Full chapter proposal for Protecting Mobile Network and Devices: Challenges and Solutions

Chapter: Exploring mobile authentication mechanisms from PIN to Biometrics including the future trend.

Authors: Florentin Thullier, Bruno Bouchard, Bob-Antoine J. Ménélas.

Abstract

The growing market of mobile devices forces to question about how to protect users' credentials and data stored on such devices. Authentication mechanisms remain the first layer of security in the use of mobile devices. However, several of such mechanisms that have been already proposed were designed in a machine point of view. As a matter of fact, they are not compatible with behaviors human have while using their mobile devices in the daily life. Consequently, users adopted unsafe habits that may compromise the proper functioning of authentication mechanisms according to the safety aspect. In this chapter, the strength and the weakness of the current schemes, from the simpler ones such as PIN to the more complex biometric systems such as fingerprint, are highlighted. Besides, we offer an evaluation, based on both existing and new criteria we suggest, chiefly focused on the usability of these schemes for the user. While each of them have benefits as well as disadvantages, we finally propose a conclusion lean toward the aftermath of authentication on mobile devices that head for new perspectives as regards *no password* and *ubiquitous* authentication mechanisms.

Keywords: authentication, mobile device, smartphone, usability.

1. Introduction

From the past decade, the market of mobile devices grew up exponentially. The Gartner Institute noticed that smartphone sales were over 400 thousand units in the second semester of 2013 [1]. These devices take a significant place in people's everyday life. Indeed, people, and more specifically young ones have their mobile devices everywhere and at any time [2] since they consider their mobile phones as an important part of their life [3]. Nielsen [4] has pointed out that in the Q4 2013, users spent more than 30 hours using applications on such devices. Besides, it should be noted that a major player of the mobile device industry used to claim that there is an application for everything. As a result, users do store private data such as pictures, videos, as well as secret information about their personal accounts (emails, social networks) on their mobile devices. However, they are, most of the time, not adequately wary about the safety of information they save on their devices [5].

Authentication refers to the process of an entity that has to become sure of the identity of another one [6]. Within a mobile device context, authentication remains the first entry point for security. Indeed, such a mechanism aims at protecting sensitive information about the user that characterize their digital identity. Over the past few years, various authentication schemes have been proposed. Hence, we divided them into three broad categories: knowledge-based, token-based and biometrics [7]. Figure 1 illustrates the whole authentication mechanisms that are currently employed with mobile devices. First of all, knowledge-based authentication schemes focus on what the user knows. Precisely, we differentiate implicit and explicit knowledge-based mechanisms. Explicit ones imply that the user has to retain new data like a 4-digit-PIN code or a password [8]. Whereas, implicit knowledge-based mechanisms call upon cognitive functions of the user, to exploit the data they already know [9]. Secondly, token-based mechanisms need the user to prove they possess a physical token that often involves a two-factor authentication process [10]. As an example, we can mention the smartcard that the user needs to own to authenticate himself or herself on his/her mobile phone. Finally, biometric mechanisms rely on the uniqueness of users' physiological or behavioral trait to perform the authentication process. Consequently, we subdivide biometrics into physiological and behavioral sets. Physiological biometrics exploit singularities of the human body like fingerprints [11] while behavioral ones require users to perform some actions to prove their identity such as gait [12].

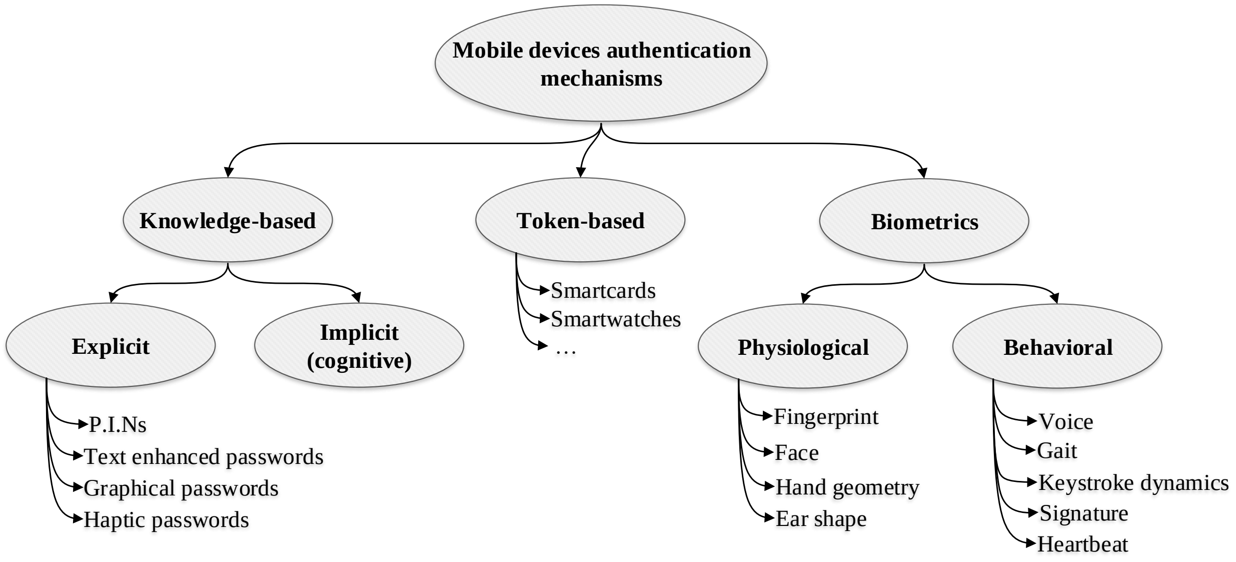

Figure 1: Taxonomy of authentication mechanisms employed with mobile devices.

Whenever we are facing a machine that has to deal with human users, therefore, we have an interactive system [13]. As pointed out by Benyon, et al. [13], a fundamental challenge with interactive systems is that human beings and machines have different characteristics. Indeed, what may be seen as strengths in a machine point of view, may also be a weakness for human being. On the one hand, machines can see Human as being vague, disorganized and emotional while they are precise, orderly, unemotional and logical. On the other hand, Human may claim to be attentive, creative, flexible and resourceful while machines are dumb, rigid and unimaginative. Such differences suggest that the key challenge is first to understand the human rather design an interactive system in the machine point of view. However, when considering authentication systems that have been proposed over the last three decades, it seems that they have been designed without any concern of the human. As an example, it was reported that half of the population does not lock their phone at all since they estimate that entering a 4-digit-PIN code involves lots of troubles, every time the mobile device has to be unlocked [14]. Moreover, it is known that users have trouble remembering all passwords they use nowadays [15]. Consequently, some people prefer to reuse the same password in multiple situations while others choose to write them down. It is clear that behaviors reported here may lead a huge impact on the security of mobile devices. Accordingly, people's authentication usage may generate serious threats for the security that a system initially provides. In fact, an effective mechanism may become a weak one because it is not used as recommended.

The main contribution of this chapter is to emphasize, *via* a critical analysis, most of the weaknesses of proposed authentication schemes, when used in real life situations. We previously pointed out that users have adopted unsafe habits in consequence of the non-user-centered design of most of the authentication process. Hence, our work aims at analyzing how proposed mechanisms whether suit or not characteristics of human users and why they are not entirely appropriate to their needs. The remainder of this chapter is organized as follows. Firstly, it will review authentication schemes that have been proposed in a mobile device context, where, for each of them, both strengths and weaknesses will be highlighted. Then, we will offer an evaluation guided by criteria that were previously proposed by Jain, et al. [16] in the field of authentication. In addition, we will increase such an assessment with criteria we suggest that stem from our critical analysis. Finally, this evaluation will conduct us to draw a conclusion and state about the aftermath of authentication mechanisms for mobile devices.

2. Knowledge-based authentication mechanisms

Knowledge-based authentication mechanisms rely upon users' ability to recall secret information. It is possible to make out two different kinds of knowledge-based techniques: explicit and implicit schemes. On the first hand, explicit ones need the user to set and learn a piece of knowledge. On the other hand, implicit ones exploit the user memory thanks to either, or both, personal information they already know, or about their everyday life preferences (*e.g.* music they like or food they enjoy).

This section describes in detail both explicit and implicit techniques and exposes that users' capacity to remember a secret remains a common denominator in the weakness of each knowledge-based authentication scheme.

2.1. Evaluation of the strength of a knowledge-based authentication scheme

The strength of a knowledge-based authentication scheme is theoretically measurable *via* the evaluation of the entropy of the password space. The password space is the total number of distinct possibilities the authentication system can support. The size S of the password space for a system having N possible entries is given by the equation (1). The length of the input to retain is expressed by k. Finally, the entropy H can be computed by using the equation (2), and the result is expressed in bits.

$$S = N^k \tag{1}$$

$$H = log_2(S) \tag{2}$$

Real use cases reveal that such an evaluation still not represent an accurate measure of the strength of a knowledge-based authentication mechanism. Indeed, since users have the possibility to choose their own secret input, they often refer to a familiar pattern rather select it randomly. As an example, Yampolskiy [17] has pointed out that 47.5% of the users chose a family-oriented information as secret input such as a child's name or a date of birth. Therefore, a lower subset of the N possibilities is truly used, since the length of passwords are generally less than eight characters [15].

