UNIVERSITY OF THE AEGEAN

SCHOOL OF ENGINEERING
DEPARTMENT OF INFORMATION AND COMMUNICATION
SYSTEMS ENGINEERING

POST GRADUATE PROGRAM
TECHNOLOGIES AND MANAGEMENT
OF INFORMATION & COMMUNICATION SYSTEMS

Authentication methods review:
How to enhance identity trust in authentication

Eleni Patmanidou
Ioannis Tsilikas

Supervisor: Dr. Maria Karyda
Professors' committee: M. Karyda, S. Kokolakis, G. Kambourakis

Samos, February 2018

Table of contents

Abstract

Context

A great variety of methods which perform authentication have been introduced in information systems over the years, spanning from using simple text passwords to applying complex biometric authentication techniques. All those methods try to corroborate a digital identity that requests access to or services from an Information System. The growing need to shield Information Technology systems and services from malicious use has encouraged research in the field and manifested an interest in knowing the existing methods as well as the proposed combinations, referred as multi-factor authentication techniques, in order to improve the identity trust.

Objective

This work aims to present authentication techniques most commonly proposed in literature and compare them in terms of their fundamental attributes. Having investigated the characteristics of the basic authentication methods and the identification risks each method imposes, we proceed to investigate how the regulatory initiatives try to control the authentication arena. Finally, we try to correlate the authentication methods, their strength and their weaknesses under the prism of identity trust building, in order to safeguard the authentication and to enhance the identity trust during the authentication procedure.

Method

An extensive literature review was performed in order to gather knowledge on authentication methods. Additionally, the research of relevant work by major consulting firms contributed to the inclusiveness of this work. From the sources investigated, a subset of around 40 papers, articles and publications were selected, that contribute to the objective of this work.

Results

A variety of single and multi-factor techniques were found and analyzed. Each authentication method demonstrates strengths and weaknesses and both are decisive in the evaluation of an authentication method. Nevertheless, the criteria upon which the methods are characterized as efficient are multidimensional and include security, user experience, and technology maturity.

Conclusion

It seems that, given the variety of information systems and the evolution of user experience, no single authentication method is a clear winner in the battle of identity trust in authentication. The designer of an information system should weight regulatory obligations, marketing needs, cost and technology maturity in order to make an authentication compromise.

This work shows that significant research has been done on authentication techniques. Nevertheless, so far, there is no definite authentication pattern which can be hailed as optimum, leading from identity corroboration to identity authentication. Therefore, there still thrives an ever-challenging field for scientists and technology industries for compromises and evolution.

1

Introduction

1.1 Authentication Landscape

Given the complexity and the expansion of the Information Systems and Services, identity corroboration becomes increasingly important and gathers attention from system administrators, Organizations, Regulators, the research community and the hackers alike.

There are many techniques to perform authentication and there are security and privacy aspects that interfere with those techniques as well as usability and cost concerns.

There is an on-going battle to conquer the authentication certainty, with big wins and loud defeats. From one part, users and marketing surveys ask for more and more frictionless authentication experience, and from the other, regulators raise the wall against fraud and identity misuse. In the middle, system administrators and the research community are investing time in building systems and theories that can cater for both “experience vs security” demands.

1.2 Scope

This Thesis investigates the authentication landscape, trying to capture the wide picture of what authentication consist today, focusing on methods which either have created considerable market footprint or have been widely endorsed for combining a significant set of attributes.

The review of the authentication methods is organized in chapters based on the piece of information authentication methods use, whether it is “something the user knows”, “something the user has” or “something the user is”. Apart from weaving the variety of techniques upon the triplet “know-have-is”, this work attempts to elaborate further on other significant dimensions such as regulatory acts, which enhance challenges to the field.

Having surveyed the basic authentication method techniques, we try to investigate how authentication can lead to identity certainty, i.e. how can we enhance identity trust in authentication, by balancing user experience and risk. Although authentication is not a new topic in Information Systems and Services, it seems that is not an exhausted one. Moreover, researchers and practitioners may agree on which criteria are considered crucial in selecting an authentication scheme, but at the end of the day, it is context, which can be the decisive parameter.

In this Thesis, we cover the major current trends in knowledge-based, possession-based and biometrics-based authentication. We do not cover emerging authentication technologies, like Internet-of-Things authentication, Blockchain, User-Managed Access and OpenID connect, that have not yet gained market momentum and are considered out of scope of this assignment.

1.3 Basic concepts

1.3.1 Authentication in relation to identification and authorization

Before elaborating on the authentication concept, its methods and schemes we should distinguish between the three concepts of “Identification”, “authentication” and “authorization”, which are integral parts of a security system and are interrelated but having totally discrete roles.

