CHALMERS
UNIVERSITY OF TECHNOLOGY

UNIVERSITY OF GOTHENBURG

Secure authentication and information transfer in a hospital environment

A comparison and evaluation of authentication systems and communication technologies

Master's thesis in Computer Systems and Networks

Viktor Ahlin

Department of Computer Science and Engineering
CHALMERS UNIVERSITY OF TECHNOLOGY
UNIVERSITY OF GOTHENBURG
Gothenburg, Sweden 2017

Master's thesis 2017

Secure authentication and information transfer in a hospital environment

A comparison and evaluation of authentication systems and communication technologies

Viktor Ahlin

Department of Computer Science and Engineering
Chalmers University of Technology
University of Gothenburg
Gothenburg, Sweden 2017

Secure authentication and information transfer in a hospital environment
A comparison and evaluation of authentication systems and communication technologies

Viktor Ahlin

Department of Computer Science and Engineering

Chalmers University of Technology

SE-412 96 Göteborg

Sweden

Telephone +46 (0)31-772 1000

Department of Computer Science and Engineering

Göteborg, Sweden 2017

Keywords: Authentication, Multilevel, Technology comparison, REST API

Abstract

I define the problem of a secure and simple assignment handover system. Next, I evaluate and compare 10 different technologies, from three approximate groups: Visual light, radio and biometric. Additionally, I combine some of these technologies evaluate and these combinations. Further, I propose some solutions that could solve the problem of designing an assignment handover system. I also develop a handover system framework that can perform a handover, thus being used to test the viability of the proposed solutions. However, no authentication was implemented into the framework, due to time constraints. Thus, the framework needs an authentication process before testing its viability in real life. Nevertheless, the framework handover system is both user-friendly and secure. Such a system also increases availability and reduce the complexity of the handover process.

Acknowledgements

First, I would like to thank my first supervisor Sally McKee, she was a great help and support when I started with my thesis project. Regrettably she could not continue on as my supervisor.

Second, I would like to thank my second supervisor Carlo A. Furia, he took over after Sally and his advice was of great assistance during the project.

Third, I would like to thank Mats Andreasen, Jan Bentzer and all the other wonderful people at Ascom. They where of great assistance, happy to answer questions or redirect me to where I could find the answers to my questions.

Finally, I would like to thank my examiner Alejandro Russo.

Contents

Chapter 1

Introduction

1.1 Background

In any shift based workplace where one person takes over another's assignments, there is a need to confirm the transaction. Depending on the environment and assignments in a given scenario, the required security and integrity of the shift change varies. In some situations a verbal exchange is enough because the consequences of an overseen assignment is minimal but in other situations the consequences could be catastrophic. An example of a shift based workplace where the consequences to human life could be dire is hospitals.

The assignment handover process needs to be quick and intuitive rather than complicated or slow. Hospitals have a high stress environment and as such it is important to limit new stress generating sources, like a complicated assignment handover system. The handover needs to be clear and distinct, there cannot be any doubt about who is responsible for what after the handover. There are assignment scheduling systems that work great when planning a whole shift but might be a little inconvenient to use if a situation suddenly arises that requires a change in the scheduled assignments, for example someone being late. On one hand, these systems makes the handover process time consuming, this both takes time away from the patients and also makes the task be perceived as cumbersome. On the other hand, if we consider how the handover system could be misused with possible dire consequences: Assignments could be actively stolen, secretly given away or accidentally transferred. Since the consequences could be dire, an easily exploited transaction protocol is not acceptable.

The system has to ensure a high degree of integrity through a defence in depth strategy. In this context defence in depth refers to preventing the

security measures from being circumvented. Even if a wrongful transaction occurs both parties should at least be aware or made aware of the action. An example is that the ID-badge is required and even if it is possible to steal a badge it is hard to not get noticed while doing so. The system also needs to be complicated enough to ensure that it is highly unlikely that accidental transactions of assignments are performed. However, it is not enough to have a very secure transfer protocol that guarantees the users' identities, and that they want to perform a handover. Another important factor is that the procedure needs to be intuitive and not overly complicated. At the end of a work shift a nurse is probably tired, which means that the system needs to be simple and intuitive enough to not become a burdensome task. It is of utmost importance to consider the user when designing a system.

I worked together with Ascom Wireless Solutions, a subsidiary of Ascom, on this project. Ascom has subsidiaries in 15 countries and employ around 1200 people [1]. They supply on-site communication systems to international customers in different industries, one of which is hospitals. When I do my evaluations on possible solutions or parts of solutions I will be basing arguments on their model and the work environment of their customers.

1.2 Aim

My objective is to design an assignment handover system that is both secure and simple to use. In order to develop a secure assignment handover system the major parts of the system must be individually considered and designed for the purpose. The design choices needs to be based on well formed arguments, since there are no previous large-scale comparisons and evaluations, the available design choices needs to be evaluated and compared. To understand the evaluations of the different technologies, of which some can be on a fairly high level, some basic concepts and theories such as cryptography also needs to be evaluated. In other words extensive research is required in order to make educated design choices. Making design choices based on assumed characteristics and availability of the technology may lead to problems later in the system development process. During the evaluation and comparison stage, different fields and approaches have to be considered, since both software and hardware design choices have considerable impact on the system.

There are many assignment handover scenarios, but I only consider the simplest one to one transfer. In this scenario the reliving nurse takes all the

current nurse's assignments. Due to time constraints I could only include a limited number of possible communication and authentication candidates in my evaluations; therefore only two biometric technologies where considered. I did not have time to get feedback on my designs from nurses but I had contact with user experience experts. The system I developed should be considered a proof of concept and should not be viewed as a fully developed system ready for use in a hospital.

1.3 Method

In the process of developing a product or service for real world use, a methodology is required during the innovation process to increase the guarantee that the result is satisfactory. One methodology for innovation is called design thinking, it combines creative and analytical approaches and benefits from collaboration across disciplines [2]. Design thinking tries to find the intersection of feasibility, viability and desirability. The process can be simplified into 5 steps, empathise, define, ideate, prototype and test [3]. Empathise is about getting to know who is the user and what is important to the user. Define is about formulating and re-framing the problem, not simply giving the user what they know they want. The define step uses the information gathered to get a clearer picture of what the user actually want. Ideate is about brainstorming and creating an array of ideas that can solve the problem, the more the better. Prototype is about drawing and create simple mock-ups to further the understanding of the ideas, the prototypes are not supposed to be good looking and it is important to not "fall in love" with an idea/prototype. Test is about controlling if the proposed idea fulfils the needs, can it be improved, this step is not about proving that the idea works but rather listening to perceptions and ideas. However, even if design thinking can be simplified into 5 steps it is important to note that it is a continuous process that does not end at the 5th step [3].

1.4 Structure

I begin by describing and explaining certain aspects that are required to understand the rest of the thesis, such as what is authentication, why more levels of authentication is better and how encryption works. Furthermore, I describe the problem that I try to solve, requirements of a solution and the limitations of my project. Moreover, I continue with presenting the research

that I will base my design choices on. Additionally, I augment the research by combining methods and technologies from the previous step to increase their performance, the merit of which is explained in the technical background. I also present design proposals for a possible solution and develop a framework to test the proposals. Finally, I end with a discussion, future works and the conclusions.

Chapter 2

Technical Background

Introduction

In this chapter I describe topics, methods and concepts that are necessary to understand some arguments and descriptions in later chapters. I do not go into too many details, merely give a general understanding about the subjects.

2.1 Principles of authentication

The purpose of authentication is to let two entities (people, computers, services) firmly believe that they communicate with each other and not with an intruder [4]. Authentication could be defined as "providing the right person with the right privileges the right access at the right time" [5]. Authentication protocols use different strategies to ensure that this belief holds true. Some protocol designers misunderstand available techniques, as a result their protocols contain redundancies and security flaws [4].

There are generally three approaches to authentication, something you have (card, token, key), something you know (PIN, password) and something you are (biometric: fingerprint, face, iris, DNA) [5]. No matter which approach that is used they each have their advantages and disadvantages [6, 7]. Some problems are that secure passwords are hard for humans to manage, tokens can be lost or stolen and biometrics raise privacy concerns [6].

2.2 Password authentication

One of the authentication strategies is to use something the user knows, that means a numeric, alphanumeric or graphical password. Numeric and alphanumeric passwords are a widely used and very familiar authentication methods. Graphical passwords are getting more common as well. Traditionally passwords have usability drawbacks that directly translate into security issues [6]. The problems with passwords mainly arises from two conflicting requirements, passwords should be easy to remember and passwords should be secure [6]. A secure password should appear random, be hard to guess, get changed frequently, not be shared between different accounts of the same user and should not be written down or stored in plain text [6]. Users have problems remembering long, pseudo-random passwords a longer period of time. Normally users adapt to the memorisation problem by decreasing complexity and number of unique passwords, also decreasing password security [6]. In 2005 a secure password should be 8 characters or more, with upper-case characters, lower-case characters, digits, special characters and lack meaningful content [6].

2.3 Multi-level authentication

Naik and Koul claim that multi-level and multi-dimensional authentication techniques are more secure than just single authentication techniques [7]. They show this with algorithms such as if a password is required for every level, n passwords are required to access the n'th level. They also claim that by adding different types of authentication methods the security increases more than by doing multiple tests of a similar nature, for example a password and a magnetic card compared to two passwords. An other study shows that multimodal methods (combining methods) are the superior way to increase accuracy and robustness of biometric systems compared to pursuing better sensors and better algorithms [8].

2.4 Cryptosystem

"Cryptography is the study of 'mathematical' systems for solving two kinds of security problems: privacy and authentication" [9]. Cryptosystems use cryptography to protect data, to make sure that only the valid users can get access to the actual data. There are two fundamentally different approaches, using a symmetric key and using a asymmetric key.

2.4.1 Symmetric

Symmetric cryptography algorithms work by having both parties share a cryptographic key (password) that is used to both encrypt and later decrypt the data. An example of a symmetric key encryption scheme is AES or Rijndael as it was originally called [10, 11]. A big advantage is that a symmetric key encryption cipher is faster than an asymmetric encryption cipher. The main drawback of symmetric key encryption is that both parties needs to have access to the secret key. The secret key is vulnerable during the sharing process. AES is a very secure algorithm that can be used in 128-bit mode, 192-bit mode and 256-bit mode. In 2011 three researchers managed to find a weakness in the AES algorithm, the practical implication was that they shortened the key length by two bits [12]. However, cracking AES-128 still takes $8 * 10^{37}$ steps, " 'To put this into perspective: on a trillion machines, that each could test a billion keys per second, it would take more than two billion years to recover an AES-128 key,' the Leuven University researcher added" [12].

2.4.2 Asymmetric

Asymmetric cryptography algorithms work by having a set of keys, one public key and one secret key. The public key of a user is used to encrypt messages to him or her which then uses their secret key to decrypt the message again. This works by both keys being mathematically related but to calculate the secret key from the public key is computationally infeasible (requiring 10^{100} instructions) [9]. Examples of asymmetric key encryption schemes are Diffie-Hellman and RSA. A big advantage with a asymmetric key encryption cipher is that the public key can be spread without revealing anything about the secret key which is needed to decrypt the encrypted message. A big drawback is that asymmetric encryption schemes are computationally intensive. One important aspect to note is that asymmetric schemes can be used to not only encrypt messages to ensure privacy but also sign messages to ensure validity, which is to say that the sender is whom it claims to be.

RSA uses the prime factorisation problem as a basis, it is a so called 'one way function'. Why the function is only 'so called' one way is because the presumed difficulty is very high making it infeasible to crack, but it still is not proven secure only presumed. However, the assumption is valid due to how lucrative an efficient solution to the prime factorisation problem would be.

The prime factorisation problem is to factorise a large integer that is the product of two different large prime numbers. Now the heart of the

problem is that it is easy to multiply the two prime numbers p and q to get n ($p * q = n$), but to acquire p and q from n is infeasible due to the many possible combinations of prime numbers that needs to be tested. If p and q are both large (recommended at least 100 digits) and truly randomly chosen prime numbers then if n is 200 digits it would take $1,2 * 10^{23}$ instructions to factor n using Schroeppel's method [13]. The known weaknesses are that p and q are not large or random enough. There are many different ways to generate random numbers but generally an analogue generator (generate number from static from a microphone or antenna) is superior to a digital generator due to them containing some degree of predictability.

2.4.3 Hybrid

Hybrid cryptography is a concept that uses asymmetric encryption to share a symmetric key that is then used to encrypt the messages. This means that the message is encrypted with a newly generated symmetric key, the symmetric key is encrypted with the public key of the receiver, then both the message and key is sent. The receiver decrypts the symmetric key with its private key and then uses the symmetric key to decrypt the message. Examples are pretty good privacy (PGP), secure sockets layer (SSL) and transport layer security (TLS).

2.5 Indoor positioning system (IPS)

Because of signal attenuation (degrading) from building materials global positioning systems (GPS) cannot provide continuous real time tracking of moving targets inside a building, instead indoor positioning systems are used [14]. IPS use various sensory information from mobile devices to locate objects or people inside a building. Examples of what the sensory information could be are radio waves, magnetic fields or acoustic signals. There are different technologies due to the local circumstances where IPS is to be used, in different environments some technologies work better than others. Each of the location determining technologies have their advantages and disadvantages in a number of areas, determine position internally or via a network connection, cost, susceptibility to interference and determination accuracy [14]. The long range sensors that determine location internally use mathematical algorithms for trilateration (distance from sensor) and triangulation (angle from sensor). Metrics used for the mathematical algorithms are angle of arrival usually measured by time difference of arrival between multiple sensors, time of arrival measured by the time it takes for the signal to travel from the

transmitter to the receiver and signal strength measured by received signal strength indication (RSSI) which is the power level received by the sensor. The network based solutions use grid topology concepts or choke point concepts. Many different IPS systems are available on the market and some are even free to use such as Anyplace [15]. In 2014 a realistic comparison and evaluation of 20 different IPS systems (some share technology base) was made and it found that 11 of these 20 had an average error of less than 3m, six of these had an average of less than 2.1m and one with an average of less than 1m [16]. However, there where circumstances that impacted the veracity of the evaluation [16]. Nonetheless, the study showed how well the systems worked in unfamiliar real life environments.

Chapter 3

Problem Specification

Introduction

In this chapter I describe the situations nurses face during the handover of assignments, transferring responsibilities during the shift change. What is problematic? Why is it problematic? What is required? How can it be done? These questions will be answered here. The information in this section is derived from briefings at Ascom and discussion with former nurses hired by Ascom as pre-sales clinic specialists.