2.2. Explicit schemes

2.2.1. Personal Identification Numbers

Example of use case scenario: commonly, users have to choose an array of four digits that they will need to remember. Then, each time the mobile device has to be unlocked, the system prompts an input field where the user needs to fill these digits in the correct order to be authorized to access the whole content of the device.

Personal Identification Numbers (PINs) are a simple way to restrain access to an entity due to their composition—from 4 to 16 digits. They appear with the growth of ATMs (Automated Teller Machines), and they are mostly used in the banking system. Regarding a mobile device context, PINs currently remain the most dominant authentication method to protect the access of these devices, as concerns 2/3 of mobile device users [18]. PINs can be applied to both the device and the user's Subscriber Identity Module (SIM)—a removable token that contains required cryptographic keys for network access. Both of the two leading mobile device operating systems (*i.e.* Android and iOS) provide this authentication mechanism.

However, PINs involve several issues considering memorability or human habits that may compromise the security offered by the system. In that sense, Clarke and Furnell [18] have assessed that 1/3 of mobile phone users who keep their phone locked *via* a 4-digits PIN method, consider such protection as an inconvenience in everyday life. As a result, users do need to retain a code that has a familiar signification, such as their date of birth [17]. Furthermore, Clarke and Furnell [18] also enhance the weakness of this authentication scheme. Indeed, 36% of the respondents have reported using the same PIN-code for multiple services. Thus, it becomes easier for an attacker to determine the correct 4-digits PIN in order to have free access to several other services where the code is set. The lack of security brought by users can also be underlined *via* another study that report 26% of PIN users shared the proper code with someone else [19].

While PINs still remain very popular, they may also be considered as weakest authentication mechanisms on the market as they offer a theoretically low entropy (*i.e.* $log_2(10^4)$). Indeed, people adopted several behaviors to cope with the large cognitive load that the system requires. All of this lead PINs authentication to be largely vulnerable to several attacks such as code guessing by social engineering, brute force, or shoulder surfing attacks [20-23].

2.2.2. Text enhanced passwords

Example of use case scenario: conversely to PINs, users have to select, at least, an array of 6 characters that are not restricted to only digits. The whole set of characters offered by the keyboard of the mobile device is legitimate. Next, the authentication depends on the same process as PINs one.

As opposed to PINs, text enhanced passwords are more complex. Usually, they are composed of several different characters such as lower and upper case letters, digits, and also non-alphanumeric characters. At first, passwords were stored in plain text files without any encryption [24]. Thereby, protect such sensitive information became crucial for numerical system. This mechanism is also provided by both Android and iOS platforms. However, as plainly regards authentication on mobile devices, text enhanced passwords remain less popular than PINs among mobile device users. Indeed, authenticate users with a complex string of characters is an inherited process that comes from traditional computing, and it was not revised at all before its arrival on mobile devices.

The market of mobile applications is vast. As an example, the Apple Store counted up to 600,000 applications, and the total number of downloads surpassed 25 billion in the year 2012 [25]. Through this immense inventory, numerous applications require the user to login in order to have access to the entire set of features they offer [26]. Text enhanced passwords also take part in the daily usage of mobile devices as regards authentication. Hence, it is now important to illustrate the weakness of this mechanism for users' memory and how such issues lead to affect mobile device security due to users' behaviors. Passwords remain theoretically a strong way to secure a system. However, they are usually long and sophisticated. Hence, much more memorizing abilities are required for the user. Indeed, Yan [15] identifies that without the memorization problem, the maximally secured password would be blended with the maximum number of characters allowed by the system, randomly arrange. This is possible to do for a machine, but almost impossible to retain for a human. Moreover, text enhanced passwords do have better entropy than PINs (*i.e.* $\log_2(94^k)$) where k is the password length and 94 is the number of printable characters excluding *SPACE*. Although, because they are everywhere, and because they were designed to a machine point of view, passwords represent a mechanism not as good as claimed. Hence, a study conducted by Riley [27] shows that more than half password users have conceded using the exact same string of characters for multiple accounts on numerical systems. Moreover, about 15% of them admit that they used to write down their list of passwords in case they forget them, while 1/3 also report using the *remember my password* function, to produce another password than the one they originally set up. The growth of the number of numerical services we use in our everyday life affects significantly the usage of passwords we have. Another study also highlights the deficiency of this mechanism as they released the "worst passwords" list, which exposed some examples such as *123456*, *password* or *qwerty* that are frequently set up by users [28]. Such examples formed perfect cases of vulnerability for the security of mobile devices. Just as PINs, text enhanced passwords are strongly exposed to brute force, dictionary, social engineering, and shoulder surfing attacks [20-23].

2.2.3. Graphical passwords

Example of use case scenario: with graphical passwords, users have to recall some pieces of visual information. There are a lot of various implementations, but the most well-known is probably the one implemented in Android that appears in the earliest version of the mobile operating system. First, the user has to set up a path between dots in a matrix as shown by the gray stroke in Figure 2. To be granted to the full access of the mobile device, the user has to reproduce the path he initially set-up. The order of the dots where the path is passing by is essential. As illustrated in Figure 2, if the user defined a path, from the lower-left-corner dot, to the upper-left-corner dot, the inverse drawing (from the upper corner, to the lower one) will not genuinely authenticate the user.

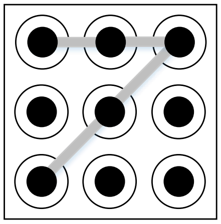

Figure 2: The Android implementation of graphical password authentication.

Knowing that humans have better abilities for recognizing and recalling visual information when compared to verbal or textual information [29], other mechanisms were imagined to use a graphical scheme instead of a sequence of characters as passwords. Since the patent was introduced by Blonder [30], multiple schemes have been designed. Biddle, et al. [31] grouped these proposed systems into three broad categories: recall-based systems; recognition-based systems, and cued-recall systems.

First of all, in a recall-based system, the first step is to choose a predefined pattern. Then, the user is presented with a selected image or a blank canvas where the secret sketch has to be reproduced each time he wants to authenticate himself. Secondly, in a recognition-based system the user is invited to select a sequence of predefined images among several others. The number of presented images is generally limited to ensure the usability. Finally, in a cue-recall system the user has to recall and target a specific part of a picture. In this way, such systems reduce the memory load that the user needs with recall-based systems. Biddle, et al. [31] have pointed out that users are more comfortable to use a graphical password than a digit or a text-based password every day. However, it is known that the Android implementation allows 389,112 possibilities [32]. Therefore, the password space is not superior to a 6-digit PIN. Moreover, as reported by Uellenbeck, et al. [32], users do not exploit the maximum potentiality of the security since some graphical schemes are evident to perform. Another relevant example of a graphical scheme may be the Picture Gesture Authentication (PGA) feature introduced by Microsoft in Windows 8 [33]. The idea behind this mechanism is to allow users to define some specific gestures (*i.e.* taps, circles and lines) over either predefined pictures, or users' personal ones. The whole set of possibilities for such a system largely relies on both the number and the nature of gestures determined. According to Sinofsky [33], when the user defines two of the most complex gesture (*i.e.* lines), there are 846,183 unique possibilities.

As a matter of fact, as assessed by Biddle, et al. [31] it is possible to say that graphical passwords do not offer a higher level of security than PINs or text enhanced passwords. Indeed, as regards an implementation such as the Android one, Uellenbeck, et al. [32] have experienced the ability to find the most common path defined, of numerous graphical schemes. They showed that it was possible to determine the right path statistically by applying a Markov Model algorithm on their dataset. Concerning gesture-based graphical authentication process, Zhao, et al. [34] have demonstrated that the framework they built was able to guess, a large portion of the picture passwords set of their study. Moreover, Aviv, et al. [35] showed that it was possible to find the graphical scheme *via* oily residues, or smudges that users leave on the touch-screen surface. They named this vulnerability smudge attack. Besides, graphical passwords also have the same other vulnerabilities as all knowledge-based authentication mechanisms: social engineering [21, 22] and shoulder surfing [23, 36]. Recently, Gugenheimer, et al. [37] have proposed a novel graphical authentication concept that claims to be robust against shoulder surfing. Through this approach, shoulder surfing attacks were reduced down to 10.5% and authors have pointed out that no participant forgot their graphical scheme. However, it is clear that their process involves a high level of memorization to recall the information due to its complexity when compared to a simple 4-digit PIN code.

2.2.4. Haptic passwords

Example of use case scenario: instead of visual information, the user has to recall a sequence of kinesthetic phenomena produced by the mobile devices. The idea is to let the user define his own sequence that he has to reproduce afterwards to access the mobile device.

