Noora Hämäläinen

BIOMETRICS AS AN ALTERNATIVE TO PASSWORDS FOR OLDER USERS

JYVÄSKYLÄN YLIOPISTO
TIETOJENKÄSITTELYTIETEIDEN LAITOS
2015

ABSTRACT

Hämäläinen, Noora
Biometrics as an alternative to passwords for older users
Jyväskylä: University of Jyväskylä, 2015, 31 p.
Information Systems Science, Bachelor's thesis
Supervisor: Woods, Naomi

This bachelor's thesis is a literacy review that aims to find out if biometrics could provide a reasonable alternative for passwords for older adults. The issues are perceived is from an older user's perspective.

The number of older adults, meaning those at the age of 65 or more, is increasing worldwide. Age comes with physical and cognition-related changes that makes this user group differ from other users, as the age-related cognitive decline effects memory. Passwords are a widely used authentication mechanism today, and rely heavily on the user's memory performance. The older adults with decreased mobility and increased isolation would benefit from web-based services, but the inconvenient authentication mechanisms may hinder their access.

The study briefly introduces the concept of authentication and then continues by examining the most common authentication techniques in more depth. This study will then discuss older adults as technology users and point out how they may differ from the average user group. Finally, biometrics are considered as an alternative to passwords, particularly for the older users.

The aging process results in many physical and cognitive changes, some of which may need to be considered while evaluating the usability of biometrics. However, there are a large amount of different biometrics applications with different characteristics. As the population of older adults is growing; their different abilities and limitations, make it difficult to draw a general conclusion for the suitability of biometrics.

Keywords: Biometrics, aging users, older users, authentication, passwords

TIIVISTELMÄ

Hämäläinen, Noora
Biometrics as an alternative to passwords for older users
Jyväskylä: Jyväskylän yliopisto, 2015, 31 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja: Woods, Naomi

Tämän kirjallisuuskatsauksena toteutetun kandidaatin tutkielman tarkoituksena on selvittää, että voisivatko biotunnisteet tarjota mielekkään vaihtoehdon salasanoille. Tutkielma keskittyy tarkastelemaan edellä mainittua tutkimusongelmaa ikääntyneiden käyttäjien näkökulmasta.

Ikääntyneiden aikuisten, joilla tässä tutkielmassa tarkoitetaan 65 vuoden iän saavuttaneita, määrä on lisääntynyt maailmanlaajuisesti. Ikääntymisprosessiin liittyy niin fysiologisia kuin kognitionaalisiakin muutoksia, joiden johdosta ikääntyneet käyttäjät poikkeavat muista käyttäjäryhmistä. Lisäksi kognitiivisten toimintojen heikkeneminen vaikuttaa etenkin muistitoiminnoista suoriutumiseen. Liikkuvuuden rajoittuessa ja eristyneisyyden lisääntyessä ikääntyneet aikuiset voisivat hyötyä verkkopohjaisista palveluista, mutta epäkäytännölliset todennusmenetelmät saattavat vaikeuttaa niihin pääsyä.

Tutkielma esittelee lyhyesti autentikoinnin eli todennuksen periaatteita ja listaa tyypillisimmät biotunnisteita hyödyntävät todennustekniikat, edeten sitten kuvailemaan ikääntyneitä teknologian käyttäjiä ja heidän erityspiirteitään keskiverto käyttäjäryhmiin verrattuina. Lopuksi arvioidaan biotunnisteiden soveltuvuutta salasanoille vaihtoehtoiseksi todennusmenetelmäksi, keskittyen etenkin ikääntyneen juuri käyttäjän näkökulmaan.

Ikääntymisen katsotaan siis aiheuttavan monia kognitiivisia ja fyysisiä muutoksia, jotka olisi syytä huomioida biotunnisteiden käytettävyyttä arvioitaessa. Erilaisten biotunnisteiden joukko on kuitenkin hyvin laaja ja vaihteleva, aivan kuten ikääntyneiden käyttäjienkin joukko, mikä vaikeuttaa johtopäätösten tekemistä näiden menetelmien yleistasoisesta soveltuvuudesta kyseiselle käyttäjäryhmälle.

Asiasanat: Biotunnisteet, ikääntyneet käyttäjät, todennus, autentikointi, salasanat

TABLE OF CONTENTS

1 INTRODUCTION

Authentication is a process of confirming that the user really is who he/she claims to be, before granting an access or permissions into a system. A user identifies him or herself with a username and then provides evidence of his/her identity in a form of a password. Biometrics is an authentication mechanism that identifies the user based on their physical and behavioral characteristics, rather than what they remember (in terms of alphanumerical passwords) or have (tokens) (Renaud, 2005.)

Biometrics are becoming more and more mainstream with the recent development in smartphone and wearable mobile digital technology. Not only have the current mobile giants, such as Samsung and Apple, been showing interest towards biometrics by filing biometric-related patents, but also law enforcement agencies and the banking sector have been attracted by the new possibilities of these authentication mechanisms. Analyst firm Gartner forecasted that by the year 2016, 30% of organizations will be using biometric authentication on mobile devices. (Caldwell, 2014.)

New implications of biometric authentication seem to surface frequently, and their usability and security has been a common interest for researchers. However, it seems that the majority of the studies have focused on the user across all age groups not considering the effect of age.

In Western Europe, the percentage of those aged 65 and over is expected to rise from 18.3% in 2010 to 25,4% in 2030 (Peine, Rollwagen, & Neven, 2014). Aging causes the physical and psychological changes in a person. This includes memory decline, for example in the working memory and in performing complex mental manipulations; in retrieving information from the long-term memory; as well as in the ability to pay attention (Erber, 2013). However, there are physical changes too, one of which can be seen for instance in a person's skin, which becomes drier, saggy and wrinkled (Erber, 2013).

Memory is a significant problem when trying to recall passwords, and therefore biometrics would seem to be a good alternative, especially for older users, since they do not burden the memory. However, some studies have suggested that the physical changes of aging people might affect the usability and reliability of biometrics. (Kowtko, 2014; Modi, Elliott, Whetsone, & Hakil Kim, 2007.)

This study aims to find out if biometrics would be a reasonable alternative for passwords from an older user's perspective. At first this study will discuss the authentication mechanisms in general, and then proceed in further detail with biometrics and introduce some applications.

Since the goal is to evaluate biometrics from an older user's perspective, this study will also aim to introduce the older person as a technology user. It will define the characteristic features and differences that need to be considered while designing biometric systems that would be usable for this age group as well.

This study has been performed as a literacy review and the referred articles were mainly retrieved from databases such as ScienceDirect, IEEE Xplore Digital Library and Google Scholar.

2 BIOMETRICS AND OTHER AUTHENTICATION MECHANISMS

This chapter introduces the most common authentication mechanisms including passwords, security devices and biometrics. The biometrics are then further observed in terms of presenting some of the biometric applications and by giving a brief outlook on their current state.

2.1 Authentication mechanisms

Authentication is one phase in a security process that regulates the accessibility of a system. At first the user is identified, meaning that the system requires the user to introduce him- or herself with a username or other previously agreed identifier. Once the user is identified, the authentication phase then follows, where the user has to prove his or her identity, (prove that they are who they claim to be). After a successful authentication, the system grants the authenticated user access to the system as well as the appropriate permissions to do actions within the system. (Renaud, 2005.)

There are several possible methods to authenticate the user. Authentication can be based on something that user is, knows, recognizes or holds (Renaud, 2005). These different methods are discussed further in the following chapters.