3.1 Real life situations

Different units work in different ways around assignments and work shifts due to their separate needs, examples of units are intensive care unit (ICU), emergency department (ED) and non-specialised wards. The manual approach used solely or in combination with a digital system in many hospitals around the world is simply pen and paper or a whiteboard. This makes it very clear to the nurses what their responsibilities and assignments are during their shift. However, this does not work well with the highly technological systems used to keep track of patients and guarantees their care. This use of separate systems leads to the need to transfer the information from the manual, analogue approach to the digital system. This requires either that the nurses spends more time during the handover or preprepared shifts that can be activated. The first approach leads to less time spent with the patients and is often perceived as being complicated and time consuming, leading to mistakes which leads to distrust and more stress. The second is very inflexible and requires that everyone is on time and ready, this is not a realistic expectation because of human nature and accidents can always happen. A

variation of the first approach is needed, a way to enter the information into a digital system, but it needs to be streamlined, quick, simple to use and secure.

3.1.1 Current approach to handling assignments

There are three main approaches used by the different wards that suit their specific needs. The first approached is to use a dedicated mobile device, in this scenario a unit is associated with a set of tasks like a room. With dedicated units a handover is as simple as just handing over the unit to the relieving nurse. The second approach is that one or two super users (often the head nurse) plan all the shifts' assignments in advance. With preplanned shifts a handover is as simple as the relieving nurse shows up and confirms her presence. The third approach is that each nurse assign tasks to themselves at the beginning of their shift. With self created shifts a handover requires that the reliving nurse first assigns herself and then when she is ready makes her presence known.

3.1.2 Current approach to handling breaks

There are three main approaches used to handle breaks these approaches are products of necessity and simplicity as well as comfort. The first approach is to simply give the mobile device to the acting head nurse, thus temporarily renounce from responsibility. The second approach is to put the mobile device in the charger, making it change status to offline. When the device is offline any alerts that are normally directed to it are instead passed on up the escalation chain to another device. Taking their device offline lets the nurses temporarily renounce responsibility until they remove it from the charger again changing the status to online. The third approach is to let two nurses assign each other as "buddies" and when one takes a break the other temporarily takes over the responsibilities. This approach is a bit similar to the second but instead of using the escalation chain a "buddy" is selected and used.

3.1.3 Practical conditions

Many wards only have one desktop available and it is usually continuously used for other tasks than managing assignments. This leads to the conclusion to not use this desktop for managing assignments, if a centralised solution is pursued it needs to be on a dedicated system.

3.2 Solution requirements

Quick Not time consuming. Every moment spent away from the needs of the patients is unwanted. If it takes 5 minutes per patient just to enter the correct assignment into the system this means that the nurse has to spend 5 minutes beyond the time to read the chart and talk to the previous nurse. This will lead to the nurses being forced to work an extra 5 minutes per patient and if a nurse has 3 patients this means 15 minutes extra spent being at work beyond the working hours. However, if the time spent during this task is on average less than one minute per patient that would be acceptable.

Simple Not cumbersome or confusing. It should be a simple and intuitive user interface that makes sure that the user is in control and understands what happens during the whole process. Long lists and navigational trees are perceived as cumbersome by most users, some users might even feel lost. First giving simplified selections that limit the information given and number of options available gives a clear picture and is easier for most users to understand. It is very bad if a user feels that it is cumbersome to use an interface, it should be so easy the user does not even consider it a task.

Clear Convincing transfer. The transfer of responsibilities needs to be clear, both parties should be convinced of whom is responsible for what after the transfer. Since responsibilities are involved it needs to be crystal clear who is responsible, both for the users and for traceability. It is bad if the users is uncertain about who has the responsibility for what assignment, both during the transfer and after. The process should be as clear as handing over a baton.

Secure Correct users and no responsibility gap. There needs to be a authentication system that verifies that the users are whom they claim to be. There also needs to be a guarantee within the system that there is no gap during the transfer where no one is responsible for the patients. It should require enough effort to circumvent the system to make it improbable, which means that it does not have to be infeasible to circumvent but that the reward compared to the effort required should make in highly unlikely. The system needs to confirm user identity, user acknowledgement and user approval. The system also needs to guarantee that there is no gap in responsibilities where no one is responsible.

3.3 Limitations

3.3.1 Simplified situation

The development will be focused on the simplified situation of a one to one handover, that refers to one nurse assuming responsibility for all patients belonging to another nurse. Other more complicated situations as one to many, where a nurse only takes one patient or just one type of alarm signal from a patient, are also important but they will not be covered in this thesis. However, solutions for the simplified situation can also work for more complicated situations with some adjustment.

3.3.2 Development process

Generally a development process has a requirement phase, a design phase, an implementation phase and a verification phase. Additionally, a user centred design process is required, in which the end user is considered at every stage in the process. Developing a medical device (MD) classed product follows the same development process but it is very important that every step is carefully documented in great detail and that each step can be traced to a previous step. The design have to meet the requirements and the implementation also have to realise the design. The implementation passes the validation if it is verified that the initial requirements are met. For example if the developers notice that a specification is infeasible it is not enough to just note that down and then continue, the design specification needs to be changed and the changes needs to be evaluated to see if they affect anything else.

I will not document all the development steps in detail and I will only use general requirement specifications. Even though the system is supposed to be used by an end user, I will only have a limited interaction with potential users.

3.3.3 Proof of concept

The software and hardware I will develop and demonstrate will not be a fully developed system, merely a proof of concept that demonstrates the solution proposal in an actual situation.

Chapter 4

Individual Technologies

Introduction

In this chapter I describe and explain how some different technologies work, as well as some of their characteristics. I aim to describe the technologies in a way that simplifies comparisons between them. The main metrics I will use to describe the technologies are cost, requirements, integrity and quality of service. These metrics might not give a fair overview of the technologies in another context, for example how simple it is to implement a technology is only a part of the requirements metric.

4.1 Visible and near visible light based technologies

Light is composed of discrete packets of energy called photons. These photons carry momentum, have no mass and travel at the speed of light [17]. Light has both particle-like and wave-like behaviour [17]. Light is classified into different categories depending on its wavelength in descending order: Radio waves, Microwaves, Infrared, Visible light, Ultra Violet, X-rays, Gamma [18]. Electromagnetic energy (light) can be described by frequency, wavelength or energy. The three properties are mathematically related in a way such that you can calculate the other two if you know one [17]. The categories of electromagnetic energy are usually described by different properties because of scientific convention that allows for the use of units that have numbers that are neither too large or too small [17].

4.1.1 Barcode

A barcode is defined as "A machine-readable code in the form of numbers and a pattern of parallel lines of varying widths, printed on a commodity and used especially for stock control" [19]. This technology is based on the idea that a black and white image can contain information . Using image processing to decode varying widths and spaces of parallel lines a serial number is retrieved. This number is then used to either identify an object or to further decipher information such as a web address [20].

One dimensional barcode

Linear barcodes are a one dimensional representation of data. Probably the most well known types are standards from GS1, various retail barcodes use their standard. GS1 formerly known as European Article Number (EAN) or Uniform Code Council (UCC), is an international non-profit organisation that supplies different standards [21]. Among these are one dimensional barcode standards that represents a varying amount of numbers.

Two dimensional barcode

Matrix code is a two dimensional barcode that can either contain more information on the same area or the same information on a smaller area compared to a one dimensional barcode [22]. QR-code is an example of a matrix code standard [23].

Attributes

Barcodes are a simple technology that is easy to implement. The requirements are a digital camera connected to a computer and barcode tag generator. Any modern phone can fulfil the first requirement so no specialised hardware is needed. The second requirement can be fulfilled by printing a barcode on a piece of paper, this is a method with high availability and low cost. However, the quality of service (QoS) cannot be guaranteed since paper is a fragile material. Since the technology is so widely available it is hard to guarantee integrity, there is no difference between a barcode in the correct place and an identical barcode on the other side of the world.

Pros and Cons

Pros: Low cost and low requirements.
Cons: No QoS guarantee and no integrity measures.

4.1.2 Infrared wireless

Infrared wireless is a wireless technology that convey data through infrared (IR) radiation. Infrared is electromagnetic energy at a wavelength longer than visible red light, but shorter than microwaves [24]. The frequencies range from 300GHz to 400THz. IR wireless systems can operate in line of sight mode that requires a visually unobstructed straight line of sight, or diffuse mode (scatter mode) where an unobstructed line of sight isn't necessary [25]. Unlike radio-frequency (RF) wireless links, IR wireless cannot pass through walls. This could be a disadvantage from an availability perspective or an advantage from a privacy perspective. IR can be used for communication or localisation. The Infrared Data Association (IrDA) is an industry sponsored organisation set up in 1993 that develop standards for IR communication hardware and software as well as interface specifications and communication protocols [24]. IR data rate is up to 100Mbps and a new standard called Giga-IR with data rate up to 10Gbps is under development [26]. IR wireless consume low power, since IR is directional and cannot go through walls it has good privacy, not harmful to humans if used correctly and has no signal conflicts or RF interference [26].

Attributes

IR is cheap to implement, an IR-emitter and IR-detector pair can be bought for $ 1,95 [27]. IR technology could be very private since the communication is directional and does not pierce solid objects, which means that if it is used correctly the connection is secure and both integrity and QoS can be guaranteed.

Pros and cons

Pros: Low cost, low requirement, integrity measures and QoS guarantee.
Cons: Complex communication requires static positioning.

4.2 Radio based technologies

Radio technology is defined as "Electromagnectic radiation with lower frequencies and longer wavelengths than those of microwaves, having frequencies lower than 300MHz and wavelengths longer than 1m" [28]. In the 1860's James Clerk Maxwell developed a theory about electromagnetic waves. He noticed that electrical fields and magnetic fields could couple together, forming electromagnetic waves. Maxwell summarised this relationship into what

is referred to as "Maxwell's Equations" [17]. Heinrich Hertz applied these theories to radio waves, his experiments solved two problems. First, he managed to prove that radio waves was a form of light. Second, how to make electric and magnetic waves wireless as Maxwell's waves (electromagnetic waves) [17]. Electromagnetic waves travel at the speed of light and can propagate through different media [17, 29].

4.2.1 Radio-frequency identification (RFID)

RFID uses electromagnetic fields to identify and get information from 'tags'. RFID is used for the same reason as barcodes but requires no line of sight to the target and can be used over greater distances. It is claimed that RFID is a probable successor to the optical barcode. However, due to tag costs and logistical complications RFID tags is unlikely to substitute barcodes in retail in the near future [30]. RFID would add a lot of functionality in retail, both for the ability to scan a whole shopping cart at once and for the ability to address the problem of item depletion on retail shelves [30]. There are two classes RFID types can be divided into and those are active and passive [31].

Passive RFID

A passive RFID tag consists of an antenna, a semiconductor chip and some encapsulation. It has an indefinite operational life and is small enough to fit into a practical adhesive sticker [31]. The passive tag is powered by the reader with one of two fundamentally different approaches, magnetic induction and electromagnetic wave capture. These two approaches takes advantage of two properties of the radio antenna, near field and far field. Both can transfer enough power to a remote tag to sustain its operation. The power needed is typically between 10μW and 1 mW depending on tag type [31]. The RFID tag could be a sticker, keychain tag, card or capsule.

Active RFID

In contrast to a passive RFID tag an active RFID tag requires a power source, either a powered infrastructure or a battery. If a battery is used as the power source the tag's lifetime is limited to the battery's capacity. One example of active RFID would be airplane transponders to identify their nationality. Batteries make the cost, size and lifetime impractical in many areas such as retail [31].

Attributes

RFID is a simple technique that is easy to implement. The requirements are a RFID reader and a RFID tag. Where the tag is fairly low cost from $ 0.40 each [32], the reader or scanner is also fairly low cost from $ 125 [33]. These prices are depending on the specifications, the examples are from products that seem reasonable in the context. Both tags and readers have a high availability so they are easy to acquire. Since line of sight is not a requirement the tags can be protected. However, metal can disrupt the signal thus QoS cannot be guaranteed if there is metal in close proximity. Due to the high availability of the technology integrity cannot be guaranteed but it is harder to circumvent RFID than barcodes.

Pros and cons

Pros: Low cost and low requirement.
Cons: No integrity measures, QoS cannot be guaranteed in the proximity of metal.

4.2.2 Near-field communications (NFC)

NFC is a set of communication protocols that enable two electronic devices to communicate. The technology builds on RFID and contactless smart-card that enable data to be read at a distance [34]. However, contrary to RFID the NFC specifications restrict the distance between device and tag to a close proximity and require user intervention. This change was desired to address security and privacy risks. In the context of NFC being used with mobile devices there are three principal modes of operation, reader/writer, card emulation and peer mode. The reader/writer mode enable reading passive RFID tags and to act on that data, visit a web page, make a call or send a text message. The reader/writer mode also enables the devices to write data to some tags, notably virtual tags in other devices [34]. The card emulation mode enables contactless business transactions, examples of use could be for identification, payment or access control [34]. The peer mode allows two devices to interact with each other and perform peer-to-peer data transfers, business cards, photos and documents [34]. These functions cause security and privacy concerns and the NFC specifications address some of these concerns: NFC requires less than four centimetres proximity for interactions, NFC requires a “tapping” consumer gesture where the devices are in this close proximity to initiate interactions, NFC should be disabled when the device is locked and the user should be able to disable the function, NFC

implementations should provide user feedback on interaction requests from other NFC devices, NFC initiated sharing of personal data should be accomplished by use of regenerated identifiers to avoid association of a device with an NFC interaction [34]. Cavoukian presents more risks and concerns about NFC as well as proposes possible mitigation techniques [34]. Several Android mobile phone models already supports NFC [35]. However, Apple waited to introduce NFC on iPhones until iPhone 6 but it was locked to only Apple Pay [36], and the NFC functionality is still locked on iPhone 7 [37].

Attributes

NFC is a relatively cheap technology to implement, many mobile devices already support the functionality, a sticker tag could be bought for less than $ 1 [38] and a desktop reader could be bought for $ 45 [39]. NFC is used as a payment method in Apple Pay and Android Pay, as such the security aspects have been considered extensively [40]. By using NFC secure channel (encrypted connection) integrity and QoS can be guaranteed.

Pros and cons

Pros: Low cost, low requirement, integrity measures and QoS can be guaranteed.

4.2.3 Bluetooth

Bluetooth also known as IEEE 802.15.1 was design for short ranged or cheap devices to replace cables. Examples of devices are, computer mice, keyboards, headphones and printers. This range of applications is referred to as wireless personal area network (WPAN) [41]. Bluetooth could be used to connect two handheld devices for communication on the 2,4 GHz radio frequency band. There are three types for different areas of use within the standard [42]: Basic Rate/Enhanced Data Rate (BR/EDR), Low Energy (LE) and High Speed (HS). BR/EDR is for medium data transfer for example mice, keyboards and supports a bit rate of 2 Mbps. LE also called Smart is designed to communicate with the existing Bluetooth devices but with “ultra-low” power consumption. HS is designed for large data transfer; for example synchronising music libraries, videos or photos in bulk.