With the emergence of modern mobile devices, the desire to exploit haptic in numerical systems in order to enhance the user experience was strong. Mobile devices such as smartphones are composed of a lot of new technologies like touch screens and sensors that provide many more possibilities regarding authentication mechanisms. Consequently, several new knowledge-based authentication schemes have been designed recently. As an example, Bianchi, et al. [38] suggested a novel approach through haptic passwords. The initial work of PINs is retained, but the user has to recall a sequence of vibrations scheme instead of a sequence of single digits. As graphic passwords, haptic ones were designed to be more convenient for users than text-enhanced passwords. The implementation proposed by Bianchi, et al. [39] attempt to avoid the memorability issues encountered by users and reduce behaviors that conduct to security vulnerabilities. However, this study also highlights that such new authentication mechanisms, still require unreasonable calls from memory. As a result, they are not the answer to fix issues provided by PINs, text passwords, or graphical passwords.

2.3. Cognitive schemes

Mechanisms we described above are all explicit methodologies for a knowledge-based authentication. However, each person has a unique set of knowledge. Thereby, cognitive passwords aim at exploiting personal facts, opinion, and interests as a means of authentication. This process is defined as a challenge-response.

The idea behind these schemes first stems from regular computer security access where users, in addition to a conventional password, have to answer some personal questions to be granted the access. However, regarding a mobile device context, such an approach should be more considered. Indeed, as we state in the first part of this chapter, users used to store more and more data on their devices. Thus, data such as pictures, music, and information from social media [9, 40] may be exploited to build a convenient cognitive process for authentication, revised to be employed with mobile devices.

The experiment led by Bunnell, et al. [41] regarding these authentication schemes showed that personal facts were better recalled than others. Despite, people socially close to the user were easily able to guess many answers, that is why, Lazar, et al. [40] have proposed a method to personalize cognitive passwords to individual users. Results obtained show that personalization increases the recall of cognitive passwords, but does not help in improving their secrecy.

3. Token-based authentication mechanisms

Example of use case scenario: token-based authentication needs the user to pocess a physical piece of hardware which has first to be coupled with the mobile device. Then, the mobile device has to verify the credentials of the token to grant access to the user.

Token-based authentication mechanisms require a hardware interaction between the user and his device to complete the authentication process. Such mechanisms involve at least a two-factor authentication (*multi-factor* is used when there is more than two) due to the commitment to attest that both the password is correct, and the user holds the token all along the authentication process. The three major types of tokens are USB token devices, smart cards and password-generating token [42]. Password-generating tokens usually imply a mobile device in the authentication process as described by Aloul, et al. [43], but the purpose is not to authenticate a user directly on his mobile device.

Thereby, these old implementations—when compared to the existence of mobile devices—are no longer applicable as they were initially designed. Nowadays, we observe the growth of smart objects and connected objects as known as the Internet of Things (IoT) [44]. Consequently, modern approaches regarding token-based authentication mechanisms appear to be more convenient with the use of such devices. As examples, smart watches are replacing USB devices while NFC tags will supplant smart cards overtime, since it is possible to bring them everywhere (*i.e.* wallets, clothes). With the fifth version of Android, Google introduces a feature called *trusted devices*. This feature aims at providing an automatic authentication mechanism that uses smart objects the user has to couple to his mobile device. As a result, as long as the mobile device detects a connection with the token hardware *via* Bluetooth, NFC, or Wi-Fi, it remains unlocked.

Regarding two-factor authentication mechanisms, Schneier [45] suggests that "they solve the security problem we had ten years ago, not the security problems we have today". The use of smart objects over the authentication process implies many cases of vulnerability issues. Indeed, whenever someone wears a smart object as a token for the authentication process, the mobile device should not be sighted off. Due to the fact that there is no need to replay the authentication process, the mobile device becomes simply accessible by anyone nearby. Another problematic situation may be observed, where both devices are stolen by the same person.

4. Biometrics

For many years, it is known that humans exhibit a various unique set of features. As an example, each human fingerprint describes a unique pattern; in the same way, blood vessels of the retina also have a unique pattern. Biometrics systems exploit these singularities in order to authenticate users. Hence, with a biometric system, there is no need for remembering or recalling any information. Instead, the singularity of interest just has to be digitized and compared to the saved one. To this end, several biometric systems necessitate the use of a scanning or recording hardware that is not always adapted to suit with mobile devices. When compared to other approaches, a vast majority of biometric solutions have a greater cost of implementation. Moreover, due to the assessment of data that come directly from the user, biometrics raise some privacy concerns. As a result, even though these systems generally offer a high level of security, and a sufficient accuracy, their usage remains limited, particularly with mobile devices.

The review of biometric authentication that we propose below does not heed sophisticated mechanisms such as blood vessels, retina or iris pattern recognitions that are way too complex in hardware requirements or computational costs, to be applied on mobile devices, presently. Retina-based systems are currently only used in highly classified government and military facilities [46]. Although, iris pattern recognition requires specific infrared hardware to authenticate users accurately [16, 47, 48]. Hence, we focus on offered mechanisms for mobile devices and those that may be materialized in coming years.

4.1. Fingerprint

Example of use case scenario: first, the user has to let the device know the pattern of one or more of his/her fingerprints. To this end, he/she has to put, several times, each desired finger on the sensor, in order to record a template of these fingerprints. Then, they can be reused to unlock the mobile devices during the authentication process.

This technology uses unique fingerprint patterns that are present in every human's fingers to authenticate users. Ridges that compose the pattern are traditionally classified into loops, arches and whorls motifs. Figure 3 illustrates three examples of these patterns.

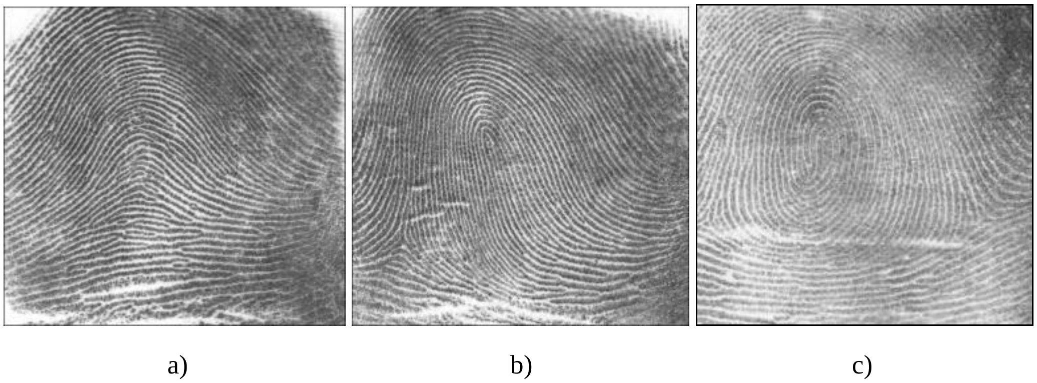

Figure 3: Ridges patterns of fingerprints where a) arch pattern; b) loop pattern and c) whorl pattern.

Fingerprint techniques were used for decades using ink to print the pattern onto a piece of paper [49]. However, several sensors were designed to perform the acquisition such as optical scanning, capacitive scanning, and ultra-sound scanning [11, 50, 51]. Due to the maturity and the flexibility of fingerprint systems it is presently, the most popular biometric system on mobile devices on the market. Indeed, fingerprint authentication deliver a high accuracy level and may be used in a wide range of environments. Moreover, with the growth of micro-technology and the emergence of mobile devices, more and more efficient, fingerprint systems were integrated into these devices as means of authentication. The most well-known example of fingerprint system used with mobile devices is the Apple *Touch ID* technology that comes from the patent of Bond, et al. [52]. This major player of the mobile device industry builds an extra capacitive sensor in all their latest smartphones that scans sub-epidermal skin layers. Furthermore, they made the acquisition of the fingerprint possible up to 360-degrees of orientation that provide a very high level of accuracy and a small error rate. Moreover, several other phone and tablet manufacturers also introduce fingerprint sensors built-in their phones. The major difference between each one resides in the location of the sensor to ensure the ease of use for end-users (*i.e.* inside the power button, at the back of the phone).

In addition, Clarke, et al. [19] assessed that 74% of mobile device users positively accept fingerprint biometric as means of authentication. Nevertheless, this mechanism has weaknesses that engender threats in its usage. It has been discovered that “most devices are unable to enroll some small percentage of users” [46]. The accuracy of fingerprint scanning may decrease to null when digits are either too wet, or too dry and also too oily. This is the moisture effect. Fingerprints also tend to deteriorate over the time because of age, wear or tear [46]. Furthermore, fingerprint authentication schemes suffer from confidentiality threats, as well as spoofing attacks that question the security they attempt to provide. Indeed, on the one hand, users may be scanned without their consent. On the other hand, Matsumoto, et al. [53] proved that artificial fingers either made of silicon or gelatin, were accepted by 11 fingerprint systems during the enrollment procedure.

4.2. Face Recognition

Example of use case scenario: as well as fingerprint authentication process, the user has to let the device knows his/her facial characteristics. To this end, he/she has to stand in front of the camera of the device while the system is processing the learning of his/her face. Then, if the face is recognized by the system, the user is granted to access the device.