Identification is the communication of an identity to an IS [1]. The users establish a connection with the IS providing an identity and such as a login or an email. The process is considered completed only after a means to authenticate themselves is provided, for example by using a password. Authentication is the process of determining that the person requesting a resource corresponds to the one who he claims [2]. Finally, authorization is a process of giving individuals an access to the system objects based on their identity privileges given to the user.

Thus, authentication systems answer to both questions:

i. who is the user?
ii. is the user really who he/she represents himself/ herself to be? That is the identity trust in authentication.

On the other hand, authorization provides the answers to the three questions:

i. is the user authorized to access a specific resource?
ii. is the user authorized to perform a specific operation? and

iii. is user authorized to perform a specific operation on a specific resource R? [1]

Each of the above steps requires an enrolment step which should be also carefully handled.

Having said that, we then need to have a link between both the claimant and the authentication service. This link is denoted channel. A channel is a support of communication between the claimant and the monitor. It can either be considered as confidential, authentic, secure or as insecure. A confidential channel is resistant to interception; an authentic channel is resistant to tampering; a secure channel is resistant to both; and an insecure channel is none.

1.3.2 Authentication factors

A basic concept of authentication is the authentication factors, which is a piece of information used to authenticate the user. Authentication factors are classified in literature [3] as:

- Factors based on something the user knows, such as a password or passphrase, including answers to secret questions (challenge-response).
- Factors based on possession, something the user has, such as a token device or smartcard.
- Factor based on inherence, something the user is, such as a biometric. This method involves verification of characteristics inherent to the individual, such as via retina scans, iris scans, fingerprint scans, finger vein scans, facial recognition, voice recognition, hand geometry, and even earlobe geometry.

Authentication techniques belonging to different factors can be combined to enhance security, which is known as multi-factor authentication (MFA). The overall authentication process for MFA requires at least two of the three authentication methods.

The authentication goal is to assert an identity, but the scope of authentication methods is very large and it can vary in many ways. The goal of authentication is to verify the identity of an entity with a given level of trust. If an authentication method cannot be fully trustable, the provided verification cannot be either. Even a good authentication technique will not be secured if the implementation allows backdoors [1].

1.3.3 Multi-factor vs Multi-step authentication

Multi-factor authentication (MFA) and multi-step authentication are two different concepts, but they are often confused. Multi-step authentication is an architectural approach to accessing resources sequentially through multiple authentication verifiers. Each authentication verifier grants access to increasingly privileged areas of the system until access to the desired resources is achieved. Authentication verifiers can be single-factor or multi-factor in nature.

Although multi-step authentication may significantly improve the security of a system, it is easier for an adversary to bypass than multi-factor authentication as there is no single point within the system that uses two or more authentication factors to authenticate a single user to a single authentication verifier. As a result, an attacker can compromise a system gaining ever increasing access while never having to overcome the requirement for multi-factor authentication. [4]

Following this Thesis, when we talk about multi* authentication we will mean MFA and we will leave aside any comparison between MFA and multi-step authentication.

1.4 Regulatory compliance

Organizations need to be aware of local and regional laws that may also define requirements for the use of MFA. For example, there may be additional requirements around consumer authentication used to initiate payments or to conduct high-risk transactions, such as the European Union Directive on Payment Services (PSD2) and the Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook. Additionally, some laws or regulations may have more stringent MFA requirements than those required by PCI DSS. PCI SSC encourages all organizations to be aware of the potential impact that local laws and regulations may have on their MFA implementations. PCI DSS requirements for multi-factor authentication do not supersede local or regional laws, government regulations, or other legal requirements. [5]

1.5 Structure of the Thesis

In the following pages there is a review of authentication methods, classified based on authentication factors. More specifically, chapter two presents knowledge based authentication techniques, chapter three describes possession-based authentication methods and chapter four elaborates on the evolution of biometric authentication. As privacy is a major topic in biometric authentication, chapter four shed a light on privacy risk and mitigation in biometrics. Each of these chapters is enhanced with discussion on the vulnerabilities or threats these techniques face and the ways these risks are confronted.

Furthermore, a chapter with the aspects of the regulatory framework that interfere with the employment of authentication methods is included in this work. Finally, we present the conclusions of our analysis in authentication methods and identity trust, which leads from corroboration to authentication.

2

Knowledge Based Authentication

Knowledge Based Authentication (KBA) is popular because of being relatively inexpensive to implement and typically requires no additional hardware. KBA schemes can theoretically be very secure, but their practical security is often limited by the lack of uniqueness and complexity of the shared secrets that humans can remember [6].