Attributes

Bluetooth is not only a radio interface standard but a whole communication stack that handles the connection and communication in the WPAN. Services

provided includes authentication, security and QoS. Bluetooth requires a module or system on chip (SoC) and licence fee for the brand and technology. Texas Instruments sells a Bluetooth SoC for $ 5 per unit [43]. Aaron Stern wrote an article about Bluetooth security 2013 for the Kaspersky lab daily [44], in the article he lists a couple of threats and possible attacks towards Bluetooth devices. He also claims that the attacks depend on exploiting the very backbone of Bluetooth connectivity.

Pros and cons

Pros: Low cost, low requirement and QoS guarantee.
Cons: No integrity measures, system security threat.

4.2.4 IEEE 802.11 (Wi-Fi)

Wi-Fi is a technology developed by the Wi-Fi Alliance and defined as any wireless local area network (WLAN) product based on the IEEE 802.11 standards. The term is used as a synonym to WLAN since it is the most used standard; however "Wi-Fi" is actually a registered trademark of the Wi-Fi Alliance [45]. IEEE 802.11 is a collection of several wireless communication standards, which uses the 2,4GHz 3,65GHz or 5GHz band. Since the initial 802.11 standard that was approved 1997, several amendments has been made that address different characteristics [46].

Attributes

IEEE 802.11 is a well-used and well developed wireless communication standard that is easy to implement. To use it a router and a network interface card (NIC) is needed, all smartphones already have a NIC. A router costs around $ 27 [47] and a network card costs around $ 14 [48]. With the 802.11e amendment QoS support is added to the standard [49]. The 802.11i amendment provides encryption and security support, with the WPA2 algorithm [50]. However, the algorithm does not guarantee security it only makes it harder for most unwanted users to access the connection [51].

Pros and cons

Pros: Low cost, low requirement, QoS guarantee and integrity measures.

4.2.5 Ultra Wideband (UWB)

UWB is a wireless radio technology, the International Organization for Standardization (ISO) and the International Electrotechnical Comission (IEC) have published the ISO/IEC 26907 standard 2009 regarding the communication use of UWB [52]. UWB was first solely used for radar, sensing and military communications but in 2002 the Federal Communications Commission of USA rules that UWB is authorized for unlicensed use. When it was proposed for civilian use there was no definitions for the signal, so the Defence Advanced Research Projects Agency (DARPA) provided the first definition. UWB could be an indoor short-range high data rate connection or long-range very low data rate connection [53]. Due to competing proposals the proposed IEEE 802.15.3a high data rate standard was withdrawn in 2006 [54]. An example that is based on one of the competing proposals is Certified Wireless Universal Serial Bus (CWUSB), with a data rate up to 480Mbps at 3m [55]. UWB for communication has potential but interest has declined due to the popularity and continued evolution of Wi-Fi [55, 56].

Attributes

Due to popularity issues finding a retailer for communication connections is hard. A retailer for localisation purposes is Zebra, but they did not show prices [57]. CWUSB uses AES encryption.

Pros and cons

Pro: Integrity measures.
Cons: Due to low market exposure many factors (cost, requirements, QoS) are unknown.

4.2.6 ZigBee

ZigBee is a wireless network standard, also known as IEEE 802.15.4. Contrary to other standards like Bluetooth and Wi-Fi that address medium to high data rates, ZigBee offers low latency and very low power consumption, but with low data rates [58]. The wireless ZigBee network use the 2,4GHz, 5915MHz and 868MHz bands with a data rate up to 250kbps. ZigBee networks can have three topologies, star, peer-to-peer and mesh [58]. Some examples where ZigBee would be a good choice would be for sensors and control devices. A multitude of proprietary wireless systems have been developed with the focus of low cost and low power consumption, for situations where high data rates are not required. However, these systems create a

interoperability problem with each other and newer systems [58]. Two different device types can participate in a ZigBee low rate WPAN (LR-WPAN): a full-function device (FFD) and a reduced-function device (RFD). The FFD has three modes of operation, PAN coordinator, coordinator and device. A FFD can talk to RFDs or other FFDs, but a RFD can only talk to a FFD [58].

Attributes

ZigBee is a wireless standard that is relatively cheap to implement, a module can be bought for $ 24.95 [59]. For security ZigBee uses AES encryption on the messages, this can protect the confidentiality, integrity and authenticity [58]. ZigBee can be configured as a wireless network or a peer-to-peer connection. There is a guaranteed time slot (GTS) option on the traffic type that can guarantee QoS, by giving each device a dedicated timeslot free of contention and latency [58].

Pros and cons

Pros: Low cost, low requirement, QoS guarantee, integrity measures.

4.3 Biometric based technologies

Rather than what a person has (token) or what a person knows (password) it is possible to use who a person is to identify her. Biological measurements such as physiological or behavioural characteristics can be used as a biometric if it satisfies the requirements: Everyone have the characteristic (universality), any two persons should be sufficiently different with respect to the characteristic (distinctiveness), the characteristic should be sufficiently invariant over time (permanence), the characteristic can be measured quantitatively (collectability) [60]. In a practical biometric system there are however some other issues, performance (accuracy, speed and resources), acceptability (user's willingness to use) and circumvention (effort needed to crack) [60]. Examples of common physiological features that are used as biometrics: Fingerprints, hand or palm geometry, retina, iris and facial characteristics [61]. Examples of common behavioural characteristics that are used as biometrics: Signature, voice (also has a physical component), keystroke pattern and gait [61]. A biometric system can depending on context work in two modes, verification and identification. In verification mode the system validates a specific person's claimed identity and the answer to this query is either true or false [60]. In identification mode the system tries to find the user's identity

from the database and the answer to this query is either the user's identity or "user not found" [60]. Biometric systems has four design components, acquisition, representation (template), feature extraction and matching [62]. The acquisition component is about how the biometric is captured/sampled. The representation or template component is about which machine readable representation completely captures the biometric information. The feature extraction component is about how the biometric data is quantified. The matching component is about establishing a metric of similarity and define a threshold of acceptance [62]. The different components have their own challenges, some of which are more complex than might be perceived at first glance.

4.3.1 Fingerprint

Fingerprints have been studied since 1684 and already in 1880 it was suggested to be a unique individual trait [62]. In the 20th century fingerprints became a formally accepted identification method by law-enforcement agencies. In the early 1960's the Federal Bureau of Investigation (FBI) home office in the United Kingdom and the Paris Police Department started developing automatic fingerprint-identification systems (AFIS's) [62]. The development of AFIS's have greatly improved operational productivity since before this fingerprint experts manually performed the fingerprint identifications.

Acquisition There are two primary methods to acquire a fingerprint image, inked and live scan (ink-less) [62]. The inked method consists of a trained professional who obtains an impression of an inked finger on a paper and then scans the impression with a document scanner. The live scan method is a collective term for a fingerprint image obtained directly from the finger without intermediate steps. In the context of an authentication system the inked method is both infeasible and socially unacceptable [62]. A popular live-scan technology is based on the optical frustrated total internal reflection (FTIR) concept. The FTIR concept works by placing a finger on a glass platen, illuminate it from underneath at a certain angle and let a camera capture the reflected light. With FTIR the "valley" and "ridges" of the fingerprint are clearly visible.

Representation The representation component has a great impact on the design of the rest of the fingerprint verification system. The unprocessed grey-scale values of fingerprint images do not remain unchanged during the creation of the images. Grey-scale representation is prevalent in optical

matching verification systems. However, grey-scale representation systems may have limited utility due to factors like brightness, image quality, scars and large distortions in the image [62]. The two most prominent structures in the fingerprint are the splitting of a ridge (end of a valley) and the end of a ridge (splitting of a valley) they are completely opposite things yet pressure variations could turn one type of structure into the other due to them being background-foreground duals of each other. Because of this reason many representation schemes treat them as the same and collectively call them minutiae [62]. The simplest minutiae representation is a list of minutiae defined by their spatial coordinates with respect to a fixed image-centric coordinate system. The American National Institute of Standards and Technology (NIST) standard representation is based on minutiae location and orientation.

Feature extraction The feature extraction component with fingerprints is quite challenging. If the ridges of a fingerprint can be perfectly located in an image, then the minutiae extraction is just the task of extracting singular points in a thinned ridge map [62]. However, in practice it is not always possible to obtain a perfect ridge map. The performance of minutiae extraction algorithms are heavily dependent on the quality of the fingerprint image [62]. Due to a number of reasons fingerprint images may not have well defined ridge structures, because of this a reliable extraction algorithm should not assume prefect ridge structures.

Matching The matching issue is about determining if two samples (test and reference) are impressions from the same finger. With minutiae representation the problem may be reduced to a point pattern matching problem. In the ideal case there are no deformations such as translation (spatial offset) and rotation (angular offset) [62]. Each minutia present in a fingerprint image also have to be exactly localised. In this ideal case fingerprint verification is only a trivial task of counting the number of spatially matching pairs between the reference image and the acquired test image. However, determining if two representations of a finger, are actually representing the same finger is a very difficult problem, for two reasons. The first reason, if the test and reference representation are indeed a mated pair, the correspondence between the minutiae in the two representations is not known. The second reason, the imaging system presents a number of challenging situations, some unique to fingerprint scenarios: Inconsistent contact, non-uniform contact, irreproducible contact, feature extraction artefacts and sensing act [62]. Considering these challenges the matching algorithm needs to establish and

characterise a realistic model of the variations among the representations of the mated pairs.

Attributes

Fingerprint verification is a relatively cheap technology to implement, a FBI certified, durable and reliable USB-scanner with pre-installed user guide can be bought for $ 79 [63]. Extreme finger dryness may make it very hard to acquire a sample with sufficient quality [60].

Pros and cons

Pros: Low cost, low requirement, strong integrity.
Cons: QoS may be compromised due to dry fingertips.

4.3.2 Face recognition

Facial recognition is probably the most commonly used method by humans to recognise individuals [60]. The technology is a non-intrusive method that records the spatial geometry and distinguishing features of the face [5]. The range of applications for facial recognition go from, a static controlled environment such as for passport photos and "mug-shots" to a dynamic uncontrolled environment such as casinos or airports [60]. There are a number of face recognition techniques some of these are 3D-scans, high resolution still images, multiple still images, multi-modal, multi-algorithm and preprocessing algorithms [64]. Face recognition gave a couple of problems and those are the pose of the head and illumination conditions. For a face recognition system to work well in practice in needs to satisfy a couple of conditions, detect if a face is present, find the face and recognise the face from any viewpoint [60]. An important thing to take note of is that since the face recognition systems use spatial geometry of distinguishing facial features they ignore hairstyle, facial hair or similar factors [5].

Acquisition An image of the face is aquired by either scanning a photo or taking a picture with a digital camera, since a video is a rapid sequence of images it can also be a source [5]. The image is then processed with a software that tries to detect if there is a face and the location of the face if there is one present [5]. How the image is acquired and under what circumstances could greatly affect the effectiveness of face recognition. If controlled circumstances is observed with conforming lighting conditions and a static pose, the later steps will be less complicated. Even if some techniques can use algorithms to

offset these problems they are not perfect, so there is a risk of errors occurring [5]. After all the best option is not to compensate for errors but avoid them completely if possible.

Representation The subject's face is represented by a template, which is a reduced set of data [5]. The different techniques that use different metrics naturally have different templates as well. Every face has numerous distinct details that make up facial features. These details are defined as nodal points and each face has approximately 80 nodal points, according to a software called FaceIt. Example of nodal points would be, distance between eyes, nose width, eye socket depth, cheekbone shape and jawline length [65]. By measuring these nodal points and generating a numerical code called a faceprint a face template is created [65].

Feature extraction Once a face has been detected and localised it can be analysed. A popular method is Principle Component Analysis (PCA), also known as the eigenface method [5]. However, if factors such as lighting, viewpoint and expression varies, then PCA is less effective [66]. A more sophisticated mathematical framework using tensors which is an approach using multi-linear algebra, is called TensorFaces [66]. The feature extraction methods can be used on both 2D images and 3D images, no matter the type of image some normalisation is used before extraction begins. On 2D images that means that preprocessing needs to correct for rotation, scale and position. On 3D images the pose is also corrected for. To correct for rotation two landmarks (eyes) are found and then used for geometric normalisation, to correct for pose a third landmark (center of lower chin) is also found [8]. Although, it is worth to note that too much normalisation may be harmful because of missing data problems outweighing the gains of normalisation, especially with 2D images [8].

Matching After a template is generated it is compared with a database of known faces, this returns a score that indicates how close the template matches the database entries. The last step is determining if the produced score is good enough to declare a match [5]. The threshold for declaring a match can be modified based on security and operational considerations [5].

Attributes

Face recognition is a non-intrusive and potentially covert way to identify users [5]. There are technical difficulties with face recognition, uncontrollable background, non-cooperative subject, moving target, lighting conditions, camera

angle and image resolution [5]. To some extent the difficulties can be reduced by controlling the subject's pose, controlling the environment and taking high resolution images. Since the system only shows probable matches, the use of a human operator that can verify potential matches might not be a bad idea [5]. To capture and log peoples faces without their explicit consent is a legal grey area, it could be argued to be against the "right to privacy". However, it is deemed that what is exposed to the public is not considered private [5]. There is Open Source software as well as commercial software available [67, 68]. A complete face racognition system can be bought for $ 76 [69].

Pros and cons

Pros: Low cost, strong integrity.
Cons: High requirements, depending on accuracy level a human operator may be needed to guarantee QoS.

4.4 Summary table

This section contains a table that summarises the descriptions of the technologies in this chapter in a simplified way.

Technology	**Cost**	**Requirement**	**Integrity**	**QoS**
Barcode	low	low	none	none
Infrared	low	low	medium	medium
RFID	low	low	none	low
NFC	low	low	high	high
Bluetooth	low	low	system threat	medium
Wi-Fi	low	low	high	high
UWB	unknown	unknown	high	unknown
ZigBee	low	low	high	high
Fingerprint	low	low	high	low
Face recognition	low	high	high	low

Chapter 5

Combined Technologies

Introduction

In this chapter I will present authentication systems that use different authentication principles and different technologies. In these scenarios wireless communication will be done with Wi-Fi if nothing else is mentioned. This is because UWB is not suitable due to a lack of information, Bluetooth is unsuitable due to lacking security and ZigBee have mostly the same properties as Wi-Fi but is not as widespread. The biometric combination studies are not based on the most recent technologies. The accuracy numbers in both section 5.1 and 5.2 are thus not up to date. However, the behaviour of the accuracy based on combining biometrics is still relevant, which is why the graphs are included nonetheless.