2.1.1 Passwords and memory-based mechanisms

Passwords are based on something that user knows: a previously agreed secret shared between the system and the user (Renaud, 2005). Passwords are one of the most common authentication mechanisms (Taneski, Henricko & Brumen, 2014).Passwords consists of a sequence of characters and digits. These characters can be either randomly generated or selected by the user (Renaud, 2005).

From a security point of view, the best and the strongest password would be the one that consists of the maximum allowed amount of characters that are randomly selected from all available characters (Yan, Blackwell, Anderson & Grant, 2005). Many systems have security policies and requirements for passwords that are intended to ensure a high entropy, even if the set of available characters is limited (Taneski et al., 2014). Unfortunately, these kinds of passwords are not something that a human memory can easily cope with (Yan et al., 2005). Password policies, like password aging, which requires that passwords are changed regularly, tend to compound these problems (Taneski et al., 2014).

According to Jakobsson and Dhiman (2013) people tend to use rules to form passwords. Passwords consist of components such as dictionary words, numbers and other characters that are used to compose a password, with rules such as concatenation, replacement, spelling mistake and insertion. Concatenation means simply putting components together ("password12"); replacement refers to replacing characters with other characters like some of letters with numbers ("p4ssw0rd"); misspelling may be intentional or unintentional ("passwrd"); and with insertion, components are inserted into each other ("pass12word"). (Jakobsson & Dhiman, 2013.)

Mnemonics are a way to create seemingly random alphanumerical passwords (passphrases) that are still reasonably easy to remember (Yan et al., 2005). The user uses a sentence to create a word, for example by taking the first letter of each word (e.g. "Passwords should include 8 or more characters!" may lead to "Psi8omc!") (Yan et al., 2005; Fukumitsu, Katoh, Bista & Takata, 2010). Using full sentences as passphrases is also an option that is proven to be more resistant to dictionary attacks than alphanumerical passwords, but the users of passphrases have been shown to experience higher login failure rates due to typographical errors (Taneski et al., 2014) The criticism towards mnemonics says that people tend to choose well-known sentences such as famous quotes or song lyrics that makes the formed mnemonic password easier to crack (Ma & Feng, 2011; Taneski et al., 2014; Fukumitsu et al., 2010). Fukumitsu et al. (2010) suggest a method where the sentence is formed based on a picture chosen by the user in order to prevent choosing phrases that can be found from the Internet.

Graphical methods are yet another form of authentication. This method utilizes the power of human's visual memory with nearly limitless capacity for pictures (Renaud, 2005). De Angeli, Coventry, Johnson and Renaud (2005) propose that graphical methods should be divided to three categories of cognometrics, locimetrics and drawmetrics. Cognometrics are based on something that the user recognizes (Renaud, 2005). Locimetrics are based on a mnemonic method of loci, where the recalled items are associated with physical locations (De Angeli et al., 2005). Drawmetrics on the other hand are methods where the user is required to redraw a previously chosen figure (De Angeli et al., 2005).

According to Renaud (2005), cognometric systems can be either recognition- or position-based. Recognition-based makes the user select a correct picture among a group of pictures, relying purely on the visual memory. Position-based requires user to identify target objects within an individual picture or to draw a previously drawn object, relying on visuo-spatial memory and precise movements. (Renaud, 2005.) Ma and Feng (2011) say that the user of graphical authentication methods can also be made to either recognize previously chosen pictures or reproduce a something that was created in the registration phase. The latter one relies on spatial recall ability in addition to the visual memory (Ma & Feng, 2011).

A study comparing regular alphanumeric passwords, mnemonic passwords, and graphical passwords suggests that using graphical passwords take longer for authentication and demand higher physical activity and higher temporal load, meaning the felt time pressure due the pace or rate of tasks (Ma & Feng, 2011). In this study there were no significant memorability differences observed between graphical and alphanumerical passwords, but it needs to be considered that the alphanumerical passwords used in this study were relatively weak and the test sample was rather small (Ma & Feng, 2011).

However, there are other results as well, as in a study by Stobert and Biddle (2013), which compared the memorability of three different types of graphical passwords that each relied on different kind of retrieval (recall, cued-recall and recognition). The study showed that the recognition-based graphical passwords were easier to remember than recall-based, which then again were better than free-recall version. However, the users experienced longer login times with the recognition-based methods of the study. (Stobert & Biddle, 2013.)

2.1.2 Security devices

Security devices are an authentication method that is based on something that the user holds. There are many different applications of such devices, and one way to categorize them is by dividing them in to two groups based on the fact whether they need to be physically plugged into something during the authentication process, or not. With this categorization two groups can be identified: smart cards and one-time password (OTP) tokens. (Piazzalunga, Salvaneschi & Coffetti, 2005.)

Smart cards, like for example an ATM card, are plastic cards with an integrated circuit and need to be plugged in to a reading device (Piazzalunga et al., 2005).

OTP tokens are often small devices with an LCD display that do not require to be plugged in to anything. They display an automatically updating authentication data that the user needs to read and then manually type in to the separate login interface of a system. The displayed data changes after every attempt, which means that the token device and the authentication server need to be in-sync. Tokens can also be delivered as software that runs on another platform, like a computer or a cellular phone. However, this is considered a less

secure option since this kind of third party device might be compromised. (Piazzalunga et al., 2005; Renaud, 2005.)

Disadvantages of hardware tokens are that users have to remember to keep the token with them, which might be an issue if there is a larger number of systems with token authentication, which leads to a larger number of tokens. Moreover, users have to remember which token belongs to which account (Renaud, 2005). Furthermore the authentication process might take a bit longer, as the user has to type in the data him- or herself. The plugged-in devices can also potentially be plugged in to a hostile machine with malicious software that may compromise their data and functions. (Piazzalunga et al., 2005.)

Tokens are possibly suited for older users. However, on top the issues with them getting mislaid or stolen, using them requires an ability to correctly type long strings, which may be affected by arthritis (Renaud & Ramsay, 2007).

2.1.3 Biometrics

Biometrics is an authentication mechanism that is based on something that the user is. They fall roughly into two categories: first, behavioral, that measures the pattern seen in the users' behavior, such as signature patterns, or voice. Second, physical characteristics focus on measuring the anatomical and physical features of a person, such as the person's fingerprint or face. (Renaud, 2005.) These live characteristics are being compared to a stored template of the person's formerly measured characteristics (Coventry, 2005).

To form such templates, the user needs to be enrolled to the system at first. At the enrollment process the patterns or features of the user are scanned to the system and stored as a template. Usually the features or patterns are scanned several times in order to rule out any additional noise or anomalies. This is also to verify that the details of the features can be re-recognized by the system, even if every scan of the same biological feature is technically different. The templates can also be encrypted or hashed to achieve a more secure storage. (Kowtko, 2014.)

Biometrics place minimal burden to the memory, since the only thing that the user has to remember is how to use the biometric device (Renaud, 2005).Coventry (2005) distinguishes two specific types of biometric applications in her article: Biometrics for identification, and biometrics for verification. Identification means to recognize the user from a group of possible users, or in other words, to find a match with the acquired biometric template from a group of templates. In verification, the acquired biometric is being matched against a specific template to verify user's identity. The identification process can be relatively time consuming if there's a large database of templates for the system to work through, and there's also a pronounced need for uniqueness in the measured features for the identification to be accurate. This excludes some of the methods making retinal and iris scanning along with fingerprints recognition,

the only methods that can be accurate in identifying the user from a large database of users. (Coventry, 2005.). These methods are further discussed in the next subchapter.

