make a secure connection between a NFC enabled mobile host and an NFC enabled access point to exchange relevant keys and thus facilitate the establishment of a secure Wi-Fi connection.

The report will document our findings regarding security risks in NFC, and also show how the NFC device exchanges keys to achieve secure connection through an NFC access point by using WPS. As an optional feature if there is time, we will look at the Ericsson mobile platform to see how it functions in a security aspect when NFC is introduced.

(Arild Løvendahl, Kim-Tommy Humborstad, Jonny Ervik, Ram Kumar, Frank Reichert, Rune Magnussen, Sølve Oppheim)

1 INTRODUCTION

NFC (Near Field Communication) is a wireless short range communication technology, allowing us to transfer over a distance of up to 10 cm, but typically around 0-2 cm. The major advantage of NFC compared to other wireless technology is its simplicity. Simply by touching a reader, another NFC device or a NFC compliant tag, transactions are initialized automatically. With applications like using it as a contactless credit card or as a contactless bus ticket, or establishing Bluetooth or Wi-Fi connections by touching a tag, NFC technology gives additional functionality to a mobile device. Estimations show that by 2012 there are about 180 million mobile devices (equivalent to 20 % penetration) equipped with this technology [1].

Combining a new wireless communication technology with establishing connections to wireless networks or other applications in one mobile device may raise potential privacy issues and security risks. Attacks against an NFC device can be performed anywhere and may not be noticed by the victim as the communication itself is contactless. Additionally, the benefit achieved from taking over an NFC device can be high. Attackers can potentially abuse your digital rights in a wireless network. The integration of both technology and application needs to go hand in hand to protect the device and consumer, but also the ones who offer you the access rights to a wireless network. However, an introduction of NFC to establish connection to other wireless network could also be a benefit regarding security and privacy in proportion to other solutions.

The topic of our thesis is “Security in NFC with Wi-Fi Protected Setup as a use case”. This is a wide and broad area of research, because of all the applications and actions that NFC is intended for. Also, security and privacy issues in general for NFC and the RFID technology have been discussed before, even some specific attacks on this technology has been proved. Our contribution to this research will be that we will introduce this technology in a new environment where we show the benefits of this technology, but also analyze security risks and privacy issues. As there could be a lot of different scenarios when implementing NFC in corporation with other standards, we concretize our thesis to a specific scenario, where the NFC standard is implemented in corporation with the 802.11 standard. We have mentioned in the thesis description that we as an optional feature if there is time will look at EMP when NFC is introduced from a security stand point. This will not be considered due to the complexity, problem area and time restraints in working with this thesis.

We want to introduce NFC in a hotel scenario, where guests can get quick access to the hotel’s wireless network on their mobile devices. In this context we will use the connection of Wi-Fi Protected Setup for NFC. We will do a threat analysis of this environment, where we will highlight the security risks and privacy issues for implementing this solution for hotels.

1.1 PROBLEM STATEMENT

Many hotels around the world today offer Wi-Fi access to their guests, either if it is free, or they charge you for the access [59]. The hotels have usually their own machines were you get internet access or they have Wi-Fi spots or zones where it is possible to get access. Setting up a connection on your personal device can be difficult for many users, and is subject to a variety of security threats from wireless sniffing to bogus access points.

NFC will be incorporated into personal devices in the near future, to provide a secure side channel for initiation, authentication and transfer of configuration settings of wireless networks. Because of its close proximity and automatic transfer with an AP, it will make the process of setting up and transfer of the network settings easier and more secure.

However, a new wireless technology will have to be incorporated into the existing 802.11 network, and is not without its own security threats. The issue of granting only registered guest's access and keeping unauthorized devices out will need a strict evaluation of threats towards this technology in respect to the 802.1x network. The need to solve these issues is to do a thorough threat analysis and risk evaluation of the new part of the system, namely NFC.

The interest of this is to take the NFC technology into a new environment, but also show how NFC will work in the well established 802.11 networks. It will show the benefits of NFC compared to the known first-time WLAN connection, and which assets that can be exploited in NFC if certain mechanisms isn't in place. Also, well known threats to setting up wireless communication can be solved through NFC. It is of current interest because NFC is not far away from being a technology that will be used in our everyday mobility. Wi-Fi access in crowded environments, like airports, malls and of course hotels, increases. This is an evaluation of a future application, and security in every new wireless technology will always be up for debate. This is because there will always be new and smarter ways to attack both the technology and networks, and the stakes will rise as we move into a future with more and more wireless technology.

1.2 SCENARIO

Stage 1 Preliminary

A guest arrives at the hotel where he has booked a room for the night or several nights. With him he has his luggage and his wireless personal devices. This could be a mobile phone, PDA or a laptop all with integrated NFC and WLAN capabilities. He comes up to the reception and is greeted by the receptionist. He is asked to hand over his identification to prove his booking, and usually a scan of his credit card. The hotel can offer Wi-Fi access, and the receptionist asks if this is something that he wants, which he accepts. Another scenario can be that if he has

booked on the internet, he has already chosen this offer and the receptionist knows this at arrival. The hotel either charge or the access is free. In the hotel there are several access points, one by the reception and one on each floor by the elevators, assuming there are several floors. The receptionist that generates a PIN number assigned to his personal ID, and prints this out with some form of contract. The contract details general information, billing, length and conduct etc. to sign. This will be his password for authentication to the network. The guest can now choose when he wants the access and where and on which device.

Stage 2 Authentication and access

He decides now to get access to the network through his mobile phone. He puts his phone up to the AP's NFC reader in close proximity to activate the NFC device. In this case, the phone has already an application installed for Wi-Fi setup, like the WPS (Wi-Fi Protected Setup). The phone then asks him to push the PIN he received in the reception. He pushes the PIN which is sent for authentication to the RADIUS server in the system. The PIN is correct according to the PIN assigned to his personal ID and he is authenticated. He then receives the configuration settings to his phone and can now connect to the internet through the hotel's wireless network, where he have to follow the guidelines stated in his contract.

1.3 PROJECT LAYOUT

In this part we will describe how the paper is presented and divided.

Chapter 1 consists of an introduction to our thesis, and a problem statement that will cover our research area and what we want to accomplish and contribute with this paper. We present our scenario where we describe the environment the research topic will cover.

Chapter 2 contains a comprehensive overview of the technologies and concepts that is relevant to our further work.

Chapter 3 consists of the system architecture. Here we build our system with all necessary parts included. This system is the system that will be analyzed.

Chapter 4 consists of our threat analysis, where possible threats to the system are gathered and explained. In the risk assessment we will evaluate the threats to their risk level. The system requirements will cover the threats found to be of great risk.

Chapter 5 contains a proposed solution to many of the requirements set through the risk analysis and risk evaluation.

Chapter 6 consists of a conclusion to our research and a proposal for further work in our research area.

2 STATE OF THE ART

In this chapter we will discuss technologies, standards and projects which are related to particular problems in this thesis.

A big part of this chapter is discussions about RFID and Near Field Communication, but also about wireless networks in the 802.11 standard. We will also take a look at some security related concepts, for authentication, access control and accounting. This is important concepts when it comes to authorization of users towards a network. Further we will discuss other security related topics, like trust, confidentiality and integrity etc. At the end we will also describe relevant work and projects which are related to our thesis.

Knowledge of all these technologies and concepts described in this state of the art chapter are essential to solve the problems in this thesis.

2.1 RADIO FREQUENCY IDENTIFICATION - RFID

RFID is radio based communication, relying on storing and remotely retrieving data using devices called RFID tags or transponders. The frequency area varies from low (125/134,2MHz), high (13,56MHz) and ultra high frequency (868-956MHz), but there also exist RFID at the microwave level (2,45MHz) and in other frequency areas.

An RFID tag is an object that can be attached to a product, animal or a person for identification purposes. The purpose of an RFID system is to enable data to be transmitted by a mobile device (the tag). It is then read by an RFID reader and processed according to the needs of a particular application. RFID chips are usually attached to antennas, which together constitutes what we call a "tag."

RFID tags can be passive, semi-passive, or active. Passive RFID tags have no internal power supply. Semi-passive RFID tags are very similar to passive tags except for the addition of a small battery. Active RFID tags have their own internal power source which is used to power any ICs that generate the outgoing signal. The radio frequency field generated by the active RFID tag is used for powering the passive devices [2].

2.2 NEAR FIELD COMMUNICATION – NFC

NFC is a short range communication standard developed by NFC Forum [3], which is a nonprofit organization. This forum consists of cooperation between several participants and is working in four different groups where they specialize in hardware, applications, security and testing.

NFC is based on RFID (which is discussed in 2.2), and the underlying magnetic field induction technology restricts the range of the communication to typically 0-2 centimetres, and maximum up to ten centimetres. It is a successor to early stage of smartcard technology found in Sony FeliCa [4] and Phillips MIFARE [5]. NFC operates in the unlicensed and globally available ISM band of 13.56MHz.

RFID and NFC are basically using the same working standards, but as mentioned the NFC standard restrict the range with use of magnetic field induction. In addition to contact less smart cards (ISO14443 [6]), which only support communication between powered devices and passive tags, NFC also provides peer-to-peer communication. NFC combines the feature to read out and emulate RFID tags and to share data between electronic devices that both have active power.

The data rates within the distances can be up to 424 Kbps depending on the tag specification. It also depends on what kind of coding schemes implemented and modulation techniques used. Similar technologies for short range communication include Bluetooth and TransferJet [7]. We do not discuss these technologies in this thesis because they are not relevant to our security discussion, but instead refers to them for interested readers.

The purpose of NFC is to exchange information or establish a connection between two units (both between devices, like two mobile phones, or between a device and a tag, e.g. a mobile phone and a smart card), with a simple “touch”, where the devices are close enough to perform a communication session without any form of configuration. The information exchanged between devices and\or tags could be used for identification, authentication, and exchange of data or setup of other communication links.

In principle a NFC device contains an RFID reader\writer which is integrated into the user device with a host controller interface, developed for NFC support. The limitation of using areas of this standard lies in the application framework, since the standard is very “general”. It can be used in many different areas, like for example bootstrapping of other communication standards, exchange of small amount of information, door locks, payment machines, ticketing, cars, TV’s and so on.

2.2.1 STANDARDS

NFC is described in the protocols NFCIP-1 [8] and NFCIP-2 [9] (Near Field Communication Interface and Protocol 1 and 2).

NFCIP-1 is standardized in ISO18092 [8], ECMA 340[10] and ETSI TS 102 190[11]. It is composed of a physical layer and data link layer, as illustrated in figure 2 with blue color. This protocol specifies different functions for the RF device. It defines the active and passive communication modes. It specifies modulation schemes, coding, transfer

speed and frame format for the interface. The protocol also defines initializing schemes and conditions for collision control.

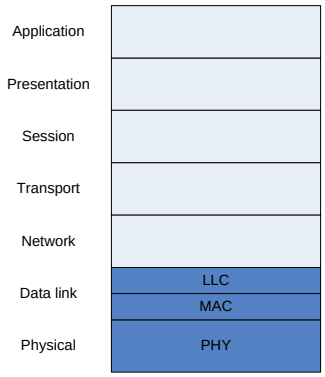


Figure 1 NFC in the OSI model

In NFCP-1 there is specified four different tag operation specifications[12], which provides the technical information needed to implement the reader/writer and associated control functionality of the NFC device to interact with other tags. All four tags are based on existing contact less products and are commercially available.

NFCIP-2 is defined in ISO21481 [13], ECMA 352[14] and ETSI TS 102 312[15]. This protocol defines how the external RF field is detected and what kind of mode it should use. The NFCIP-2 standard allows interoperation with NFC, Proximity Card [6] and Vicinity [16] devices and readers by defining a mechanism for selecting the three operation modes as part of establishing the connection.

2.2.2 SYSTEM ARCHITECTURE

Typical system architecture of a Near Field Communication system is illustrated in figure 2. A NFC communication is based on point to point, and therefore the two devices can communicate at the same time. The figure illustrates a NFC device 1, which want to initiate a connection with the NFC system, which contains a NFC reader\writer. This system is further connected to a host controller interface (HCI) which is an interface between the NFC system and an enterprise subsystem. This enterprise subsystem could for example be an access point, where NFC is used to pair two WLAN devices.

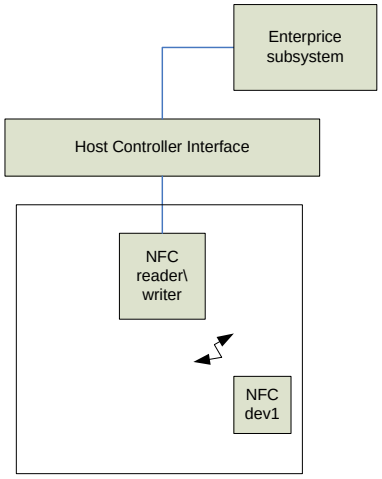


Figure 2 System architecture of a Near Field Communication system

2.3.2 COMMUNICATION MODES

The NFC interface can operate in two different communication modes; passive and active. In the active mode both devices are active and generate their own RF field. In passive mode the passive device must use inductive coupling to transmit data.

In passive mode, a passive device can be powered by the RF field of an active NFC device and transfer data using load modulation. The passive devices do not require an internal power recourse, which means that in scenarios where an NFC mobile phone is used for payment, the phone does not require battery to use the NFC device.

In active mode, both NFC devices are generating their own RF fields when they want to send data. Only one of the devices can generate an RF field and send data at a time, therefore no duplex functionality is implemented.

Generally, only two devices can communicate at the same time, but in passive communication mode the initiator (which is active) is able to communicate to several passive devices at the same time. This is realized by a time slot method, which is used to perform a Single Device Detection (SDD). The maximum number of time slots is limited to 16. A target responds in a random chosen time slot that can lead to collision with the response of another target. In order to reduce the collisions, a target may ignore a polling request set out by the initiator. If the initiator does not receive any response, it has to send the polling request again [8, 10, 11].

2.3.3 INITIATOR AND TARGET

NFC defines two different modes for a device in a given session. One of the communication participants are the initiator and the other is the target.

The initiator is the one who wants to communicate and initiates the communication. The target receives the initiator's communication request and sends back a reply. This concept prevents the target from sending any data without first receiving a request message from the initiator. Regarding the passive communication mode, the passive device acts always as the NFC target. In this case the active device is the initiator, which is responsible for generating the RF field. In the case of an active configuration in which the RF field is alternately generated, the roles of initiator and target are strictly assigned to the one who starts the communication. By default, all devices are NFC targets and only act as a NFC initiator device if it is required by the application [8, 10, 11].

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

Figure 3 Possible combinations of active\passive with initiators\targets

It is not possible to initiate communication between an initiator and a target where both devices are passive, like figure 3 shows. This is because none of the devices would be able to generate any RF field. Therefore none of them are able to either request or respond to any messages [8, 10, 11].

2.3.4 NFC ITEMS

In terms of NFC there are some important items we have to describe, to avoid any misunderstandings.

NFC Interface is the interface component which enables a host to communicate with a NFC device or NFC tag. This could for example be an interface on a NFC enable Mifare reader.

NFC Device is a device that acts like a contact less reader/writer. Such devices can communicate directly with each other, like in active communication mode, and/or with NFC tokens. An NFC device shall support the ISO14443 and ISO18092 standards.

NFC Token is a physical entity, compliant with one of the mandatory NFC Forum tag specifications [12]. An NFC Token cannot communicate with other NFC Tokens, but its content can be read or written to by an NFC Device [12].

2.3.5 NFC CONNECTION SCENARIOS

In our use case there are four possible scenarios for setting up a Near Field Communication which involve different types of units, described in table 1 and illustrated below. The tag is typically used to receive configuration settings from an AP and exchange these settings with a NFC enabled WLAN device for setting up the wireless network. The tags will not be further described in this thesis, but only illustrated for the scenario and example purposes.

Unit A	Unit B
Access Point	NFC tag
Mobile NFC device	NFC enabled Access Point
Mobile NFC device	NFC tag
Mobile NFC device	Mobile NFC device

Table 1 Different scenarios

Access Point – NFC tag

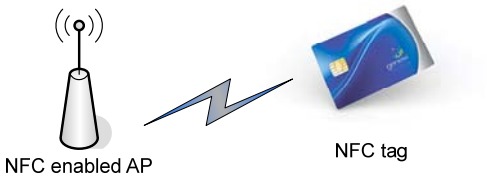


Figure 4 NFC Scenario 1

In this scenario a Near Field Communication is established between the NFC enabled Access Point and an NFC tag. This is a typical passive NFC communication, where the Access Point is the initiator and the tag is the target.