5.1 Face recognition 2D and 3D

Both methods for face recognition have their advantages and disadvantages based on circumstances. For example 2D images are generally easier and less expensive to acquire. On the other hand, a perceived benefit of 3D data is less variation due to make-up and different light condition. One of the main motivations of 3D recognition is to overcome the problems of illumination changes, expression variation and pose variation [70]. From an exdperiment using principle components analysis (eigenfaces) for both 2D and 3D separately it was found that 2D performed slightly better than 3D but the fusion of them performed significantly better than either one alone as can be seen in figure 5.1 [70].

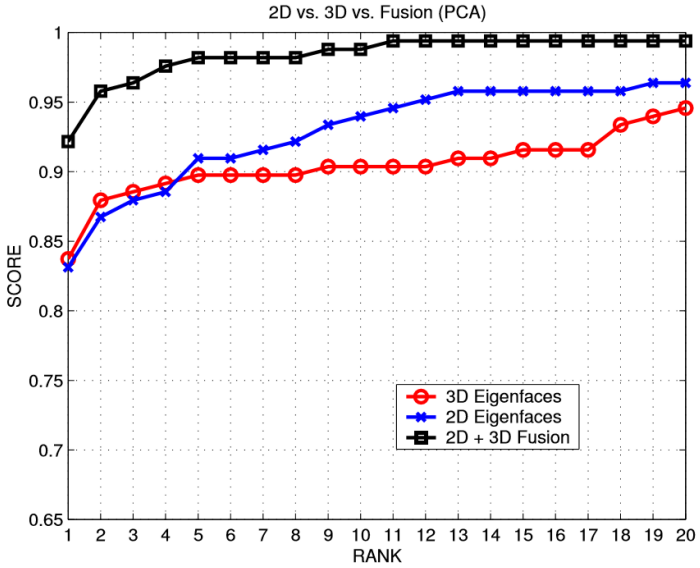

Figure 5.1: Graph showing a performance comparison [70] (2003). With true pass rate versus the degree of the biometric algorithms certainty of a match. Ranks are a possible user matches with rank 1 being the most likely match and the score represents the accuracy within those ranks. The 2D + 3D fusion has a more than 90% accuracy rate to correctly identify the most likely match.

Evaluation

The combined system is more accurate and can handle more variations that each system alone might find it hard to overcome. The hardware requirements are greater since two kinds of sensors are needed. The software requirement is greater as well since the results from the two different tests need to be combined into one result. However, there is documentation for how this can be done, so only actual implementation is required. The total cost is greater than for a system using only a single method. The deployment cost is relatively low, because the cost is fixed and can be amortised over many users.

5.2 Fingerprint and face recognition

Both biometric methods are fairly popular but due to intraclass variations in biometric characteristics an identification can only be made with certain confidence [71]. To decrease the influence of the variations on the ultimate

decision making, introducing another metric is a viable solution. Increasing the efficiency of the system mean, reject fewer genuine individuals and accept fewer impostors. These concepts are connected since if less impostors are accepted then fewer genuine individuals will be as well and vice versa. However, a study showed that by combining the biometrics the overall performance was enhanced in both respects as can be seen in figure 5.2 [71].

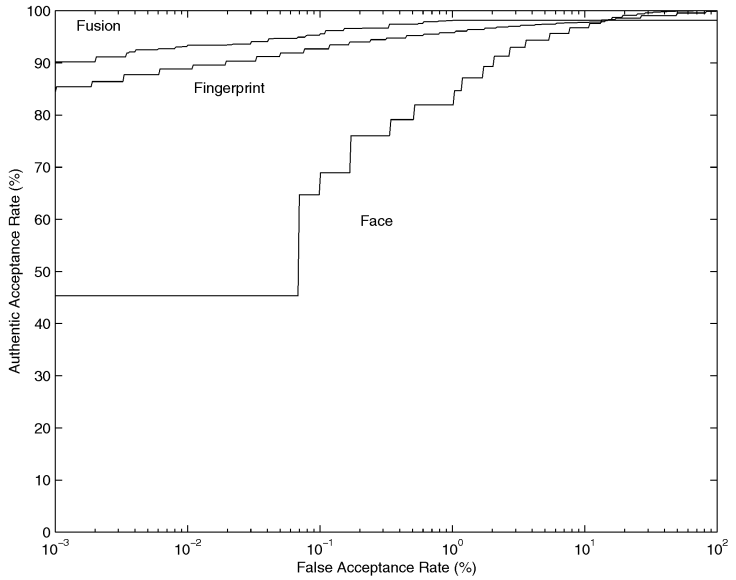

Figure 5.2: Graph showing a performance comparison [71] (1998). With true pass rate versus false pass rate tolerance. To the left the match requirements are stricter, but the success rate is also lower.

Evaluation

The combined system is more accurate and can handle more variations that each system alone might find it hard to overcome. The hardware requirements are greater since two kinds of sensors are needed. The software requirement is greater as well since the results from the two different tests need to be combined into one result. However, there is documentation for how this can be done, so only actual implementation is required. The total cost is greater than for a system using only a single method. The deployment cost is potentially very low, because the cost is fixed and can be amortised over many users. Complete systems are available and can be bought for $ 75.87 [69].

5.3 Keycard (ID-card), NFC and Numerical password

First, accessing a mobile device with a username and password. Second, using an ID-card with an RFID (NFC) tag to ID the user to a desktop application. Final, use NFC to connect the mobile device with the desktop and use the username on the mobile device to confirm the ID of the user on the desktop. This would require the user to possess two items and remember a password. What is required to circumvent the system would be to acquire a mobile device with the user already logged in, the same user's ID-card and have access to the desktop. It is unlikely the user would be unaware of the situation if this scenario occurred. Another way to circumvent the system would be for the attacker to know the login information of the user, possess a mobile device, possess the targeted user's ID-card and have access to the desktop. In this scenario the two key parts to prevent an attack would be to restrict access to the mobile devices and make sure the login credentials are complex enough to be difficult to guess. A third way to circumvent the system would be to replay the information from the keycard tag and from the NFC connection but it is a very improbable and beyond the scope of reasonable security. If the desktop is additionally supervised it would give some level of traceability.

Evaluation

From the user's perspective an ID-card with a radio tag is not uncommon and the use of a mobile device the requires a login is also common. No new unknown technologies or added items to carry around. The hardware requirements are high, a keycard (ID-card with keycard functionality), a NFC enabled mobile device, readers for both the keycard and NFC. The software requirements are low, since the approach is very straight forward. Total costs would be high since all users need a keycard and all users active at the same time need an NFC enabled mobile device, $ 50 per user and 1000 users gives a cost of $ 50'000 (as an example). Deployment costs are potentially low, if keycards and NFC enabled mobile devices are already in use, then the fixed cost of implementation can be amortised over many users.

5.4 Graphical password, IR (location) and Numerical password

First, accessing a mobile device with a username and password. Second, stand in the designated area where the mobile device can make contact with a locational beacon through IR. Final, open the application and enter a graphical password, which is sent asymmetrically encrypted and signed to a local web-server. This would require the user to posses an item, remember two fundamentally different passwords and stand in a specific location. What is required to circumvent the system would be for the attacker to acquire a mobile device with the user already logged in, know the user's graphical password and avoid getting found out while standing in the designated area. It is possible to learn the graphical password by shoulder surfing but depending on the placement of the designated location an invalid user might be very suspicious. Another way to circumvent the system would be for the attacker to acquire a mobile unit, know both the user's login information and their graphical password. The key parts to prevent an attack in these scenarios are to restrict access to the mobile devices, make sure that both the login information and the graphical password are complex enough to be difficult to guess. A third way to circumvent the system would be for the attacker to posses a device that can simulate the behaviour of the mobile device, replaying both IR signal and correct message. To make the method in this scenario even more difficult would be to not only send the graphical password encrypted and signed but also include some time sensitive data. This forces the attacker to replay the message very soon afterwards for it to be valid or posses the user's secret key and know how the time sensitive data component is made. However, to circumvent the the replay guarded system is very improbable and beyond the scope of reasonable security. If the designated location is additionally supervised it would give some level of traceability.

Evaluation

From the user's perspective using a mobile device that requires a login is common, standing in a specific location to gain access is a simple concept and remembering a graphical password is easier than a numerical for most users [6]. Thus remembering two different passwords is not too hard and standing in a specific location is intuitive, depending on where these locations are placed it can also be an effortless component. The hardware requirements are relatively high, a mobile device with a touch-screen and IR positioning functionality as well as IR positioning beacons. The software requirements

are relatively low, only implementing the positioning component requires a little extra effort otherwise the approach is very straight forward. The total cost is relatively high since all users require a IR positioning enabled mobile device, $ 50 per user and 1000 users gives a cost of $ 50'000 (fictive example). The deployment costs are potentially very low if IR positioning enabled mobile devices are already in use, then the fixed cost of implementation can be amortised over many users.

5.5 IR (data), Keycard (ID-card) and Numerical password

First, accessing a mobile device with a username and password. Second, using an ID-card with an RFID (NFC) tag to ID the user to a desktop application. Final, open the application and connect to the desktop with line of sight IR. The IR connection will confirm the user's identity and perform a key exchange. This would require the user to possess two items, remember a password and have access to the desktop. What is be required to circumvent the would be for the attacker to acquire a mobile device with the user already logged in, acquire the user's keycard and have access to the desktop. It is unlikely the user would be unaware of the situation in this scenario. Another way to circumvent the system would be for the attacker to know the login information of the user, possess a mobile device, possess the targeted user's ID-card and have access to the desktop. In this scenario the two key parts to prevent an attack would be to restrict access to the mobile devices and make sure the login credentials are complex enough to be difficult to guess. A third way to circumvent the system would be to replay the information from the keycard tag and from the IR connection but it is a very improbable and beyond the scope of reasonable security. If the desktop is additionally supervised it would give some level of traceability.

Evaluation

From the user's perspective an ID-card with a radio tag is not uncommon and the use of a mobile device the requires a login is also common. No new unknown technologies or added items to carry around. The hardware requirements are high, a keycard (ID-card with keycard functionality), an IR connection enabled mobile device, readers for both the keycard and IR. The software requirements are low, since the approach is very straight forward. Total costs would be relatively high since all users need a keycard and all users active at the same time need an IR enabled mobile device, $ 50 per

user and 1000 users gives a cost of $ 50'000 (fictive example). Deployment costs are potentially low, if keycards are already in use they can be used for this purpose as well and mobile units with IR functionality may already be in use, then the fixed cost of implementation can be amortised over many users.

5.6 Barcode, Graphical password and Numerical password

First, accessing a mobile device with a username and password. Second, scan a barcode containing the key to generating the symmetrical encryption key required for contacting a local application-server. Final, enter a graphical password that is sent to the application-server for verification. This would require the user to possess an item and know two fundamentally different passwords. What is required to circumvent the system would be for the attacker to acquire a mobile device with the user already logged in, know the user's graphical password and have access to the barcode. It is possible to learn the graphical password by shoulder surfing but depending on how often the barcode is changed access to the original may be required and the placement of the original barcode may make an invalid user very suspicious. Another way to circumvent the system would be for the attacker to acquire a mobile unit, know both the user's login information and their graphical password as well as possessing the barcode. The key parts to prevent an attack in these scenarios are to restrict access to the mobile devices, make sure that both the login information and the graphical password are complex enough to be difficult to guess. A third way to circumvent the system would be for the attacker to posses a device that can simulate the behaviour of the mobile device, reading the barcode and sending the correct message. To make the method in this scenario even more difficult would be to not only send the encrypted graphical password but also include some time sensitive data that is digitally signed. This forces the attacker to replay the message very soon afterwards for it to be valid or posses the user's secret key and know how the time sensitive data component is made. However, to circumvent the the replay guarded system is very improbable and beyond the scope of reasonable security. If the original barcode location is additionally supervised it would give some level of traceability.

Evaluation

From the user's perspective using a mobile device that requires a login is common, scanning a barcode is a simple concept and remembering a graphical password is easier than a numerical for most users [6]. Thus remembering two different passwords is not too hard, barcodes can be scanned with either a dedicated scanner or processed from an image, both methods are simple and intuitive. The hardware requirements are relatively high, a mobile device with a touch-screen and camera or dedicated barcode scanner. The software requirements are relatively low, because the approach is very straight forward and barcode processing software is available on the market at a low cost. The total cost is relatively high since all users require a mobile device that can process barcodes, $ 50 per user and 1000 users gives a cost of $ 50'000 (fictive example). The deployment cost is potentially very low if such mobile devices are already in use, then the fixed cost of implementation can be amortised over many users.

5.7 Fingerprint, Keycard (ID-card)

First, using an ID-card with an RFID (NFC) tag to ID the user to a desktop application. Final, scan a fingerprint to verify the users identity. This would require the user to posses and item, have access to a desktop and have suitable fingers, with that means that the hands are not dry and the fingerprints are not damaged. What is required to circumvent the system would be for the attacker to acquire the keycard and fingerprint of a user. The effort required to use someone else's fingerprint varies with which fingerprint system is used, for some adhesive tape could be enough, for others that also scan superficial blood vessels thus making it very hard to fool the system. Circumventing a more secure fingerprint system with additional sensors is beyond the scope of reasonable security. For fingerprint scanners to work the hands cannot be dry because that lowers the quality of the image taken and damages such as cuts or burns affect the accuracy. To provide some level of fault tolerance more than one fingerprint could be stored per user in case the main one has been damaged. If the desktop is additionally supervised it would give some level of traceability, even if someone managed to circumvent the fingerprint.

Evaluation

From the user's perspective using a keycard in not uncommon and using their fingerprint is very intuitive. However, not all users might be comfortable having their biometric data stored by someone. Other users might have

degraded fingerprints due to their work or accidents. Otherwise, it is simple for the user to keep track of a keycard and not necessarily hard to take care of one's hands. The hardware requirements are relatively low, a keycard and a fingerprint reader. The software requirements are also relatively low, because the solution is straight forward and the fingerprint software is included when the fingerprint scanner is bought. The total cost is relatively low with one keycard per user and one fingerprint reader, $ 1 per user and 1000 users gives a cost of $ 1000 (fictive example). The deployment cost is potentially very low if keycards are already in use, then the fixed cost of implementation can be amortised over many users.