As for verification, these requirements are much more modest, but then again, the user is required to provide an identifier. This identifier determinates which template is going to be used for comparison. For example in ATM the bankcard functions as the identifier (and also as a token). (Coventry, 2005.)

There has been many different methods and applications of biometric authentication introduced over the years. The following chapter describes a few of these methods and applications, as well as some practical vendor examples of such applications that are prevalent.

2.2 Biometric applications

There are a number of different biometric applications focusing on different human features, and using different methods to capture them. This chapter introduces the most common applications, as well as discusses a few of the emerging technologies. I will first examine physical biometrics; I will then continue by reviewing behavioral biometrics.

Fingerprints recognition is based on the patterns found on a person's fingertip. It utilizes several methods including optical, ultrasonic, capacitive, thermal, and pressure, to scan these patterns. (Coventry, 2005.)

The optical method uses a camera to scan the fingerprint and could be affected by discoloration, dirt or damage of fingers, even cold fingers; and it is also prone to fraud (Coventry, 2005; Jakobsson, 2013).

The ultrasonic method is based on high frequency sound waves that penetrate the dermal layer of the skin, and measures as the waves reflect off the epidermal layer of the skin (Jakobsson, 2013). This method has been considered to be more effective over the optical or capacitive methods for its higher resolution and the ability cope with dry fingers (Coventry, 2005).

Capacitive method was defined by Jakobsson (2013) to be imaging the fingerprint by "taking advantage of the fact that segments of the ridges act as one plate of a capacitor and the pixels of the sensor array acting as the other" (p. 93). The capacitive method is not as vulnerable to dirt or fraud as the optical method, but it is more demanding for the user. This is because it needs a specific pressure to be applied, and it is affected by cold fingers, and age-related issues. (Coventry, 2005.) The scanner recognizes the location and direction of ridge endings and bifurcations of the finger print (Coventry, 2005). The patterns on one's finger are believed to be unique even if major similarities can be seen within family members (Jakobsson, 2013). Coventry (2005) states that according to the Biometric Report 2000-2005, the quality of fingerprints can be affected by race, gender, occupation and age. Women often have finer fingerprints than

men, and the fingerprint of a manual laborer may have seem worn or damaged. Furthermore, the skin of a child is softer and thus produces less well-defined prints, and then again, the skin of an older adult also loses moisture an elasticity, which may also affect the print quality (Coventry 2005).

Leung, Fong and Hui (2007) suggest using the print of an entire palm instead of just the finger. In their tests these palmprints achieved more favorable false-rejection and false-acceptance rates than fingerprints in the compared tests that were done by others.

Another issue is that users of fingerprint scanners may worry about the hygiene of the device (Coventry, 2005). However, Diamond Fortress Technologies have introduced a mobile application called "Onyx" that can tackle these concerns. It uses the mobile device's camera to capture the fingerprint, so there's no need to touch the device (Goode, 2014). Other concerns include a possible hostile party trying to access the fingerprint protected system, using an artificial or even severed finger (Coventry, 2005). Even though there are still issues with the mechanism, the banking industry, as well as border control agencies have been using fingerprint applications to accelerate their services (Caldwell, 2014).

Fingerprints can be used for identification as well for verification (Coventry, 2005). The differences between identification and verification were explained in the previous subchapter.

Eye verification can be configured to focus on different components of an eye to recognize the user. Examples of such components of an eye include irises, eye veins and retinas. (Coventry, 2005.)

According to Alan Goode (2014), iris scanning is being considered as one of the best methods of biometric authentication. An accurate iris scan requires a camera with the ability to take infra-red images. However, this requirement rules out most of the cameras that are currently integrated to mobile devices. Also according to Leung et al. (2007) capturing iris scans can be relatively difficult and intrusive.

The scanning of eye veins is a more recent technique which requires a camera with the capability to record a video with a minimum of 720p (HD) video resolution. Again, most of the modern smartphones do have a sufficient camera to enable this, and there has been commercial applications for mobile devices for instance by EyeVerify. (Goode, 2014.) Retina scanning scans the layer of blood vessels in the back of the eye to recognize the user (Coventry, 2005). Retinal and iris scanning can be used in identification as well as for verification (Coventry, 2005).

Facial recognition can be either two or three dimensional, and focuses on specific features of the face to create a map or profile. This method requires a camera and is often associated with complications in terms of getting a good enough picture of the target. Some implications of facial recognition have been known to be liable to spoofing pictures of people's faces or even drawings. (Goode,

2014; Renaud, 2005.) However, the countermeasures to tackle this issue have introduced new additional requirements like liveliness i.e. the user has to smile or move a bit while being scanned (Kowtko, 2014).

This particular method has also been a rising concern towards possible privacy issues (Caldwell, 2014). This could perhaps be because it is one of the few occasions where biometrics can be captured passively, without any interaction from the target (Coventry, 2005). There has also been reports by New York Times claiming that the US National Security Agency (NSA) is collecting a database of pictures of people's faces for their facial recognition systems. According to the contractor Edward Snowden, the NSA is gathering such data from databases of airline passengers, foreign national identity cards, as well as through intercepting videoconferences. (Caldwell, 2014.) Despite the issues, facial recognition methods have been employed by border control (Caldwell, 2014) and commercial applications have been developed by companies such as Facebanx or KeyLemon (Goode, 2014).

Finger and palm veins are another instance of biometric authentication. The pattern of a person's vast blood vessel network is unique even with identical twins. The veins are usually scanned using near-infrared and far-infrared techniques (Lee, Khalil-Hani & Bakhteri, 2012.)

Dong, Yang, Yin, Liu & Xi (2014) suggest that finger vein verification is one of the most promising biometric techniques, and presents four advantages that have raised it to such a position: It is a non-contact method (1) that requires a live-body presence (2) in the authentication process, which means that it is hygienic and cannot be easily spoofed. It also characterized by a high security level (3) and small size of the biometric reader device (4). They also mention there is much research attempting to find the most effective way to extract the features from the captured image of the veins. This research has polarized according to whether the finger vein network is being segmented, or not in the extractions process. Furthermore, methods that are based on the segmented vein networks are reliant on the quality of the images. (Dong et al., 2014.)

Hence, the banking industry has shown an interest in this method. The Bank of Lanzou in China launched an AMT with finger vein authentication in 2014 and other banks have been trying them out in various service scenarios (Caldwell, 2014).

Cardiac rhythm can also be used as a biometric. Electrocardiogram (ECG) measures the unique electric signal of the heart that is hard to misrepresent. The ECG biometric application can be either characteristic- or waveform-based. Characteristic-based features are measured from the fiducial point in one ECG complex, and are thus easier to obtain. Fiducial points are the equivalent to the peaks and boundaries of the three major waves that can be seen in an ECG trace. Waveform-based features need one or more ECG complexes and use coefficient values. (Safie, Soraghan & Petropoulakis, 2011.)

"Nymi", a wearable band by Bionym is an example of commercial application that can capture the owner's heartbeat, using it for verification purposes. It can even be paired with other devices using the Bluetooth low energy (BLE) technique and be used as an authenticator to access them. (Goode, 2014.) According to Biometric Technology Today (2015), banks in the UK and Canada have already been carrying out trials of these bands, with online banking access and contactless card transactions.