Face recognition is the most natural means of biometric authentication because humans also perform this evaluation in their everyday interactions. This authentication scheme may also be plainly integrated into an environment that allows image acquisition such as mobile devices, where a large majority of them have a frontal camera. Moreover, methods to acquire an image of the face is assessed as non-intrusive [16]. Most of the time, facial recognition systems rely on the analysis of facial features such as the position of the eye, the nose the mouth and distances between these features [54]. The evolution of both hardware and software lead facial recognition to become faster and to provide a better level of accuracy than before. Besides, it should be noted that a facial recognition may be continuously achieved. Indeed, the user may perform the authentication by his/her face, and then, the system may automatically verify that it is always the same face that using the device when it is not in sleep mode.

From few years, Google offered a face-based authentication system. Although it was not genuinely successful, the improvement in attendance of the new version of the operating system still not accurately identifies the user in numerous cases such as low lighting environment. As a matter of fact, Adini, et al. [55] have pointed out this problem as a major drawback in facial recognition, as well as a high complexity in the background. In addition, physical changes such as hairstyle or beard variations, and wearing hats or glasses [56], may greatly affect the matching rate of face recognition systems. Such systems also have troubles to identify very similar individuals such as twins [57] and to keep a satisfying level of accuracy when physical changes occur owing to the age [58]. Finally, the fact that a user may be scanned without his consent raises serious threats according to confidentiality.

4.3. Hand geometry and ear shape

Example of use case scenario: as every biometric system, both hand and ear recognition need to learn from user unique physical features. Depending on the implementation, this process may be performed, several times, through either optical analysis, or *via* the capacitive touch-screen of the mobile device. Finally, the user has to repeat once the same process, each time the device has to be unlocked.

Both hand geometry and ear shape biometric authentication mechanisms are based on the fact that nearly every individual’s hands and ears are shaped differently. These body parts also remain practically the same after a certain age.

As regards ear shape as a means of authentication, Alphonse Bertillon’s researches helped to develop such biometric systems as he worked particularly on the classification of this body part [59]. Several more recent studies on the subject have shown that the acquisition of the ear was exclusively made with cameras [60-62]. In that sense Descartes Biometric has released, short while ago, the most mature ear-shape-based authentication system of the market*: Helix*. This software exploits the proximity sensor of the front camera on the mobile device. The user needs to place the device from 6 to 12 inches in front of his ear. Then, 30 images per second are recorded, processed and finally compared to the stored template. Moreover, the company offers the possibility to configure the accuracy threshold at a higher level. However, the record of ear images with the front camera of the mobile device may be disturbing for users in their daily usage. In that sense, the Yahoo research department yet offers an experimental approach that handles the capacitive sensors embedded in the screen of mobile devices, to record the topography of the ear. According to Hornyak [63] this system correctly identified users at 99.52 percent of the time. This rate is based on a test that involved 12 participants. Such a system appears to deliver a more appropriate ease of use for users since it mimicking the act of calling.

On another side, hand geometry recognition is the ability to compare dimensions of fingers and the localization of joints, shape and size of the palm, and also phalanges disposition. However, hand geometry is not distinctive enough to accurately identify a large set of individuals. Therefore, such systems may not be used in an authentication process, but rather in a verification process. Just as ear recognition, several studies involve a camera through the hand-record process [64-66]. By contrast, the report of Hornyak [63] noticed that the Yahoo research department also worked on a hand geometry recognition software. This experimental system allows the authentication of mobile device users in the same way as their ear recognition system. Both phalanges and palm identifications are possible, and the same matching rate of 99.52% was communicated applied to this system.

Ear shape recognition and hand geometry appear to be encouraging ways in order to authenticate users on their mobile devices since they aim to be more usable for such devices. The example we presented above expose very simple techniques, which are easy to use and which do not require any additional sensor than these already built-in the mobile device. Moreover, these examples show up promising results. However, these two authentication schemes also admit drawbacks. As concern ear shape, when recorded with a camera, hairs, hats or piercings may compromise the identification process. Nevertheless, these limitations should be lower when using the capacitive sensors of the mobile device touch screen. Regarding hand geometry, jewelry and arthritis will involve matching errors in both cases.

4.5. Voice: speaker recognition

Speaker recognition techniques are classified as a behavioral biometric. Indeed, they focus on vocal characteristics produced by the speech and not on the speech only. These features depend on the dimension of the vocal tract, mouth, and nasal cavities, but also rely on voice pitch, speaking style, and language [67] as represented in Figure 4.

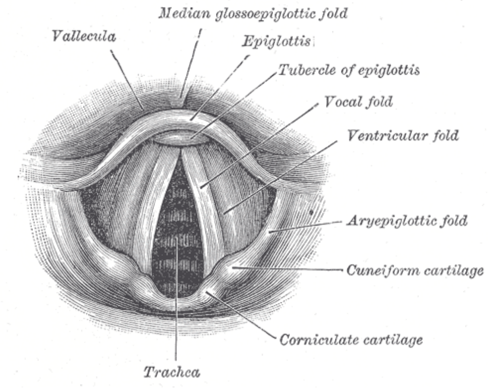

Figure 4: Anatomical diagram of vocal folds or cords.

There are two leading methods to process speaker recognition: text-dependent and text-independent [68, 69]. Text-dependent recognition involves the user to pronounce a predefined passphrase. It is considered as a voice password and used both for the enrollment and the verification process. By contrast, text-independent systems are able to identify the user, for any text, properly. However, Boves and den Os [70] have identified a third type of speaker recognition technique that is a combination of the two others: the text-prompted method that randomly select a passphrase the user needs to pronounce each time the system is used. Speaker recognition is an inexpensive solution to authenticate users on their mobile devices since no additional sensor is required. In addition to, speaker recognition is another mechanism that may be able to authenticate users continuously. Indeed, a first recognition may be achieved to grant the access to his/her owner, but such a process may also be performed each time the device either, or both, receive or emit a phone call. As an example of practical implementations, Google also introduces in *Smart-Lock,* the *trusted voice* feature. As all text-dependent-based speaker recognition, the user has to enroll his voice by pronouncing “Ok Google” three times. Then, the user must pronounce the same passphrase during the authentication process. Whenever the record matches both the voice model and the passphrase, the access to the mobile device is granted.

However, speaker-recognition-based authentication mechanisms admit several major drawbacks. In the first place, since such systems are viewed as behavioral, the current physical, medical or emotional condition of the user may considerably affect the accuracy. Voice is also likely to change over time due to the age. Moreover, speaker recognition techniques are rarely noise resistant. Then, various loud background noises make such systems almost impossible to use in public places such as bars or public transports. Finally, speaker recognition techniques are singularly exposed to security threats. It is possible for an attacker to record or imitate the voiceprint of the user to perform a fraudulent authentication afterwards [71].

4.6. Gait

Example of use case scenario: the process of authentication *via* gait analysis is independent of any action from the user. The mobile device is able to determine whether he/ she is walking or not and then perform a recognition to unlock the device automatically in a continuous manner.

Gait recognition is a technology based on the analysis of the “rhythmic patterns associated with walking stride” [72]. The observation that each human’s walking style is different leads to the development of advanced biometric authentication systems that exploit such behavioral characteristics.

Accordingly, studies have proposed a gait analysis mechanism based on an accelerometer to collect features that create the gait template [12, 73]. It is possible for such a system to be integrated with mobile devices since they include built-in inertial sensors (*i.e.* accelerometer, gyroscope). As a matter of fact, gait recognition may become a convenient way to authenticate users as they always keep their mobile devices within their pocket or a bag. It is fair to say that it constitutes a human-centered system since the authentication process is wholly imperceptible to the user.

Withal, gait is not as stable over time due to changes in body weight. Such a physical change is not the only way for this human behavior to change. Indeed, brain damages, injury and also inebriety may involve from a short time to a long time or permanent variation in the manner of how individuals walk [74, 75].

4.7. Keystroke dynamics

Keystroke dynamics are based on the measurement and the assessment of the human’s typing rhythm on numerical systems. This process allows the creation of a digital print upon users’ interaction with devices that are rich in cognitive qualities [76]. Characteristics of this user behavior are fairly unique to each person and hold a high potential as an authentication mechanism. With the growth of capacitive touch screens, keystrokes patterns are now capable of providing even more unique feature for the authentication than only typing rhythm, which includes key press duration, latencies, typing rate, and typing pressure. Such characteristics may be measured up to milliseconds order precision [77] and more recent studies have pointed out high accuracy level [78, 79]. Thus, it is nearly impossible for an attacker to replicate a defined keystroke pattern without an enormous amount of effort. The main benefit of keystroke dynamics pattern recognition is that anything except an extra software layer is required. Moreover, keystrokes analysis may be employed as continuous authentication process for free typing instead of one-time authentication such as fingerprint. However, since touch keyboards only appear when users are granted the full access, it is not possible to perform the authentication process *a posteriori*. As a result, keystroke dynamics may only be employed to verify continuously that the current user is well and truly the owner of the mobile device afterwards. Thus, such a system must not be self-sufficient and requires to be coupled to a non-continuous authentication scheme as regards a mobile device usage.