5.8 NFC, Numerical password, Secondary user identification

First, accessing a mobile device with a username and password. Final, use NFC to "tapp" the user's mobile device with another user's device, whom is authorised to confirm the first user's identity. This would require the user to posses an item, remember a password and have access to an authorised user. What is required to circumvent the system would be for the attacker to acquire a mobile device with an authorised user logged in and know the user's password. The key parts to preventing this scenario is to limit the access to the mobile devices and limit the number of authorised users. Since this method requires an "inside man" or stealing an active mobile device from someone, focusing on making the mobile devices more firmly attached to their user would increase the systems security. In the case of an "inside man" atleast traceability is supplied.

Evaluation

From the user's perspective "tapping" device with another user might be cumbersome if the user is unavailable or hard to find, a key part to the system is making user that the authorised users are limited enough to ensure that the system is secure yet numerous enough to be highly available. The authentication method itself is simple and intuitive. The hardware requirements are relatively high with a NFC enabled mobile device. The software requirements are relatively low due to the straight forward approach. The total cost is high with NFC enabled devices for all users, $ 50 per user and 1000 users gives a cost of $ 50'000 (fictive example). The deployment cost is potentially low if NFC enabled mobile devices are already in use, then the fixed cost of implementation can be amortised over many users.

5.9 Summary table

Combination	**User requirement**	**Hardware requirement**	**Software requirement**	**Total cost**	**Deployment cost**
Face 2D & 3D	Low	High	Medium	Medium	Low
Face & Finger	Low	Medium	Low	Low	Low
Keycard, NFC & Num pw	Low	High	Low	High	Low
Graph pw, IR(pos) & Num pw	Medium	High	Medium	High	Low
IR(data), Keycard & Num pw	Low	High	Low	High	Low
Barcode, Graph pw & Num pw	Medium	High	Low	High	Low
Finger & Keycard	Low	Low	Low	Low	Low
NFC, Num pw & second user	Medium	High	Low	High	Low

Chapter 6

Solution proposals

Introduction

In this chapter I will present proposals that could solve the problem defined earlier in chapter 3. The solution could be of three different natures, centralised, decentralised and semi centralised. Centralised solutions refer to limiting the user's access to the system to a very specific place, such as a desktop. Decentralised solutions refer to enabling the user to access the system from almost any place. Semi centralised solutions refer to a mix of centralised and decentralised, perhaps only a part of the access to the system is centralised.

6.1 Usage scenarios

The usage scenarios as defined in chapter 3 are managing assignments with nothing preplanned at the start of the shift and managing assignments with respect to breaks in the middle of the shift.

6.1.1 Shift change/beginning of shift

There are two approaches on how to deal with the shift change event. The first approach is that the reliving nurse does not have to meet up with the current nurse. When the reliving nurse is ready she assigns tasks to herself from all tasks in that department and the current nurse get a notification that she no longer has sole responsibility for those assignments. The second approach is that the reliving nurse meets up with the current nurse. When the reliving nurse is ready she seeks out the current nurse and selects tasks from the current nurse's assignments. With the first approach the disadvantages

are the complexity of selection from all assignments and availability of the desktop from which the selection is made. With the second approach the disadvantage is that the current nurse needs to have time to participate in the process. The advantages of the second approach is that since the pool of assignments to be selected from is smaller the interface can be very simple and enable decentralised solutions. However, if the reliving nurse needs to take assignments from several current nurses, the need to meet up with several nurses that may not be immediately available might be very cumbersome.

6.1.2 Breaks

In the scenario of a nurse taking a break she needs to find someone to temporarily take over the responsibility for all her assignments. The characteristics of this scenario are, a temporary task, all assignments are transferred at once and it occurs during an active shift. From the characteristics it is possible to make some draw some conclusions, a selection of specific tasks is unnecessary since all will be used, both nurses will interact again. The tasks could be grouped and marked as temporary for the reliving nurse to later simplify the returning process. This break handover scenario has less security requirements depending on how it is implemented, due to its temporary nature.

6.2 At a station with a NFC enabled mobile device

This is a centralised solution where the current nurse identifies herself to a desktop by starting an application on her mobile device and connects it to the desktop with NFC. She could then view her assignments at the desktop and select some or all assignments for transfer. After the current nurse has selected and confirmed the assignments to be transferred the relieving nurse identifies herself to the system in the same manner as the current nurse did, with her mobile device connecting with NFC. The relieving nurse can then review the assignments and confirm. Only after the relieving nurse has confirmed are the changes committed to the system.

6.3 Remotely with a NFC enabled mobile device

This is a decentralised solution where the current nurse and the relieving nurse both opens an application on their mobile devices, respectively enters their graphical password, respectively selects send mode or receive mode and taps them together. When the mobile devices are tapped together the units connect with each other through NFC, exchange information and sends a message to a local server. The local server uses the information it receives about the users to initiate the transfer of all the current nurse's assignments to the relieving nurse. Both users are then asked to confirm the transfer and when the server has received confirmation from both users the changes are committed.

6.4 Remotely with a IPS enabled mobile device

This is a decentralised solution where the current nurse opens an application on her mobile device, enters a graphical password and selects that she would like to be relieved. The application sends a message to a local server that initiates the transfer. The relieving nurse then opens the application on her mobile device, enters a graphical password and select that she would like to relieve another nurse. With the help of IPS the nurses that are close and wish to be relieved are displayed. The relieving nurse then selects the current nurse, this information is sent to the local server which now has all the information it needs to perform the transfer. The current nurse is sent a confirmation asking if she indeed wants to be relieved by the other nurse, when she confirms the transfer the local server commits the changes and sends a notification that the transfer is complete to the relieving nurse.

6.5 At a station with a keycard and fingerprint scanner

This is a centralised solution where the reliving nurse identifies herself to a desktop by first holding her keycard to a keycard reader and then her finger to a fingerprint scanner. The nurse can then view all the assignments belonging to the department in question and/or the assignments that has been preassigned to her. The nurse selects assignments and confirm the

selection. After the confirmation the system performs the changes and the nurses currently responsible for those assignments are sent a notification that the relieving nurse for the relevant selected assignments has arrived.

6.6 Remotely with a barcode reading mobile device

This is a decentralised solution where the relieving nurse opens an application on her mobile device, enters a graphical password and scans a barcode at a location that corresponds to each assignment she wants to select. After each barcode is scanned an update is sent to a local server that prepares to transfer these assignments to the nurse in question. When the relieving nurse is satisfied with the selected assignments she confirms the selection, which sends a message to the server to commit the changes. After the confirmation the system performs the changes and the nurses currently responsible for those assignments are sent a notification that the relieving nurse for the relevant selected assignments has arrived.

6.7 Remotely with a barcode reading device and at a station with a keycard

This is a semi centralised solution where the reliving nurse opens an application on her mobile device, enters a graphical password and scans a barcode at a location that corresponds to each assignment she wants to select. After each barcode is scanned an update is sent to a local server that prepares to transfer these assignments to the nurse in question. When the relieving nurse has selected all her assignments she goes to a desktop and identifies herself with a keycard. At the desktop the nurse can view all the assignments she has selected and possible preplanned assignments that was not selected. The relieving nurse then confirms the selection and the system commits the changes. After the confirmation the nurses currently responsible for those assignments are sent a notification that the relieving nurse for the relevant selected assignments has arrived.

Chapter 7

Development Of The Hardware Framework

Introduction

In this chapter I present the hardware that I use for my framework, with the goal of describing the hardware specifications I base my designs on and the reasoning behind my choices. Firstly, in section 7.1 I present relevant hardware that is already available in Ascom affiliated hospitals. Secondly, in section 7.2 I present the hardware that I use for the framework. Finally, in section 7.3 I discuss hardware that I did not use in the framework, but considered using and how I considered implementing them into the framework.

7.1 Existing hardware support

Some hardware is already available at the hospitals supplied by Ascom. The available hardware can simply be incorporated in the framework design without any need for specific development.

7.1.1 Keycard

A keycard is an item that works as a key, there are different types of keycards but the most common is RFID or NFC based. There are other keycard designs such as magnetic strip and smart cards with chip. In Swedish hospitals they use Citrix smart cards for access control, instead of using a username and password to login they just plug in their card which contains all necessary information.

7.1.2 MyCo (Android)

The MyCo is a smart device Ascom has developed as an extended part of their system. It is very durable, ergonomic and has passed several standard certifications for different regions for example EU and USA. It is primarily used to allow hospital employees quick and effortless access to important information.

- Android 5.1 Lollipop
- Supports third party applications
- Barcode reader API supports 1D and 2D
- Positioning system (associated access point, Ekahau RTLS and Cisco MSE)
- Wi-Fi a/b/g/n

7.1.3 MyCo v.2 (Android)

The MyCo v.2 is an upgraded version of the first MyCo, with the notable new features of IR positioning, NFC support and Google Mobile Services ready.

- Android 5.1 Lollipop
- Supports third party applications
- Barcode reader API supports 1D and 2D
- Positioning system (associated access point, IR, Ekahau RTLS and Cisco MSE)
- Wi-Fi a/b/g/n
- NFC
- Google Mobile Services

7.2 Hardware used in the framework

In this section I describe the hardware I used in my developed framework, I also comment on the requirements for the developed system. The goal of this section is to present what hardware I used and the reasoning behind why I made these choices.

7.2.1 Desktop framework

The hardware framework used for developing the desktop application was a computer that supported an Ethernet connection. The requirements for running the software is minimal, since no complex or computation heavy tasks are performed on the client side.

I did not implement any authentication process, due to time constraints, thus no keycard or smart card reader was used. The most important function for the testing framework is to demonstrate that a simple and secure transfer of assignments is possible. That the authentication part works is a known fact since it is already in use, which is why I choose to not implement this functionality.

7.2.2 Android framework

The hardware framework used for developing the Android application was a MyCo v.2; however a v.1 would have sufficed. The requirements for running the Android application is Wi-Fi support and at least Android API level 22 which corresponds to Android 5.1 Lollipop, because of URLConnection() for HTTP connections.

I did not implement any authentication process, due to time constraints. Neither did I implement any use of NFC, also due to time constraints.

During a conference call with a nurse working with Ascom on testing new products and services I learned that access to a desktop is limited for most nurses but everyone has access to a Android device. Thus my main priority was to implement the whole handover system to the Android platform.

7.3 Hardware considered but not used

There are a couple of authentication approaches I would have liked to implement. However, due to time constraints I could not implement them, these approaches would have impacted the required hardware. The authentication approaches I considered are: Keycard, Android with NFC simulating a keycard, Android with NFC scanning a keycard and Android with NFC connecting to another Android with NFC and finally IR positioning. Primarily I would have wanted to implement a NFC connection/transfer between Android devices since that would have been a very good approach, both intuitive and secure. Next, I would have wanted to implement an indoor positioning system; with IPS I could have implemented a "transfer zone" a user needs to be within to transfer assignments. Using a "transfer zone" would increase traceability if it is not possible to guarantee that the nurses meet each other face to face.

Chapter 8

Development Of The Software Framework

Introduction

In this chapter I will begin by presenting the software that was available before I started developing my framework. The purpose of this chapter is to describe how I developed my software framework and also how to perform some vital parts such as communicate with a server's REST API. In section 8.1 the relevant operations that the Ascom server already supports are described. In section 8.2 the methods that do more than just implement the server API functions are described. In section 8.3 I present my UI and further discuss it, most importantly I describe the UI I would have wanted to develop if not for time constraints. In section 8.4 I continue by describing similar topics as in 8.2 and 8.3 but for my Android application: Notable differences with Android development, communicate with a server's REST API and UI design. The desktop application is developed with C# and the Android application is developed with Java.

8.1 Existing software support

Some software is already available such as a server application programming interface (API) for handling the assignments. These APIs can directly be used and any hardware driver can also be directly used, without the need to develop my own.

8.1.1 Server API

The Ascom Unite server already supports many actions with its web server API. The web server API works by sending http messages to establish the communication between the sever and client. Both XML and JSON can be used to format these HTTP messages, the format used is determined in the header. There are a couple of basic parameters that needs to be configured before using the web server API by a third party program.

```
baseAddress = new Uri("https://hostname/Services.WebApi/");

handler = new HttpClientHandler { Credentials =
     new NetworkCredentia( "username", "password" ) };

Client = new HttpClient(handler) { BaseAddress = baseAddress };

Client.DefaultRequestHeaders.Accept.Add(
     new MediaTypeWithQualityHeaderValue("application/json"));
```

HTTP messages can now be created and sent to the targeted base address, for each message the address needs to be completed (base + rest). Additionally, for 'PUT' messages the content needs to be correctly supplied as well. I added the ConfigureAwait(false) setting to prevent deadlock due to awaiting incomplete tasks. If dynamic variables, such as id numbers, needs to be entered into the rest address then the String.Format() method is very useful.

```
response = await Client.GetAsync(
                restAddress).ConfigureAwait(false);

response = await Client.PutAsJsonAsync(
                restAddress,
                content).ConfigureAwait(false);
```

The response object here represents the whole HTTP message not the content, from the object it is possible to get status codes of the request message and the content of the response message. If the content should be interpreted as a specific data type or custom data contract that is both possible and simple.

```
response.IsSuccessStatusCode (Bool if code 200, OK)

response.StatusCode.ToString()

content = await response.Content.ReadAsAsync<datatype>();
```

Search users

Search users is a server supported method, which allows a user to search the user database. There are three parameters that can be specified for this method. First, it is possible to specify a pattern the user would like to search for. Second, it is possible to specify how many of the search results the user would like to fetch. Final, it is possible to specify from which index in the database the user would like to start the search. Since there has not been a demand to be able to pattern search for usernames, this functionality has not been implemented.

Search users II

There is another server supported method to fetch a user from the user database. The second method only takes one parameter and that is a user ID number. The method either returns the information regarding the user with that ID number or does not return any result.

Get assignments

Get assignments is a server supported method, that gets a user's assignments. The method takes two arguments: user ID and a boolean for only active assignments. Get assignments then returns a list of that user's specified assignments, if only active is chosen then the inactive assignments are ignored.

Set user assignments

Set user assignments is a server supported method, that sets the parameters for a collection of assignments. The method takes four arguments: IDs of the locations (room/bed/corridor), ID of the work shift, ID of the owner (organisation) and a collection of the changed assignments. Only the selected locations are affected by the change. One parameter in each assignment is the user responsible for that assignment, other parameters are ID of the user's device, location ID) and ID of the work shift.

Commit changes

Commit changes is a server supported method, that activates any changes made. In other words, after set user assignments is used nothing actually change until the commit changed method is used. The method takes two

arguments, the ID of the work shift in question and the ID number of the version of the assignments for that shift that should get activated.