Behavioral biometrics are methods that are based on measuring a person's behavioral patterns. This includes for example measuring the time, stroke speed, spacing, letter formation and stylus pressure while writing a signature, or the speed and patterns for typing particular words on a keyboard. (Coventry, 2005.)

Voice recognition is also a behavioral biometric that analyzes the characteristics of a person's voice, such as its frequency, duration and cadence (Coventry, 2005). This method requires a device with a microphone (Goode, 2014). The banking industry has been interested in utilizing this method to authenticate their customers (Caldwell, 2014; Goode, 2014). Voice recognition is also a highly hygienic version of a biometrics application, that would make it suitable for healthcare settings as well (Goode, 2014). According to Leung, Fong and Hui (2007) voices can be easily copied and manipulated, and moreover, they are prone to noise corruption also.

Other biometrical methods have also been proposed, but are not yet as widely commercialized or even implemented. Examples of these methods are based on recognizing a person's earlobe, ear shape, smell, gait, key pressure, laughter, finger bones, facial thermograms, inner ear bones, and lip shape (Coventry, 2005). Some of these proposals are just thoughts and ideas, not yet implemented, but for example Sistemas-company is developing a new biometric technique that would identify people based on their personal odour (Caldwell, 2014). "Ergo", applications by Descartes Biometrics, lets users sign into their Android phone using ear recognition (Caldwell, 2014). It uses the touchscreen of a mobile phone to identify the user's ear, and also uses behavioral biometrics in addition to the ear measurements (Goode, 2014). This application recognizes how the user's ear and cheek are pressed against the touchscreen and the speed and tilt of the phone while it is brought to the ear (Biometric Technology Today, 2014).

Biometrics encompasses a wide variance of methods and applications that specialize on different aspects of the human being. The prevalence of these methods and the relative current technological conditions are discussed in the next chapter.

2.3 Biometrics now

According to Kowtko (2014), the most used biometric applications at the moment are fingerprint, iris and facial recognition. The research on biometrics has been greatly driven by the military, especially in the US, where military agencies have been sponsoring much of the research (Coventry, 2005). More recently, the mobile device industry has shown an increased interest towards these technologies. Smartphones are becoming a luxury item to an everyday commodity, with over one billion devices sold during 2014 (Gartner, 2015). As these devices become more and more a part of the everyday life, they provide a new platform for biometric applications (Caldwell, 2014; Goode, 2014).
Leading smartphone manufacturers Apple and Samsung have integrated fingerprint scanner biometrics into the fifth generation of their high-end smartphones. Apple introduced fingerprint sensors that could be connected to its AppleID features, instead of just using it to lock and unlock the device. Later, Samsung stepped up the game with the Galaxy S5 smartphone that allows third party access to its fingerprint sensor. This creates new openings for many third party service providers. According to an analyst firm Frost & Sullivan, biometrics-related revenue from smartphones will increase from $53.6m in 2013 to $396.2m in 2019. (Goode, 2014.)Another rising trend on the mobile device field is the wearable technology. This includes wristband, watches, and glasses embedded with various technological features. Goode (2014) calls the wearables as the next wave of personal computing that is just about to "kick off". The markets have already seen wearable products that can capture biometrics, and use them to verify user's identity.
However, the possible privacy issues revolving around biometrics have been a recurring topic during the 2014 (Caldwell, 2014). Back in 1997 when biometrics were a newer form of technology, Woodward reviewed them in his paper "Biometrics: privacy's foe or privacy's friend?", and suggested that this emerging technology would not need any "striking new legal vision to regulate it".

2.4 Evaluating biometrics

Since this study aims to portray the usability of biometrics from a certain user group's point of view, a small introduction to usability evaluation is needed.

The performance of a biometric application is usually determined by two measures: False Acceptance Rate (FAR) and False Reject Rate (FFR). The FAR signifies the likelihood that the wrong person could access the system, and the FFR means the likelihood that legitimate users will be denied access. (Coventry, 2005.) Kowtko (2014) also suggests another statistical measure called Equal Error Rate (EER). This is the point in which both FAR and FRR meet, and he states that "when evaluating such systems [biometrics], it is important to find a low

threshold where the false rejection and false acceptance meet". These measures are interconnected so when FFR rises, FAR lowers and vice versa. These numbers might often be calculated based on tests done in a laboratory setting, and may thus fail to predict the rates in an actual live environment with large populations of variable users. (Coventry, 2005.)

The usability of a biometrical application is usually measured with two metrics as well: Failure to enroll (FTE) and Failure to acquire (FTA). FTE signifies the number of users who cannot even enroll due to a lack of quality in their input samples, and thus can never access the system. FTA identifies the users that fail to generate good enough images, while using the device in order to authenticate themselves. (Coventry, 2005; Peacock, Ke & Wilkerson, 2005.)

This chapter began by introducing the different authentication mechanisms including passwords, security devices and biometrics. The biometrics were given a closer look by introducing various biometric applications and their current position. As the biometrics and the related phenomenon have been discussed, we will proceed to observe the older adults as technology users. This includes a view on the common cognitive and physical changes associated with aging, and to what extent they affect the ability to use technology, especially biometrics and passwords. These possible affects are then further discussed in the proceeding chapter.

3 OLDER USERS

The number of older adults, (aged 65 years and over), is increasing worldwide (Czaja & Lee, 2007). In Western Europe, the percentage is expected to rise from the 18.3% in 2010 to 25.4% by 2030 (Peine et al., 2014). Even if the use of technology increases among this age group, according to the statistics by the U.S. Census Bureau from 2005, there is still an age-based digital divide in the USA. The digital divide refers to the unequal access and utilization of ICT; and these statistics show that only about 26% of older adults use the Internet, while the Internet usage percentages among people of age 50-64 were 64% and 80% within those of age 30-49. (Czaja & Lee, 2007.)

Czaja & Lee (2007) point out that aging is a highly individualized process. This makes the group of older adults very heterogeneous and their abilities, skills and experiences vary greatly among the group. Moreover, the heterogeneity among older users is even more significant than among the younger user groups. (Czaja & Lee, 2007.) This means that the chronological age of the technology user cannot be used as a prediction of their abilities but as "an index of potential physical and behavioral changes that occur with adulthood" (Czaja & Lee, 2007).

The following subchapters will introduce some of the psychological and physiological effects of aging while considering an elderly person as a technology user. The impact of these changes will be discussed more in detail later.

3.1 Cognitive aging

"Cognitive aging is not simply development in reverse" (Renaud & Ramsay, 2007). However, people do change while they age and some of the notable changes can be seen in cognitive and perceptual performance. (Renaud & Ramsay, 2007). In this subchapter it will be discussed how the aging affects different parts of memory, the ability to learn, and pay attention.

Czaja and Lee (2007) distinguish two types of intelligence, fluid and crystallized. The aspects related to the so called fluid intelligence are generally seen to decline with age. The fluid intelligence is associated with processing and reasoning components as well as the aptitude for learning. Then again the so called crystallized intelligence, meaning the knowledge acquired through education and experience, does not usually decrease during the aging process but it either remains stable or increases. (Czaja & Lee, 2007.) The modern memory theories say that the human memory consists of several different memory systems (Baddeley, 2009b). Some of these parts of memory are more prone to the effects of aging than others (Baddeley, 2009a). Following shortly introduces some of these memory systems and how age affects them.