Knowledge Based Authentication techniques vary from simple alphanumeric passwords to graphical password schemes. In the following paragraphs, these two basic categories of KBA methods are presented. Additionally, there is a review of the threats in which they are susceptible to as well as the proposed mitigation actions or techniques to combat the risks. The chapter ends up with the conclusion, which gives the gist of the before-mentioned analysis.

2.1 Alphanumeric passwords

The most common authentication system is a combination of username and password. It relies on the fact that the user has to remember the password and keep it a secret [7]. Users tend to select alphanumeric passwords that are short and easy to recall by using explicit semantic memory. Semantic memory is one of the two types of explicit memory which deliberately and consciously uses Long Term Memory in order a person to retrieve information. Semantic memory represents the storage of factual knowledge, including information about people and objects, without the individual recalling how or where such knowledge was obtained [6].

This kind of passwords can be easily compromised because they can be guessed. However, if a user picks a complex password and hard to guess password, it most commonly be hard to remember. Since users can remember a limited number of alphanumeric passwords, they often write down their passwords or use same password for multiple accounts [7]. On the other hand, human brain has remarkable ability to remember thousands of images with detail

[2]. Based on this notion several alternative password mechanisms have been introduced. Graphical password is one of them, and it is based on pictures or patterns.

2.2 Graphical password schemes

Human psychology supports the assumption that images are easy to remember whereas text is difficult to keep in memory and it is because of this memorability advantage, a significant interest in graphical password has risen [7].

Picture Superiority Effect Theory reveals that pictures can be recognized and recalled easily by human brain, enhancing the ability to remember. Graphical passwords have been used in authentication for mobile phones, ATM machines, E-transactions [2]. Graphical password systems can be classified into three categories:

1. Recognition based authentication
2. Recall based authentication
3. Cued recall based authentication

2.2.1 Recognition based

In a recognition based scheme, a set of images is given and the user needs to identify correct images that the user had already set in order to authenticate (e.g., Use Your Illusion (UYI)). In UYI scheme, the login screen displays 9 images randomly positioned in a 3 × 3 grid and the user needs to recognize and select a right image amongst false ones [7].

Jensen et al. [2] proposed picture recognition in which user had to select a sequence of images from a matrix of 5 x 6 thematic images which formed a password. This password is to be registered and every time the users have to authenticate themselves they are prompted to select the same images in the correct order to provide the graphic password. The drawback of this method appeared to be the narrow password space due to the limited number of pictures. In a similar logic another technique called Passfaces used a grid of 9 images of faces and prompted the user to select 4 out 9. Nevertheless, Davis et al. [8] after a long-term study and implementation of their own version (Faces) raised the concern that Passfaces can be predictable as they are affected by race, gender and attractiveness.

Another method which was developed in order to avoid shoulder surfing attack was by Sobardo and Birget [9], in which the user is asked to select objects during registration and select them again each time during authentication. The basic flaw of this method was that in order to extend the password space 1000 objects were used during registration, which made the selection of the pass-objects difficult since the screen was too crowed by objects.

Dhamiga and Perrig [10] proposed a scheme called “Déjà vu” based on human ability to remember previously seen images. In this method, the user has to select few images from a set of images and perform the same at login time. All abstract images were generated using Andrej Bauer’s Random Art. They showed 90 % success rate using “Déjà vu” while only 70% using text-based password and pins [2]. Akula and Devisetty’s proposed a similar method using less memory, but still larger that text-based passwords.

Hong et al. [11] proposed a scheme, which is designed as a challenge response system to be resistant to malware. During registration, a login screen is presented to the user, which is divided into grids with an icon in each of the grids. Every icon has a number of variations and user has to select pass-icons from the login screen and a string corresponding to each variation of pass -icons. At login time the system user is challenged with recognizing the pass -icons from a randomly generated login screen presenting a grid of icons with variation icons. Once the icons have been correctly identified, user has to enter string corresponding to the variation of particular pass-icon. Registration and login process in this scheme is time consuming [2].

2.2.2 Recall based

For mobile devices, a graphical password scheme named pattern lock has gained popularity amongst the Android OS users (Aviv et al. 2010). The mobile screen shows a 3 × 3 grid of contact points, which the user is prompted to connect and create the pattern he/she initially registered. Android pattern lock provides 389112 distinct patterns for 9-point combination, while the PIN method, in which the users select in the virtual keypad, a four-digit personal identification number (PIN) to unlock their device for screen lock provides 10000 different combinations [7].