4.8. Signature

Example of use case scenario: generally, a blank canvas is prompted to the user where he/she has to make his/her personal signature. The analysis is based on the way the signature is produced by exploiting pressure, direction, acceleration; rather than only a comparison of the signature pattern itself. The first step resides in the definition of such a model to compare with, and then, the user has to reproduce his signature each time the mobile device has to be accessed.

Signatures were used for decades in the concrete world while people need to enact documents. The same idea is used over numerical systems for authentication purposes. Signature recognition is considered as a behavioral biometric since it is based on the dynamic of making signature rather than a unique comparison of the signature itself.

Since users have to reproduce their signature on a mobile device touch screen, the identification process may determine dynamics, owing the measurement of the pressure, the direction, the velocity and the acceleration and the length of the strokes. Initially, the hardware used to record individual's signatures was not convenient enough for users [80]. However, with the advent of capacitive touch screens on mobile devices, the use of such an authentication process became user-friendlier. Moreover, a unique extra software layer is required to make it work.

Despite, as for every behavioral biometric system, people's physical and emotional condition may considerably affect an authentication mechanism based on signature recognition. Besides, it is important to note that this is the only biometric authentication scheme that is possible to be deliberately changed by the user even though any replication requires lots of effort.

4.9 Heartbeat

Recently, Sufi, et al. [81] have introduced the use of the electrical activity of the heart as a novel biometric authentication mechanism. Since the heartbeat is evaluated as unique for each person [82], such a system requires a record of an electrocardiogram (ECG or EKG) as illustrated in Figure 5. Hence, as biometric authentication schemes we described above, the first step of the process consists in an enrollment phase. Unique features are extracted to build a template, then compared through the identification process.

Figure 5: Example of an ECG curve.

Exploiting ECG as means of authentication is suitable across a wide range of people. Indeed, heartbeat samples may be collected from any part of the body such as fingers, toes, chest, and wrist. Thus, people who suffer from large injuries may be authenticated, continuously or not, by using such a system. As we saw before, connected objects and in a broader sense, IoT, begin to take a measurable place through the numerical environment [44]. In that sense, a Canadian company patented a wristband that is fully compliant with mobile devices *via* a companion application. This band is able to authenticate a user wearing it by his/her heart signature [83].

Such a system seems to be largely reliable as reproducing heartbeat signature depends upon sophisticated skills and hardware. Therefore, it is nearly impossible for an attacker to spoof such authentication systems. Since it may be considered as a behavioral biometric, several factors may seriously affect its accuracy such as daily activities and nutrition facts, stress level, and weariness.

4.10. Evaluation of the accuracy

As we have seen in above sections, biometric systems are not devoid of potential errors over the authentication process. These systems can make two types of errors: false acceptance rate (FAR), and false rejection rate (FRR). Figure 3 graphically illustrates these types of errors in detail. On the one hand, FAR or also false match rate (FMR) is the probability that the system incorrectly declares a successful match between the input pattern, and one stored in the database. FAR is obtained by the equation (3) where F_a is the number of false acceptances, and V_i is the number of imposter verification.

$$FAR = \frac{F_a}{V_i} \tag{3}$$

On the other hand, FRR or also false non-match rate (FNMR) is the probability that the system declares a failure while the input pattern matches with the template stored. FRR is obtained by the equation (4) where F_r is the number of false rejections, and V_g is the number of genuine verification.

$$FRR = \frac{F_r}{V_g} \tag{4}$$

Generally, the matching algorithm performs a decision using some parameters as a threshold. Graphically expressed both FAR, and FRR, by opposition to the given threshold, represent the relative operating characteristic (ROC). This plot allows finding the equal error rate (EER) as shown in Figure 6. EER is the rate at which both accept and reject errors are equal. This rate is commonly used to evaluate biometrics. Indeed, the lower the EER is, the more accurate the system is considered to be. The report by Mansfield and Wayman [84] describes in detail the performance evaluation for biometric systems.

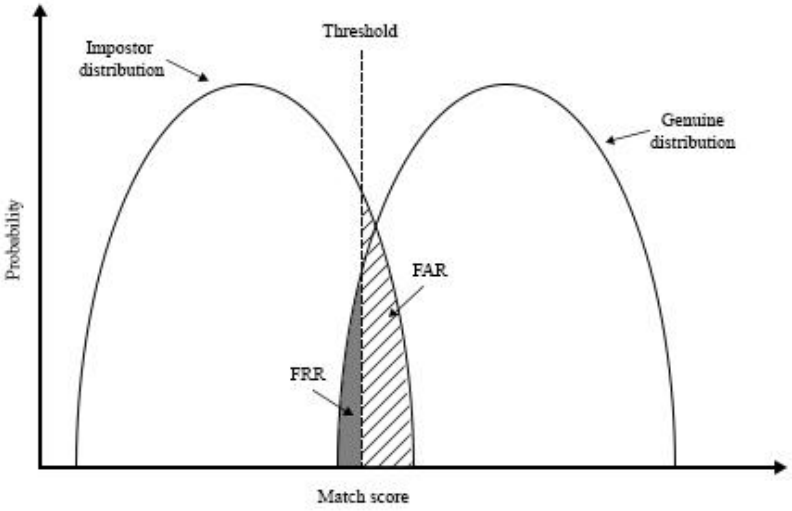

Figure 6: Biometric system error rates, where curves show false acceptance rate (FAR) and false rejection rate (FRR) for a given threshold.

Several studies [85-87] exhibit the performance of various biometric authentication mechanisms regarding evaluation criteria described above as illustrated in Table 1.

Table 1: Evaluation of various biometrics performances [85-87].

	EER	**FAR**	**FRR**	**Conditions**
Face recognition	-	1%	10%	Varied light: indoor, outdoor
Fingerprint	2%	0.1%	2%	Rotation and exaggerated skin distortion
Hand geometry	1%	0.14%	2%	With rings and improper placement
Iris	0.01%	≈ 0%	0.99%	Indoor
Voice recognition	6%	3%	10%	Text dependent and multilingual
Keystrokes	1.8%	7%	0.1%	6 months recorded data

The required accuracy for a biometric system depends chiefly on the need of the application. Presently, biometric system designers aim at reducing false acceptance rates. However, the false rejection rates undeniably grow. To cover FRR up, most of current designs offer to bypass the biometric system that fails and suggest the user to perform another authentication scheme instead. The use of such a fallback mechanism represents a multi-factor authentication scheme. Biometric was often introduced as an encouraging way to end with the use of passwords (knowledge-based schemes). However, since both Apple and Google recently released their respective biometric technologies *Touch ID*, *Nexus Imprint* and *Smart-Lock*, mobile device users still have to set up a more traditional authentication mechanism such as PIN before enabling these features. As a matter of fact, we may affirm that passwords are still not dead contrary to everything said. Nevertheless, as claimed by Kokumai [88], threats that can be thwarted by biometric authentication that operated together with rescue passwords, still remain less secure than just only a knowledge-based authentication mechanism. Indeed, a two-factor authentication system must be treated as a conjunctive statement in opposition to a disjunctive statement. In other words, both the main system and the fallback one have to authenticate the user properly, and not just one, as offered by the main biometric solutions available on the market.

5. Discussion

Based on the above critical analysis, it is possible to say that each authentication mechanism we assessed concede some advantages, as well as drawbacks. In order to state about the aftermath of authentication, here we discuss the whole set of proposed mechanisms.

First, we offer an examination of knowledge-based authentication schemes *via* both the theoretical and real measure of the password space entropy that each of them provides – as illustrated in Table 2. Theoretical entropy is inevitably greater than the real one since users do choose their own piece of knowledge. The main deficiency of PINs resides in their simplicity, as they remain easy to guess by almost everyone. Text-enhanced passwords are an excessively complex solution for mobile devices users that force them to choose easy-findable identification codes. Finally, graphical and haptic passwords provide an adequate level of security, but still remain easy to obtain *via* shoulder surfing attacks or smudge attacks.

Table 2: Evaluation of knowledge-based authentication mechanisms for mobile devices *via* the password space entropy metric: H – High; M – Medium; L – Low.

	Knowledge-based		
	Explicit		
	PIN	*Text enhanced passwords*	*Graphical & haptic passwords*
Theoretical password-space entropy	L	H	M
Real password-space entropy	L	L	M

Secondly, we suggest an empirical evaluation of biometrics authentication mechanisms based on previous related work of Jain, et al. [16] in 1999. As assessed in above sections, several novel studies aim at improving biometric processes to be more accurate and fast, as regards mobile devices [78, 89-91]. As a matter of fact, this study requires some improvement. Hence, changes we introduced mainly focus on the performance criteria. Moreover, we include heartbeat authentication that was not discussed in their work. Our evaluation is based on the same criteria suggested by Jain, et al. [16] which were defined by biometric experts. Such a guideline is described as follows:

1. Universality: Biometric solutions rely upon singularities of the human body or behavior, but the ability of such mechanisms to accurately identify the genuine user largely varies between each one. Consequently, Jain, et al. [16] have suggested to quantitate the fact that each person should have the characteristic.