Mobile NFC device – NFC enabled Access Point

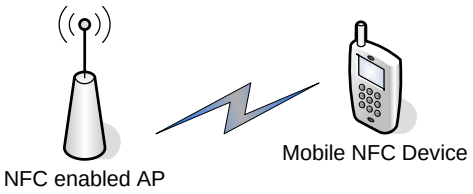


Figure 5 NFC Scenario 2

In this scenario, a Near Field Communication is established between the NFC enabled Access Point and a mobile NFC device. This is a typical active NFC communication in peer-to-peer mode, where both devices can be active.

Mobile NFC device – NFC tag

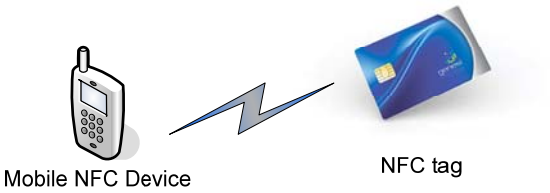


Figure 6 NFC Scenario 3

In this scenario, a Near Field Communication is established between the mobile NFC device and an NFC tag. This scenario is similar to the first scenario with a mobile NFC device as the initiator instead of the Access Point.

Mobile NFC device - Mobile NFC device

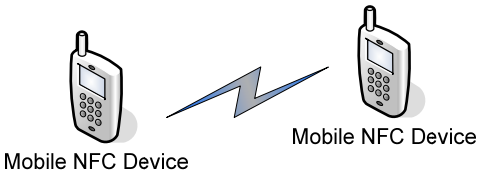


Figure 7 NFC Scenario 4

In this scenario, a Near Field Communication is established between two mobile NFC devices. This scenario is similar to the second scenario where two devices are connecting in an active peer-to-peer mode.

2.3.5 COLLISION AVOIDANCE

In order to not disturb any other NFC communication or any current infrastructure running on the carrier frequency, an Initiator shall not generate its own RF field as long as another RF field is detected. To start communication with the Target device, either in the Active or the Passive communication mode, an Initiator shall sense the presence of an external RF field.

If the Initiator do not detect any RF field within a given timeframe, the RF field shall switch on. In addition to the initial RF Collision Avoidance, an RF collision avoidance response during activation shall be required in the Active communication mode. This is to avoid collision of data by simultaneous response from more than one target. A more detailed specification of the collision avoidance can be found in the NFCIP-1 specification [8,10,11].

2.3 WIRELESS NETWORKING – (802.11)

There are many different types of wireless networking standards. This chapter will mainly focus on the 802.11 infrastructure standard, which is the most well-known wireless networking standard today.

This standard is used in different environments, like home, business, and public –wireless networks. Even if the main focus of our thesis is the infrastructure network, we will briefly introduce both infrastructure and ad-hoc mode of the 802.11 standard. This is illustrated in figure 8 and figure 9.

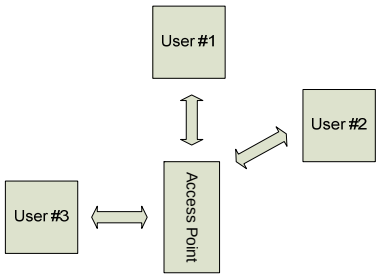


Figure 8 WLAN Infrastructure mode

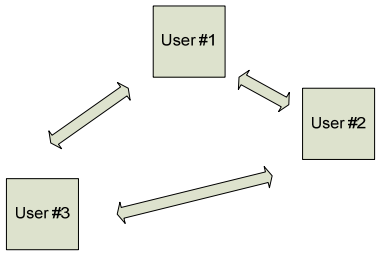


Figure 9 WLAN Ad-Hoc mode

Figure 8 and figure 9 illustrates the two different modes in the 802.11x standard.

In the **infrastructure** mode, the access point contains most of the network functionalities. It can provide different access schemes with or without collisions. Collisions may occur if medium access of the wireless nodes and the access point are not coordinated. However, if only the access point controls the medium access, collisions are not

possible. This setting may be useful for quality of service guarantees like minimum bandwidth for certain nodes [17].

In the **Ad-Hoc** mode, no infrastructure is needed. As figure 9 shows, each node can communicate directly with other nodes, so a node can forward a message to another node. With this we mean that if node A want to communicate with node C which is out of range, it can send the message to node B who are in range of both A and C, and then forward the message from A to C. The nodes have to implement medium access mechanism. These mechanisms are to handle hidden or exposed terminals, and priority mechanisms to provide a certain quality of service [17].

2.3.1 IEEE 802.11 STANDARD

The IEEE standard 802.11 specifies the well-known family of wireless LANs where many products are available. It specifies the physical and medium access layer adapted to the special requirements of wireless LANs. It also offers the same interface as the other 802.x LANs to maintain interoperability to higher layers. As illustrated in figure 10 the 802.11 standard is implemented in the physical layer and the lower part of the link layer. Higher layer is as mentioned common to all 802.x networks [17].

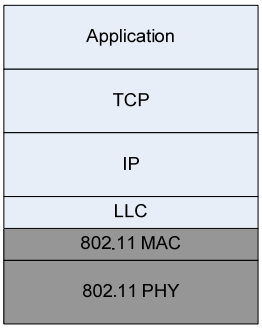


Figure 10 802.11 in the OSI model [18]

2.3.2 SYSTEM ARCHITECTURE

Typical system architecture for an infrastructure 802.11 network is illustrated in figure 11.

Several nodes, called **stations** (STA and STB) are connected to **access points** (AP). The stations are terminals with access mechanism to wireless medium and radio contact to the access point. The stations and access point which

are within the same radio coverage form a **basis service set** (BSS). The example in figure 11 shows two BSSs – BSS A and BSS B, which are connected via a distribution system. A **distribution system** connects several BSSs via the access point to form a single network and thereby extend the wireless coverage area. Such a network is called an **extended service set** (ESS) and has its own identifier, the **ESSID**. This identifier is the given "name" for a network and is used to separate different networks. It is also used to hide the actual IP address for the interface. The ESSID is similar to the SSID, which is used as the identifier on single wireless access points or wireless routers. The **portal** is a device which is used to provide the wireless users' access to other types of LANs, for instance to the internet via a gateway. The gateway is simply a device to connect two different networks together, like a router. The illustrated **server** in figure 11 is only for illustration purposes. This is to show the possibilities in such network architecture [17].

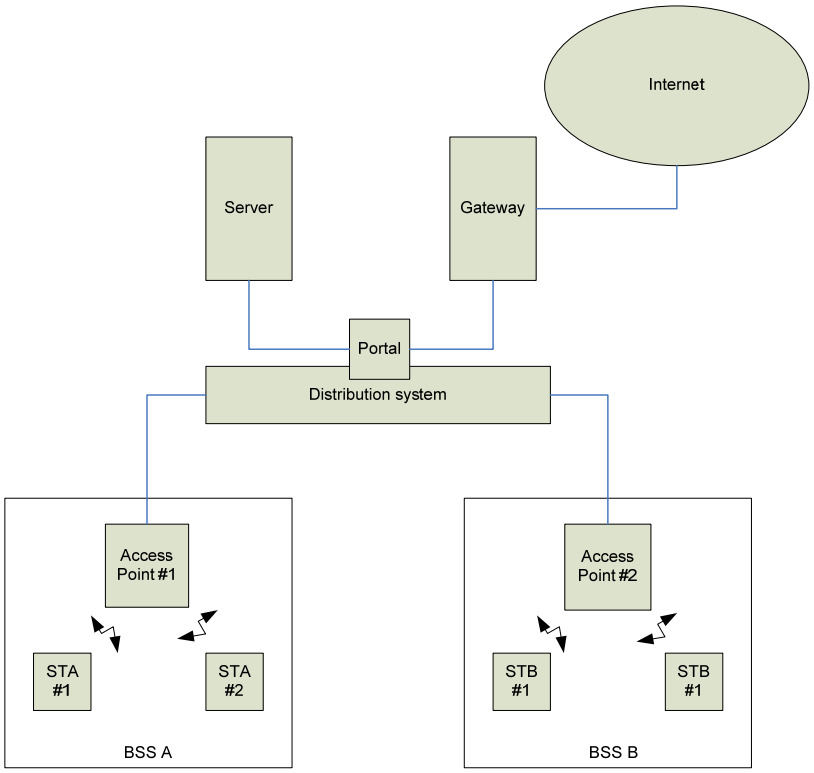


Figure 11 Architecture of an infrastructure-based 802.11 network [17]

2.4 NFC AS A SECURE SIDE CHANNEL FOR PAIRING 802.11 DEVICES

As mentioned in the introduction, one of the major problems when we want to establish a connection to 802.11 networks is to establish trust between the user device and the system device (usually an access point), especially

for first-time connections. When data transfer is over the air, it is vulnerable to both passive and active attacks. The challenges are the exchange of secret information and to initiate the communication channel with the correct node. Communicating over the air makes it very hard to establish a trusted path. As the basis of our thesis, we introduce alternative ways to establish trust and secure communication. NFC is introduced as a secure side channel to the pairing process of 802.11 devices. The idea of a secure side channel is relatively simple, and has several useful properties, which is listed below.

- Communication is totally isolated from other networks and channels (Therefore it is called side channel) and should therefore give an extra protection against both active and passive attacks.
- Trust should be easier established between the two communicating devices, even for first time connections, due to the physical encounter.
- Point to point.

We assume that each WLAN device is equipped with a NFC device. The secure side channel only works as point to point, and requires the communicating devices to be close to each other. In this way, the channel is isolated, kept secure and makes sure that the actual device is identified.

There are mainly two possibilities of implementing NFC as a secure side channel when pairing two WLAN devices:

1. Implementing the NFC channel only when we exchange credentials, like PIN code and configuration settings, like illustrated in figure 16. This means that the very first communication is going across the 802.11 network.
2. Implementing the NFC channel in the whole process, which means that the NFC channel is introduced from the very beginning until the setup process of WLAN access with the configuration settings are being initiated. Because no other network channel than NFC are being introduced in this mode, this would be the most secure possibility of implementing NFC.

Even if a side channel enables communication over such a short range, wireless threats will still be there, but has been limited.

2.5 REMOTE AUTHENTICATION DIAL IN USER SERVICE (RADIUS)

RADIUS is a networking protocol that uses access servers to provide centralized management of access to networks. It is described in RFC2138 [20] where a remote client can exchange authentication, access control, accounting and configuration information with a RADIUS server. The RADIUS server can authenticate a user or

device from its database or user identification and authentication parameters. Figure 12 illustrates a process where a user device wants access to a wireless network, and is exchanging information on the wireless interface with the Access Point, which further is communicating with the RADIUS server on the Ethernet link. The user database can either be an external database or an internal database in the RADIUS server [22].

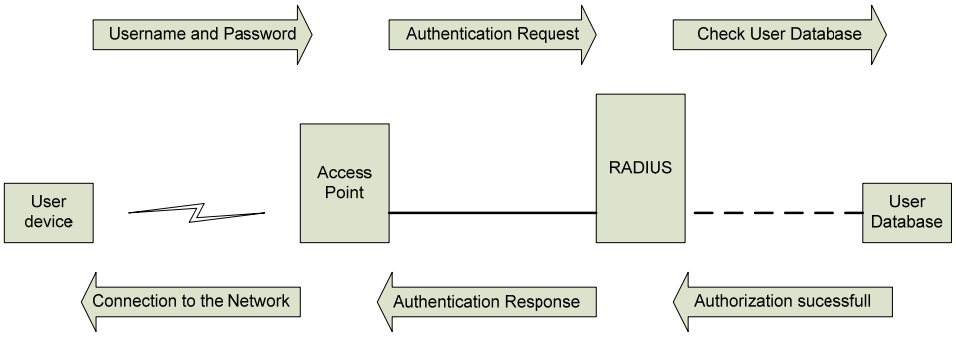


Figure 12 Authentication, access control and accounting process with a RADIUS server [21]

As figure 12 shows the user device which wants to be authenticated towards the network (here; the Access Point) sends it username or\and password to the Access Point which forwards it to the RADIUS server. The RADIUS server checks the user database, and in this scenario the user exists with the correct username and password where the RADIUS server responds with a successful authorization to the Access Point. The Access Point can then authenticate the user and “give” the user device wireless network access [22].

2.6 EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

The EAP is essential to authentication and authorization of users in an infrastructure wireless network. Figure 13 shows a typical EAP flow in authenticating a user in a wireless network.

EAP defines the end-to-end message format used in simple request\response mode of interaction between the client and authentication server. This protocol is defined in RFC2284 [26], but there is several extensions with additional support to different authentication methods, like RADIUS support, which is defined in RFC3579. In 802.1x networks the EAP messages are encapsulated using EAPoL (EAP over LAN), and sent over the network link [23,25].

As illustrated in figure 13, a session starts with an EAPoW, which actually is the same as EAPoL, but the term EAPoW are widely used when the EAP messages are encapsulated in 802.11 frames and sent across the wireless network.

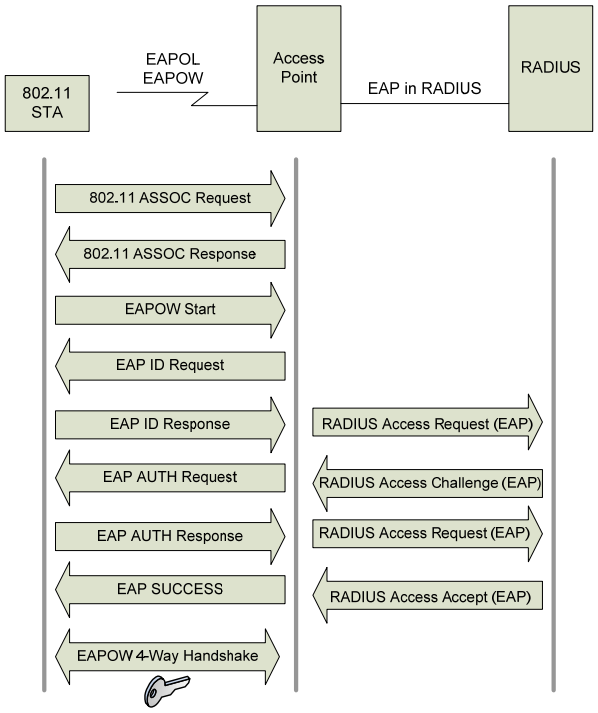


Figure 13 Typical EAP flow when authenticate a user device towards a wireless network [24]

As introduced above, figure 13 illustrates an authorization session between a user device and a system. First the client is sends an 802.11 association request with information about the network interface card such as MAC, supported data rate etc. and the SSID of the network it wishes to associate with. Second, the access point responds with the clients' request (if accepted) with information regarding the association, such as association ID and supported data rate. The client will now start the EAP session, where it transmits an EAPOW start to the access point. The access point responds with an EAP ID request, to obtain the identity of the client where it responds with its identification, like username and password. When the access point has received these credentials, it forwards them to the authentication server (the RADIUS) which authenticates the client using a chosen authentication method supported by EAP. If the authentication server verifies the clients' credentials, it returns an accept

message to the access point. The access point processes and accepts the message with an EAP success message to the client. The client is now authenticated, and will get access to the wireless network [24].

2.7 WI-FI PROTECTED SETUP - WPS

Wi-Fi Protected Setup is an optional certification program developed by the Wi-Fi Alliance to make it easier and more secure to establish security-enabled wireless networks.

As wireless Wi-Fi networks have become very popular, they have been exposed to several securities and privacy - related problems. An important reason to this is the lack of knowledge about security among users. For instance, in home environments where users are setting up their Wi-Fi networks without security; the network can be accessed from around 100 meters away. If you live in the middle of a city, you can just imagine the risk of being attacked by a malicious user in your neighborhood. Actually the coverage reaches a large number of clients capable of receiving the signal. Some estimates done by the Wi-Fi Alliance, says that up to 60-70% of successfully configured wireless networks have never been configured with any kind of security [61]. With this in mind, the Wi-Fi Alliance has tried to develop an easy and secure method for implementing security into wireless networks with the Wi-Fi Protected Setup [27].