Jemryn et al. [12] proposed another technique called Draw a secret (DAS) in which the user was asked to draw something during registration using a stylus or finger and repeat it in each login [2]. The idea behind this technique seems to be similar to Android pattern lock application, in a more abstract way. Microsoft has created Let-me-In, a graphical password interface similar to DAS.

In addition, SFR company developed a visKey for mobile devices user has to select an image from the images stored in the device and tap on the spots in sequence [2]. This sequence is registered to login user has repeat the same procedure. There is a certain tolerance area around the spots pre-defined by users, as it is difficult to touch at same exact spots, but on the other hand, a certain precision should be appointed to ensure that it will not be easy to crack and the number of spots must quite as much to prevent against brute force attacks.

A method imbued with the same principle is Pass-Point, introduced by Wiedenbeck et al. [2] in which the user has to select a background and click on points in the image during registration. In every logon, the user is asked to repeat the clicks in the initial sequence.

In GrIDsure users choose a pattern on a grid during registration and at login, users are shown a grid, each square containing a randomly chosen digit (0 to 9). They show acknowledgement of their pattern by typing the digits on their pattern's squares. The patterns are resistant to an observation attack because each digit appears twice. [6]

2.2.3 Cued recall based

Cued recall uses a different technique. Chiasson et al [13] proposed the usability of a method they called Cued Click Points (CCP). Instead of making multiple clicks on single image like Pass-point, user has to make single click on multiple images. The images come in sequence one after the other. An image appearing next in sequence is determined by the click made in the previous image. In a comparative study, they performed between CCP and Pass-Point the users appeared more favorable of CCP, since seeing each image triggered their memory of where the corresponding point was located. Another advantage is that making click on a single image results in larger password space, leading to larger resistance to shoulder surfing attack.

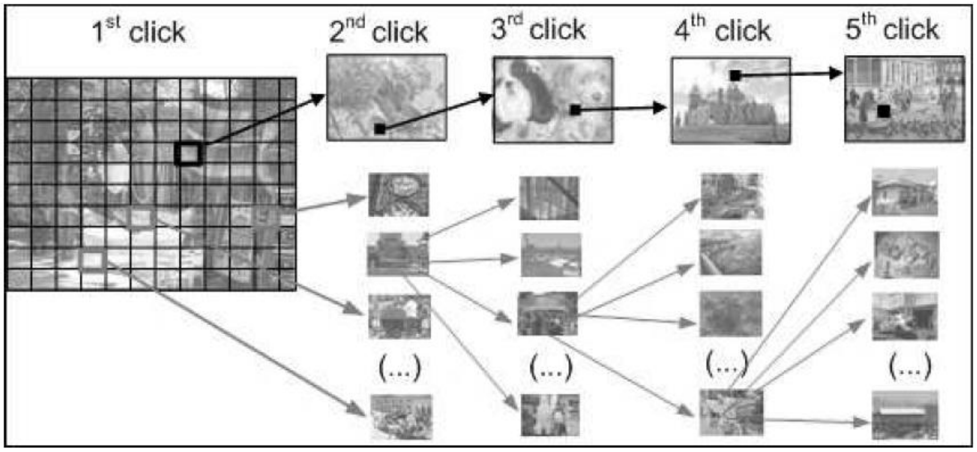


Figure 1 CCP passwords can be regarded as a choice-dependent path of images [13]

Recently, Nayak et al. proposed PCCP (Persuasive cued click points), which uses extra features in order users to create stronger passwords and enhance security [14].

2.3 Threats in KBA

2.3.1 Shoulder surfing attack

Passwords can be stolen by making observation on the user's screen or keyboard as they are logging in. Capturing images during CCP can be easier than capturing the pointer of the mouse during Pass-point and by just knowing this information attackers could brute force the system until the right image appeared. In addition, Draw-A-Secret can be weak in case the screen is captured during login [2]. The pattern password for mobile devices is vulnerable to security attacks such as smudge attacks and shoulder surfing attacks.

2.3.2 Hotspots

Hotspots are specific areas in the image that have higher chances to be selected as part of users' passwords. If these hotspots were predicted through hotspot analysis, attackers could build a dictionary of passwords containing combinations of these hotspots [6]. Pass-points is more vulnerable to this type of attacks, in case the username is compromised [8], compared to CCP in which attackers would have to analyze multiple images, involving those not belonging in the subset of images the user has picked.