Long-term memory storages holds information over long periods of time. It divides into explicit (intentional retrieval) and implicit memory (retrieval through performance). (Baddeley, 2009b.) Episodic memory is part of the explicit memory and refers to the ability to recall specific experiences and past events (Baddeley, 2009b). According to Baddeley (2009a), episodic memory related tasks decline with age. He presents the associative deficit hypothesis by Naveh-Benjamin (2000) that suggest that "the age deficit in memory comes from an impaired capacity to form associations between previously unrelated stimuli". According to Baddeley (2009a) the effects of age are most prominent in free call with no external clues. Another part of the explicit memory is semantic memory, which refers to the ability to recall facts and knowledge of the world (Baddeley, 2009b). The semantic memory is maintained during the aging process and it continues to accumulate, but even there can be seen some decline in speed and reliability of access (Baddeley, 2009a).

Working memory refers to the memory system that focuses on the temporary maintenance and manipulation of information, thus serving as a sort of a mental workspace (Baddeley, 2009b). Albeit working memory seems to be prone to the effects of aging, however it is not clear which parts of it are most vulnerable (Baddeley, 2009a). Short-term memory is yet another memory system and it storages small amounts of information for a short period of times (Baddeley, 2009b). Baddeley (2009a) says that the short-term memory is relatively well preserved during the aging process.

Time-based and event-based prospective memory, which are refers to the ability to remember to do something at a certain time or in a certain situation, is also seen to decline with age. However, but may be improved with retrieval cues or compensation strategies. Yet the decline of prospective memory is mostly seen in laboratory settings and older participants can even be seen to outperform the younger ones in tests that relate prospective memory tasks that are closely related to their daily life. (Baddeley, 2009a.)

Then again visual memory does not seem to be affected by the cognitive decline (Renaud, 2005) and the recognition memory is often relatively well preserved during the aging process (Baddeley, 2009). It has been shown that older adults are much better at recognizing items that they have previously encoun-

tered, than remembering the context of that previous encounter (Baddeley, 2009). If the ability to recognize a familiarity of an item is rather well preserved but the ability to recollect the original experience not so as it seems, it may affect to recognition tasks where both of these would be needed (Baddeley, 2009).

According to Renaud and Ramsay (2007) the age-related memory limitations are a significant issue that needs to be considered by "not requiring the users to remember nonsensical and unrelated facts such as passwords and/or usernames".

As for learning, the aging affects one's ability to learn at least in terms of the learning rate (Renaud & Ramsay, 2007). Learning usually involves processing some material, which usually takes more time for an older learner (Baddeley, 2009a). This, with reluctant "I'm too old to learn" –attitudes may hinder the learning process (Renaud & Ramsay, 2007). However, older adults perform very well, in terms of speed, when learning tasks where the responses are obvious; but the real problem arises when the tasks that require learning are new and unobvious. The reason why this is so problematic for older technology users is that the continuously and rapidly evolving technology keeps on bringing us to situations where such learning may often be needed (Baddeley, 2009a).

In some studies of the effects of aging on learning and memory, the performance of younger subject groups can be seen to decline close to the older subject group performance, if the younger ones are required to perform multiple simultaneous tasks (Baddeley, 2009a).

The ability to pay attention reduces with age as well (Renaud & Ramsay, 2007). Attention can be divided into selective and divided attention. Selective attention refers to one's ability to focus on to a certain thing and filter out any extra stimuli. The selective attention is seen to have diminished with age. (Renaud & Ramsay, 2007.) Baddeley (2009) refers to Hasher, Zacks and May (1988, 1999) suggesting that this reduced ability to filter out irrelevant stimuli is the major cognitive effect of aging and refers also to other studies proposing that the decline seen in the working memory span could be caused by this.

Divided attention requires the person to pay attention to multiple things at the same time and is not as clearly affected by age since its performance depends on the complexity of the task on hand (Renaud & Ramsay, 2007). Baddeley (2009) points out that there's considerable evidence that age impairs ability to divide attention between two sources, but these results may reflect the overall work load rather than ability to focus on two simultaneous tasks. He explains that if the older adult has greater difficulties with the individual tasks they are bound to have even more difficulties while trying to do them simultaneously.

There are psychosocial factors affecting the technology using situations as well. The increased isolation, loneliness and poor health associated with aging may lead to depression. The use of computers could decline the loneliness and nega-

tivity as it provides new channels for socialization and the users are not left out of the increasingly technological society. (Renaud & Ramsay, 2007.) Computer-related anxiety have been seen to increase with age (due to the insensible error messages and jargon) but then again the successful user experiences with technologies such as the ability to use email, may improve the feeling of well-being and competence. (Renaud & Ramsay, 2007.)

The concept of time may also differ during the aging process. Renaud and Ramsay (2007) say that "older users tend to be less impatient and do not what to be hurried". They see this as an remarkable notion since the web design is all about getting the response to the user as soon as possible since they are known to be impatient. The older users like to take their time and are not as bothered by a slower performance of the system. (Renaud & Ramsay, 2007.)

Baddeley (2009) presents Salthouse's (1996) macro theory that proposes that "the cognitive effects of aging can all be explained by the reduced speed of processing that is a marked feature of aging" but also points out that there's evidence that suggest that the memory decline would be separate from this more general decline in cognitive functions with age.

It should also be mentioned that the cognitive decline can also be accelerated by medical conditions such as Alzheimer's disease or dementia (Baddeley, 2009a). Alzheimer's disease is rarely diagnosed among the under 65-year-olds, but 15-20% of over 85-year-olds are diagnosed with it (Juva, 2013).

3.2 Physical changes of aging

Aging comes with physical changes as well. This chapter presents some of the age-related changes that are relevant while evaluating one's ability to use biometric devices or passwords, including changes in vision, hearing and mobility. However, the relevance of these changes to biometrics is discussed more at length in the next chapter.

Aging users may have failing vision so they might not be able to see fine details such as small fonts on the screen (Renaud & Ramsay, 2007). Also discriminating colors, especially the yellow color (commonly used to attract attention) becomes harder as the eye lenses yellow with age (Renaud & Ramsay, 2007).

Eye-related illnesses including age-related macular degeneration (AMD), glaucoma, diabetic retinopathy, cataracts, and blindness may also affect the ability to perform visually demanding procedures (Kowtko, 2014). In Finland one in three over 65-year-olds experience cataract-related changes that limits their ability to see, and in those over 85 years old, the incidence of catacract-related changes rises to 70% (Seppänen, 2013). This may be relevant to eye-related biometric methods as well as the ability to use a biometric device.

Many older users also experience difficulties of hearing. This means that all viable information delivered through sounds, should be presented in another form as well, so the hearing-impaired users do not get left out. (Renaud & Ramsay, 2007.) This should be considered especially with voice recognition biometrics, if there is spoken instructions.

Aging comes also with a loss of collagen that makes skin become loose and dry (Modi et al., 2007). This is relevant in the case of finger print based authentication as explained later on in the next chapter.

One's ability to move can likewise be affected by aging. Increased arthritis, joint stiffness, and lack of exercise can lead to decreased movement and independence (Kowtko, 2014). Arthritis or otherwise decreased mobility can also make mouse and keyboard usage difficult and especially hider tasks where there is a time constraint present (Renaud & Ramsay, 2007). Clicking on small objects can be difficult and the slow reaction times of older users may cause problems to double click objects, for instance (Renaud & Ramsay, 2007).