Wi-Fi Protected Setup provides the Wi-Fi Protected Access (WPA\WPA2) generated automatically by an Access Point. Also the SSID, which is specifying the network name of the wireless network, could be automatically generated by the Wi-Fi Protected Setup enabled Access Point [27].

2.7.1 COMMUNICATION MODES

There are two different methods to create a communication channel for exchanging relevant information between an Enrollee\User and an Access Point\Registrar. It is called an In-band channel, which is a standard WLAN channel and an Out-Of-Band channel, which is an external channel separate to the standard WLAN channel.

Using an **In-band channel** means that the given Wi-Fi connection is used to deliver both authentication and configuration settings data. The procedure for an in-band communication mode is identical for both the PIN entry and PBC method (described in chapter 2.7.2).

When using an **Out-Of-Band channel,** a separate channel is used to exchange authentication and configuration settings data between an Enrollee and Registrar. Example of out-of-band channel is UFD (USB Flash Drive) and NFC, which is proposed in the WPS specification. The procedure for an out-of-band communication mode is identical for both the UFD and NFC method [27].

2.7.2 SETUP METHODS

Wi-Fi Protected Setup support four different methods to establish a secure connection and exchanging security related setup configuration to a wireless device;

PIN (Personal Identifier Number entry), in which a PIN has to be read from either a sticker on the user device or a display on the Access Point (if there is one), and entered by the user. This PIN is also described as a device password, which refers to a unique password for an Enrollee.

PBC (Push Button Configuration), in which the user simply pushes a physical or software button both on the user device and the Access Point within a time frame of 120 seconds.

NFC (Near Field Communication), in which a user simply has to bring the new user device close to the Near Field Communication reader\writer at the Access Point to allow a Near Field Communication between the devices. NFC Forum compliant RFID tags can also be used. This method will be described further in chapter 2.3.x.

UFD (USB Flash Disk), in which the user uses a USB sticker to transfer data between the new user device and the Access Point.

The UFD and the NFC method is still a proposed setup method, and with UFD there is still no indication that this method will be certified as one of the methods in the Wi-Fi Protected Setup specification [27].

2.8 PRIVACY AND SECURITY

This sub chapter intends to give an overview of essential security related topics in communication systems, which involves different kind of users and system devices.

Today's' users are usually dependent upon equipment with inbound security and privacy solutions. Many of these solutions are often not valued high enough by the manufactures. They are more concerned about functionalities and cost.

Both NFC and wireless 802.11 communication devices are dependent on parameters such as security, privacy, trust and anonymity. It is very hard to define these factors independently and in many ways is integrated. The ultimate or preferred goal is to develop a user-friendly communication solution that is able to communicate in a secure way and give away as little as possible about user to unwanted participants [28,29,30].

2.8.1 PRIVACY ISSUES

Privacy has always been a disputed issue in the information and communication technology. Personal privacy means that a user is able to control information which directly or indirectly could be used to identify an entity or person. This could be connection history, physical address or location–to organizations or individuals. Privacy relates to the control of personal information, where a system has restricted permissions to certain objects of specific users.

NFC devices raise many privacy concerns. A passive NFC device responds to reader requests without alerting their owners. Such passive NFC devices can often be activated automatically when they are moving into an active RF field. All NFC devices emit unique identifiers, even devices that protect data with cryptographic algorithms. As a consequence, a person carrying a passive NFC device effectively broadcasts a fixed serial number to nearby readers, providing a ready NFC device for physical tracking. Such tracking is possible even if a fixed tag serial number is random and carries no intrinsic data [31].

The threat to privacy increases when a physical device id (like MAC or DiDi and DiDt) is directly or indirectly combined with personal information. For example, if a device id is combined with personal related information stored somewhere in the system, and the user are doing a transaction with the user device, a malicious user would be able to create a link between the device id and the personal information of the user. This is a well known problem, and is not unique in our case, but also relevant to other wireless technologies, such as Bluetooth [32].

2.8.2 SECURITY ISSUES

Even if the infrastructure mode within 802.11 wireless networks has a predefined infrastructure, NFC does not have any. All network services are configured and created on the fly. It is obvious that the lack of an infrastructural support opens for wireless link attacks. Therefore, security in a Near Field Communication session becomes inherent weak. Security is an important issue for Near Field Communication, especially for those security sensitive applications, and also because there is no obvious security functionality implemented in the Near Field Communication standards. Many of the security issues in wireless infrastructure network within 802.11 are already discussed in many papers and projects. These issues could also be relevant issues that affect the security and privacy in the NFC system. To secure a communication session in our hotel scenario, we have to consider the following attributes: integrity, confidentiality, availability. These attributes must be considered and evaluated, because any weaknesses in one of them would affect the security level in the entire system.

Integrity attribute ensures that the data is being identically maintained during any operation, as in transfer, storage, and retrieval. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network link. Integrity guarantees the message from being

corrupted. Integrity level is usually ensured by the use of mathematical code, such as the Message Integrity Code (MIC) [33].

Availability ensures the survivability of network services despite denial of service attacks. A denial of service attack could be launched at any layer in a Near Field Communication session. On the physical and Media Access Control (MAC) layer, an adversary could perform jamming to disrupt the communication on the physical channels. On the higher layers, an adversary could bring down high-level services. One of these targets is the key management service, an essential service for any security framework [33].

Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as user related data, requires confidentiality. Leakage of such information to outsiders or intruders could have devastating consequences. Session data must also remain confidential in certain cases, because the information might be valuable for intruders to identify and to locate their targets. [33].

2.8.3 TRUST

Trust is one of the most critical elements in the use of modern communication systems. No trust, could compromise an entire system. Trust establishment in Near Field Communication is still an open field for discussion. A Near Field Communication connection is established without any mutual authentication according to the standard, but instead intended to be implemented in the specific application. In combination with other wireless technologies like 802.11, is a great challenge.

By verifying the relationship between two entities, makes it easier to take proper security measures. A trust model specifies, evaluates and sets up trust relationships among entities. Trust modeling is a technical approach to present trust for digital processing. Trust modeling is now given more attention than before. By applying an organized trust model between every connected device, each node could easily maintain trust constraints. This could be implemented by adding incoming devices to different trust lists [34,35].

2.8.4 ANONYMITY

Anonymity is a result of not having to reveal personal characteristics such as a name, unique electronic identification or description of physical appearance to be exposed in a communication session. Anonymity is not an absolute condition, which means that the degree of anonymity one may have varies with circumstance and environment etc [36].

As mentioned earlier, a unique identifier like MAC, DiDi and DiDt represent a big security and privacy problem. By monitoring the wireless networks any person could easily disclose and track any communication device based on the MAC or DiDi and DiDt address.

One of the best methods to achieve anonymity is to assign communication devices with pseudo random identifier (PRI) that changes periodically. This will prevent an attacker from monitoring people and devices because of its randomness [36].

2.8.5 CRYPTOGRAPHY

Cryptography is the making of "secret codes", and comes from the cryptology which is the art and science of making and breaking "secret codes". The cryptography provides the basis for secure communication and in order to strengthen encryption security within a system, one could increase the cryptography key length. The original information is known as the plaintext, and the result of the encryption is cipher text [33].

In general, we can categorize the cryptography in symmetric and asymmetric. These two methods have their benefits and drawbacks.

Symmetric cryptography is a class of algorithms that uses trivially related and often identical cryptographic keys for both encryption and decryption. The keys are representing a shared secret between two or more parties that can be used to maintain a private information link [33].

Benefits:
- Simple encryption process
- Use of known algorithm
- Security is dependent of the key length

Drawbacks:
- Shared key must be agreed upon both parties
- Number of keys is equal to number of communication partners
- Authentication of origin or receipt cannot be proven
- Key management

Asymmetric cryptography is also known as public-key cryptography, which is a form of cryptography in which the key used for encryption differs from the key used for decryption. In asymmetric cryptography a user has a pair of cryptographic keys – one public key and one private key [33].

Benefits:
Hard to break
Key exchange
Support for infrastructure
Certificates

Drawbacks:
Considerably slower encryption algorithms
Rarely used for bulk transfers
Not proven to be mathematically secure
Software encryption is approximately 100 times slower than hardware encryption [3]

2.8.6 WIRELESS THREATS

Wireless LANs are open for attacks especially because of their open transport medium over the air, and easy availability of cheap attack tools. An unsecured wireless LAN does not only invites attacks but can also become the source of malicious activities. So, continuous monitoring of the wireless LAN and enforcing wireless LAN security policies are of prime importance. Wireless LANs are easy targets for a host of attacks. With a Wi-Fi enabled laptop and a handful of open source tools it is easy for one to launch a long list of attacks on any WLAN. If you have deployed wireless LANs, knowledge on these attacks is essential to identify and fix those [38].

A **passive attack** occurs when someone listens to or eavesdrops on network traffic. Armed with a wireless network adaptor that supports promiscuous mode, the eavesdropper can capture network traffic for analysis using easily available tools, such as Network Monitor or AirSnort [37]. Passive attacks are by their very nature difficult to detect. Passive attacks on wireless networks are extremely common, almost to the point of being ubiquitous. But, the legal response is severely limited. Only if it could be determined the "listener" was actively attempting to crack any encryption used on the network or otherwise interfering or analyzing wireless traffic with malicious intent would he or she be susceptible to being charged with a data-related crime, but this would depend on the country or state in which the activity took place. Figure 14 illustrates a typical passive attack scenario.

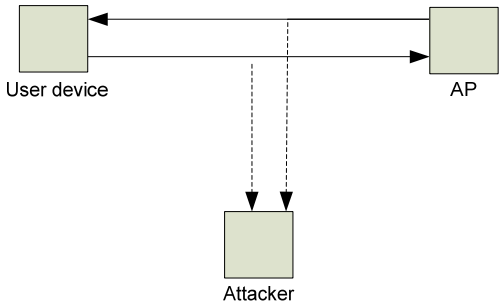


Figure 14 Typical passive attacks scenario

Once an attacker has gained sufficient information from the passive attack, the hacker can then launch an **active attack** against the network. There are a potentially large number of active attacks that a hacker can launch against a wireless network. For the most part, these attacks are identical to the kinds of active attacks that are encountered on wired networks. These include, but are not limited to, unauthorized access, spoofing, and Denial of Service (DoS) and Flooding attacks, as well as the introduction of Malware and the theft of devices. New variations of traditional attacks specific to wireless networks have emerged along with specific terms to describe them, such as "drive-by spamming" in which a spammer sends out tens or hundreds of thousands of spam messages using a compromised wireless network. Unauthorized access and spoofing are the most common threats to a wireless networks. **Spoofing** occurs when an attacker is able to use an unauthorized station to impersonate an authorized station on a wireless network. Once the attacker has authenticated and associated with the wireless network, he or she can then run port scans, use special tools to dump user lists and passwords, impersonate users, connect to shares, and, in general, create havoc on the network through DoS and Flooding attacks. These **DoS attacks** can be traditional in nature, such as a *ping flood, SYN, fragment, or Distributed DoS (DDoS)* attacks, or they can be specific to wireless networks through the placement and use of *Rogue Access Points* to prevent wireless traffic from being forwarded properly [39].

Placing a rogue access point within range of wireless stations is wireless-specific variation of a man-in-the-middle attack. If the attacker knows the SSID in use by the network and the rogue AP has enough strength, wireless users will have no way of knowing that they are connecting to an unauthorized AP. Using a rogue AP, an attacker can gain valuable information about the wireless network, such as authentication requests.

Jamming is a special kind of DoS attack specific to wireless networks. Jamming occurs when spurious RF frequencies interfere with the operation of the wireless network. In some cases, the jamming is not malicious and is caused by the presence of other devices, such as cordless phones, that operate in the same frequency as the wireless network. Intentional and malicious jamming occurs when an attacker analyzes the spectrum being used by wireless networks and then transmits a powerful signal to interfere with communication on the discovered frequencies. Fortunately, this kind of attack is not very common because of the expense of acquiring hardware capable of launching jamming attacks. Figure 15 illustrates a typical active attack scenario [3].

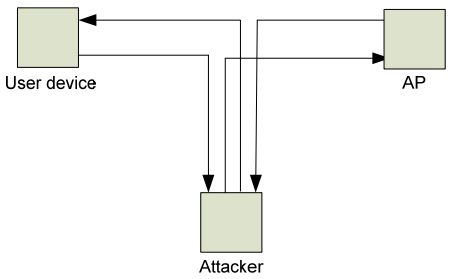


Figure 15 Typical active attacks scenario

2.9 RELATED WORK

Since NFC is a new technology, the security issue for transferring sensitive data is not well documented, but in the paper [40] shows us a general comprehensive analysis of security with respect to NFC. It is not limited to a certain application or a scenario, but uses a systematic approach to analyze the various aspect of security whenever an NFC interface is used. In [41], there is a different approach where they look at security measures in NFC use cases and devices. They derive different use cases and applications based on the technology, and show assets and interfaces of an NFC device that could be a possible target of an attacker. They further apply different attacks on the operation modes and how devices could be protected against such attacks, and then present guidelines on how to improve security and privacy issues.

The first connection between personal devices can be difficult in terms of security associations and infrastructure, and with [42] shows how this can be done with a side channel like NFC among others to set this up. With its personal device, a user has a number of devices to communicate with, and that communication can be a hassle especially, mainly due to setup problems. In [43] they use NFC as connectivity between different devices. They analyze different scenarios and establish the communication requirements to establish connectivity between the mobile phone and other devices.

NFC is a short range technology, but as long as it is a wireless technology it has many of the same security issues as other wireless technologies. In [44], the Bluetooth technology vulnerabilities are analyzed, and many of the same threats can be derived to NFC in a threat analysis. Also, wireless network security through 802.11, Bluetooth and handheld devices are analyzed in terms of confidentiality, integrity and availability in [45] with recommendations.

3 PROPOSED SCENARIO ARCHITECTURE

The purpose of this chapter is to create a specific architecture and review of our scenario. First we create a system architecture with all relevant components and a briefly descriptions of these, and why they are a part of the system. We identify all functions in a system review, with an implementation structure. Further we identify all assets that we want to be protected in the system, and describe them briefly.

We address all functions and components in the entire system, with possible subjects. The functions in the system refer to actual functionality which must be identified. Components refer to physical or virtual objects in the system e.g. piece of information that has to be protected. Subjects are possible entities who are responsible for the communication.

The system architecture described in this chapter is based on the system architecture for wireless infrastructure network discussed in chapter 2.3, and the system architecture for Near Field Communication discussed in chapter 2.2. These architectures are put together in one functional system architecture, which forms our scenario. This system architecture is further illustrated and described in chapter 3.1.

3.1 SYSTEM ARCHITECTURE

This subchapter describes the components in our hotel scenario, which is illustrated in figure 16. The scenario is configured with two access points, to illustrate the practical need for a distribution system. It is also a point that one access point at a hotel would never be enough to cover the entire area of a functional wireless network. The RADIUS and database server could ideally be the same server if the network is limited to one hotel, but ideally separated if the RADIUS is centralized and used in corporation with several hotels. Our scenario is limited to one specific hotel, but the servers are divided into two separated servers for the illustrations' purpose.

In the next subchapters we have described the different items in our system architecture.