2.3.3 Brute force attack

Text based passwords have password space of 94^N. Graphical passwords have an advantage over text based passwords in this kind of attacks. The same goes with Recall based Password, which is more secure than recognition based methods. Of the above-mentioned methods, Draw-A-Secret is the most resistant to this attack. [2]

2.3.4 Spyware attack

The traditional text-based passwords are susceptible to malware attacks in contrast to graphical passwords

2.4 Mitigating threats in KBA

2.4.1 Password strength

A method to avoid the brute force and dictionary attacks is by increasing password strength. It is generally accepted that the length of the password determines the security it provides, however, it is not exactly true: the strength of the password is rather related to its entropy. For example, a user chose, say, a password of seven characters is said to provide between sixteen and twenty eight bits of entropy [1]. The users also need to create strong pattern passwords or PINs as well as make efforts to protect them.

2.4.2 Challenge-response schemes

Some KBA systems resist both observation and social engineering attacks, where users are deceived into revealing their authentication secret. In the so-called challenge-response schemes, users prove their knowledge of the secret without revealing the entire secret itself, thereby hiding it from observers.

2.4.2.1 *CAPTCHA*

Over the last few years[1] an Internet security tool called CAPTCHA (short for Completely Automated Public Turing Test To Tell Computers and Humans Apart) has been widely adopted in order to protect users against bots.

Challenge-response protocols are also used to assert things other than knowledge of a secret value. CAPTCHA distinguishes human users from computers by presenting a challenge, i.e., a puzzle [15]. The effectiveness of this application stems from the inability of computers to process distorted images and text as well as humans [16]. The challenge sent to the viewer is a distorted image of some text, and the viewer responds by typing in that text. The distortion is designed to make automated optical character recognition (OCR) difficult and preventing a computer program from passing as a human.

Further research in Carnegie Mellon University has led to an improved scheme called reCaptcha project. reCAPTCHA uses an advanced risk analysis engine and adaptive CAPTCHAs to prevent bots from malicious actions, when in parallel valid users pass through with ease. reCAPTCHA doesn’t depend solely on text distortions to separate humans from machines. Rather it uses advanced risk analysis techniques, and evaluates a broad range of cues that distinguish humans from bots [17]. Another feature of reCAPTCHA is that it is used for book digitization by turning words that cannot be read by computers into CAPTCHAs for people to solve. Word by word, a book is digitized and preserved online for people to find and read.[2] There is also an audio alternative of CAPTCHA for the visually impaired users. Although the apparent positive attributes of CAPTCHA there is a lot of pending discussion on the internet about the considerable time lost during Captcha usage[3].

2.4.3 Obscured feedback

Obscured feedback offers the simplest defense to shoulder-surfing.

[1] In 2000, Carnegie Mellon University computer science graduate student Luis von Ahn, along with his advisor Manuel Blum, created a new cyber security tool called CAPTCHA.

[2] YouTube video in which Luis von Ahn explains reCaptcha: https://www.youtube.com/watch?time_continue=13&v=euRAfUGX8wY

[3] https://www.youtube.com/watch?v=MHgtzTzT-oM

Some applications are:

- Text password systems implement obscured feedback by hiding characters in password fields with dots.
- Apple iPhones mask password characters after one second or after another character is typed.
- Obscured input is implemented, where the method of credential input is hidden (e.g. covered keypads or various PIN alternatives for touch displays).

2.5 Conclusion

Graphical passwords demonstrate a set of attributes resistant to security threats presented above. On top of that, they are very resistant to phishing and social engineering, since they cannot be revealed in the way that text-based can. Nevertheless, analysis has shown that authentication process is slower in graphical password [2]. Leverage between security and usability of graphical passwords is the main challenge for researchers.

Idrus et al. [1] classify text and graphical password methods as "Static authentication by a shared secret". In their review, they denote the major concern about passwords, which is the lack of security transmission over a channel. The solution to this problem would be providing evidence of identification without sending the password over an ambiguous channel. Having said that, in the next section we present One-time passwords (OTPs).

3

Authentication based on possession

Authentication based on possession is an authentication based on what the user has. Possession-based authentication is also referred to as token-based authentication. In most cases, the piece of information that the user possesses whether it is a smart card or a one-time password, this factor is not the only requirement to solve the authentication "equation". In other words, it is usually used as the second factor in a multi-factor authentication scheme.

In this chapter, possession-based factors are classified in the "One-time password tokens" the "Software certificates" and the "Cryptographic tokens", while an additional section is dedicated to introduce the U2F authentication method. Alongside with their description we attempt to capture the intrinsic vulnerabilities and show the context in which they can be operated efficiently.