Renaud & Ramsay (2007) argue that the limited mobility and increased isolation of the older adults could be relieved by web-based services, such as home-based purchasing and near-instant communication, but they also raise the inconvenient identification and authentication mechanisms of such services as one of the restrainers on way for the spread of these services through the older user group. Even if there has been a lot of thought but in how to design pages to suit the needs of the older adults, the authentication in web-based services still relay greatly on memory recall and an errorless typing of a string, a task that can be effected by the age or age-related illnesses (Renaud & Ramsay, 2007).

This chapter explained age related changes in cognition and physiology. There are indeed changes in, for instance, memory and mobility, which may affect the ability to use certain authentication mechanisms. The next chapter will discuss in more detail how these changes are related to using passwords and biometrics, aiming to clarify if either of these authentication methods serves the needs of an older user.

4 BIOMETRICS AS AN ALTERNATIVE FOR OLDER USERS

After discussion of passwords, biometrics and older users, we move on to consider passwords and biometrics as an alternative to passwords for older users. At first, biometrics and passwords are compared from a more general point of view and then their suitability for older users is evaluated more in detail.

4.1 Biometrics as an alternative to passwords

Passwords are potentially a very secure authentication method, but as the choosing of a secure enough password is left up to the user, the reality may be different (Renaud & Ramsay, 2007). Users are often not aware of the security risks or the importance of choosing a strong enough password, and are thus seen as the weakest link in the security chain of password-based systems (Taneski et al., 2014). The password can be forgotten, stolen, guessed, or broken by persons of ill intent (Renaud & Ramsay, 2007).

Human memory has its limits for learning sequences of items, with the short-term capacity being limited to around seven items. Furthermore these items need to be in familiar forms, such as words or familiar symbols. (Yan et al. 2005.)

Nowadays, with the rising amount of accounts, people tend to be burdened by the amount of passwords they need to remember, which can lead to insecure password behavior, such as choosing weaker passwords and reusing them or even writing them down (Renaud, 2005; Jakobsson & Dhiman, 2013). The average user has 25 accounts but only 6.5 passwords that are shared across 3.9 websites (Jakobsson & Dhiman, 2013; Taneski et al, 2014). The reuse can also be approximate meaning that the user chooses new passwords that closely resemble the old one (“PassWord” and “passWORD11”) (Jakobsson & Dhiman, 2013).

The biometrics have been pointed out to be a good solution since using them requires no memory (Rane, Ye, Draper & Ishwar, 2013), they cannot be easily lost (Rane et al., 2013) and according to Rane et al. (2013) they cannot be easily forged either. However this might depend on the biometric application in question, as for instance, Goode (2014) and Renaud (2005) note that facial biometrics can be in some cases, fooled with pictures of a person.

This leads to the other concerns revolving around biometrics. They cannot be easily and unlimitedly changed like passwords, since a person has only a limited number of features, likes fingers, that can be used (Rane et al., 2013). Furthermore the privacy issues of biometrics have been a highly discussed topic over the past year (Caldwell, 2014). Rane et al. (2013) discussed the naturally variable and noisy nature of biometric measurements that makes storing them with cryptographic hashes problematic, since the cryptographic hashes are extremely sensitive to noise. If the biometric measurements are stored as they are, without the cryptographic hashing and the device they are stored at gets stolen, the attacker may gain access to the enrollment biometric (Rane et al., 2013).

A compromised password can usually be easily changed, but a compromised biometric template may not, due to the previously mentioned limits in features. Furthermore the compromisation may also lead to a significant privacy loss, since the biometrics are tied to the unique physical characteristics and the identity of an individual. (Rane et al., 2013.) Other hindrances include that there might be some extra expenses while adopting a biometric authentication method, in case the user has to purchase a biometric reader device to use the method (Kowtko, 2014).

Renaud and Ramsay (2007) say that ideally, the complexness of the authentication mechanism would be tailored to the situation. It may not be convenient to choose an extremely strong and long password to protect "fairly innocuous web content" (Renaud & Ramsay, 2007). When it comes to combining these two authentication methods, Jakobsson (2013) says that if biometrics are used as the primary authentication method and backed up with another method, such as passwords, the users are more prone to forget the password due to the infrequent use.

While considering the possibilities of biometrics as they gain more popularity as an authentication mechanism, it needs to be remembered that it is not realistic to expect the websites to accommodate new security mechanisms immediately and the passwords are most likely going to be used for years to come, even if other mechanisms would be proven better (Jakobsson 2013).

These general insights on the convenience of passwords and biometrics lead us to observe them from an older user's perspective.

4.2 Biometrics as an alternative to passwords for older users

The previously introduced general pros and cons of passwords and biometrics apply to the aging users as well, but there are also a few other factors that need to be considered with this particular user group. The effects of aging that are relevant in terms of technology usage were introduced in the chapter 3 and are now taken into consideration with passwords and the biometrics applications.

Using passwords requires the ability to type correctly, that can be affected by age-related illnesses such as arthritis or tremors. Furthermore, the passwords do not often echo the user interface, meaning that the already typed characters to not appear on the screen, but are replaced by dots or other such marks. Users with limited attention span may have difficulties keeping track of what they have already typed without any visual cues. (Renaud & Ramsay, 2007.)

As said before, the memory-related issues are pronounced with age and passwords tend to be inflicted by memory-related demands that may be hard to cope with. A study by Pilar, Comes and Stein (2012) suggested that age does not affect the recall of passwords, but the amount of passwords does. However: the younger participants in this study had more passwords and they were also longer.

When considering biometrics and older users, biometric applications need to be evaluated from an aging user's perspective:
With *fingerprints recognition* it needs to be acknowledged that aging results in loss of collagen, making the aging skin is loose and dry. This decreased firmness of the aging skin affects the quality of fingerprints. (Modi et al., 2007.) According to a study by Modi et al (2007) the fingerprint quality varies among age groups and the variance is more pronounced with those over 62 years of age. Furthermore many conditions, such as arthritis, may affect the user's ability to interact with the sensor of the biometric reader, further reducing the quality of the sample (Modi et al., 2007). If the reader device requires precise physical tasks, like placing a finger and keeping it still, physical limitations in dexterity and vision as mentioned before (Renaud & Ramsay, 2007), may need to be considered.

Cataracts and other iris related diseases can affect the ability to use *eye verification* based biometrics. A study done by the Federal University of Sao Paulo-Vision institute and the University of Sao Paulo revealed that the eyes, which have undergone a cataract surgery, were more challenging for iris recognition scanners to authenticate and verify. This led to an increased number of false rejections, but according to Kowtko (2014) the issue could be fixed by re-enrolling to the system after the surgery, in other words rescanning the eyes to create new template to be stored in the system. (Kowtko, 2014.) As explained in the previous chapter, cataracts are an increasingly common finding as a person passes the age of 65 (Seppänen, 2013). Then again, as mentioned before, aging

users may have failing vision for small details (Renaud & Ramsay, 2007) and this may be relevant while considering the ability to eye verification, for example if the user needs to focus their eyes to a certain point.

Facial features change with age (Leung et al., 2007), which is something that needs to be considered with *facial recognition.* The aging of soft and hard tissues can reshape the features of the face and it has been discussed if its procession could be predicted or modelled, and a few different approaches have been proposed to model this aging process (Patterson, Sethuram, Albert, Ricanek & King, 2007). One of these, the image-based approach, was named as one of the most promising for face recognition related aging process modelling by Patterson et al. (2007). Also conditions like the state after a stroke, congestive heart failure or hard veins may affect the facial features (Kowtko, 2014). Once again vision related issues may need to be considered (Renaud & Ramsay, 2007) if the method requires the user to direct their faces to a point or if there are a lot of visual instructions involved.