2. Uniqueness: Some physical traits of the human body (*e.g.* face) remain largely close in some cases (twins). Therefore, Jain, et al. [16] have proposed to evaluate the probability that two individuals are potentially the same, in terms of characteristics.

3. Permanence: Physical or behavioral features of the human used with biometrics may gradually evolve. This criterion figures out the invariance of these characteristics with time [16].

4. Performance: The inability of a biometric system to identify a user with a 100% accuracy, lead to identifying the related performance offered by each one [16].

5. Collectability: Most of the time, the biometric authentication process involves additional hardware or a major computing complexity with mobile devices. This criterion refers to the evaluation of how simple a characteristic is quantitatively measurable [16].

6. Acceptability: All biometric techniques still not become the custom. Then, it is important to state the users' acceptance rate, according to such mechanisms [16].

7. Circumvention: The last criteria reported by Jain, et al. [16] refers to the easiness of mimicking a singular trait or behavior with biometric systems. Such an evaluation delivers the strength rate of biometric systems in front of fraudulent attacks (*e.g.* spoofing attack).

Table 3: Evaluation of biometric authentication mechanisms for mobile devices according to criteria proposed by Jain, et al. [16]: H – High; M – Medium; L – Low. Improvements are identified by **bold**.

	Biometrics								
	Physiological				Behavioral				
	Fingerprint	*Face recognition*	*Ear shape*	*Hand geometry*	*Voice recognition*	*Gait recognition*	*Keystroke dynamics*	*Signature*	***Heartbeat [91]***
Universality [16]	M	H	M	M	M	M	L	L	**M**
Uniqueness [16]	H	L	M	M	L	L	L	L	**M**
Permanence [16]	H	M	H	M	L	L	L	L	**L**
Collectability [16]	M	H	M	H	M	H	M	H	**M**
Performance [16]	**H**	**M** **[89]**	**H** **[63]**	**H** **[63]**	**M**	**M** **[78]**	**M** **[90]**	L	**M**
Acceptability [16]	M	H	H	M	H	H	M	H	**H**
Circumvention [16]	H	L	M	M	L	M	M	L	**H**

Finally, we estimate that several criteria were missing to perform a proper evaluation of authentication mechanisms. Consequently, we introduce four new criteria based on the above critical analysis of these schemes we proposed. As a matter of fact, we define the following guideline:

1. Confidentiality: Several authentication scheme designs such as fingerprint involve to either, or both, record or store data that relate to the secrecy of the user. To ensure that the information users provide remain in their privacy regards is a crucial interest in the case of security threats.

2. Intrusive: Several authentication mechanisms reviewed in this chapter involve providing information or features relating to the user. This criterion focuses on the ethical concern of the data that use to be collected during the authentication process. This criterion mainly focuses on cognitive schemes as well as biometric ones. Indeed, the authentication process requires to handle data that directly concern users and that may be performed without their broad agreement.

3. Ease of use: The major drawback of authentication mechanisms is predominantly due to the way that Humans have to interact with these systems. In that sense, we suggest evaluating how the user is involved in the interaction process and how the system focuses on what people want to do rather than possibilities offered by the technology.

4. Usage frequency: Since most of more used authentication schemes also remain the weakest ones, we offer to identify to the popularity of the mechanisms when applied to secure a mobile device.

Table 4: Evaluation of the whole set of authentication mechanisms for mobile devices *via* criteria we suggest: H – High; M – Medium; L – Low.

	Knowledge-based				**Token-based**	**Biometrics**								
	Explicit			Implicit		Physiological				Behavioral				
	PIN	*Text enhanced passwords*	*Graphical & haptic passwords*	*Cognitive-based passwords*		*Fingerprint*	*Face recognition*	*Ear shape*	*Hand geometry*	*Voice recognition*	*Gait recognition*	*Keystroke dynamics*	*Signature*	*Heartbeat*
Confidentiality	L	L	M	H	H	M	M	M	M	M	L	H	M	L
Intrusive	N/A	N/A	N/A	M	N/A	M	H	M	M	L	L	L	L	H
Ease of use	M	L	M	M	M	H	M	M	M	M	H	H	M	H
Usage frequency	H	L	H	L	M	M	M	L	L	M	L	M	M	L

Based on such an evaluation, it is possible to affirm that most of authentication schemes raise some inconveniences for users since most of them are considered as not easy to use. Besides, proposed mechanisms that do not involve users in the process of authentication namely transparent for them, such as gait recognition or keystroke dynamics were identified as convenient. As a matter of facts, it is clear that the future trend for authentication on mobile devices will turn into systems that focus on the users first. As an example, it is known that people do spend a considerable amount of time in a few key locations such as home or work as assessed by Hayashi and Hong [92]. In that sense, ubiquitous mechanisms that will be able to learn about users' habits and that will not require any passwords or tokens are close. Indeed, studies in that field of research expose promising results [93], but efforts should probably pay more attention to such a key idea in coming years.

Nowadays, authentication mechanisms remain an important field of interest for researchers and leaders of mobile device industry. According to major players on the market, it should be noted that both Apple and Microsoft took the biometric band respectively, with the *Touch ID* technology and the launch of Windows 10 [94]. Despite, Google seems to want to see further since their Advanced Technology and Projects *(*ATAP*)* division is currently working on an experimental multi-modal biometrics system based on behavioral analysis: the "Project Abacus". The system will identify a genuine user *via* a "trust score" calculated through a real-time analyze of users' voice recognition, keystroke dynamics and touch gestures, facial recognition, and location. The firm presented research results at its annual conference of 2015 and claimed that the entropy of such a system is now ten times higher than the most valuable fingerprint system of the market. While the project is still in development, Google aims to integrate such a system into next versions of the Android operating system. Hence, this research project simply confirms the trend in the evolution of authentication for a near future.

6. Conclusion

The present review of mobile device authentication mechanisms leads us to maintain that each of the schemes we have introduced concedes several strength and weakness aspects. Since knowledge-based mechanisms were designed to a machine point of view, they first involve an enormous amount of memory efforts from users. Behaviors they consequently adopt to overcome a system they are not comfortable with, yield several threats and weaknesses as regards the security of their mobile devices. Token-based authentication schemes are not devoid of weaknesses as well. However, with the ongoing of the Internet of Things, such mechanisms appear to be more convenient than knowledge-based systems and will certainly keep growing. Presently, biometric methods become more and more popular and easy to reach for everyone. Some remain just too much intrusive for users or lead them to believe that providing personal and unique features describing them is an important threat according to their privacy. Nevertheless, biometric techniques are, overall, very accurate, but also accept certain dysfunctions. However, gather a number of biometric mechanisms together, allow the entropy of the entire multi-factor system to extend and consequently increase its accuracy. The major drawback of biometrics resides in the fallback mechanism designed to cope false rejections and let a genuine user proceeds to his authentication properly. Nevertheless, most of current biometric solutions for mobile devices available on the market such as *Touch ID* or *Smart-Lock* have adopted this method.

As we state that the human factor is the fundamental drawback for authentication mechanisms since they involve lots of interaction with users; we consider that the aftermath of such systems should singularly take care of this criterion. Such mechanisms already evolve to become no password systems. Although, they currently provide a better convenience, however, they do not provide a better security. Based on such an evaluation, we assume that the optimal solution should be able to recognize a genuine user without the need for any interaction of his/her part. To be really accurate and secure, such a solution should be based on users' habits of the everyday life (what does he/she do all along his/her day, in which order?) that involve collecting the most of the possible relevant patterns *via* the mobile device. However, it is important to consider that such a solution implies a large set of information more than just for one user. The processing of all of this knowledge, considering each mobile device users, will undeniably increase the cost in hardware requirements. This observation now questions us about ecological issues related to the growth of the number of brand new data centers everywhere in the world.

References

[1] R. Van Der Meulen and J. Rivera, "Gartner Says Smartphone Sales Grew 46.5 Percent in Second Quarter of 2013 and Exceeded Feature Phone Sales for First Time," 2013.

[2] T.-A. Wilska, "Mobile phone use as part of young people's consumption styles," *Journal of consumer policy,* vol. 26, pp. 441-463, 2003.

[3] G. Goggin, *Cell phone culture: Mobile technology in everyday life*: Routledge, 2012.

[4] Nielsen, "Smartphones: so many apps, so much time," 2014.

[5] H. Falaki, R. Mahajan, S. Kandula, D. Lymberopoulos, R. Govindan, and D. Estrin, "Diversity in smartphone usage," in *Proceedings of the 8th international conference on Mobile systems, applications, and services*, 2010, pp. 179-194.

[6] G. Lowe, "A hierarchy of authentication specifications," in *Computer Security Foundations Workshop, 1997. Proceedings., 10th*, 1997, pp. 31-43.

[7] S. Z. Li, *Encyclopedia of Biometrics: I-Z* vol. 1: Springer Science & Business Media, 2009.