3.1 One-time password (OTP) tokens

OTPs came as the evolution of ID/password method, in an attempt to avoid replay attacks static passwords suffer from, since the mechanism is based on the generation of a different password for each use. OTP tokens are most commonly devices with a display screen showing the alphanumeric characters. They are popular in multi factor authentication, playing the role of the second factor [4].

There are several categories of OTP:

- Physical one-time PIN tokens
- Out of band tokens
- Application-generated codes
- Shared list of passwords

3.1.1 Physical one-time PIN tokens

This method uses a physical token that displays a onetime PIN on its screen, which is user for authentication. The time on both the physical token and the authentication service are synchronized. When the user attempts to authenticate with the passphrase displayed in OTP the authentication service knows what to expect and authorizes access to resources [4].

OTP devices can be divided in Single-factor OTP devices, which reveal the code to the user without other requirements and Multi-factor OTP devices, which in order to generate one-time passwords may require activation through a second factor of authentication. This can be achieved through some kind of integral entry pad, an integral biometric (e.g., fingerprint) reader or a direct computer interface (e.g., USB port), enhancing security aspects [18]. Evolving on this idea U2F was developed, which will be elaborated on a later stage in this paper.

The physical OTPs are also classified [1] as:

- **Counter synchronised OTP**, or "Mathematical hash chain OTP" or "Mathematical key chain OTP". In most cases it has a button, which every time it is pressed generates a password. Most are based on the Leslie Lamport-scheme [19].
- **Time Synchronised OTP.** The token has an internal clock and new passwords are generated from the value of the current timestamp. The value of the generated password usually changes every one or two minutes.

3.1.2 Out of Band Tokens

The user has to be authenticated through an unsecured channel, but the authentication service provides the user with a random OTP through another channel, which is considered secured, and where the claimant is already authenticated. Then the claimant transmits the OTP through the unsecure channel to prove true identity [1].

The OTP can be provided to the claimant via SMS messages, emails or through voice call to a device. The corresponding phone number or email address are given by the user during enrollment. In the logon process, the user requests from the authentication service a password which upon receiving they provide back to complete authentication and is granted or denied access.

An advantage of this multi-factor authentication method is minimization of the cost for the system owner; however, there are also a number of disadvantages [4], such as:

1. Absence of reception or malfunction of cellular networks may prevent OTPs from reaching their destination (SMS, email) delaying the whole process.
2. SMS messages are delivered via VoIP or internet messaging platforms is not considered secure enough.
3. Devices or cellular networks can be compromised and OTP can be intercepted by attackers.

A common attack known as "SIM swap" allows attackers to set up the user's phone number on their own phone device and get SMS codes. They perform the same process people follow when they purchase a new device and move their phone number to it. Another form of interception is by taking advantage of flaws in the connection system used for roaming (SS7) and route SMS messages elsewhere [20]. That's why the National Institute of Standards and Technology is no longer recommending the use of SMS messages for two-factor authentication [21].

3.1.3 Application-generated codes

In a similar fashion like OTP sent over a secure channel, they can be generated by an app on the user's device. Google Authenticator[4], which Google offers for Android and iPhone and Authy[5] by Twilio use an open standard and it's possible to add many types of accounts.

New codes will be generated by the app every 30 seconds and during logon users need to enter the current code displayed in the app as well as their password when they logon. The advantage here is that it does not require a cellular signal at all and is more difficult to be intercepted, since the code is generated in the device and is not transmitted over a network.

Also, some services like Blizzard's Battle.net Authenticator[6] have their own dedicated code-generating apps, which the users can configure to determine whether its use will be in every login or not.

[4] https://play.google.com/store/apps/details?id=com.google.android.apps.authenticator2&hl=el