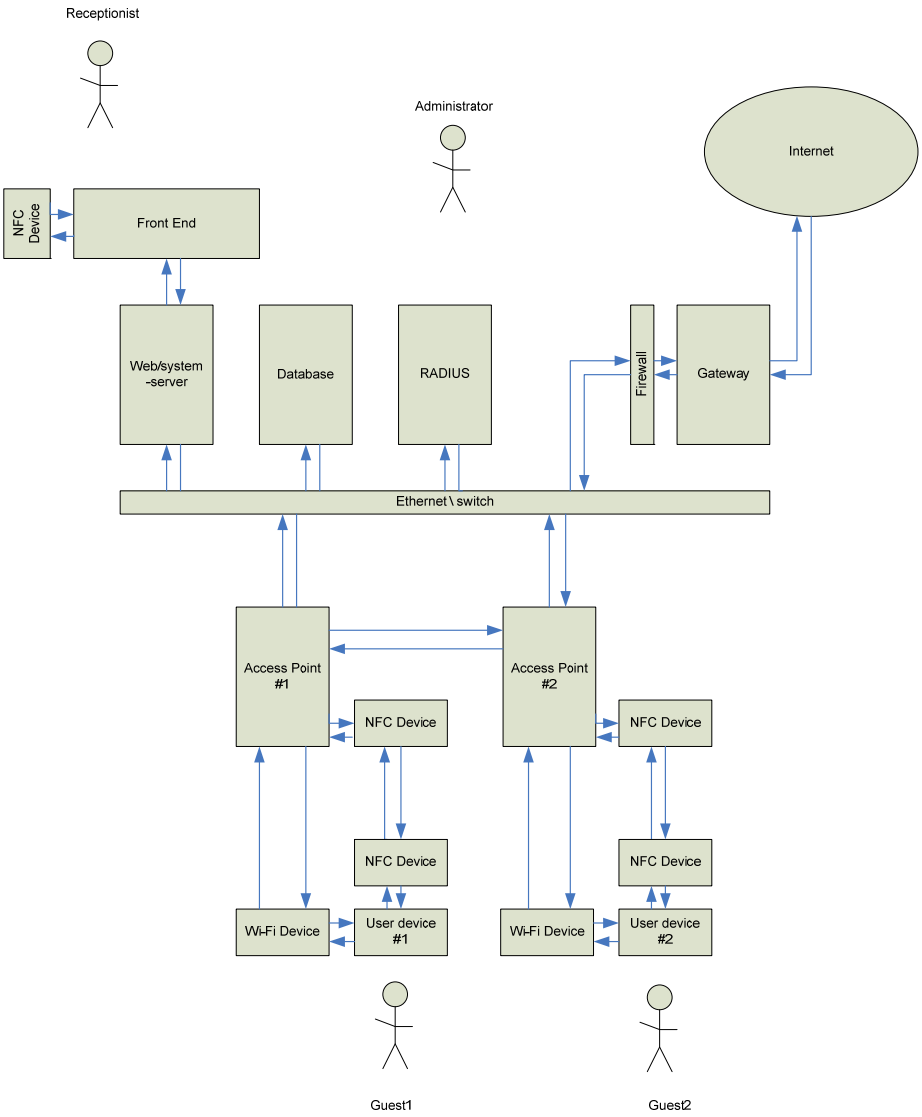


Figure 16 System architecture

3.1.1 FRONT END

To register guests at the hotel we need a system to do this as simple and effective as possible. The front-end system is a web application with a graphic user interface in form of a web application. This application shall be used for registration of users in the hotel, with information like guest id, name, room number, check in and checkout status. Information related to the WLAN access shall also be registered, which would contain information about the registration and user device and password. This shall be connected to a given guest id. The front end system shall also have implemented a NFC device for easily communication with the system via a mobile device.

This shall be used in situation where the receptionist can easily swipe the mobile device for registering of the device ID.

The receptionist shall be able to register a new order for a guest who wants WLAN access, where the receptionist generates a new PIN (password) for the user to authenticate its NFC device at the Access Point when he or she wants WLAN access.

3.1.2 WEB SERVER

The web server shall serve the front end system and provide necessary services at the front end and to the database server. In addition, it shall be able to run services to manage the registration of devices both at the access point and for the NFC device.

3.1.3 DATABASE SERVER

The database server shall contain all relevant information about the general guest registration and the registration of WLAN guest accounts. The database shall at least contain one table for guest registration with a guest id and one table for guest devices which are supposed to be used in the hotel network. There must be a relation between the two tables. The database server shall also be able to communicate with the RADIUS server to provide authentication of users in the database.

3.1.4 REMOTE AUTHENTICATION DIAL IN USER SERVICE (RADIUS)

The RADIUS server is integrated in our scenario to be able to authenticate, authorize and account all guests at the hotel who wants access to the wireless network. It shall provide all relevant security features to such a network. This server could be the same physical server as the database server, but in an environment with many users and high amount of data exchanged, it should be two separated servers. The functionality of a general RADIUS server is described briefly in chapter 2.5 and in more detail at [20].

3.1.5 FIREWALL

The firewall in our scenario shall prevent attacks from outside intruders, and block all unused ports both from inside and outside. The configuration and policies shall follow *the guidelines on firewall and firewall policy* given by NIST [46] in addition to restricted use of usual ports which could harm the system and organization.

3.1.6 GATEWAY

The gateway is actually a gateway router simply to interconnect a network to other networks. In our scenario the network at the hotel are being interconnected to the internet. This gateway router shall support Dynamic Host Configuration Protocol (DHCP) and Network Address Translation (NAT). The DHCP must be supported to provide IP addresses to the clients (guests' devices) while NAT must be supported to provide mapping of external IP addresses into internal IP addresses, so the data can be forwarded directly from the router to the intended destination within the hotels' network. There are also security aspects within the NAT, for example mapping that will "hide" the clients on the internal network towards the internet.

3.1.7 ACCESS POINT #1 \ #2

The access point is intended to provide the hotel guests wireless network connection. The system shall have at least one Access Point in the lobby and at least one on each floor at the hotel, to provide network with satisfactory signal strength. The access point shall be able to communicate with each other with a satisfactory overlap on separated channels, to cover the entire hotel with wireless network connection.

3.1.8 NFC DEVICE

The NFC device is a part of a user or system unit, such as a mobile phone or an access point. The NFC device is integrated to enable secure pairing with the wireless network at the hotel. The NFC device shall support point-to-point mode in NFC, as described in chapter 2.3.2.

3.1.9 USER DEVICE #1 \ #2

The user device is a hand held personal device like a mobile phone, PDA or laptops etc. This device must support the NFC device with a host controller interface [47]. The user device must also have a front end system, to make it useful for a user. This front end shall be an application for setting up an NFC connection, enter a PIN value, performing a mutual authentication with the system, receive configuration data for the wireless network, and then bring these further to the operating system at the handheld device to achieve a WLAN connection.

3.1.10 GUEST #1 \ #2

The guest illustrated in our scenario is a user of the specific system, who wants access to the wireless network, with fast, easy and secure setup. He or she is typically familiar with the technology and has the knowledge to use mobile devices (such as mobile phone, PDA, laptop etc), wireless network and internet. We assume that the user

has the relevant knowledge and experience to perform the task, because if not, a whole new area of security and privacy issues must be considered.

3.1.11 RECEPTIONIST

The receptionist is assumed to be a trusted part at the hotel. In this context we mean that this person is not a risk to the security and privacy for the system, even if he or she is an involved subject. The security and privacy issues regarding the receptionist and even the rest of the employees at the hotel are considered transparent. If this trust does not exist, the issues increases drastically, like described in 3.1.10.

3.2 SYSTEM REVIEW

This subchapter presents an overview and description of the system in our scenario. Figure 17 gives an overview of the structure of our system model. The idea of creating a system review like figure 17 illustrates and its descriptions are based on [48] where UMTS functions are described by ETIS. In our communication system there is four important components; **communication**, **functions**, **subjects** and **objects**. The main purpose of this description is to identify all communication interfaces and modes, the important functions used and also the specific subjects and objects involved within our scenario. The identification of these will make it easier to move further and identify the assets. It also gives a complete overview of our scenario with its functionalities. Some components described here have been described earlier in chapter 3.1.

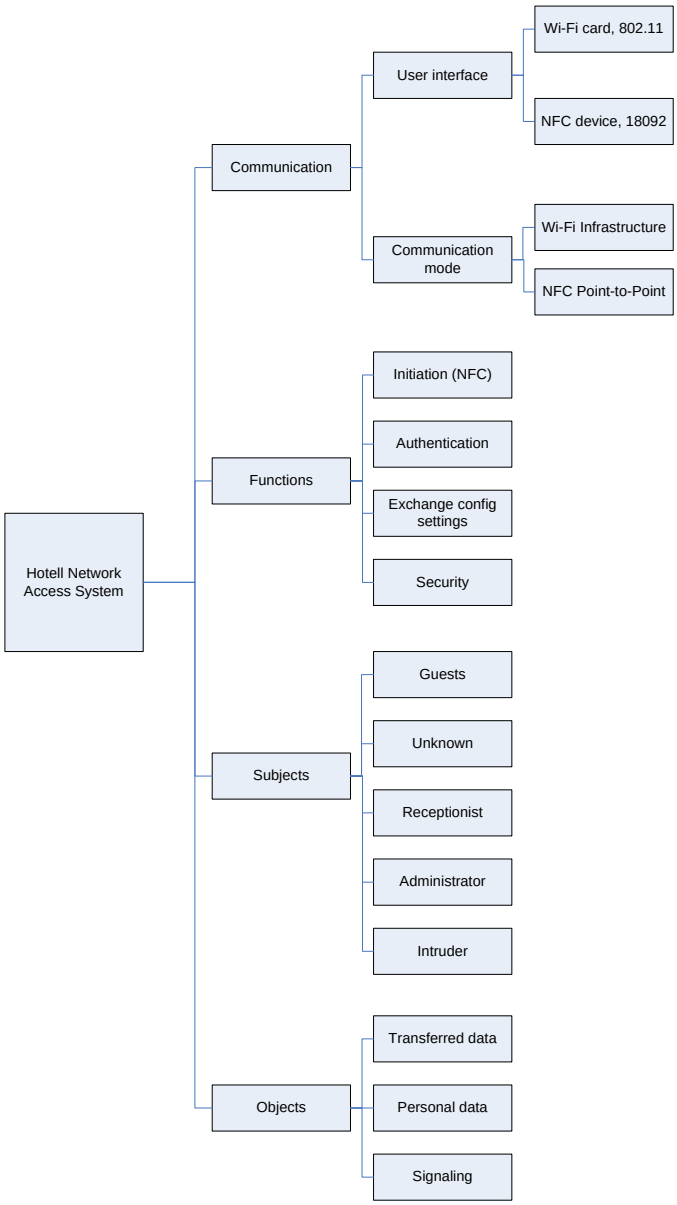


Figure 17 Implementation structure

3.2.2 COMMUNICATION

The communication part in figure 17 refers to user interface and communication mode for the Network Access System.

In the **user interface**, we have two different types of communication devices which shall be supported by the system. The **Wi-Fi 802.11 card** is the interface in any device with WLAN support, such as a smart phone, PDA or

laptop. This is an integrated WLAN card, USB or PCMIA -WLAN card, with support to both WPA and WPA2. The **NFC 18092 device** must be integrated in all devices who wish to initiate a WLAN connection securely with the use of a secure side channel, like NFC.

In the **communication mode**, we have proposed two different modes to our hotel scenario. For Wi-Fi 802.11 wireless network communication, we are limiting this network to the **infrastructure mode**, which means that all clients must communicate through the wireless access point. Therefore ad-hoc communication mode is not supported. In the communication mode for NFC, we are limiting our scenario to use only the **NFC peer-to-peer mode**, which is specified in the 18092 standard, as mentioned earlier. This peer-to-peer limits the communication session to two specific entities, which is described more in detail in chapter 2.2.

3.2.3 FUNCTIONS

In our use case we have addressed four different main functions which will be important throughout our security analysis.

The **initiation of a Near Field Communication session** is dealing with important information about the users and the system, and is therefore an important part of our system. This is the first phase where users and system must obtain mutual trust to each other. In this function, information like the NFC device ID is exchanged between the communication participants.

The **Authentication** function is the part where the guests are sending their identities and PIN codes, and also where the users either gets access to the wireless network or not. It is a session of messages between the guests' device, the access point and the authentication server. This is one of the most important sequences during the setup phase.

The **exchange of configuration settings** contains information about the given wireless 802.11 network, with the network identifier, cryptographic key (WPA or WPA2) and so on. This information is the actual information we want to hide, because we want to prevent intruders from exposing the network traffic, and to get access.

The **security** is an important issue in the Near Field Communication system. As security is not implemented in the Near Field Communication standard, it has to be implemented in the software. When using Near Field Communication as a secure side channel for initiation and setup of other wireless network standards, the use of Diffie Hellmann is ideal for trust between the participants on the side channel. The Diffie Hellmann is kind of an asymmetric cryptography algorithm, which is described in chapter 2.8.5. There are also other potential security solutions for our scenario, which will be discussed in chapter 5. The security functionality on the wireless network and the relevant components are also of importance. They have to function in relation the new technology, NFC.

3.2.4 SUBJECTS

The subjects in the Hotel Network Access system are divided in to users, possible intruders, system devices and procedures.

In our scenario a **User** is a guest who wants access to a wireless network at the hotel. The user must have a user device with support for both NFC and 802.11 networks. An **unknown** subject is an unknown user to the 802.11 network or the Near Field Communication system, who is not authorized to use the network access system. This can be either a user who has not yet been authorized as a legal user (guest at the hotel) or a potential intruder. The **receptionist** is a user who is considered trusted, and is the one who physically can give guests access to the wireless network. The receptionist must first register the guest with the necessary information and generate the PIN code. The **administrator** is a user with full access and control over the hotel network access system. This user is also considered trusted part, and is intended to be the one who controls and maintains the network. A possible **intruder** refers to a malicious user who intends to get access to secure or private data on either the 802.11 network or an ongoing NFC session. An intruder could be an unauthorized user or a legally user (an identified guest at the hotel).

3.2.5 OBJECTS

The objects in the Network access system is divided into control data, personal data and signaling data. **Control data** include all data sent across the nodes within the system, like request and reply –messages. This is general data, which is not related to any users. It also includes **personal data**, which is the unique device ID, PIN code, and potential cryptographic keys which are unique for a user. **Signaling data** through the communication link is also included as an object in this review. Such data can be session data, time stamps, expire time on specific data (for instance TTL) and so on.

3.3 INFORMATION FLOW

The information flow in a system is important to describe. This is to get an understanding of how the system shall work, and to help identify possible security issues. Figure 18 shows the information flow when a user (hotel guest) wants to achieve wireless network connection. NFC is introduced when the user are requested to enter the PIN, and when the system shall transmit the configuration settings to the user. Figure 19 shows how the NFC channel is initiated and connected. In this subchapter a user refers to as a guest in our hotel scenario.

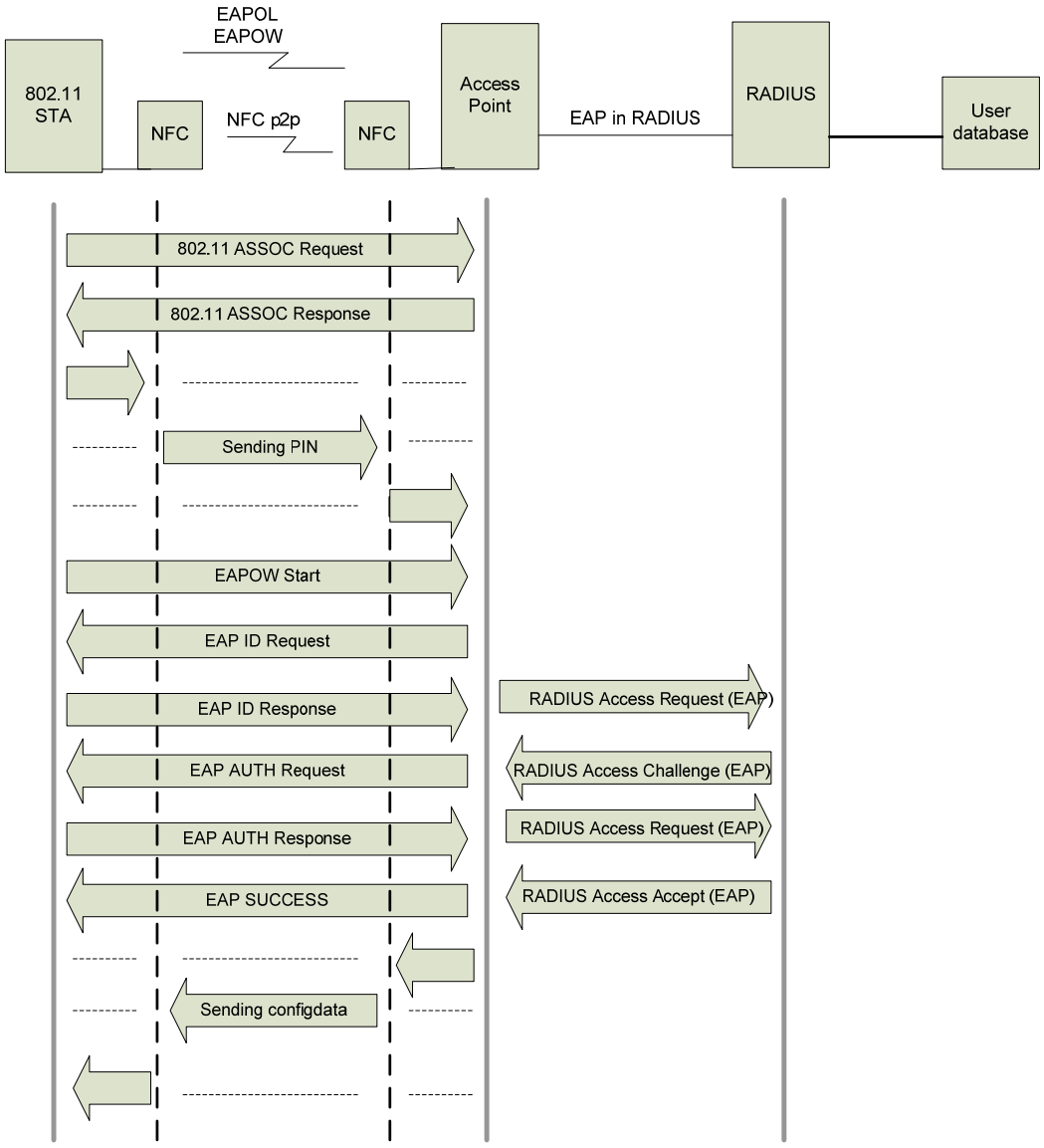


Figure 18 Information flow in the scenario

Figure 18 illustrates the information flow when a user initiates a NFC setup configuration method in the proposed WPS specification [27]. In this specification, the Wi-Fi alliance suppose that a user first are connecting the access point with 802.11 association message, and get a list of possible setup methods, where the user chooses NFC as the setup method and transmit the PIN code to the access point, which starts the authentication of the user. When the authentication with EAP as described in chapter 2.5 has finished, the NFC is introduced again to transmit configuration settings for the 802.11 network from the access point to the user.