[8] L. Lamport, "Password authentication with insecure communication," *Communications of the ACM,* vol. 24, pp. 770-772, 1981.

[9] M. Zviran and W. J. Haga, "User authentication by cognitive passwords: an empirical assessment," in *Information Technology, 1990.'Next Decade in Information Technology', Proceedings of the 5th Jerusalem Conference on (Cat. No. 90TH0326-9)*, 1990, pp. 137-144.

[10] J. Xu, W.-T. Zhu, and D.-G. Feng, "An improved smart card based password authentication scheme with provable security," *Computer Standards & Interfaces,* vol. 31, pp. 723-728, 2009.

[11] A. Jain, L. Hong, and R. Bolle, "On-line fingerprint verification," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 19, pp. 302-314, 1997.

[12] D. Gafurov, K. Helkala, and T. Søndrol, "Biometric gait authentication using accelerometer sensor," *Journal of computers,* vol. 1, pp. 51-59, 2006.

[13] D. Benyon, P. Turner, and S. Turner, *Designing interactive systems: People, activities, contexts, technologies*: Pearson Education, 2005.

[14] N. Ben-Asher, H. Sieger, D. Telekom, A. Ben-Oved, N. Kirschnick, J. Meyer*, et al.*, "On the need for different security methods on mobile phones," 2011.

[15] J. Yan, "Password memorability and security: Empirical results," *IEEE Security & privacy,* pp. 25-31, 2004.

[16] A. K. Jain, R. Bolle, and S. Pankanti, *Biometrics: personal identification in networked society*: Springer Science & Business Media, 1999.

[17] R. V. Yampolskiy, "Analyzing user password selection behavior for reduction of password space," in *Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International*, 2006, pp. 109-115.

[18] N. L. Clarke and S. M. Furnell, "Authentication of users on mobile telephones – A survey of attitudes and practices," *Computers & Security,* vol. 24, pp. 519-527, 10// 2005.

[19] N. L. Clarke, S. M. Furnell, P. M. Rodwell, and P. L. Reynolds, "Acceptance of subscriber authentication methods for mobile telephony devices," *Computers & Security,* vol. 21, pp. 220-228, 2002.

[20] S. Hansman and R. Hunt, "A taxonomy of network and computer attack methodologies," *Department of Computer Science and Software Engineering, University of Canterbury, Christchurch, New Zealand,* vol. 7, 2003.

[21] T. N. Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social phishing," *Communications of the ACM,* vol. 50, pp. 94-100, 2007.

[22] G. L. Orgill, G. W. Romney, M. G. Bailey, and P. M. Orgill, "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems," in *Proceedings of the 5th conference on Information technology education*, 2004, pp. 177-181.

[23] F. Tari, A. Ozok, and S. H. Holden, "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords," in *Proceedings of the second symposium on Usable privacy and security*, 2006, pp. 56-66.

[24] R. Morris and K. Thompson, "Password security: A case history," *Communications of the ACM,* vol. 22, pp. 594-597, 1979.

[25] F. Cuadrado and J. C. Dueñas, "Mobile application stores: success factors, existing approaches, and future developments," *Communications Magazine, IEEE,* vol. 50, pp. 160-167, 2012.

[26] M. A. Sasse, S. Brostoff, and D. Weirich, "Transforming the 'weakest link'—a human/computer interaction approach to usable and effective security," *BT technology journal,* vol. 19, pp. 122-131, 2001.

[27] S. Riley, "Password security: What users know and what they actually do," *Usability News,* vol. 8, pp. 2833-2836, 2006.

[28] SplashData. (2014, Janvier, 20). *« 123456 » Maintains the Top Spot on our Annual « Worst Passwords » List*. Available: http://splashdata.com/splashid/worst-passwords/

[29] E. A. Kirkpatrick, "An experimental study of memory," *Psychological Review,* vol. 1, p. 602, 1894.

[30] G. E. Blonder, "Graphical password," ed: Google Patents, 1996.

[31] R. Biddle, S. Chiasson, and P. C. Van Oorschot, "Graphical passwords: Learning from the first twelve years," *ACM Computing Surveys (CSUR),* vol. 44, p. 19, 2012.

[32] S. Uellenbeck, M. Dürmuth, C. Wolf, and T. Holz, "Quantifying the security of graphical passwords: The case of android unlock patterns," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013, pp. 161-172.

[33] S. Sinofsky. (2011). *Signing in with a picture password*. Available: http://blogs.msdn.com/b/b8/archive/2011/12/16/signing-in-with-a-picture-password.aspx

[34] Z. Zhao, G. J. Ahn, and H. Hu, "Picture gesture authentication: Empirical analysis, automated attacks, and scheme evaluation," *ACM Transactions on Information and System Security,* vol. 17, 2015.

[35] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge Attacks on Smartphone Touch Screens," *WOOT,* vol. 10, pp. 1-7, 2010.

[36] A. H. Lashkari, S. Farmand, D. Zakaria, O. Bin, and D. Saleh, "Shoulder surfing attack in graphical password authentication," *arXiv preprint arXiv:0912.0951,* 2009.

[37] J. Gugenheimer, A. De Luca, H. Hess, S. Karg, D. Wolf, and E. Rukzio, "ColorSnakes: Using Colored Decoys to Secure Authentication in Sensitive Contexts," in *Proceedings of the 17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, 2015, pp. 274-283.

[38] A. Bianchi, I. Oakley, and D. S. Kwon, "The secure haptic keypad: A tactile password system," in *Conference on Human Factors in Computing Systems - Proceedings*, 2010, pp. 1089-1092.

[39] A. Bianchi, I. Oakley, and D. S. Kwon, "Counting clicks and beeps: Exploring numerosity based haptic and audio PIN entry," *Interacting with Computers,* vol. 24, pp. 409-422, 2012.

[40] L. Lazar, O. Tikolsky, C. Glezer, and M. Zviran, "Personalized cognitive passwords: an exploratory assessment," *Information Management & Computer Security,* vol. 19, pp. 25-41, 2011.

[41] J. Bunnell, J. Podd, R. Henderson, R. Napier, and J. Kennedy-Moffat, "Cognitive, associative and conventional passwords: Recall and guessing rates," *Computers & Security,* vol. 16, pp. 629-641, 1997.

[42] F. F. I. E. Council, "Authentication in an internet banking environment," *Financial Institution Letter, FIL-103-2005. Washington, DC: Federal Deposit Insurance Corp.(FDIC). Retrieved March,* vol. 18, p. 2005, 2005.

[43] F. Aloul, S. Zahidi, and W. El-Hajj, "Two factor authentication using mobile phones," in *Computer Systems and Applications, 2009. AICCSA 2009. IEEE/ACS International Conference on*, 2009, pp. 641-644.

[44] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks,* vol. 10, pp. 1497-1516, Sep 2012.

[45] B. Schneier, "Two-factor authentication: too little, too late," *Commun. ACM,* vol. 48, p. 136, 2005.

[46] "Biometrics: Identity Verification in a Networked World (Book Review)," vol. 58, ed, 2002, pp. 698-698.

[47] J. Daugman, "How iris recognition works," *Circuits and Systems for Video Technology, IEEE Transactions on*, vol. 14, pp. 21-30, 2004.

[48] R. P. Wildes, "Iris recognition: an emerging biometric technology," *Proceedings of the IEEE,* vol. 85, pp. 1348-1363, 1997.

[49] J. Berry and D. A. Stoney, "The history and development of fingerprinting," *Advances in fingerprint Technology,* vol. 2, pp. 13-52, 2001.

[50] K. L. Kroeker, "Graphics and security: exploring visual biometrics," *Computer Graphics and Applications, IEEE,* vol. 22, pp. 16-21, 2002.

[51] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," *Information Forensics and Security, IEEE Transactions on,* vol. 1, pp. 125-143, 2006.

[52] R. H. Bond, A. Kramer, and G. Gozzini, "Molded fingerprint sensor structure with indicia regions," ed: Google Patents, 2012.

[53] T. Matsumoto, H. Matsumoto, K. Yamada, and S. Hoshino, "Impact of artificial gummy fingers on fingerprint systems," in *Electronic Imaging 2002*, 2002, pp. 275-289.

[54] M. Dabbah, W. Woo, and S. Dlay, "Secure authentication for face recognition," in *Computational Intelligence in Image and Signal Processing, 2007. CIISP 2007. IEEE Symposium on*, 2007, pp. 121-126.

[55] Y. Adini, Y. Moses, and S. Ullman, "Face recognition: The problem of compensating for changes in illumination direction," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 19, pp. 721-732, 1997.

[56] A. M. Martínez, "Recognizing imprecisely localized, partially occluded, and expression variant faces from a single sample per class," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 24, pp. 748-763, 2002.

[57] P. J. Grother, G. W. Quinn, and P. J. Phillips, "Report on the evaluation of 2D still-image face recognition algorithms," *NIST interagency report,* vol. 7709, p. 106, 2010.