[5] https://authy.com/

[6] https://eu.battle.net/support/en/article/24520

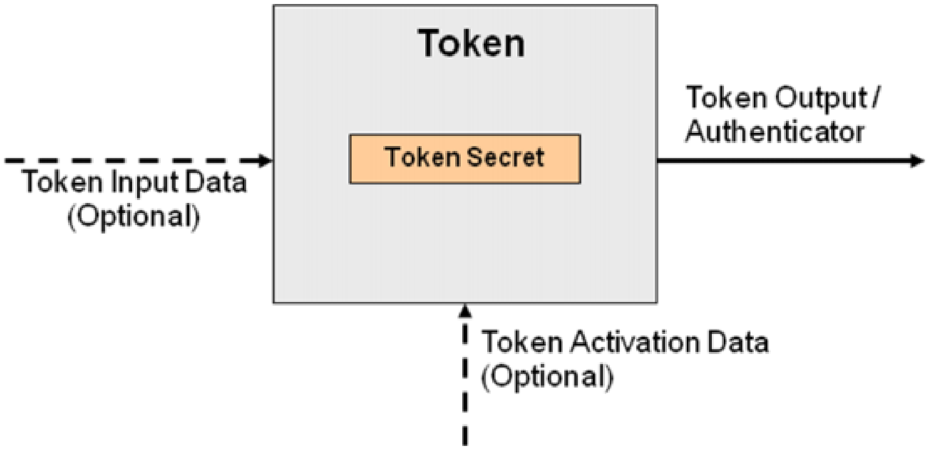

Token
Token Secret
Token Output / Authenticator
Token Input Data (Optional)
Token Activation Data (Optional)

Figure 2 Token Model [18]

3.1.4 Shared list of passwords

In this method, the claimant and the authentication service share copies of the same list of passwords. The list can be ordered, so the only allowed passwords are those following the last one used, and if it is not, each password from the list can be used only once [4]. The list is usually provided by the authentication service after the claimant shows evidence of ID using another channel, proving proof of identity, for example by showing ID in person in the administration office of the authentication service[7].

3.2 Software certificates

In this multi-factor authentication method, a software certificate stored on a device is used as a second factor. During authentication process, the system first accesses the user's software certificate, which is stored in a file, in the registry or in the Trusted Platform Module (TPM) of their device. Then, the software installed on the device assists the user to verify their identity by signing an authentication request with the user's private key. Upon receiving the authentication request

[7] i.e. Bank's branch

the authentication service verifies that it is signed by the valid and correct private key and grants permission to resources [4].

The weakness of this method relies on the fact that if the device is compromised the attackers can initiate authentication requests in the owner's behalf. Also, if the keys and certificates are stolen from the device, the attackers can initiate from their own infrastructure similar requests. Thus, organizations are recommended to use software certificates for low risk transactions or systems. Hardware cryptographic modules are preferred over software due to their immutability, smaller attack surfaces, and more reliable behavior. [5]

3.3 Cryptographic Tokens

Cryptographic tokens may be embedded into a device or stored on separate, removable media. A private key resides in a hardware cryptographic module (or physical security token) that is physically separate from the mobile computing device. Access to either the mobile computing device or cryptogram stored on the token does not grant access to the other, thus maintaining the independence of authentication factors. The following form factors support a secure element (SE), a tamper-resistant cryptographic component that provides security and confidentiality in mobile devices.

- **SD Card with Cryptographic Module.** A non-volatile memory card format for portable devices.
- **Removable UICC with Cryptographic Module**. The Universal Integrated Circuit Card (UICC) configuration is based on the GlobalPlatform Card Specification v2.2.1 [GP-SPEC].
- **USB Token with Cryptographic Module.** A device that plugs into the USB port and apart from storage properties may also include cryptographic processing capabilities—e.g., cryptographic mechanisms to verify the identity of users. USB token implementations that contain an integrated secure element (an integrated circuit card or ICC) are suitable for use in the authentication process [5].

3.4 Fast IDentity Online (FIDO) protocols

The Fast IDentity Online (FIDO) Alliance[8], an open industry association comprising over 250 member organizations, which includes Google, Microsoft,

[8] https://fidoalliance.org/about/overview/

PayPal, American Express, MasterCard, VISA, Intel, ARM, Samsung, Qualcomm, Bank of America, and many other massive companies was formed in July 2012 to address the lack of interoperability among strong authentication methods, as well as the problems users face with creating and remembering multiple usernames and passwords. The FIDO specifications were created to offer a more secure and user-friendly alternative to password-based logins on the web.

The FIDO specification comprises two protocols: Universal Authentication Framework (UAF) and Universal Second Factor (U2F). UAF protocol enables relying parties to offer passwordless authentication by using a local authentication method to register a device that has established trust with the user. U2F protocol allows relying parties (RPs) to augment a password with a second factor using a preregistered hardware token or a mobile device. FIDO 2.0 builds on the UAF and U2F protocols, addresses both use cases, and forms the basis for the W3C Web Authentication API standard.