No studies concerning the effect of age on *finger and palm veins recognition* was found within the limits of this literacy review. However, vein recognition is a relatively new technique (Dong et al., 2014), but it also involves interacting with a reader. As mentioned before, the older adults may have medical conditions that limit their ability to interact with biometric readers such as the fingerprint reader.

The effects of aging on *cardiac rhythm recognition* were not discovered during this literacy review either. However it was found that heart related medical conditions, like heart failure, are common among aging people. According to the European Society of Cardiology (2015) every fifth person in the developed countries will develop a heart failure that is an incurable, but preventable disease. Kowtko (2014) sees congestive heart failure as the leading cause for hospitalization of the age group 65 and older and lists rapid or irregular heartbeat as one of its symptoms.

Behavioral biometrics like handwriting can be affected by aging in terms of writing speed, which is seen to decrease with age and the decline is notable with those at the age of 60 or over (Faundez-Zanuy, Sesa-Nogueras & Roure-Alcobé, 2012). A study by Faundez-Zanuy et al. (2012) found evidence that age would also affect the False Acceptance Rate of handwriting-based biometrics, resulting older users to be more likely incorrectly verified as someone else. Then again the ability to recognize one's own handwriting does not degrade with age, not even in cases of a stroke or dementia, but utilizing this notion would need a method that would rely on recognition done by the user rather than the system (Renaud & Ramsay, 2007).

Many older users have difficulties of hearing (Renaud & Ramsay, 2007) that may need to be considered while using a *voice recognition* method if all the user instructions are given out loud.

In biometric applications presented in the chapter 2.2 there is often a biometric device that is used to capture the biometric. As mentioned before, the older adults may experience medical conditions that affect their mobility and ability to interact with biometric readers. Kowtko (2014) also points out that the majority of older adults do not have smartphones sufficient enough to be used as biometric reader this might mean additional costs when starting to use biometrics.

When it comes to alternative solutions, cognometric authentication, which is based on recognizing or graphical authentication based on visual memory, would also be a noteworthy alternative for passwords and biometrics, since they do not rely on perfect recall or require to purchase any additional devices (Renaud & Ramsay, 2007). Another interesting suggestion is to use electroencephalography (EEG) signals as biometrics (Pham, Ma, Tran, Nguyen & Phung, 2014). Pham et al. say that EEG-based biometrics would combine the "advantages of both password-based and biometric-based authentication systems, yet without their drawbacks" since they are biometric information, but the brain pattern observed is correspond to a particular mental task, which itself cannot observed. They add that the EEG signals are very difficult to mimic, let alone nearly impossible to steal or force, since the brain activity is sensitive to stress and mood.

5 DISCUSSION AND CONCLUSION

This literacy review examined biometrics as an alternative to passwords. Passwords were found to be the most common authentication method at the moment, even if it has some usability issues in terms of human memory limitations and the increasing amount of passwords to remember. This supremacy of passwords is not expected to rapidly stop, even if a better alternative authentication method would surface, since it would take time for the technology service providers to adopt the new technique.

As for the biometrics as an alternative to passwords, it was found that there are many different technologies, with different advantages and disadvantages, all gathered under the same roof of biometrics. Certain biometrics might be better suited for certain users, situations and environments than others. It is questionable whether one can say that biometrics are usable or not, since there are so many different biometric methods, each of which has its own quirks.

Furthermore, human features are not static as they are affected by the aging process. The traditional biometric method, that takes a template of a human feature once and then keeps comparing it to the live feature, would work just fine if humans were static and their features would remain unchanged through the years. Since the features may naturally slightly differ so the biometric system has to be robust enough to recognize even the slightly altered feature while simultaneously keeping the false acceptance rate low.

If there are many biometrics with different characteristics, so are there many kind of users with different capabilities. The older adults differ from the average technology user. Their rate of processing and learning may be slower which needs to be considered if there's time constraints or if the technology is unfamiliar to them and not even anyhow related to anything they might have experienced before. Older adults may also have impaired mobility that may affect tasks that require very exquisite motor skills. They may also suffer from conditions that may affect the ability to use some of the biometric applications. Then

again, the older adults are a very heterogeneous group that makes reaching conclusions that would relate to all of them very difficult.

In conclusion some of the biometric applications may be worth considering as an alternative for some of older users, however the changing features and the possible limitations pose some challenges for the biometric recognition system. More research on the older users' ability to use biometrics would be needed in order to say whether they are a suitable solution or not. Then again passwords have certain memory related issues, but it was not clear if these issues were related to the age at all, rather than involving all age groups.

This literacy review collects together information on passwords, biometrics, and older users, as well as the suitability of these authentication methods for the older users. It also reveals a research gap when it comes to the older user's ability to use biometrics. Not too much research was found on the topic, especially when it comes to some of the newer biometric applications, such as cardiac or vein pattern biometrics. The proposed future research would include more detailed research on the suitability of different biometric applications for older users as well as their user experiences with biometrics and how would they actually feel about using them instead of other methods, such as passwords.

Altogether it seems that biometrics are still getting a lot of attention and new promising techniques are coming along. It would be interesting to see whether these development projects are driven by goals of ensuring the highest enough security level or reaching a pleasant user experience, and if they are considering the users across all age groups in their development. Also combining different biometrics to get more accurate systems, like the formerly mentioned "Ergo", may create new options, but this increased complexity may also result in decreased usability for some, if aging users and their known issues with some of the biometric methods are not considered. Mobile devices with ever multiplying amounts of sensors may also accelerate the use of biometrics by providing a platform for further innovations. If institutions such as banks are starting to adopt these new techniques, there is a need to consider if they are a good solution for everyone.

Concerning the limits of this study, there were some articles that were inaccessible due the limits of this research project that could have given additional views on the matter. The material gathering was limited to the chosen article databases and the searches were done with keywords. The gathered material was completed with a couple of chosen books that were relevant to the topic. Perhaps by continuously following a number of distinguished biometric and gerontechnology journals, instead of just performing database searches, a more comprehensive view of the current state of these fields and their relationships may be acquired. Also this study did not include any empirical research that could have addressed the research gaps found from the available material.

REFERENCES

Baddeley, A. (2009a). Memory and aging. In A. Baddeley, M. W. Eysenck & M. C. Anderson (Eds.), *Memory* (p. 293-315). East Sussex: Psychology Press.

Baddeley, A. (2009b). What is memory? In A. Baddeley, M. W. Eysenck & M. C. Anderson (Eds.), *Memory* (p. 1-17). East Sussex: Psychology Press.

Banking sector embraces multiple biometric modalities. (2015). *Biometric Technology Today, 2015*(4), 1. doi:http://dx.doi.org/10.1016/S0969-4765(15)30048-5

Caldwell, T. (2014). 2014 – a year in biometrics. *Biometric Technology Today, 2014*(11), 9-11. doi:http://dx.doi.org/10.1016/S0969-4765(14)70180-8

Coventry L. (2005). Usable Biometrics. In Cranor, L. F. & Garfinkel, S. *Security and usability: Designing secure systems that people can use* (pp. 175-198). Sebastopol, CA: O'Reilly Media Inc.

Czaja, S. J., & Lee, C. C. (2007). The impact of aging on access to technology. *Universal Access in the Information Society*, 5(4), 341-349.

De Angeli, A., Coventry, L., Johnson, G., & Renaud, K. (2005). Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems. *International Journal of Human-Computer Studies, 63*(1), 128-152.