[58] A. Lanitis, C. J. Taylor, and T. F. Cootes, "Toward automatic simulation of aging effects on face images," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 24, pp. 442-455, 2002.

[59] A. Bertillon, *Identification anthropométrique: instructions signalétiques*: Impr. administrative, 1893.

[60] T. Yuizono, Y. Wang, K. Satoh, and S. Nakayama, "Study on individual recognition for ear images by using genetic local search," in *wcci*, 2002, pp. 237-242.

[61] M. Choraś, "Ear biometrics based on geometrical feature extraction," *Electronic letters on computer vision and image analysis,* vol. 5, pp. 84-95, 2005.

[62] H. Chen and B. Bhanu, "Contour matching for 3D ear recognition," in *Application of Computer Vision, 2005. WACV/MOTIONS'05 Volume 1. Seventh IEEE Workshops on*, 2005, pp. 123-128.

[63] T. Hornyak, "Yahoo wants you to use your ears and knuckles to unlock your phone," 2015.

[64] A. Kumar, D. C. Wong, H. C. Shen, and A. K. Jain, "Personal verification using palmprint and hand geometry biometric," in *Audio-and Video-Based Biometric Person Authentication*, 2003, pp. 668-678.

[65] A. Ross and A. Jain, "A prototype hand geometry-based verification system," in *Proceedings of 2nd Conference on Audio and Video Based Biometric Person Authentication*, 1999, pp. 166-171.

[66] R. Sanchez-Reillo, C. Sanchez-Avila, and A. Gonzalez-Marcos, "Biometric identification through hand geometry measurements," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 22, pp. 1168-1171, 2000.

[67] A. Eriksson and P. Wretling, "HOW FLEXIBLE IS THE HUMAN VOICE?–A CASE STUDY OF MIMICRY," *Target,* vol. 30, p. 29.90, 1997.

[68] G. R. Doddington, M. A. Przybocki, A. F. Martin, and D. A. Reynolds, "The NIST speaker recognition evaluation–overview, methodology, systems, results, perspective," *Speech Communication,* vol. 31, pp. 225-254, 2000.

[69] B. Gold, N. Morgan, and D. Ellis, *Speech and audio signal processing: processing and perception of speech and music*: John Wiley & Sons, 2011.

[70] L. Boves and E. den Os, "Speaker recognition in telecom applications," in *Interactive Voice Technology for Telecommunications Applications, 1998. IVTTA'98. Proceedings. 1998 IEEE 4th Workshop*, 1998, pp. 203-208.

[71] Y. W. Lau, M. Wagner, and D. Tran, "Vulnerability of speaker verification to voice mimicking," in *Intelligent Multimedia, Video and Speech Processing, 2004. Proceedings of 2004 International Symposium on*, 2004, pp. 145-148.

[72] M. P. Rani and G. Arumugam, "An efficient gait recognition system for human identification using modified ICA," *International journal of computer science and information technology,* vol. 2, 2010.

[73] M. O. Derawi, C. Nickel, P. Bours, and C. Busch, "Unobtrusive user-authentication on mobile phones using biometric gait recognition," in *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010 Sixth International Conference on*, 2010, pp. 306-311.

[74] J. E. Boyd, "Synchronization of oscillations for machine perception of gaits," *Computer Vision and Image Understanding,* vol. 96, pp. 35-59, 2004.

[75] S. Sarkar, P. J. Phillips, Z. Liu, I. R. Vega, P. Grother, and K. W. Bowyer, "The humanid gait challenge problem: Data sets, performance, and analysis," *Pattern Analysis and Machine Intelligence, IEEE Transactions on,* vol. 27, pp. 162-177, 2005.

[76] M. S. Obaidat, "A verification methodology for computer systems users," in *Proceedings of the 1995 ACM symposium on Applied computing*, 1995, pp. 258-262.

[77] C. Senk and F. Dotzler, "Biometric Authentication as a service for enterprise identity management deployment: a data protection perspective," in *Availability, Reliability and Security (ARES), 2011 Sixth International Conference on*, 2011, pp. 43-50.

[78] Y. Deng and Y. Zhong, "Keystroke Dynamics Advances for Mobile Devices Using Deep Neural Network."

[79] M. Trojahn, F. Arndt, and F. Ortmeier, "Authentication with keystroke dynamics on touchscreen keypads-effect of different N-Graph combinations," in *3rd International Conference on Mobile Services, Resources, and Users (MOBILITY)*, 2013, pp. 114-119.

[80] V. S. Nalwa, "Automatic on-line signature verification," *Proceedings of the IEEE,* vol. 85, pp. 215-239, 1997.

[81] F. Sufi, I. Khalil, and J. Hu, "ECG-based authentication," in *Handbook of Information and Communication Security*, ed: Springer, 2010, pp. 309-331.

[82] M. G. Khan, *Rapid ECG interpretation*: Human Press, 2008.

[83] S. Z. Fatemian, F. Agrafioti, and D. Hatzinakos, "Heartid: Cardiac biometric recognition," in *Biometrics: Theory Applications and Systems (BTAS), 2010 Fourth IEEE International Conference on*, 2010, pp. 1-5.

[84] A. J. Mansfield and J. L. Wayman, *Best practices in testing and reporting performance of biometric devices*: Centre for Mathematics and Scientific Computing, National Physical Laboratory Teddington, Middlesex, UK, 2002.

[85] A. K. Jain, S. Pankanti, S. Prabhakar, L. Hong, and A. Ross, "Biometrics: a grand challenge," in *Pattern Recognition, 2004. ICPR 2004. Proceedings of the 17th International Conference on*, 2004, pp. 935-942.

[86] P. J. Phillips, A. Martin, C. L. Wilson, and M. Przybocki, "An introduction evaluating biometric systems," *Computer,* vol. 33, pp. 56-63, 2000.

[87] A. Jain, D. Maltoni, D. Maio, and J. Wayman, "Biometric Systems Technology, Design and Performance Evaluation," ed: London: Spring Verlag, 2005.

[88] H. Kokumai, "Password-dependent password-killer," ed, 2015.

[89] M. E. Fathy, V. M. Patel, and R. Chellappa, "Face-based active authentication on mobile devices," in *Acoustics, Speech and Signal Processing (ICASSP), 2015 IEEE International Conference on*, 2015, pp. 1687-1691.

[90] C. Nickel, T. Wirtl, and C. Busch, "Authentication of smartphone users based on the way they walk using k-NN algorithm," in *Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2012 Eighth International Conference on*, 2012, pp. 16-20.

[91] N. Belgacem, R. Fournier, A. Nait-Ali, and F. Bereksi-Reguig, "A novel biometric authentication approach using ECG and EMG signals," *Journal of medical engineering & technology,* pp. 1-13, 2015.

[92] E. Hayashi and J. Hong, "A diary study of password usage in daily life," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, 2011, pp. 2627-2630.

[93] N. Micallef, M. Just, L. Baillie, M. Halvey, and H. G. Kayacik, "Why aren't users using protection? Investigating the usability of smartphone locking," in *17th International Conference on Human-Computer Interaction with Mobile Devices and Services*, ed New York, 2015, pp. 284-294.

[94] B. Joe. (2015). *Making Windows 10 More Personal and More Secure with Windows Hello*. Available: http://blogs.windows.com/bloggingwindows/2015/03/17/making-windows-10-more-personal-and-more-secure-with-windows-hello/

About authors

Florentin Thullier is currently an M.Sc. candidate in computer science at the University of Quebec at Chicoutimi (UQAC). He received a first B.Sc. in computer science from the University of La Rochelle (2013) and a second B.Sc. in computer science from the University of Quebec at Chicoutimi in 2014. He obtained a scholarship from Bell Canada to pursue his research project that is in the field of Human-computer interaction and speaker authentication with mobile devices.

Bruno Bouchard is an associate professor and the research Chair in Ambient Intelligence and Assistive Technologies at the University of Quebec at Chicoutimi (UQAC). He received a Ph.D. in computer science from the University of Sherbrooke (Canada) and he completed a postdoctoral fellowship at the University of Toronto (Canada). He is the cofounder and the director of the LIARA lab, which develops smart home technologies dedicated to people suffering from cognitive impairments. The lab conducts real size experiments in a smart home prototype infrastructure financed by the Canada Foundation for Innovation (CFI Leaders Opportunity Fund). Dr. Bouchard has received the precious support of multiples sponsors, such as: NSERC, FQRNT, CFI, CIHR, Bell Canada, UQAC and multiples companies. His main research interests are ambient intelligence, smart environments, sensors, data mining and activity recognition.

Bob-Antoine Jerry Menelas is an assistant professor of Computer Science, at University of Quebec at Chicoutimi, Canada. He holds a M.Sc. (2006) from University of Angers, France and a Ph.D. (2010) from University of Paris-Sud XI, France in computer science. Before joining University of Quebec at Chicoutimi (Canada) in 2011, Dr. Menelas was a postdoctoral fellow at University of Calgary, Canada. His research interest is centered on Human computer interaction. It includes include interactions with mobile devices, Virtual Reality, Haptics, visualization and serious games.