8.2 Developed desktop software

My implementation of the get assignments method, set assignments method and the commit changes method only uses the server API methods, with some additional error handling code.

8.2.1 Get user

My implementation of this server supported method queries the server for all users with the supplied first name and then it searches the received list of users for surname or username match. Ideally the username should be used directly since it should be unique contrary to most names. If the method finds the user it returns the user's data contract, otherwise it returns different error messages depending on why a specific user could not be found.

8.2.2 Handover

The handover method performs the transfer of all the first user's active assignments to the second user. The method gets the active assignments of the first user, changes the user id for the assignments to the second user's and changes the associated mobile device ID from the first user's to the second user's device. This new updated version of the assignments is then sent to the server which replies with the new version ID of the active work shift's assignments. At this point no changes have been made to the system yet, in order to avoid any down time due to a system update the changes are first prepared and loaded but not committed. When the system is prepared for committing the changes it replies with the work shift version ID, which is used to actually commit the changes.

8.3 Desktop user interface

User interface (UI) refers to how a user can interact with a system. An example is an industrial control panel, another example is a graphical user interface. In other words, UI refers to the way a human user can provide input to the system. A UI can be mechanical, text-based or graphical. UI design is about presenting information and options to the user with an appropriately level of complexity, depending on who the intended user is.

8.3.1 Developed desktop user interface

The user interface I developed enables transferring the active assignments of one user to another (figure 8.1). The UI allows a user to search the user database for specific users, the search is based on the target user's name. If a search is inconclusive or lacks results that is notified to the user. After the target user is found it is possible to select the user as either the source or destination of the transfer of active assignments. When there is a current user (source) as well as a new user (destination) it is possible to commence with the handover of active assignments. If both source and destination is the same user the handover will not initiate (transfer to self is redundant), if the source does not have any active assignments the system notifies the user of this fact.

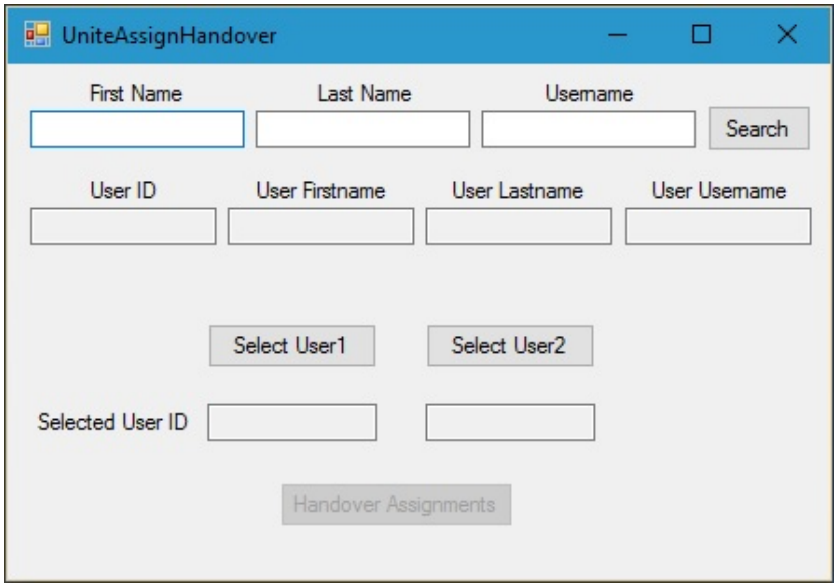

Figure 8.1: The desktop user interface I developed.

8.3.2 More ideal desktop user interface

If time had allowed I would have liked to develop a better user interface. An interface that allowed for more options, at the same time as it is even easier to both understand and use. This interface would consist of three different approaches: Handover all active assignments, handover some active assignments and assign tasks to yourself. The UI would be built to first require a user to authenticate him- or herself and then select one of the three approaches (figure 8.2).

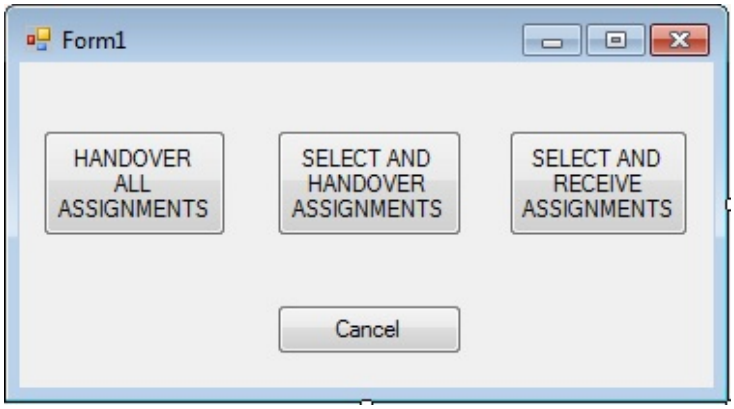

Figure 8.2: Interface prompting the user to select one of three approaches

The first approach would consist of simply letting another user authenticate him- or herself to the system and then confirm the intention to handover all active assignments (figures 8.3 and 8.4).

Figure 8.3: Waiting for the other user's authentication.

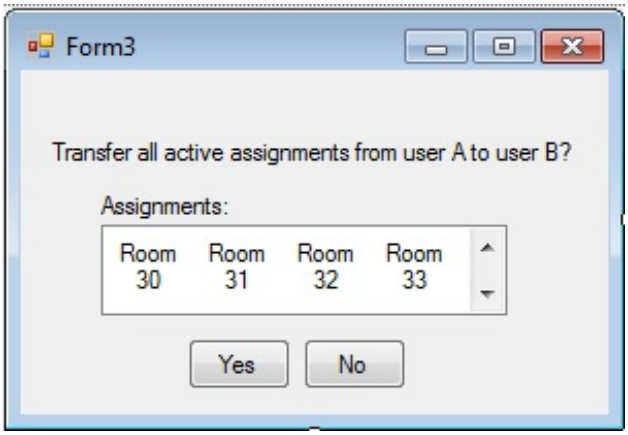

Figure 8.4: Waiting for confirmation before committing any changes.

The second approach would consist of choosing assignments from a list of the users active assignments by drag and drop (figure 8.5). When all desired assignments have been selected, confirm the selection, let another user authenticate themselves and finally confirm the intention to handover the selected assignments (figure 8.6).

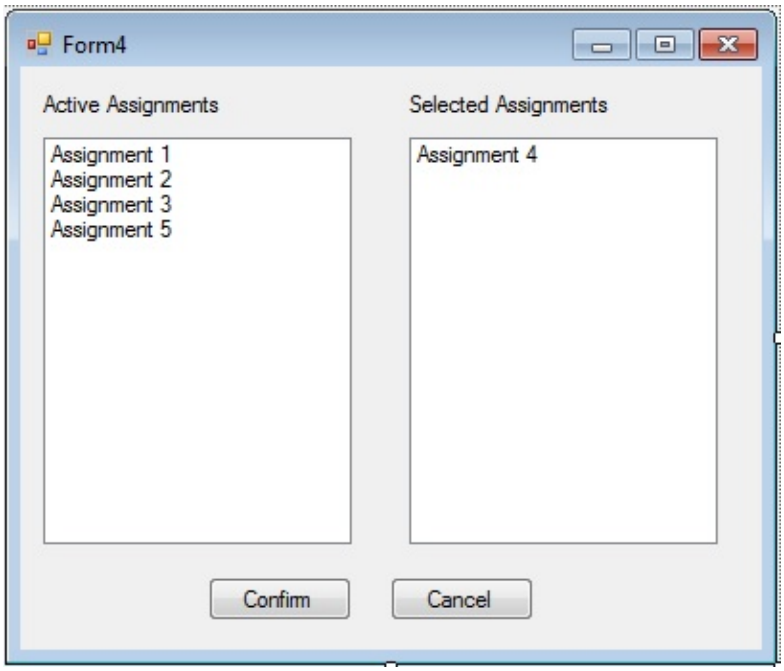

Figure 8.5: Select active assignments from the list, to be transferred.

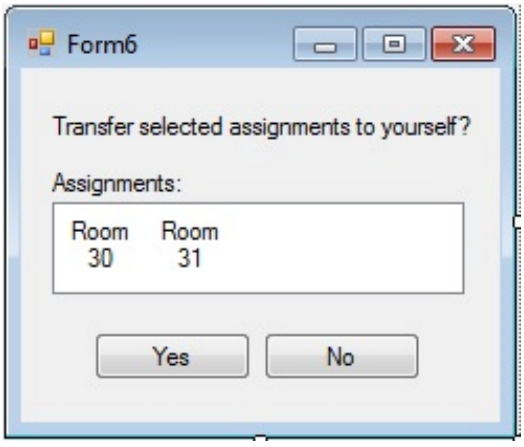

Figure 8.6: Waiting for confirmation before committing any changes.

The final approach would consist of a topological view that allows the user to see what the assignments represent (figure 8.7): Perhaps a corridor of rooms, if greater detail is required a selected room could show a view of the beds within. Each selected assignment is represented and shown in the topological view, granting a user friendly overview. After the selection is complete and is confirmed by the user a list of the selected assignments is shown and after a secondary confirmation the selected tasks are assigned to the user.

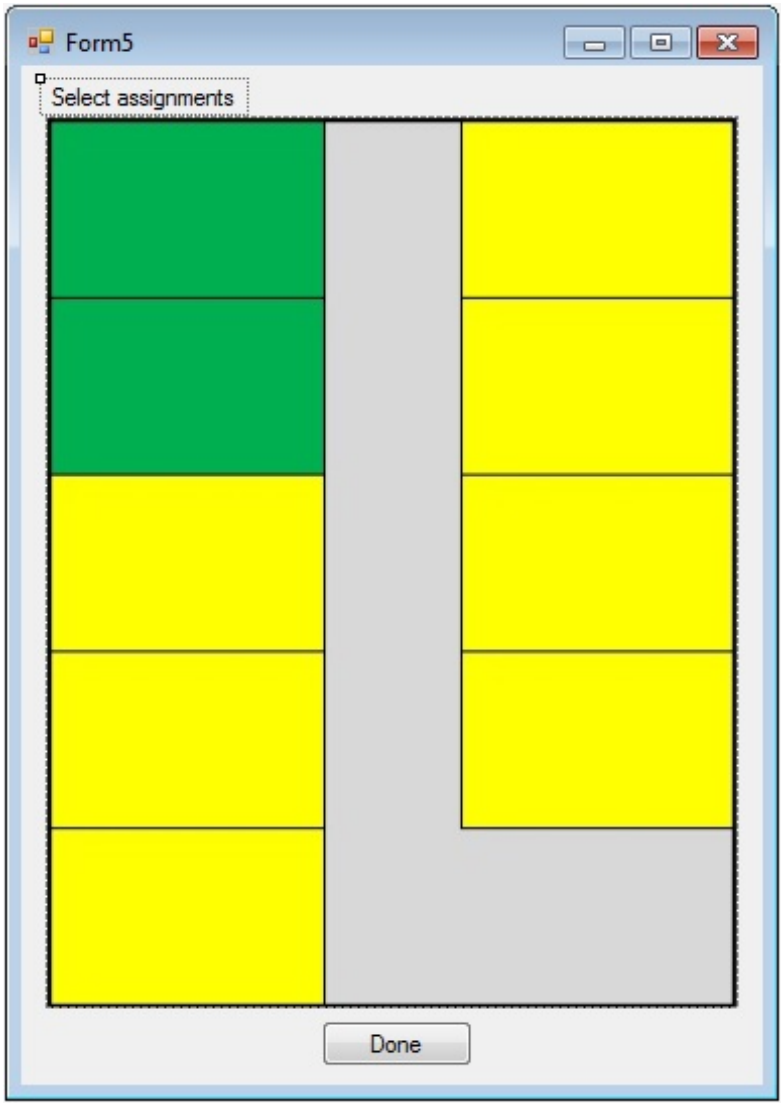

Figure 8.7: Corridor with rooms: Green=Selected, Yellow=Not Selected

8.4 Developed Android software

Developing an Android application in Java is not very different from developing desktop software. There are however a couple of differences that have to be considered: Application life cycle, activities/services, broadcasts and the available libraries are limited by the minimum targeted Android version (API level).

I developed the same functionalities for the android platform as for the desktop platform. Some details and objects are different due to the different programming languages but the behaviour and possibilities are the same. A simple GET interaction with the server API is described below.

```
url = new URL( baseAddress.append(restAddress) );

conn = (HttpsURLConnection) url.openConnection();

conn.setRequestMethod("GET");

conn.setRequestProperty("Accept", "application/json");

auth = "username:password";

encodedAuth = Base64.encodeToString(
          auth.getBytes(),
          Base64.DEFAULT );

conn.setRequestProperty(
          "Authorization",
          "Basic " + encodedAuth);

bufferReader = new BufferedReader(
          new InputStreamReader(
                  conn.getInputStream()));

responseContent = bufferReader.readLine();

gson = new Gson();

data = gson.fromJson(
          responseContent,
          datatype.class);
```

8.4.1 User interface

The user interface for the Android application is more well developed than the desktop UI. It is not the same as the more ideal UI example I gave in section 8.3.2 but it follows the same principles.

The first screen a user sees when they run the application is prompting them to supply their user ID (figure 8.8). Ideally this part would be automated and the application can get the information based on the active user logged in to the device. This access control property is called single sign-on. After the user is known the application could request a password to further confirm the users identity. However, I implemented neither an automatic user ID fetch or password authentication, due to time constraints. For the Android UI I use the users unique ID but their names could also be used, I simply used the ID because it was simpler to implement and I have already proven that name search works previously in the desktop UI.

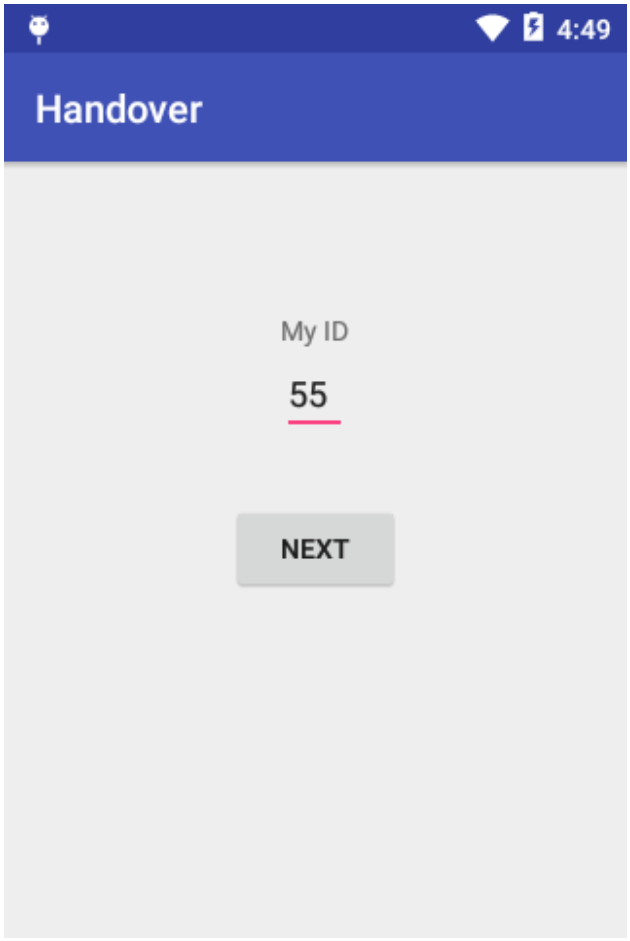

Figure 8.8: First interface (authenticate/identify), supplied with an user ID.