Figure 19 intends to make it clear how the process in a Near Field Communication session in the Wi-Fi Protected Setup method appear after the association with the 802.11 interface, and what kind of data the system is suppose to exchange. The NFC connection is unencrypted, which is default in the NFC standard.

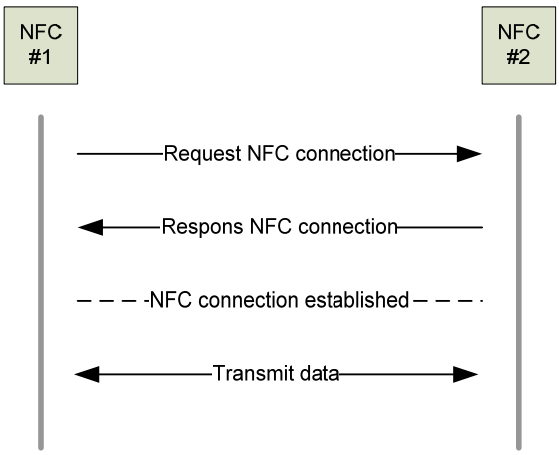


Figure 19 Initiation flow within NFC

In the first step the initiator sends a request for connection to the target. In this request, the initiator sends its unique device ID, to identify itself. If accepted, the target responds this request with its own unique device ID. The NFC channel is now connected, and the communication participants can start transmitting data. This method does not implement any encryption or exchange of credentials, and has therefore no technical security implementations.

This process will occur when a guest wants WLAN access, and initiates a WLAN connection, where the system asks the user to enter a PIN code. When the user enters the PIN code, the NFC channel is created, and the PIN code is transmitted over this secure side channel. When this is done, the NFC channel is closed, and reopened in the next process, where the configuration settings are sent from the access point to the user.

3.4 ASSETS

Now when we have presented the scenario system architecture with the specific components, a system review with the logical and physical components and the typical information flow, it is important to identify all important assets, which we want to protect in the system.

The assets are directly or indirectly related to the NFC channel. Indirectly relation to the NFC channel means assets that can also be located in another part of our system architecture (outside of the NFC part). These assets must also be considered in our evaluation. Table 2 lists the assets which we want to protect. We describe briefly why they are important to protect, and the security related discussion will be further presented in chapter 4.

	Description
1	Device ID
2	user device
3	Radio link
4	Stored data on device
5	Transmitted data
6	Configuration settings
7	PIN[1]
8	Authentication
9	Personal privacy
10	Anonymity

Table 2 Assets to protect

The unique **device ID** (DiDi and DiDt) in the NFC standard and the MAC in the 802.11 standard is certainly an asset in our system, which we want to protect. This is mainly because these identifiers can expose the user's identity, and is therefore a privacy concern.

The **user device** is a physical unit like a mobile phone with an integrated NFC device and an 802.11 device. This asset is important to the system. If a guest are already authorized and looses or get the smart phone stolen a huge security and privacy problem would arise. This is a general security and privacy problem, and is a threat to systems because of the exposure of network settings.

The **radio link** in both NFC and 802.11 infrastructure networks is an important asset, even if the standard specifies that the maximum range in NFC is 10 centimeters. In the 802.11 standard is of bigger concern, because the range is up to around 100 meters dependent on different parameters, such as environment.

[1] Also described as device password

Stored data on a device is a critical asset, because sensitive information, like configuration settings could be exposed to a malicious user if he\she gets access to this data.

Transmitted data is information sent across one of the wireless channels, and could be configuration data or user relevant identity data. This is data a potential intruder would be able to expose if he gets access to the radio link, source or destination.

The **configuration settings** are the critical data we want to protect against a potential intruder. These settings could be accessed either on a physical device or on the wireless channel.

The **PIN code** is the device password in our scenario. If an intruder gets access to the device password, it would be able to misuse the owner's identity and configuration settings and further get access to the wireless network on behalf of another users' identification.

The **authentication** between a user and the NFC system is an asset in form of information exchanged through this session. For instance public keys and session information, time stamp and so on could be misused by a potential intruder.

Personal privacy is user related information which is critical regarding each user's identification. Expose of such information could lead to tracing of guests at the hotel, and the intruder could further use this in different attacks and misuse identities.

Anonymity is closely related to the personal privacy. It is related to user's right to be anonym toward other users, but not towards the system.

4 SECURITY CONSIDERATIONS AND ANALYSIS

In figure 20, we show the layout of our analysis and solution part. First we evaluate the trust boundaries in the system (4.1) and show where the points of attack are for compromising the assets (4.2). Through an evaluation of possible threats, we describe a list of potential threats to the assets we want to protect (4.3, 4.4 and 4.5). In the risk assessment (4.6) we want to find the threats that oppose the highest risk in our system through an analysis of likelihood and impact. With this classification of threats and their risks we can then set up some requirements that we think the system should cover (4.7). In a proposed solution part (Chapter 5), we come up with different countermeasures that this system will have to consider to protect against what we have found.

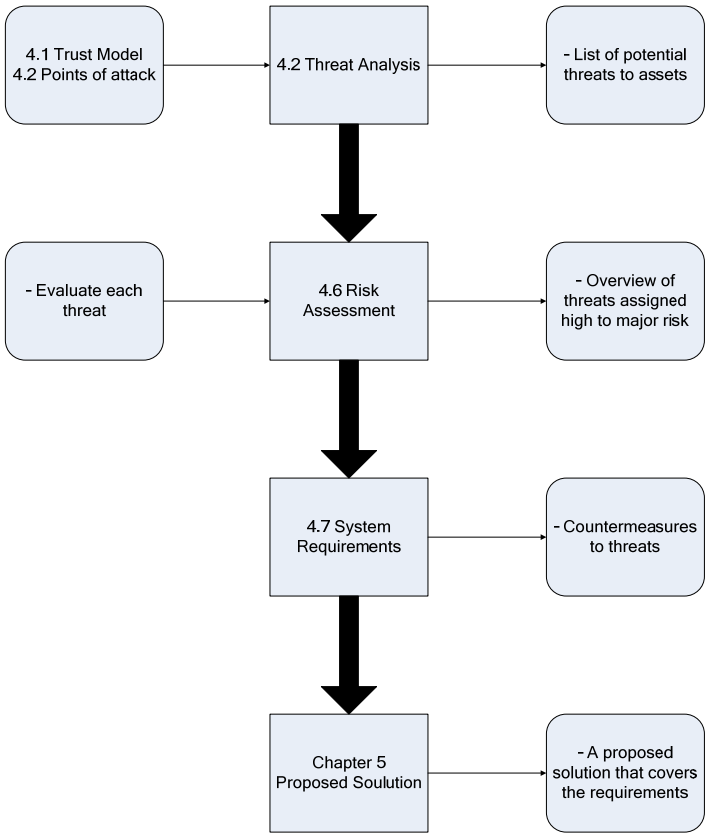
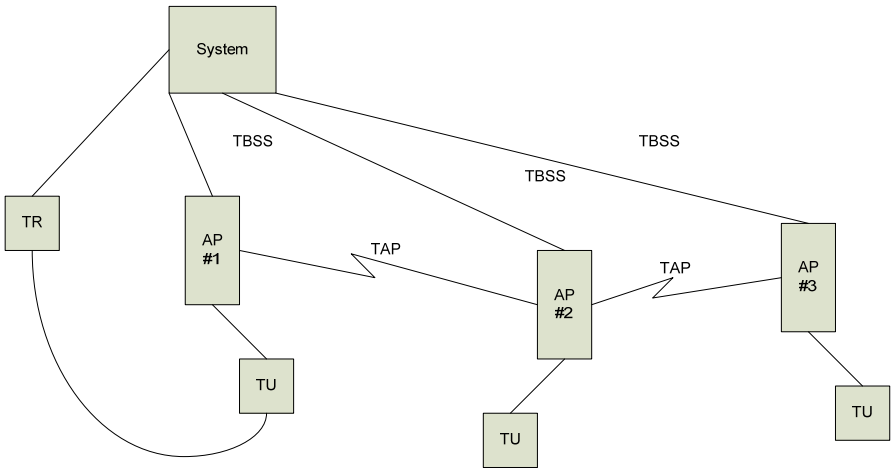


Figure 20 Progress of security consideration and analysis

4.1 TRUST MODEL

This sub chapter intends to describe the trust boundaries between the different entities in our system. With a networked group of computer systems, servers, access points and users, they share a trust. If one of these trust

boundaries is compromised, then the impact ripples throughout the entire system. In our system scenario there are several entities that must provide mutual trust when they are authenticated to each others. Figure 21 illustrate a simplified connectivity of trust between related entities in our system.



System – Rest of the system (see figure 16 – above Ethernet interface)
TBSS – Trusted Basic Service Set (A trusted system within one Access Point)
TAP – Trusted Access Point (Trust between two or more Access Points)
TU – Trusted User (A trusted user of the system)
TR – Truster Receptionist (A trusted receptionist at the hotel)

Figure 21 Simplified illustration of trust connectivity

In our system we have proposed five crucial trust boundaries between different entities. These trust connections are important for the security of our system. Lack of trust between one of these entities would increase the security and privacy level of the whole system.

Trust between the different entities is determined by whether a person matches the established criteria or not. This is discussed further in the five trust boundaries.

Trust between system and user is mainly regarded to the trust of the user involved in this system. The PIN codes and public keys create the trust between these entities. It is very important that the user is very careful with these credentials. The user must keep the PIN code secret, and not give the private key in the public key pair to anyone. It is also important to protect these data against potential malicious users. Also, it is important that the crucial information is stored securely in the system. The user must not share configuration settings with anyone else at any circumstances. This would harm the trust between these entities, and could be a potential treat to both the security and privacy to the system. Also the system must save identification data of the user securely.

Trust between receptionist and user is very important before any technical initiation starts. This trust boundary deals with the PIN code, where the receptionist generates and delivers it to a given guest physically. It also deals with all the other information about the guest, which is stored in a database. The receptionist has limited access to the system.

The criteria of mutual trust between the receptionist and user are that the receptionist is acting as a trusted and loyal employee. And that the user actually is a guest and not a random person with fake identity and so on.

Trust between user and access point includes the NFC session, where the cryptographic keys, PIN code and the configuration settings are exchanged. Because the access point and the built in NFC device are physical devices we consider as one. The initial part of a connection session in both the NFC and Wi-Fi session is the most critical one when it comes to trust. First the user must trust that it is actually the hotel's access point it is communicating with. When using the public key exchange in combination with the PIN code exchange, it is important that the user can trust the access point. But this is of course mutual, because the access point must be sure that it is the actual owner of the PIN code it is communicating with.

The criteria of mutual trust between the user and access point would be that the user actually is a legal user with its own identity and its own public keys and PIN code. Also, the user has to trust that it is a legal access point.

Trust between access point and system in our scenario, is considered to be a trusted path between the access point and the system. We consider this part of the system to be transparent.

Trust between the access points is considered as a trusted path, because of the same reasons as the trust path between an access point and the system.

4.2 THREAT ANALYSIS

The purpose of this chapter is to list possible security threats to the Wi-Fi NFC system, detailing what the threats achieve, how they are carried out and where in the system they could occur. The starting point is to look at what assets we want to protect (described in 3.4) and identify the points of attack; their access point, which will be evaluated later in the chapter.

The potential adversaries to a user and the network are outsiders wanting access to the network without being registered in the hotel database, but also other guests (described in 3.2.4). The motivation can be that they don't want to pay for access or they want to hide their identity towards the system, but also exploit user privacy or

preventing authorized users from connecting. Their goals can be to abuse others access rights to compromise the network, criminal activity or disrupt and destroy connectivity.

This figure shows us our architecture model with the points of attack that we have divided it into. The focus of this architecture is that we want to highlight the threats towards the use of NFC in such a system, and therefore we look closer into the NFC communication and the devices used. The rest of the interfaces and entities are being treated as other parts of the system.

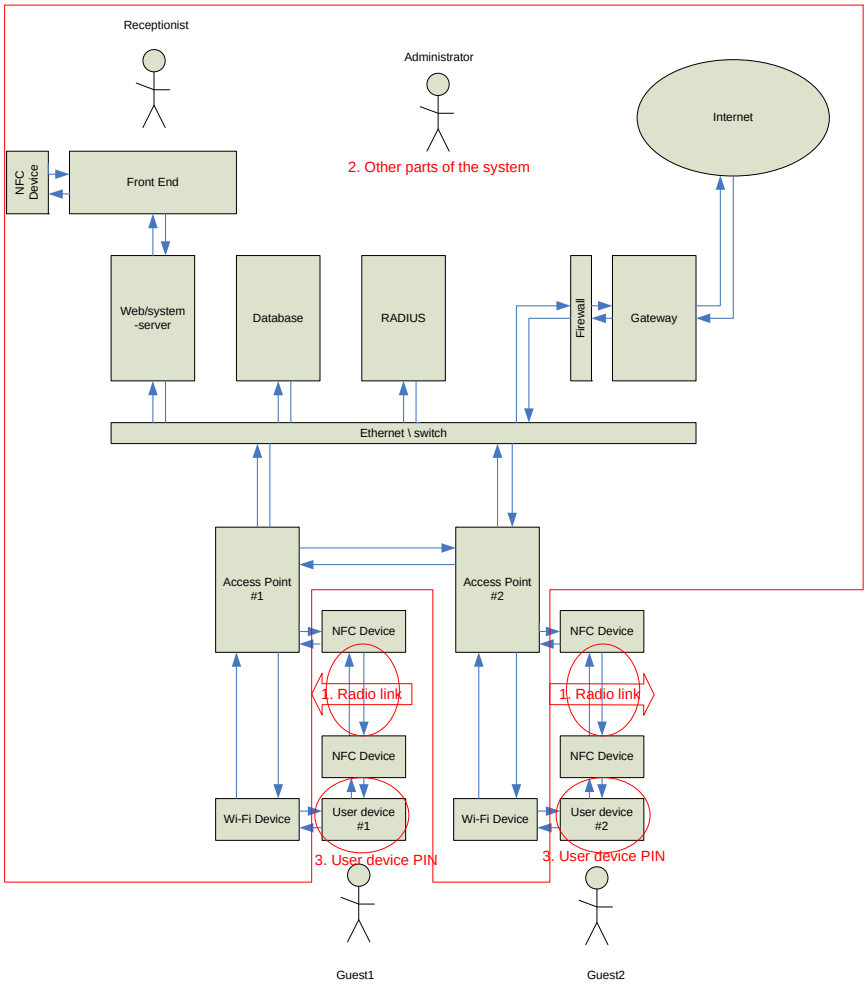


Figure 22 Potential threats in the network system

A number of security threats in these categories are subsequently treated in the remainder of this chapter according to the following points of attack shown in figure 22.