Ear biometrics for android as apple eyes iris. (2014). *Biometric Technology Today, 2014*(2), 1. doi:http://dx.doi.org/10.1016/S0969-4765(14)70020-7

Erber, J. T. (2013). *Aging and older adulthood* (3rd ed. ed.). Malden Mass.: Wiley-Blackwell.

European Society of Cardiology (ESC). (2015). One in five people will develop heart failure. *ScienceDaily*. Retrieved September 7, 2015 from www.sciencedaily.com/releases/2015/05/150505111934.htm

Faundez-Zanuy, M., Sesa-Nogueras, E., & Roure-Alcobé, J. (2012). On the relevance of age in handwritten biometric recognition. In *Security Technology (ICCST), 2012 IEEE International Carnahan Conference on* (pp. 105-109). IEEE.

Fukumitsu, M., Katoh, T., Bista, B. B., & Takata, T. (2010). A Proposal of an Associating Image-Based Password Creating Method and a Development of a Password Creating Support System. In *Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on* (pp. 438-445). IEEE.

Gartner (2015, March 3.) Gartner Says Smartphone Sales Surpassed One Billion Units in 2014. Accessed May 8, 2015 http://www.gartner.com/newsroom/id/2996817

Goode, A. (2014). Bring your own finger – how mobile is bringing biometrics to consumers. *Biometric Technology Today, 2014*(5), 5-9. doi:http://dx.doi.org/10.1016/S0969-4765(14)70088-8

Jakobsson, M. (2013). Can biometrics replace passwords? In *Mobile Authentication: Promlems and Solutions.* (pp. 91-100) Springer New York. doi:10.1007/978-1-4614-4878-5_7

Jakobsson, M., & Dhiman, M. (2013). The benefits of understanding passwords. In *Mobile Authentication* (pp. 5-24). Springer New York.

Juva, K. (2013, September 23rd). Lääkärikirja Duodecim: Alzheimerin tauti. Accessed November, 9, 2015 http://www.terveyskirjasto.fi/terveyskirjasto/tk.koti?p_artikkeli=dlk00699

Kowtko, M. A. (2014). Biometric authentication for older adults. *Systems, Applications and Technology Conference (LISAT), 2014 IEEE Long Island,* 1-6. doi:10.1109/LISAT.2014.6845213

Lee, Y. H., Khalil-Hani, M., & Bakhteri, R. (2012). FPGA-based finger vein biometric system with adaptive illumination for better image acquisition. *Computer Applications and Industrial Electronics (ISCAIE), 2012 IEEE Symposium on,* 107-112. doi:10.1109/ISCAIE.2012.6482079

Leung, M. K., Fong, A. C. M., & Hui, S. C. (2007). Palmprint verification for controlling access to shared computing resources. *Pervasive Computing, IEEE*, 6(4), 40-47.

Dong, L., Liu, F., Xi, X., Yang, G. & Yin, Y. (2014). Finger vein verification based on a personalized best patches map. *Biometrics (IJCB), 2014 IEEE International Joint Conference on,* 1-8. doi:10.1109/BTAS.2014.6996234

Modi, S. K., Elliott, S. J., Whetsone, J., & Hakil Kim. (2007). Impact of age groups on fingerprint recognition performance. *Automatic Identification Advanced Technologies, 2007 IEEE Workshop on,* 19-23. doi:10.1109/AUTOID.2007.380586

Peacock A., Ke X. & Wilkerson M. (2005). Identifying Users from Their Typing Patterns. In Cranor, L. F. & Garfinkel, S. Security and usabil-ity: Designing secure systems that people can use (pp. 199-220). Sebastopol, CA: O'Reilly Media Inc.

Patterson, E., Sethuram, A., Albert, M., Ricanek, K., & King, M. (2007, September). Aspects of age variation in facial morphology affecting biometrics. In *Biometrics: Theory, Applications, and Systems, 2007. BTAS 2007. First IEEE International Conference on* (pp. 1-6). IEEE.

Peine, A., Rollwagen, I., & Neven, L. (2014). The rise of the "innosumer"—Rethinking older technology users. *Technological Forecasting and Social Change, 82*(0), 199-214. doi:http://dx.doi.org/10.1016/j.techfore.2013.06.013

Pham, T., Ma, W., Tran, D., Nguyen, P., & Phung, D. (2014). Multi-factor EEG-based user authentication. In *Neural Networks (IJCNN), 2014 International Joint Conference on* (pp. 4029-4034). IEEE.

Piazzalunga U., Salvaneschi P. & Coffetti P. (2005). The Usability of Security Devices. In Cranor, L. F. & Garfinkel, S. Security and usabil-ity: Designing secure systems that people can use (pp. 221-244). Sebastopol, CA: O'Reilly Media Inc.

Pilar, D. R., Jaeger, A., Gomes, C. F. A., & Stein, L. M. (2012). Passwords usage and human memory limitations: A survey across age and educational background. *Plos One, 7*(12), e51067.

Rane, S., Ye Wang, Draper, S. C., & Ishwar, P. (2013). Secure biometrics: Concepts, authentication architectures, and challenges. *Signal Processing Magazine, IEEE, 30*(5), 51-64. doi:10.1109/MSP.2013.2261691 *2013 International Conference on,* 1-7. doi:10.1109/ICCAT.2013.6521970

Renaud K. (2005). Evaluating Authentication Mechanisms. In Cranor, L.F. & Garfinkel, S. *Security and usability: Designing secure systems that people can use* (p. 103-128). Sebastopol, CA: O'Reilly Media Inc.

Renaud, K., & Ramsay, J. (2007). Now what was that password again? A more flexible way of identifying and authenticating our seniors. *Behaviour & Information Technology*, 26(4), 309-322.

Safie, S. I., Soraghan, J. J., & Petropoulakis, L. (2011). Pulse active ratio (PAR): A new feature extraction technique for ECG biometric authentication. *Signal and Image Processing Applications (ICSIPA), 2011 IEEE International Conference on,* 16-21. doi:10.1109/ICSIPA.2011.6144124

Seppänen, M. (2013, January 12th). Lääkärikirja Duodecim: Kaihi (harmaakaihi, katarakta). Accessed November 9, 2015 http://www.terveyskirjasto.fi/terveyskirjasto/tk.koti?p_artikkeli=dlk00921

Stobert, E., & Biddle, R. (2013, July). Memory retrieval and graphical passwords. In *Proceedings of the Ninth Symposium on Usable Privacy and Security* (p. 15). ACM.

Taneski, V., Hericko, M., & Brumen, B. (2014). Password security—No change in 35 years?. In *Information and Communication Technology, Electronics and Microelectronics (MIPRO), 2014 37th International Convention on* (pp. 1360-1365). IEEE.

Woodward, J. D. (1997). Biometrics: Privacy's foe or privacy's friend? *Proceedings of the IEEE, 85*(9), 1480-1492. doi:10.1109/5.628723

Yan J., Blackwell A., Anderson R. & Grant A. (2005). The Memorability and Security of Passwords. Teoksessa Cranor, L. F. & Garfinkel, S. Security and usability: Designing secure systems that people can use (pp. 129-142). Sebastopol, CA: O'Reilly Media Inc.

Feng, J. & Ma, Y. (2011). Evaluating usability of three authentication methods in web-based application. *Software Engineering Research, Management and Applications (SERA), 2011 9th International Conference on,* 81-88. doi:10.1109/SERA.2011.18