The second screen a user gets to lets them choose what kind of action they would like to perform (figure 8.9). The choices a user can select from are quick handover, handover or debug.

Figure 8.9: Select handover approach interface.

The quick handover was meant to use NFC to transmit the ID of the first user to the second user's device, which then performed a handover of all active assignments (figure 8.10). The interface is composed of two buttons and a text field. The two users that wish to perform a handover each press their respective button, the text field continuously supplies instructions and descriptions during the process.

Regrettably, I did not have time to actually implement the use of NFC into the system. However, the functionality is important enough to not remove the interface from the framework, even though the functions supporting NFC have not been developed.

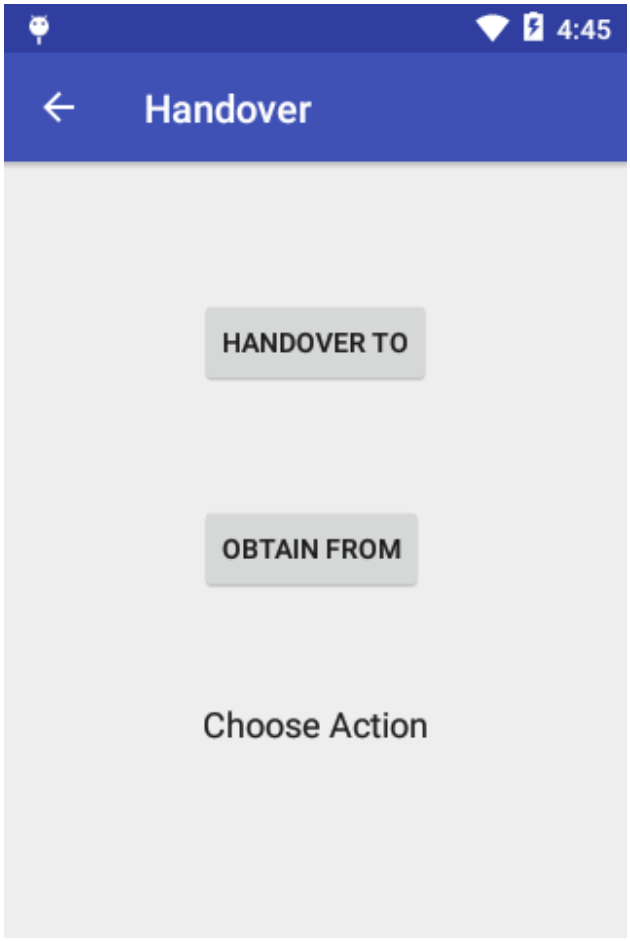

Figure 8.10: Quick handover interface, receive or handover assignments.

The handover interface requires the user to search for a second valid user in the user database (figure 8.11). The search result is then shown and if a valid user is found the interface also displays if that user has any active assignments. If the second user indeed has active assignments the first user can handover those assignments to him- or herself. It is possible for more than one user to be assigned to a task.

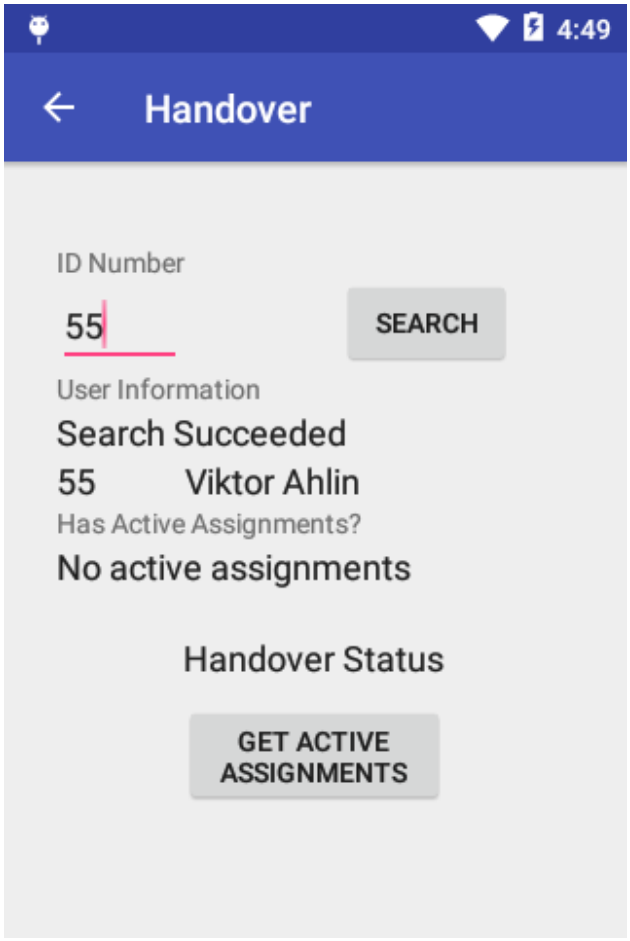

Figure 8.11: Standard handover interface, fetch a copy of another user's active assignments.

The debug interface works exactly like the desktop UI, any two users can be searched for and an handover between them can be performed (figure 8.12). This interface is mainly for testing purposes, but could be used by a head nurse to perform a handover for other nurses.

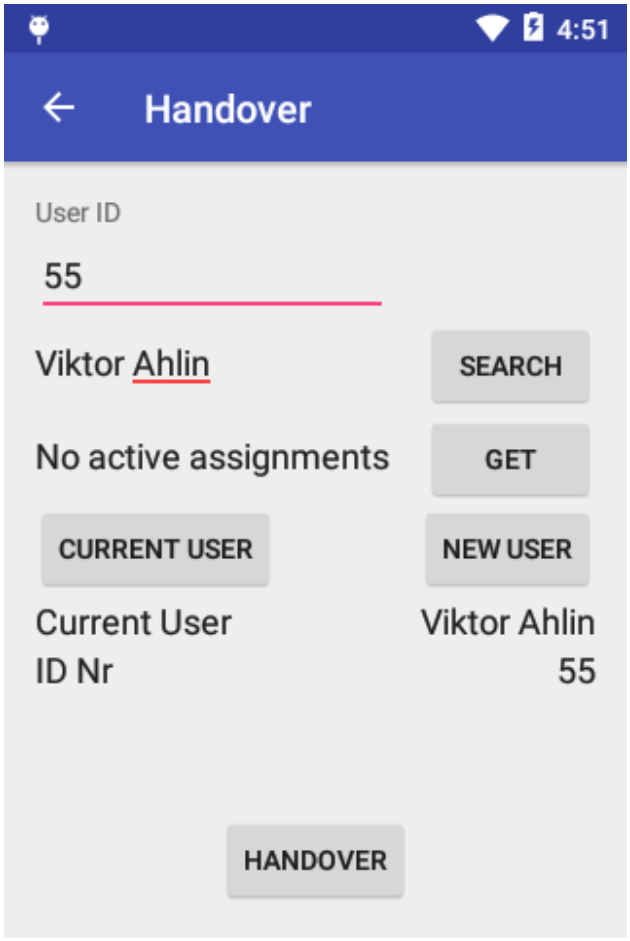

Figure 8.12: Debug interface, transfer active assignments from any user to any user. Used for debugging or by a super user (head nurse).

Finally, after any attempt to transfer assignments a confirmation dialogue appears (figure 8.13). The dialogue contains information concerning the status of the transfer, if it succeeded or failed. Because it is a confirmation dialogue the user is be able to acquire this information before moving on. Thus, eliminating any uncertainty about if the user is responsible for the assignment or not.

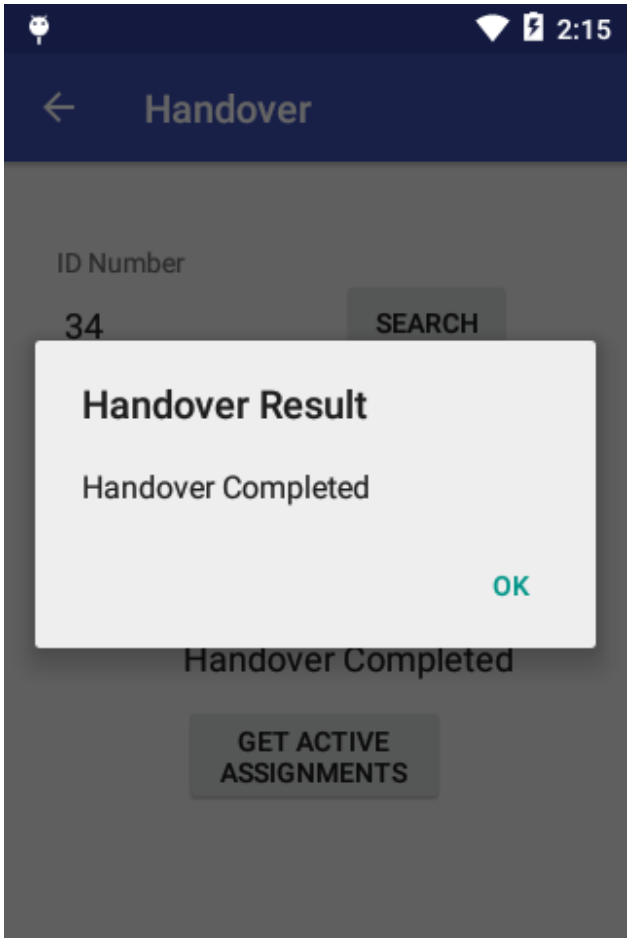

Figure 8.13: Dialogue confirming that the user knows the result of the handover.

Chapter 9

Discussion

There are a couple of things about this thesis that I would like to comment, both about the preparatory background research as well as the developed system framework.

Firstly, the research into biometric authentication methods was not as substantial as I first planned. There are many different biometrics and most of them also have different algorithms to define and compare biometric templates.

Secondly, having an audit trail for transactions such as an assignment handover is important, logging actions for traceability purposes is vital if something goes wrong. This logging should be performed by the server.

Thirdly, before a handover of assignments is performed the rights of the receiving nurse needs to be checked to confirm that she is cleared to accept the assignments. Some assignments requires a specialised nurse and some do nor have any particular requirements.

Fourthly, when a transfer of assignments is executed a message should be sent to the current/previous user responsible for those assignments. Notifying the current user that another user has claimed responsibility for one or more of their assignments. In the assignment data contract from the server there is an ID for the current users mobile device, which can be used to send a message to that device.

Finally, it would be good if there was additional support on the server side, keeping collections of the assignments each user last handed over. This could create a break handling process that is both easy to use and does not compromise the system by using the escalation chain. Such a process would let a nurse handover her assignments, go on a break, come back from the break and simply request her assignments again.

Chapter 10

Future work

Taking the next step to expand upon this work can lead down different paths. The first path is to develop, test and compare more approaches to each other. The second path is to pick a certain approach and try to develop it to its limit, thus finding its potential. The third path would be to go back and add even more technologies or ways to implement concepts to the background research and comparison, for example more about biometrics.

Chapter 11

Conclusions

In this thesis I first describe some basic concepts and assisting technologies that are either used or referred to in the thesis. I present the problem this thesis tries to solve, which is a secure and simple assignment handover. I then evaluate and compare 10 different technologies, the technologies could be placed into three approximate groups (visual light, radio and biometric). I continue by combining some of these technologies, then evaluate and compare these combinations. From these evaluations I propose a couple of solutions that could solve the specified problem of a secure and simple assignment handover. I also develop a handover system framework that can perform a handover which can be used to test if the proposed solutions are viable. I did not have time to implement any authentication process into the testing framework. However, questioning that the authentication methods work by themselves is beyond the scope of this thesis.

From this thesis I drew three main conclusions, the topics of these conclusions are: extensive background research, approaching background research and potential of smartphones.

The first conclusion is that making a more extensive comparison between available technologies from time to time is very beneficial. If I had been able to spend more time developing the handover system for both desktop and Android, the developed system would have been better. However, my more extensive preliminary research has given my project a very strong foundation, which is easier to later build on and gives more weight to my design choices and arguments. Although I am satisfied with my result and preliminary research; I would not recommend performing such extensive comparisons too often, since they are time consuming. In a constantly evolving field such as security and authentication It is important to review more than the most likely candidates from time to time. Basing the selection of candidates on a more extensive overview enables a more well informed and objective selection,

likely producing a better result.

The second conclusion is that by considering problems thoroughly, more options are available when designing a system. With considering problems thoroughly I mean with the intent of finding 'possible solutions' instead of just 'a solution'. It is possible to solve a software problem with a hardware solution as well as the other way around. An example of this would be to distribute a symmetric encryption key using another media, such as a barcode.

The third and final conclusion is that smartphones can be used as a authentication tool. There is great potential in integrating smartphones into the authentication process, given how widespread their use is and the capabilities of most models. Particularly the Android devices with NFC support, since NFC is very suitable for authentication and handshake purposes.

The framework I developed and described in this thesis only needs an addition of an authentication process before testing how viable the system is in real life. It is my strong belief that implementing the system with my suggestions concerning authentication will lead to a both user-friendly and secure handover system. Such a system would also increase the availability of the handover process as well as reducing its complexity.

Bibliography

[1] Ascom official website. https://www.ascom.com/corp/about-us/brief.html. Accessed: 2017-02-17.

[2] Stanford University d.school. Design thinking. http://dschool.stanford.edu/dgift/. Accessed: 2016-11-21.

[3] Stanford University. Webinar - design thinking. https://www.youtube.com/watch?v=vSuK2C89yjA. Accessed: 2016-11-21.

[4] Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. *ACM Transactions on Computer Systems*, 8(1):18–36, February 1990. http://courses.cs.washington.edu/courses/csep552/16wi/papers/burrows-banlogic.pdf Accessed: 2016-11-16.