1. **NFC radio link**
2. **Other parts of the system**
3. **User device or PIN**

In the following subchapters we will assign an ID to every threat associated with attacks, and then place these in a table as a reference to each specific attack.

4.3 THREATS ASSOCIATED WITH ATTACKS ON THE NFC RADIO LINK

The radio link between the AP's NFC device and the users NFC devices represents a significant point of attack in the system, shown as point of attack number one in figure 21 and specified in figure 19. The threats are divided into the following categories that deals with the violation of the well known security issues of confidentiality, integrity and availability, which is described in the following subchapters.

- Unauthorized access to data
- Threats to integrity
- Denial of service attacks
- Unauthorized access to network

4.3.1 UNAUTHORIZED ACCESS TO DATA

These threats deal with the confidentiality issue of the sensitive data transferred, but also the control and signaling data. These sensitive data include device ID, configuration settings and PIN number. To accomplish this sort of attack, an intruder needs to have the right equipment. This is because of the limit in range that NFC is communicating over. Therefore, sophisticated equipment is needed, either through a big antenna to perform it from a greater distance or equipment in short proximity of the reader that can capture the signal, unnoticed by the user or the hotel personnel.

1a **Eavesdropping user data**: intruders may eavesdrop user data sent on the NFC radio link.

After the NFC connection is established all the sensitive information about the PIN and ID, but also the configuration settings of the network are transferred over this connection. If an intruder is able to eavesdrop on this link, all the assets will be compromised.

1b **Eavesdropping control and signaling data**: intruders may eavesdrop control data or signaling data on the radio link between the users NFC device and the AP.

When a user wants to establish a NFC connection, request and response messages from the users NFC device and the AP's NFC device are transferred. In these messages both their device ID is sent. If an intruder is able to eavesdrop this portion of the communication, the asset of device ID can be compromised, and further the compromise of both personal privacy and anonymity assets.

1c **Traffic analysis**: Intruders may observe the time, rate, length, sources or destinations of messages on the radio link to obtain access to information.

4.3.2 THREATS TO INTEGRITY

These threats are active attacks on the transaction of messages over the NFC channel. By achieving this, an intruder need to perform this before the answering device starts with the answer, this means that the answering device needs to answer after a long time to make this possible. The intruder has to have great knowledge and sophisticated equipment to successfully perform this, like in the eavesdropping attack. If these attacks are performed successfully, it can compromise all the assets exchanged over the NFC channel.

2a **Manipulation of user data**: Intruders may modify, insert, replay or delete user data on the radio link between the NFC devices.

2b **Manipulation of control or signaling data**: Intruders may modify, insert, replay or delete signaling data or control data on the radio link between AP's NFC device and NFC device.

4.3.3 DENIAL OF SERVICE ATTACKS

The threat of DoS attacks is always relevant to wireless systems. This will compromise the availability for a user and can also be destructive to the equipment. An attack like this will make it impossible for users to get configuration settings of the network. The intruder needs to have jamming equipment that sends a strong signal on the 13.56 MHz frequency, and can be performed against the NFC user device or the AP's user device.

3a **Physical intervention:** Intruders may prevent user data, signaling data and control data from being transmitted on both radio links by physical means. An example of physical intervention is jamming.

3b **Protocol intervention:** Intruders may prevent signaling data or control data from being transmitted on the radio link by inducing specific protocol failures. These protocol failures may themselves be induced by physical means.

4.3.4 UNAUTHORIZED ACCESS TO NETWORK

4a **Masquerading as another user:** An intruder may masquerade as another user towards the network. The intruder first activates the NFC device towards the user, and then tries to use his connection to authenticate.

4.4 THREAT ASSOCIATED WITH ATTACKS ON OTHER PARTS OF THE SYSTEM

This part of the system is left out of our thesis description and will not be analyzed or evaluated as mentioned earlier. This part is a regular wireless network that we have described as a trusted part of the system in this report. We will just make some references to RFC papers and other papers that deal with the security issues in the different parts of the system.

- Security Considerations for RADIUS [49] and [50]
- Security Considerations for AAA [51]
- EAP security [52]
- Hacking techniques in wireless networks [53]

4.5 THREATS ASSOCIATED WITH ATTACKS ON NFC DEVICES FOR USER AND AP OR PIN

These threats associated with attacks towards the NFC devices and PIN is either divided separately or in a combination. Both are physical entities, in that that the PIN number is given out to an authorized user on for example a little note or piece of paper and the user device is a handheld device with enabled NFC.

5a **Use of a stolen authorized user device:** Intruders may use stolen user devices to gain unauthorized access to network.

If an intruder is able to steal a user device that has authorized access, this means that the PIN is already pushed and have received the configuration settings. This can compromise all user data transferred on the radio link, but also sensitive information about the user.

5b **Use of a borrowed user device and PIN:** Users who have been given authorization to use borrowed equipment may misuse their privileges.

An authorized user with an authorized user device may lend its device to another user/intruder. In this scenario the intruder can expose and exploit the configuration settings and the access to the network.

5c **Use of a stolen PIN:** Users may use a stolen PIN to access network.

To get access to a PIN, the receptionist print out a number that will be associated with the device using it. If an intruder is able to steal this number before the authorized user actually associates its device with it, intruders can get access with its own device by using this PIN number.

5d **Manipulation of device ID:** Users may spoof the device ID of a user device and use a valid PIN with it to access network.

The intruder can spoof the device ID, the same way as MAC spoofing. The device ID is a unique ID for each NFC device, and with an eavesdropping attack on the radio link it is possible for the intruder to get access to the unique device ID and change its device ID to the authorized device. This is also possible by activating a passive user device. The intruder can take its device in close proximity of a user device and activate the device with request/response message where the device ID is transferred between the devices.

5e **Integrity of data on user device:** Intruders may modify, insert or delete applications and/or data stored on the user device. Access to the user device may involve breaching physical or logical controls.

5f **Eavesdropping the PIN number:** Intruders may eavesdrop the PIN number.

As long as the PIN is distributed on a physical entity, an intruder can glance or look over the shoulder of a user to see the PIN number and use this to activate its own device before the user activates his.

5g **Confidentiality of certain user data on the user device:** Intruders may wish to access personal user data stored by the user or the user itself want access after time expired on the user device.

Configuration settings and other sensitive information must be stored on the device, for access purposes. The threat here is that a user or intruder who gets access to this information can still use this after the contract of access is expired.

5h **Brute force on PIN number:** intruders may try to access network by guessing PIN number that matches the network.

As long as the device ID is associated with the personal information about a user in the system after it has been authorized with the PIN. An intruder can use its own device; walk up to the AP and trying to push PIN numbers until it succeeds. Users can choose when and where they want to authenticate their device. A PIN that has been issued, but not been used, can be associate to a device that is owned by an intruder.

Now that we have mapped out the threats we find relevant to the points of attack described, we show a table of which assets in the system that is compromised through the different threats.

Threat ID	Compromise of assets									
	Device ID	User device	Radio link	Stored data on device	Transmitted data	Configuration settings	PIN	Authentication	Personal privacy	Anonymity
1a	x		x		x	x	x		x	x
1b	x						x	x		
1c			x		x					
2a	x				x	x	x			
2b	x		x		x			x		
3a		x	x							
3b		x	x							
4a	x		x						x	x
5a	x	x	x	x	x	x	x	x	x	x
5b	x	x	x	x	x	x	x	x	x	x
5c						x	x	x		
5d	x		x		x	x		x	x	x
5e		x		x						
5f			x			x	x			
5g		x		x					x	
5h							x			

Table 3 Compromise of assets

We will now use this analysis to evaluate which threats that are of great risk to the system, and why they represent the risk level we assign to them through a risk assessment evaluation.

4.6 RISK ASSESSMENT

In this chapter the threats will be evaluated as regards to the combined likelihood of occurrence and severity of impact. The threat analysis and the assessment of risks has followed the procedure outlined in ETSI Technical Report ETR 332 [48], A practical approach to threat modeling [54] and Threat modeling as a basis for security requirements [55]. Extensive research on 802.11 threats and the assessment of risks has been done before by other researchers to great extent and is not the focus of the analysis. The assessment of risk will focus on threats that compromise the assets and the authentication process regarding NFC in a distributed system like this scenario is. Note that this evaluation is done from the situation as it is before any security mechanisms have been applied.

The table shows us how we evaluate the risk of each threat, and find the threats we analyze to be of high to major risk towards the assets we want to protect in the system. Table 4 is derived from the paper [60].

Consequence/ Impact/ Severity						
	5 Major	**5**	**10**	**15**	**20**	**25**
	4 Very high	**4**	**8**	**12**	**16**	**20**
	3 High	**3**	**6**	**9**	**12**	**15**
	2 Moderate	**2**	**4**	**6**	**8**	**10**
	1 Minor	**1**	**2**	**3**	**4**	**5**
	Value level descriptors	**1** Very unlikely Rare	**2** Unlikely Seldom	**3** Likely Occasionally	**4** Very likely Frequently	**5** Almost certain Often
	Likelihood/Frequency/Probability					

	Low Risk
	Medium Risk
	High Risk
	Very High Risk
	Major Risk

Table 4 Consequences, Impacts and Severities

With the threats associated with attacks on the NFC link, NFC devices and PIN we assign a value from the table on each threat and find its exposure value by multiplying them together. We then find the threats that we evaluate to be of high, very high or major risk to the system (12 – 25 in exposure factor). Impact value shows us how severely the system is compromised through what type of assets that can be extracted. Likelihood of occurrence shows us how easy the attack can be preformed and the probability of such an attack.

Threat descriptor	Impact value	Likelihood of occurrence	Exposure factor	Exposure ranking
1a	5	3	15	3
1b	4	3	12	4
1c	2	3	6	6
2a	4	2	8	5
2b	3	2	6	6
3a	5	4	20	1
3b	4	2	8	5
4a	4	3	12	3
5a	5	4	20	1
5b	5	1	5	7
5c	5	4	20	1
5d	5	1	5	7
5e	3	1	3	9
5f	3	1	3	9
5g	5	4	20	1
5h	5	4	20	1
5i	4	4	16	2

Table 5 Threat, Impact and likelihood of occurrences

These threats have been evaluated as high to major risk in the system from the points of attack described in the threat analysis. Here we will describe why we think these threats oppose the risk level we have associated them with. These threats will be our center point in the system requirements and proposed solution for the system.

1a **Eavesdropping user data**: intruders may eavesdrop user data sent on the NFC radio link. **(High risk)**

We have evaluated this threat to be 15 in exposure factor and represent a high risk. Because of the limited range in NFC, the success of this attack is very much up to the intruder's knowledge and resources. This is because the equipment needed is sophisticated. With the right equipment this attack is likely, and will have major impact, because of what the user data contain.

1b **Eavesdropping control and signaling data**: intruders may eavesdrop control data or signaling data on the radio link between the users NFC device and the AP. **(High risk)**

This threat is set to 12 in exposure factor and represents a high risk. This is because the exchange of device ID is done before the NFC connection is established. This can have very high impact on user privacy and can be exposed in a later session. To achieve this, an intruder needs sophisticated equipment, and great knowledge as in 1a, with these parameters in order this attack is likely.

3a **Physical intervention:** Intruders may prevent personal data, signaling data and control data from being transmitted on the NFC radio link by physical means. An example of physical intervention is jamming. **(Very high risk)**

This threat represents a 20 in exposure factor and is set to very high risk. This is because an intruder with the right equipment can jam the frequency both on the users and AP's NFC device to disrupt it from connecting or to destroy the equipment. This has major impact on the systems connectivity, but also the user device from accessing other NFC enabled entities.

4a **Masquerading as another user:** An intruder may masquerade as another user towards the network. The intruder first masquerades as an AP towards the user, then hijacks his connection after authentication has been performed. **(High risk)**

This threat is set to 12 in exposure factor and therefore represents a high risk in our risk assessment table. This is because an intruder can activate a device in passive mode if it is close enough. In this way the intruder can get access to a user's device ID, and can use this later in some form. This has very high impact on the user's device ID to be misused and is likely to occur. This is an active attempt in contrast to 1b which is passive.

5a **Use of a stolen user device:** Intruders may use stolen user devices and unauthorized access to network. **(Very high risk)**

This threat is set to 20 in exposure factor and represents a very high risk. The use of a stolen device represents a great impact on the assets we want to protect. This threat represents a great privacy risk especially, and lets the intruder anonymous access the system. The device is either authenticated or the intruder has to have a valid PIN, or it have to perform a brute force attack to discover a valid PIN.

5c **Use of a stolen PIN:** Users may use a stolen PIN to access network. **(Very high risk)**

This threat is set to 20 in exposure factor and represents a very high risk. A stolen PIN that has not been authenticated to the system will give the intruder access and will assign his own device to the personal data of a user in the system.

5f **Eavesdropping the PIN number:** Intruders may eavesdrop the PIN number. **(Very high risk)**

We have found this threat to be 20 in exposure factor and represent a very high risk. Intruders may take a glance or look over a shoulder when a PIN number is issued to a user, if it is physically handed out. With this PIN number an intruder can initiate connection towards an AP and push PIN and assign his device to this user, to get access to the network. To achieve this, the intruder has to use the PIN before the user does.

5g **Confidentiality of certain user data on the user device:** Intruders may wish to access personal user data stored by the user or the user itself want access after time expired on the user device. **(Very high risk)**

This threat is set to 20 in exposure factor and represents a very high risk as we see it. When the network settings are transferred to a user device, it will be stored in the device. If there is no time expiration of data stored on device, the probability that these settings will be accessed again after contract time is very likely. Also, the chance of disclosure is apparent.

5h **Brute force on PIN number:** intruders may try to access network by guessing PIN number that matches the network. **(High risk)**

This threat is set to 16 in exposure factor and represents a high risk. This is because anyone with an enabled NFC device can go up to an AP and initiate a connection. The PIN number is the way of authenticating device to user. If an intruder can try out as many PIN numbers as possible without getting noticed or rejected from the system, the chance of getting it correct is relatively big. The PIN is a random number generated by the system, and with typing a correct one it will attach this device to a random guest who has not carried out its authentication.

If we look at these threats described as high to major risk to the assets, we see that eavesdropping on the communication link between the different devices will compromise both privacy and security. Eavesdropping is a passive attack. With access to device ID, a PIN number and configuration settings gives an intruder direct access or the tools to achieve it. We see that physical intervention can be an effective attack, but this depends upon what the attacker wants to achieve. With physical intervention the attacker may want to disrupt the system or damage it. There is always a major risk of stolen equipment, user devices or PIN numbers. Here the responsibility lies in the hands of the user, but the system can do some precautions that we will look at in the next chapter 5.

4.7 SECURITY REQUIREMENTS

In this chapter we will list the security requirements as derived from the threat analysis and risk assessment. The requirements are set in connection to the treats that they cover and that we found to be of importance to protect the assets in the system. These requirements will make up for our proposed solution, where we tackle these issues to protect our assets. After each requirement we will describe which threats from our threat analysis that the requirements will cover. Many of the requirements will cover the same threats, but from different stand points and combinations.

4.7.1 REQUIREMENTS FOR CONFIDENTIALITY

To protect confidentiality on the NFC radio link, there have to be security implemented on the application layer, because NFC in itself doesn't offer any protection.

1 We want the network to protect the confidentiality of user data transferred over the NFC link.

This requirement will cover the threat of eavesdropping the user data on the NFC link described in threat 1a from the threat analysis and protect device ID, radio link, transmitted data, configuration settings, personal privacy and anonymity shown in table 3.

2 We want it to be possible for the user to check whether or not his user data is confidentiality protected. This should require minimal user activity.

This requirement will also cover the threat of eavesdropping user data on the NFC link described in threat 1a from the threat analysis and protect the same assets as in requirement 1.

3 We want to protect the confidentiality of certain signaling data and control data on the NFC link.

This requirement will cover the threat of eavesdropping signaling and control data described in threat 1b and traffic analyses described in threat 1c over the NFC link and protect the assets of device ID, transmitted data, radio link, PIN and authentication shown in table 3.

4 We want to protect the confidentiality of user-related data stored by the user on the user device.

This requirement will cover the threat to integrity of data on user device and confidentiality on certain user data on the user device described in threat 5e and 5g, and will protect the assets of user device, stored data on device and personal privacy shown in table 3.

4.7.2 REQUIREMENTS FOR INTEGRITY

To protect the integrity between the data exchanged on the NFC radio link, there have to be security implemented from the application, because NFC itself doesn't offer any protection. Some of these requirements cover threats that aren't set to high risk or more, but are part of the application protection and will therefore be treated.

5 We want to protect against unauthorized modification of user data on the NFC link.

This requirement will cover the threat of manipulation of user data described in threat 2a and protect the assets of device ID, transmitted data, configuration settings and PIN derived from table 3.

6 We want to protect against unauthorized modification of certain signaling data and control data on the NFC link.

This requirement will cover the threat of manipulation of signaling and control data, but also the threat of protocol intervention described in threat 2b and 3b, and protect the assets of device ID, user device, radio link, transmitted data and authentication shown in table 3.

7 We want to protect against unauthorized modification of user data stored on the user device or to the PIN number.

This requirement will cover the threat of integrity of data on user device described in threat 5e, and protect the assets of user device and stored data on device shown in table 3.

8 We want to ensure that the origin and integrity of applications and/or data downloaded to the user data can be checked. It may also be necessary to ensure the confidentiality of downloaded applications and/or data.

This requirement will cover the threat of confidentiality of certain user data on user device described in threat 5g, and protect the assets of user device, stored data on device and personal privacy derived from table 3.

9 We want to ensure the origin, integrity and freshness of authentication data.

This requirement will cover the threat of eavesdropping on signaling and control data, but also modification of signaling and control data. These threats are described in threat 1b and 2b, and will protect the assets of device ID, transmitted data, radio link, PIN and authentication shown in table 3.

4.7.3 REQUIREMENTS TO USER DEVICE AND PIN NUMBER

10 We want to control access to a PIN number so that it can only be used to access the network by the user to whom it was issued or by users explicitly authorized by that user.

This requirement will help cover the threat of use of stolen authorized user device and eavesdropping the PIN number described in 5a and 5f, and if successful will protect every asset described as shown in table 3. The threat of stolen devices is something the system itself can't protect itself from; therefore in reality this requirement will not protect every asset described.

11 We want to blacklist particular user devices from accessing the network.

This requirement will help cover the threat of stolen authorized user devices, stolen PIN and manipulation of device ID described in 5a, 5c and 5d. This will help protect all assets described as shown in table 3. This requirement also helps with the issue of stolen devices, but not alone as a final protection.

12 It shall not be possible to get access to a PIN that is only intended to be used for one specific user device.

This requirement also tackles the same threats as in the prior requirement, but covers more the PIN issue of the problem.

13 A valid PIN shall be required to access the wireless network.

This requirement covers the threat of a stolen PIN described in threat 5c, and will help protect the assets of PIN, configuration settings and authentication as shown in table 3.

4.7.4 REQUIREMENTS ON SECURITY ON THE SYSTEM

14 It shall be possible to prevent intruders from obtaining unauthorized access to the network by masquerading as authorized users.

This requirement cover the threat of masquerading as another user and use of stolen PIN described in threat 4a and 5c, and will protect the assets of device ID, radio link, configuration settings, PIN, authentication, personal privacy and anonymity as shown in table 3.

15 It shall be possible for users to be able to verify that the AP are authorized to offer configuration settings on behalf of the hotels wireless network at the start of, and during, initiation.

This requirement cover the threat of traffic analysis and masquerading as another user described in threat 1c and 4a, and will help protect the assets of device ID, radio link, transmitted data, personal privacy and anonymity shown in table 3.

16 It shall be possible to prevent intruders from restricting the availability of the radio connection by logical means.

This requirement will cover the threat of physical and protocol intervention and brute force attack on PIN number described in threats 3a, 3b and 5h. This will help to protect the assets of user device, radio link and PIN derived from table 3.

We have now assigned the threats to the requirements we want to tackle in our proposed solution.

5 PROPOSED SOLUTION

This chapter will propose solutions that cover the requirements set to our system in 4.7. These requirements will be set to the proposed solutions in form of a table 6 first, and then be described in the following sub chapters. As we see from the table, many of these solutions cover the same requirements. This is because many security and privacy issues overlap each other, and cannot be reviewed as simple incidents that only need one solution to be solved. That is why security and privacy for a system or technology is a complex matter in regard to all the factors that have to be evaluated and processed.

Proposed solution	Covered requirement
Control NFC activation in user device	4, 14
Dynamic Identifier	14
Securing data over the NFC radio link	1, 2, 3, 4, 5, 6, 7, 8, 9, 15
Rejection of unwanted devices	11, 12, 16
Expire of data	4
Register device ID at check-in	10, 13

Table 6 Proposed solutions with covered requirements

5.1 CONTROL NFC ACTIVATION IN USER DEVICES

In user devices the NFC protocol initiates a connection session automatically when the NFC interface is activated by another NFC device. This could be a problem if user device get activated unknowingly by an intruder with intent. To prevent this activation we propose a feature an activation button for single connections. This could be an optional feature that the user can control itself. This function could be implemented as follows:

If we want to activate the NFC interface in each single connection, the NFC 18092 protocol shall be manually started if the user chooses to do so. The NFC device shall be set to a SENSE state. When the SENSE state is set, the device shall be powered. It than shall recognize the SENS_REQ or ALL_REQ commands as specified in the 18092 standard [8]. With this solution, a user will never be automatically connected to other devices, unless he or she is aware of it. This would be an optional security feature to avoid involuntary activation and read-out.

5.2 DYNAMIC IDENTIFIER

When a connection between NFC devices is initiated, the unique identifier of each device is being sent across the radio channel. This could lead to a serious security and privacy problem. Therefore we propose the use of dynamic identifiers.

A dynamic identifier is a Pseudo Random generated Identifier (PRI) which is a generated random sequence that is different and statistically independent from the original device ID. A pseudo-random sequence is a sequence that is not completely random, but very hard to distinguish from a true random sequence. A pseudo-random sequence is also difficult to predict, because the first few elements of the sequence is very difficult to determine [56].

One important reason for using pseudo random identifier is that it's desirable to make communicating devices anonymous to improve privacy. Instead of using the static identifier (such as DiDi and DiDt -address) we instead make use of a long, random identifier. Each communication device bases their identification on a local pseudo random generator. This would make identification very hard for every participant in a communication sequence and prevent tracking of devices [56].

The implementation of NFC proposed so far exchanges the unique ids between the communicating devices. This exchange will be improved by this solution. This is to prevent the probability of getting logged (tracked) at several static nodes in different network access systems.

5.2.1 PSEUDO RANDOM GENERATED IDENTIFICATION

The PRI would be able to replace the physical identifiers in the current system, but should be a voluntary setting. This is because visible hardware identifiers could be mandatory in some functions.

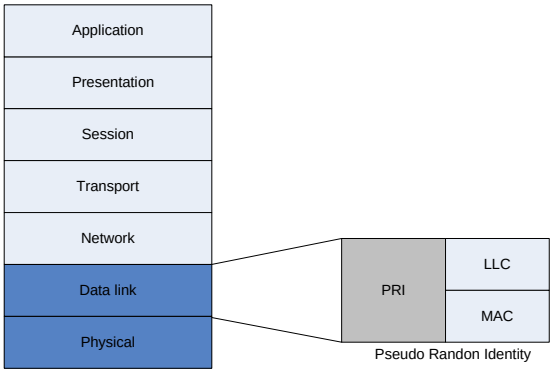


Figure 23 PRI in the OSI model

The PRI should be implemented in the OSI-model at the same layer as the existing DiDi and DiDt addresses (layer 2), in order to let the medium know where to deliver data packets. In Figure 23 we have added PRI in layer two in addition to the existing MAC and Logical Link Control (LLC) to keep compatibility. The PRI layer is pretty much the same as the MAC layer, but it could vary in length. The value should not indicate anything in order to enforce anonymity. The use of PRI layer could be thought of as a DiDi and DiDt address. The random identifier shall be randomly generated often enough to maintain privacy for the user, but also within a time frame where the system

can block unwanted devices, as described in chapter 5.4. This means that a condition for devices that has implemented PRI, will not be able to generate 3 different randomized identifiers within 3 seconds, but 1 unique random identifier every 5minutes.

In this proposed sub solution there is no needs of extra collision preventions, because this is already integrated in the NFC protocol with the use of a random value beside the unique identifier. This means that the random identifier could be identical to the random value, but the probability of that is low according to our estimates. If this coincidence occurs the collision handler in the NFC protocol will initiate and solve the problem.

5.3 SECURING DATA OVER THE NFC RADIO LINK

As mentioned earlier the purpose of the secure side channel is to safely exchange critical initial data. When the NFC devices are connected to each other on the wireless radio link, the idea is to exchange public keys to ensure encrypted information flow over the radio link. It is also important that the communication participants can be sure of whom they are communicating with. We propose to implement cryptography in the entire procedure of the authentication procedure over the NFC channel.

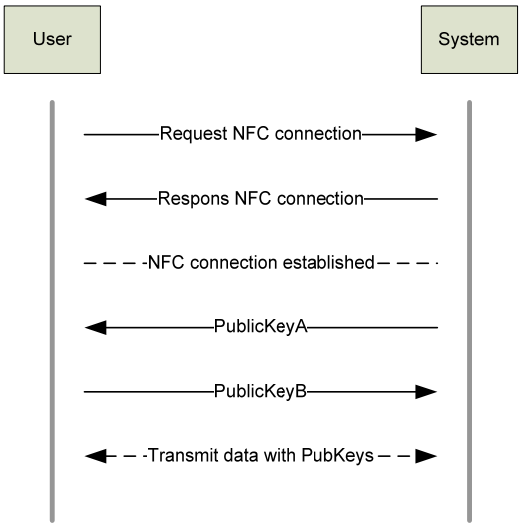


Figure 24 Information flow when implementing NFC as a secure side channel with exchange of public keys

Figure 24 illustrates a session where a User is initiating a NFC communication and activates the NFC protocol. The System then responds with an “acknowledge” message. The first three steps are identical with the ones illustrated in figure 19 in chapter 3.3. When the NFC connection is established, the system (target from the NFC initiation

session) then initiates a public key exchange session. When this is done, the communication participants can start a secure communication over the NFC channel.

The public key is mathematically related to the private key, but it should not be possible to deduce the private key from of public key(s). The private key is kept secret, while the public key may be distributed. This is called public key cryptography, and is an asymmetric encryption method, which is discussed in chapter 2.8.5.

When communication participant's exchanges critical data over the NFC channel, it shall include the use of a random value, public keys and certificates. The User shall generate a random number (Rand. r), add digital signature (d), and finally encrypt it (e) and send it to the System. The System must be the owner of the public key the User received and used for the encryption. If so the System is able to decrypt the data transmitted by the User. If the System doesn't send its own public key to the User, it would not be able to decrypt and can't give the correct response to the User. The System adds +1 to the received random number (r+1), adds its digital signature (d) and finally encrypts it (e). Then it sends it back to the User. The User is the one who initiated the secure communication, and knows its public key. If the User is able to decrypt, and the random number is increased by one (r+1), the challenge response procedure is correct. The User now knows for sure that it is the System that it communicates with.

When adding the digital signature, one can verify each other's keys with just one challenge response since the digital signature is related on the private key. In that way, the System is able to see if the User gives him the right key in the challenge response, even if the User is the one who initialized the challenge. (The User is the one who wants to verify the System's key, and with digital signature the System is able to verify the User's key at the same time.)

The cryptographic mechanism in the pairing process has also been implemented in the proposed WPS specification, but do not include the random number and the certificates. Such supplement of security mechanisms would increase the security.

5.4 REJECT UNWANTED DEVICES

To prevent disturbance and unwanted devices to connect to the NFC enabled AP, we propose a solution where the system can reject and blacklist devices. This could be devices which try to connect to the system within a given time frame. For example, a device that tries to connect to the system 3 times or more within 5 seconds shall be rejected from the system and can't connect within 10 minutes.

The system shall reject or blacklist unwanted user devices based on the identifier of the device. This could either be the unique device identifier or the random generated identifier described in chapter 5.2. This shall be managed in the initiation of a NFC session, where the system receives a connection request. The system shall check the identifier of the initiator up against its blacklist and reject a connection if the identifier is found. The system can also register devices that act suspicious. The NFC 18092 standard has already implemented an identifier exchange in the initiation part of the protocol. A check of device ids is needed before the system responds to the user's request. A check like this would be implemented in the software part of the system device.

5.5 EXPIRE OF DATA

This solution is not related specifically to the NFC part of the system, but will protect the asset of configuration settings. When a guest at the hotel receives the configuration data to the WLAN, there must be an expire-time value on the configuration data and cannot be used when the expire-time period has passed. This is to prevent misuse of the configuration data after a guest checks out of the hotel.

This solution can be solved in combination with the well known lease timer in the DHCP server, where the guest's device will get new releases until the he checks out. This can be solved with a manual operation, or an automatic timer that releases the user device from the network. Also the data exchanged from the system (the access point) should be inactivated and deleted from the user device. The expire-time on the specific configuration data shall contain a field that specifies deletion of the configuration data. This can be solved with the well known time-to-live value.

5.7 REGISTER OF DEVICE ID AT CHECK-IN

To connect the user device with the personal information about a guest, we propose that the front end desk has access to a NFC reader. With this reader, the receptionist registers the user device with its device ID at check-in. This means that when the guest arrives at the hotel, and wants access to the hotel network, the receptionist swipes the user device of the guest and register the device ID. The system then stores it in the database, and connects it to the personal information about the guest. This will make it impossible for an intruder to associate its own device to an authorized user, because a PIN will then be generated and associated to these unique ID connections. A stolen PIN, eavesdropping of PIN or a brute force attack on PIN cannot be accomplished without the registered user device, because there will only be one unique device ID to this PIN number.

This is a very simple and easy way to pair device with person, because the process done by the receptionist is only to exchange the request/response messages containing the device ID. The NFC reader can only be accessed and used by the hotel receptionists.

6 DISCUSSION

The master thesis definition states our research area to be security in NFC with WPS as a use case. This means that we have looked at the security in NFC when network settings will be transferred over a NFC radio link. WPS is a proposed application that can be used for this purpose. Choosing a scenario where this can be of interest to research, we have proposed a scenario at a hotel. A hotel is where many people come and go. We build system architecture for this scenario, taking into account all the different parts to analyze. Many hotels today offer Wi-Fi access and our work could help the evaluation of implementing such a solution. Taking this all into consideration, we feel that we need to give a threat analysis of this new part to the 802.11 network. These mean threats to the NFC radio link and to the devices used for this link, but also the process of authenticating devices through this link.

First we discuss our findings in the threat analysis. With a new wireless technology, the wireless transfer channel is always exposed. Though the range between the two devices is minimal, making it harder to get access to than other wireless connections, it is still open for attacks and must be considered. Another issue with this radio link that is considered is that the protocol offers no security mechanisms to protect the communication. This is up to the applications issuers, according to the NFC forum [3]. We find therefore violation of confidentiality and integrity to be present, through eavesdropping, traffic analyze and manipulation of data. How this is possible is described in [40], and the methods to perform these attacks must be developed. Through building the system architecture, we also describe all the assets we want to protect in the system. They are the crucial data that we don't want to be exposed. One of the well known threats to wireless communication is denial of service attacks, and NFC is not different. Disruption, damage and system operability is in jeopardy, so this threat is very relevant. Last, but not least we also see the threat of masquerading a device as another user. A NFC device gets automatically activated when it is in close proximity of other devices. This is a weakness and a threat in that an intruder can get access to one asset we want to protect in the system, namely the device ID which is used to link device to person in this network.