[5] John D. Woodward Jr., Christopher Horn, Julius Gatune, and Aryn Thomas. Biometrics: A look at facial recognition. Technical report, Rand Corp., 2003. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA414520 Accessed: 2016-11-14.

[6] Susan Wiedenbeck, Jim Waters, Jean-Camille Birget, Alex Brodskiy, and Nasir Memon. Authentication using graphical passwords: Effects of tolerance and image choice. In *Proceedings of the 2005 Symposium on Usable Privacy and Security*, pages 1–12, 2005. http://doi.acm.org/10.1145/1073001.1073002 Accessed: 2016-11-17.

[7] Tanvi Naik and Sheetal Koul. Multi-dimensional and multi-level authentication techniques. *International Journal of Computer Applications*, 75(12), 2013. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.402.9441&rep=rep1&type=pdf Accessed: 2016-11-17.

[8] Kyong I. Chang, Kevin W. Bowyer, and Patrick J. Flynn. Face recognition using 2d and 3d facial data. In *Workshop on Multimodal User Authentication*, December 2003. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.697.3724&rep=rep1&type=pdf#page=25 Accessed: 2016-11-15.

[9] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6), November 1976. http://math.boisestate.edu/~liljanab/MATH308/NewDirectionsCryptography.pdf Accessed: 2016-12-01.

[10] Joan Daemen and Vincent Rijmen. The block cipher rijndael. In *International Conference on Smart Card Research and Advanced Applications*. Springer, 1998. https://www.researchgate.net/profile/Vincent_Rijmen/publication/220962914_The_Block_Cipher_Rijndael/links/09e4150c0520ee1247000000.pdf Accessed: 2016-12-01.

[11] Advanced encryption standard (aes). http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard. Accessed: 2016-12-01.

[12] Aes encryption cracked. http://www.theinquirer.net/inquirer/news/2102435/aes-encryption-cracked. Accessed: 2016-12-01.

[13] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2), February 1978. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA606588 Accessed: 2016-12-08.

[14] Kevin Curran, Eoghan Furey, Tom Lunney, Jose Santos, Derek Woods, and Aiden McCaughey. An evaluation of indoor location determination technologies. *Journal of Location Based Services*, 5(2), June 2011. https://pdfs.semanticscholar.org/c214/477f7e82ff398c3badbd0cf716b8e2240c0b.pdf Accessed: 2016-12-15.

[15] Anyplace official website. https://anyplace.cs.ucy.ac.cy/. Accessed: 2016-12-15.

[16] Dimitrios Lymberopoulos, Jie Liu, Xue Yang, Romit Roy Choudhury, Vlado Handziski, and Souvik Sen. A realistic evaluation and comparison of indoor location technologies: Experiences and lessons

learned. In *Proceedings of the 14th International Conference on Information Processing in Sensor Networks*, 2015. http://eprints.networks.imdea.org/997/1/competition_IPSN2015.pdf Accessed: 2016-12-15.

[17] NASA Mission:Science. Anatomy of an electromagnetic wave. http://missionscience.nasa.gov/ems/02_anatomy.html. Accessed: 2016-11-14.

[18] NASA Mission:Science. Introduction to the electromagnetic spectrum. http://missionscience.nasa.gov/ems/01_intro.html. Accessed: 2016-11-14.

[19] Oxford University Press. Definition of barcode. https://en.oxforddictionaries.com/definition/barcode. Accessed: 2016-09-21.

[20] Eisaku Ohbuchi, Hiroshi Hanaizumi, and Lim Ah Hock. Barcode readers using camera device in mobile phones. In *International Conference on Cyberworlds*, 2004. http://www2.informatik.uni-halle.de/agprbio/AG/Lehre/ABV_SS07/material/Ohbuchi04.pdf Accessed: 2016-09-21.

[21] Gs1 official website. http://www.gs1.org/. Accessed: 2016-09-21.

[22] J.E. Thomas. High density matrix code. http://www.google.com/patents/US4263504, 1981. US Patent 4,263,504 Accessed: 2016-09-22.

[23] Tan Jin Soon. Qr code. *Synthesis Journal*, 2008. https://foxdesignsstudio.com/uploads/pdf/Three_QR_Code.pdf Accessed: 2016-09-22.

[24] Technologyuk. https://www.technologyuk.net/telecommunications/communication-technologies/infrared-communication.shtml. Accessed: 2016-10-24.

[25] Margaret Rouse. Ir wireless (infrared wireless). http://searchmobilecomputing.techtarget.com/definition/IR-wireless. Accessed: 2016-10-24.

[26] Irda official website. http://www.irda.org/. Accessed: 2016-10-24.

[27] sparkfun.com. https://www.sparkfun.com/products/241. Accessed: 2016-12-20.

[28] Fifth Edition American Heritage® Dictionary of the English Language. Definition of radio. http://www.thefreedictionary.com/Radio. Accessed: 2016-11-14.

[29] tpub.com. behaviour of radio waves in different media. http://armycommunications.tpub.com/ss0130a/Behavior-Of-Radio-Waves-In-Different-Media-18.htm. Accessed: 2016-11-14.

[30] Ari Juels. Rfid security and privacy: A research survey. *IEEE Journal on Selected Areas in Communications*, March 2006. https://www.researchgate.net/profile/Ari_Juels/publication\3236246_Rfid_security_and_privacy_a_research_survey_IEEE_J_Sel_Area_Comm/links/00b4953bbe80a8c975000000.pdf Accessed: 2016-09-22.

[31] Roy Want. An introduction to rfid technology. *Pervasive Computing*, 2006. https://www.cs.colorado.edu/~rhan/CSCI_7143_002_Fall_2001/Paper/rfid_intro_01593568.pdf Accessed: 2016-09-22.

[32] atlasrfidstore.com. https://www.atlasrfidstore.com/omni-id-iq-400p-roll-of-1000/. Accessed: 2016-09-22.

[33] atlasrfidstore.com. https://www.atlasrfidstore.com/thingmagic-nano-embedded-rfid-reader-module/. Accessed: 2016-09-22.

[34] Ann Cavoukian. Mobile near field communications. *ISSA Journal*, August 2012. https://c.ymcdn.com/sites/www.issa.org/resource/resmgr/journalpdfs/feature0812.pdf Accessed: 2016-09-22.

[35] nfcworld.com: list of nfc capable phones. http://www.nfcworld.com/nfc-phones-list. Accessed: 2016-10-24.

[36] gototags.com: iphone7 nfc support? https://gototags.com/blog/will-apple-finally-support-nfc-tag-reading-ios-10-iphone-7/. Accessed: 2016-10-24.

[37] zipnfc.com: iphone7 still no nfc. https://zipnfc.com/index.php/blog/post/view/identifier/iphone7-no-to-nfc-tags. Accessed: 2016-10-24.

[38] store.gototags.com. http://store.gototags.com/nfc-tags/ready-made-nfc-tags/ready-made-nfc-stickers/. Accessed: 2016-10-24.

[39] store.gototags.com. http://store.gototags.com/hardware/desktop-hardware/desktop-nfc-readers-and-writers/. Accessed: 2016-10-24.

[40] radio-electronics.com. http://www.radio-electronics.com/info/wireless/nfc/nfc-near-field-communications-security.php. Accessed: 2016-10-24.

[41] Jin-Shyan Lee, Yu-Wei Su, and Chung-Chou Shen. A comparative study of wireless protocols: Bluetooth, uwb, zigbee, and wi-fi. In *The 33rd Anual Conference of the IEEE Industrial Electronics Society (IECON)*, November 2007. http://eee.guc.edu.eg/Announcements/Comparaitive_Wireless_Standards.pdf Accessed: 2016-09-22.

[42] bluetooth.com. https://www.bluetooth.com/what-is-bluetooth-technology/how-it-works. Accessed: 2016-09-26.

[43] Texas instruments. https://store.ti.com/ProductAccessories.aspx?ProductId=38494. Accessed: 2016-09-26.

[44] Kaspersky official blog. https://blog.kaspersky.com/bluetooth-security/1637/. Accessed: 2016-09-26.

[45] Wi-fi alliance official website. http://www.wi-fi.org/. Accessed: 2016-09-27.

[46] Guido R. Hiertz, Dee Denteneer, Lothar Stibor, Yunpeng Zang, Xavier Pérez Costa, and Bernhard Walke. The ieee 802.11 universe. *IEEE Communications Magazine*, January 2010. http://xavierperezcosta.com/publications/IEEE%20Com%20-%2080211%20Universe.pdf Accessed: 2016-09-27.

[47] netonnet.se.
https://www.netonnet.se/art/dator/natverk/routermodem.
Accessed: 2016-09-27.

[48] amazon.com. https://www.amazon.com/
Internal-Computer-Networking-Cards/b?ie=UTF8&node=13983711.
Accessed: 2016-10-03.

[49] Stefan Mangold, Sunghyun Choi, Peter May, Ole Klein, Guido Hiertz, and Lothar Stibor. Ieee 802.11e wireless lan for quality of service. http://eclass.gunet.gr/modules/document/file.php/DI121/%CE%A3%CE%B7%CE%BC%CE%B5%CE%B9%CF%8E%CF%83%CE%B5%CE%B9%CF%82/802_11e.pdf Accessed: 2016-10-03.

[50] Arash Habibi Lashkari, Mir Mohammad Seyed Danesh, and Behrang Samadi. A survey on wireless security protocols (wep, wpa and wpa2/802.11i). http://www2.it.lut.fi/wiki/lib/exe/fetch.php/courses/ct30a2001/opiskelijat/2008/a_survey_on_wireless_security_protocols_wep_wpa_and_wpa2_802.11i_.pdf. Accessed: 2016-10-03.

[51] Vishal Kumkar, Akhil Tiwari, Pawan Tiwari, Ashish Gupta, and Seema Shrawne. Vulnerabilities of wireless security protocols (wep and wpa2). *International Journal of Advanced Research in Computer Engineering & Technology*, 1, April 2012. http://ijarcet.org/wp-content/uploads/IJARCET-VOL-1-ISSUE-2-34-38.pdf Accessed: 2016-10-03.

[52] ISO/IEC. *ISO/IEC 26907:2009*, 2 edition, November 2009. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=53426 Accessed: 2016-10-21.

[53] Ian Oppermann, Matti Hämäläinen, and Jari Iinatti, editors. *UWB Theory and Application*. John Wiley & Sons, Ltd, 2004. http://bbs.hwrf.com.cn/downebd/14536d1142862780-wiley_uwb_theory_and_applications_7191.pdf Accessed: 2016-10-03.

[54] Uwb forum and wimedia alliance committed to commercializing uwb. https://web.archive.org/web/20070217143201/http://www.uwbforum.org/index.php?option=com_content&task=view&id=121&Itemid=2. Accessed: 2016-10-21.

[55] Neal Leavitt. *For Wireless USB, the Future Start Now*. IEEE Computer Society, July 2007. http://www.123seminarsonly.com/

Seminar-Reports/008/23199473-Wireless-Usb.pdf Accessed: 2016-10-21.

[56] Uwb - ultra-wide band. https://www.lifewire.com/ultra-wide-band-817953. Accessed: 2016-10-21.

[57] Zebra official website. https://www.zebra.com/us/en.html. Accessed: 2016-11-21.

[58] Patrick Kinney. Zigbee technology: Wireless control that simply works. In *Communications design conference*, volume 2, pages 1–7, 2003.

[59] sparkfun.com. https://www.sparkfun.com/products/11215. Accessed: 2016-12-20.

[60] Anil K. Jain, Arun Ross, and Salil Prabhakar. An introduction to biometric recognition. *IEEE Transactions on Circuits and Systems for Video Technology*, 14(1), January 2004. http://www.cse.msu.edu/~rossarun/BiometricsTextBook/Papers/Introduction/JainRossPrabhakar_BiometricIntro_CSVT04.pdf Accessed: 2016-11-3.

[61] Simon Liu and Mark Silverman. A practical guide to biometric security technology. *IT Pro*, January-February 2001. https://intranet.dcc.ufba.br/pastas/gaudi/biometrica/papers/id/PraticalGuideBiometric-00899930.pdf Accessed: 2016-11-3.

[62] Anil K. Jain, Lin Hong, Sharath Pankanti, and Ruud Bolle. An identity-authentication system using fingerprints. *Proceedings of the IEEE*, 85, September 1997. http://biometrics.cse.msu.edu/Publications/Fingerprint/JainEtAlIdentityAuthUsingFp_ProcIEEE97.pdf Accessed: 2016-10-26.

[63] bayometric.com. https://www.bayometric.com/secugen-hamster-iv-fingerprint-reader-scanner/. Accessed: 2016-10-31.

[64] P. Jonathon Phillips, Patrick J. Flynn, Todd Scruggs, Kevin W. Bowyer, Jin Chang, Kevin Hoffman, Joe Marques, Jaesik Min, and William Worek. Overview of the face recognition grand challenge. In *IEEE Computer Society Conference on Computer Vision and Pattern*

Recognition, 2005.
http://ivizlab.sfu.ca/arya/Papers/IEEE/Proceedings/C%20V%20P%20R-%2005/Face%20Recognition%20Grand%20Challenge.pdf
Accessed: 2016-11-15.

[65] Kevin Bonsor and Ryan Johnson. How facial recognition systems work. http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm, 2001. Accessed: 2016-11-15.

[66] M. Alex O. Vasilescu and Demetri Terzopoulos. Multilinear image analysis for facial recognition. In *International Conference on Pattern Recognition*, August 2002.
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.697.3724&rep=rep1&type=pdf#page=25 Accessed: 20016-11-15.

[67] Open scource vision initiative. http://docs.opencv.org/2.4/modules/contrib/doc/facerec/facerec_tutorial.html. Accessed: 2016-11-15.

[68] List of different software for face detection and recognition. https://facedetection.com/software/. Accessed: 2016-11-15.

[69] aliexpress.com. https://www.aliexpress.com/item/Factory-price-Biometric-Fingerprint-Face-Recognition-Time-Attendance-System-32640545401.html?spm=2114.40010508.4.75.tKxS25. Accessed: 2016-11-15.

[70] Kyong I. Chang, Kevin W. Bowyer, and Patrick J. Flynn. Multi-modal 2d and 3d biometrics for face recognition. In *IEEE International Workshop on Analysis and Modeling of Faces and Gestures*, 2003.
https://pdfs.semanticscholar.org/10c7/9df4f44b5e4c08f984f34370d292f31ef309.pdf Accessed: 2016-11-22.

[71] Lin Hong and Anil Jain. Integrating faces and fingerprints for personal identification. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 20(12), December 1998.
http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=F8A3E82D4731583793954AB1FBEE2545?doi=10.1.1.105.2223&rep=rep1&type=pdf Accessed: 2016-11-22.