We are aware of the threats to assets in other parts of the system, but this is out of our research area. What is directly related to the use of NFC technology is the device in hand or the device integrated in the AP. The threat of stolen devices that are already authenticated is of course a major risk, but this is more a matter of a personal reasonability that the system or the device itself can't protect itself from. We also mention the possibility of exploiting borrowed equipment. Also, the threat of exploiting confidentiality and integrity in devices is relevant, because the network settings must be stored in the device somewhere, and can be read out or manipulated with.

The last category of threats we have decided to analyze is the threat of compromising the authentication of devices. In our proposed scenario, we have decided that a PIN is the device password for authentication. This is a well known method to use in many different systems. The threats to PIN are of course the threat of knowing or learning the PIN and use it before the righteous owner. If this is the only way to authenticate the device and link it

to the person, then this is maybe the biggest threat to access the network settings. Another threat is brute force attacks.

Through this analysis of different threats we then come to our risk evaluation. We have here tried to consider the different threats in proportion to the assets that can be compromised. That means the impact it has on the system and likelihood of occurrence. We found here that the major threat to the radio link is eavesdropping, because if this is successfully performed all assets we want to protect will be compromised. As mentioned earlier, the radio link has no protection to begin with. We also see that the threat to integrity is present, but the main aim for an intruder is to gain access to the network, and therefore getting all information about authentication and configuration settings through eavesdropping is of a greater risk. Denial of service attacks are also a risk to the system. Assets cannot be read out, but the whole system in terms of availability is at risk. We also set theft of ether device or PIN to a great risk. As talked about, access to the assets is almost avoidable. The threat of keeping network settings stored on device, which we call confidentiality of data on user device is also a great risk we have found. This is because if the guest has checked out, the hotel doesn't want him to still have access to network. The possibility of exploiting this information is very real. There are several threats that we have evaluated to be of medium to minor risks. These threats are not considered and are not the center of our further work, but could be covered in solutions. Now we have discussed the threats we consider and what we will try to solve in a proposed solution, but first discuss the requirements we want to set to the system, in an attempt to solve many of these threats and attacks that we find the NFC part of the network is open for.

To minimize the probability for attacks on the NFC radio link, we want to protect both confidentiality and integrity of data transferred over this channel. Also, we want to protect the confidentiality and integrity of the data stored on the device. This is to prevent the use of the network after the contract has ended, but also to prevent the network settings to be leaked to other unauthorized users. Now that we have assigned some requirements to the radio link, we want to protect the system from unauthorized authentication. We assign requirements for use of PIN, in that only authorized users will get access with the right PIN. This means that intruders can't use a valid PIN and assign their own device to the network. Also, an intruder can't use brute force to guess a valid PIN, and get access through another user. Another issue to deal with is brute force or flooding of the channel. There is a need to have a requirement where the system can blacklist some devices from accessing. Also, a requirement that doesn't regard the system, but more a protection for the user device, is that an intruder can't activate another device without the user's knowledge.

Now, that we have looked at the threats, risks and requirements we have assigned to our proposed system within the confinement of NFC, we will now discuss our proposed solutions. They will try to cover and protect against these issues raised. We want to cover the requirements of protecting confidentiality and integrity of data transferred over the NFC channel. We propose to encrypt the data flow over the radio link, with the use of random values, public keys and certificates. This will make the data unreadable for an eavesdropper, and uphold the

integrity of data transferred. This process would have to be assigned to the application, because as stated earlier the NFC protocol has no security implementations. WPS also propose a similar way to secure the NFC radio link in their description [27]. That may solve many of these issues described with strong encryption, but without the use of certificates that we propose in our solution. To protect against the use of network settings after contract expiration, we propose an expire-time value on the configuration data which will make the configuration data useless when expire period has passed. This means that when contract time is passed this data will delete itself automatic, so that access to this will not be possible. This solution is not related to NFC especially, but will protect the assets related to the system. Another solution to the requirements is to be able to reject certain devices from accessing or trying to access and blacklist them in the system if unwanted behavior occurs. In the initiation process the unique ID is exchanged, and the system can then check if this ID is listed or not. If so it can reject its attempt. This check will have to be implemented in the application layer of the system. In the case of the requirement of protecting user device from being activated by unwanted devices, we propose the possibility of an activation button on user device, where the user controls when and who he wants to communicate with. This will give a user more control over its own device, and also a more responsible role for accidental encounters.

Finally we will discuss some issues regarding temporary IDs versus device ID. We propose a solution to use PRI (Pseudo Random Identifier) as described in 5.2, where users can protect their device ID from being read and misused by intruders. A random sequence is used to hide the device ID. This is a good way to protect privacy and anonymity, and prevent tracking of device ID in a future communication. In this scenario, this solution may not be the best solution towards protecting authentication of devices. Therefore, we also propose a solution where the receptionist registers the guest's device when he checks in. This means that when the guest arrives at the hotel, and wants access, the receptionist swipes his personal device through a NFC reader, like they do with the credit card, to record the device ID in the system. This ID is then linked to his personal ID and a PIN is generated from both this unique identifiers. This means that no other device can associate itself to this PIN, and will solve many of the threats to PIN and the authentication. A relevant question to ask is maybe why not giving him access immediately when the receptionist registers his device. This could be a solution, but we want to give the guest the freedom of choosing when or where he decides to access, and maybe there is a cost issue in that he doesn't need or want to pay for access right away. This gives the guest an optional choice.

There are probably other solutions to the requirements we have assigned to the system, but this is solutions both to system in question and to the implementation of NFC technology and its applications in devices to consider.

7 CONCLUSION AND FURTHER WORK

7.1 CONCLUSION

The title of the thesis “Security in NFC with Wi-Fi Protected Setup as a use case” is a broad and complex area of research. We have discussed this topic with some of the security experts in the field, Professor Vladimir Oleshchuk and PhD. Geir Køien from UiA to find the right approach to cover both the thesis title and description. We choose to select a specific scenario where we do a security analysis of NFC technology incorporated in an 802.11 network for a hotel. Here we describe our proposed scenario and build our system architecture, and examine the assets that the system wants to protect. The NFC technology is introduced into this environment as a secure side channel for first time connection to a network. This gives the thesis a unique look at the security and privacy issues that is considered. With NFC as a secure side channel for initiation, authentication and exchange of network settings, we have performed a security analysis that must be considered before any implementation strategies will take place. Like any other wireless technologies, a threat analysis and requirements have been done. Before the analysis, a comprehensive research of the topic has been done. Security considerations are a complex and difficult area to cover, and to consider a new technology that has not been implemented yet in most devices is challenging.

Most papers today don’t discuss the security aspect of the NFC technology. Some have looked at these issues in general [40], [58]. By integrating NFC into a wireless network for a hotel is what we have looked at. We have found out that NFC also is up against many of the same threats that other wireless technologies face. The advantage for NFC is that it is a short range communication standard. This means that the distance over the air is compromised to less than 10 cm. On the other hand there is no security in its standard and it is up to the application to provide it. That is why we have found that the threats to confidentiality and integrity are very relevant. Also, denial of service attacks can be performed. We have also found threats to the device itself and to the authentication process that can cause problems in a scenario like this. In a hotel context there are many encounters between people and technology. We have found some solutions that can deal with the threats we have analyzed. Many of them are simple to implement, and many will maybe already be implemented when NFC becomes a trusted technology for mobile devices. There are many issues which will still be up for debate, but we have proposed some solutions that can improve security or be developed further.

What we contribute to this research area is to incorporate the NFC technology into an 802.11 network and represented a comprehensive threat analysis of our scenario. We have evaluated the risks of these threats and proposed requirements for the system to protect the assets. Finally, we have proposed some solutions that will further protect both the system and user.

7.2 FURTHER WORK

Since there is no prototype made for this system, the first thing to do should be to implement a formal model which could be used to eliminate the logical errors and do the fine adjustments. SDL [62] or Promela [63] should be well suited methods for such purpose. The SDL would make it possible to simulate the functionality process from start to end of processes, while Promela would make it possible to verify the logic of a system.

A formal model for the proposed solution should consist of typical WLAN and NFC properties in additional to the added functionality in the proposed solution. After making sure that devices are able to exchange information with each other as proposed and the added functionality in the solution works, one might start the testing. Security and privacy is the vital parts, and by attacking such a model with logical expressions (e.g. Promela) one could be able to discover and solve security or privacy weaknesses. With a formal model like this, one might be able to “attack” the proposed framework described in the thesis. The use of formal methods is an efficient way of testing abstract system-models for eliminating critical bugs, errors and weaknesses, but such methods takes a lot of time. Further, a simulator or a model at a lower level could be made in order to evaluate the performance aspects, and maybe optimize it if possible.

8 BIBLIOGRAPHY

This chapter includes all references used throughout this thesis in ascending order related to the pages the references are used in. Some references have an access date, which is related to the last accessed date on the internet. Other references have no access date, and are typical books or papers.

#	Description	Access date
[1]	J. Collins, "ABI Research Insight: No OTA, No NFC," http://www.abiresearch.com/, 10 2007.	25.01.08
[2]	RFID Journal www.rfidjournal.com	25.01.08
[3]	NFC Forum www.nfc-forum.org	25.01.08
[4]	FeliCa webpage by Sony www.sony.net/Products/felica/	27.01.08
[5]	Mifare webpage by NXP\Phillips www.nxp.com/products/identification/mifare/	27.01.08
[6]	14443 standard ISO, Identification cards - Contactless integrated circuit(s) cards - Proximity cards - Part 1: Physical characteristics (ISO/IEC 14443)	-
[7]	Sony Develops New Close Proximity Wireless Transfer Technology "TransferJet". Published by Sony Corp.Info, www.sony.net/SonyInfo/News/Press/200801/08-002E/index.html	25.01.08
[8]	ISO, Information technology - Telecommunications and information exchange between systems - Near Field Communication - Interface and Protocol (NFCIP-1)	-
[9]	ISO, Information technology - Telecommunications and information exchange between systems - Near Field Communication Interface and Protocol -2 (NFCIP-2)	-
[10]	International, Standard ECMA-340 2nd edition / December 2004 (NFCP-1)	-
[11]	ETSI, Near Field Communication (NFC) IP-1;Interface and Protocol (NFCIP-1)	-
[12]	NFC Forum, Specifications www.nfc-forum.org/specs/	28.01.08
[13]	ISO, Information technology -- Telecommunications and information exchange between systems -- Near Field Communication Interface and Protocol -2 (NFCIP-2)	-
[14]	Ecma International, Standard ECMA-352 Near Field Communication Interface and Protocol -2 (NFCIP-2)	-
[15]	ETSI, Near Field Communication Interface and Protocol-2 (NFCIP-2)	-
[16]	ISO, Identification cards -- Contactless integrated circuit cards -- Vicinity cards -- Part 2: Air interface and initialization (ISO/IEC 15693-2)	-
[17]	Jochen Schiller, Mobile Communication second edition, Addison-Wesley 2006 (ISBN 0-321-12381-6)	-
[18]	Jochen Schiller, Mobile Communication second edition, Addison-Wesley 2006 (ISBN 0-321-12381-6) page 210	-
[19]	Jochen Schiller, Mobile Communication second edition, Addison-Wesley 2006 (ISBN 0-321-12381-6) page 208	-
[20]	RFC2138,RADIUS, www.rfc-archive.org/getrfc.php?rfc=2138	10.02.08
[21]	Wi-Fi Planet, AAA with RADIUS server image, www.wi-fiplanet.com/img/2008/08/Tutorial%20-%20Geier%20E%20-%201051%20-%20Figure%201.png	10.02.08
[22]	Wi-Fi Planet, Interworking of an 802.1x RADIUS Server Setup, www.wi-fiplanet.com/tutorials/article.php/3764186	10.02.08

[23]	Kurose, Ross, Computer Networking, Pearson Education 2005 (ISBN 0-321-26976-4) page 720	-
[24]	Securitysceptic.com, 802.1x message exchange, www.securityskeptic.com/ieee8021xandeap.htm	15.02.08
[25]	IEEE 802.1x EAP over LAN\WLAN Authentication and Key Management, www.javvin.com/protocol8021X.html	15.02.08
[26]	RFC2284, EAP, www.ietf.org/rfc/rfc2284.txt	15.02.08
[27]	Wi-Fi Alliance, Wi-Fi Protected Setup Specification version 1.0h, Dec 2006	-
[28]	Jason I. Hong, Jennifer D. Ng, Scott Lederer and James A. Landay: "Privacy RiskModels for Designing Privacy-Sensitive Ubiquitous Computing Systems", ACM,2004	-
[29]	Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge.: "Location Disclosure to Social Relations: Why, When, & What People Want to Share" ACM, 2005	-
[30]	Wikipedia, Data Privacy, http://en.wikipedia.org/wiki/Data_privac	28.02.08
[31]	Ari JUels, RFID Security and Privacy: A Research Survey, RSA Laboratories, 2005	-
[32]	M. Jakobsson and S. Wetzel. Security weaknesses in Bluetooth., Springer-Verlag,2001	-
[33]	Mark Stamp, Information Security, Principles and Practise, WILEY2007	-
[34]	Perlman, R.:"An overview of PKI trust models" IEEE Network,1999	-
[35]	Stinson, Pellissier, Andrews, Defining and Applying Genereic Trust Relationships in a Networked Computer Environment, 2000	-
[36]	http://en.wikipedia.org/wiki/Anonymity	28.02.08
[37]	Airsnort Webpage, http://airsnort.shmoo.com/	28.02.08
[38]	ManageEngine, Wireless LAN Security, http://manageengine.adventnet.com/products/wifi-manager/wireless-lan-security.html	01.03.08
[39]	Stallings, Brown, Computer Security Principles and Practice, Pearson Education 2008 (ISBN 0-13-600424-5,978-0-13-600424-0)	-
[40]	Haselsteiner & Klemens Breitfuss, Philips Semiconductors, Security in Near Field Communication (NFC) Strengths and weaknesses, Ernst 2007	-
[41]	NFC devices: Security and Privacy, Gerald Madlmayr & Josef Langer, 2008	-
[42]	Security associations for personal devices, N. Asokan, Nokia, 2007	-
[43]	Personal device integration, content access and simple pairing procedures, Øystein Sandnes, UNIK, 2008	-
[44]	Bluetooth network vulnerability to disclosure, integrity and denial of service attacks, Keijo Haataja, UoK Finland, 2005	-
[45]	Wireless Network Security, Tom Karygiannis & Les Owens, NIST SP 800-48, 2002	-
[46]	Wack,Cutler,Pole, NIST, Guidelines on Firewalls and Firewall Policy	-
[47]	ETSI, HCI support for NFC, http://www.eetindia.co.in/ART_8800507301_1800001_NT_3dc4ea6f.HTM	15.03.08
[48]	ETSI, ETR332, Security requirements capture	-
[49]	IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines RFC 3580	-
[50]	Remote Authentication Dial In User Service (RADIUS) RFC 2865	-
[51]	Guidance for Authentication, Authorization, and Accounting (AAA) Key Management RFC 4962	-
[52]	EAP Security, Extensible Authentication Protocol (EAP) RFC 3748	-

[53]	Hacking techniques in wireless networks, www.cs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm	-
[54]	Tom Olzak, A Practical Approach to Threat Modeling, March 2006	-
[55]	Suvda Myagmar Adam J. Lee William Yurcik, University of Illinois, Threat Modeling as a Basis for Security Requirements	-
[56]	Wikipedia, Pseudo Random Number Generator, http://en.wikipedia.org/wiki/Pseudorandom_number_generator	-
[57]	GSMA, mobile NFC technical guidelines, November 2007	-
[58]	Madlmayer, Langer, Kantner, Scharinger, FFG, NFC Devices: Security and Privacy, 2008	-
[59]	JiWire Wi-Fi Advertising Network, Wi-Fi Finder and Hotspot Directory, jiwire.com	25.01.08
[60]	Risk Management, 2005, www.deat.gov.za	20.03.08
[61]	Wi-Fi Alliance. *Wi-Fi CERTIFIED™ for Wi-Fi Protected Setup: Easing the User Experience for Home and Small Office Wi-Fi® Networks*. Wi-Fi Protected Setup White Paper	-
[62]	SDL Forum Society, Specification and Description Language, www.sdl-forum.org	01.05.08
[63]	Wikipedia, Process or Protocol Meta Language, http://en.wikipedia.org/wiki/Promela	01.05.08