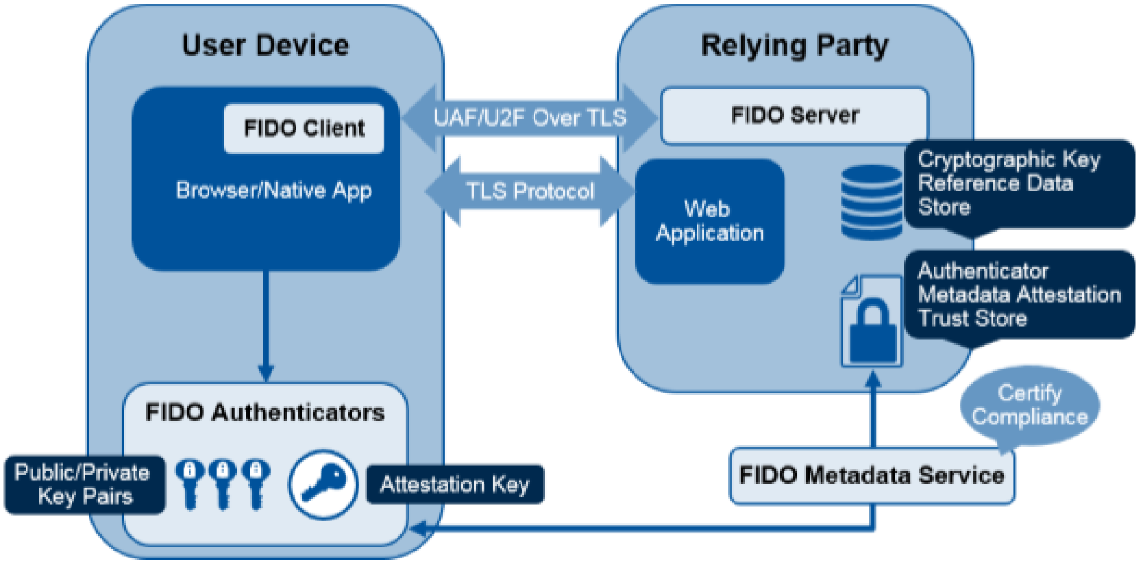


Figure 3 FIDO core components and interactions [22]

3.4.1 Universal 2 factor (U2F) authenticator

This multi-factor authentication method uses a physical token or card (called U2F security key or U2F authenticator) as a second factor. Software on the user's device prompts the user to either press a button on the U2F security key, tap it using Near Field Communication (NFC) or via Bluetooth. In doing so, the U2F security key uses public key cryptography to verify the user's identity by signing a challenge/response request from a service, which had been passed through via a web browser or mobile app. The service then verifies that the response is signed by the valid and correct private key for that service, and decides whether to grant access to resources. [4] The FIDO U2F Security Key to provides two-factor authentication across a variety of services which support the FIDO U2F protocol, including Facebook, Google's Gmail, Google Cloud and G Suite, GitHub, Dropbox, and Dashlane.

As being a part of the browser itself, it gives advantages over typical two-factor authentication. First, the browser uses encryption to ensure the authenticity of the website, so users will not be tricked into entering their two-factor codes into fake phishing websites. Second, the browser sends the code directly to the website, preventing Man-in-the middle attacks. In addition, passwords can be simplified with U2F and a website instead of asking for a long password, typically asked in two-factor authentication, it may request a four-digit PIN and the press of a button on a USB device to log in. [20]

The FIDO alliance has also implemented UAF[9], which requires no password. Instead, it might use biometrics like the fingerprint sensor on a modern smartphone to authenticate the user with various services.

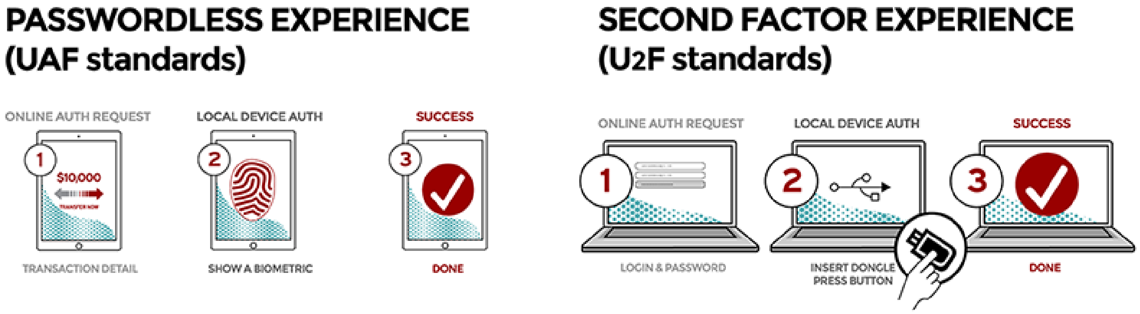


Figure 4: UAF and U2F schematic description [23]

U2F methods can be secure and efficient, provided some measures are taken, such as:

- Ensure users do not store U2F security keys with their devices.
- Ensure users receive a visual notification each time an authentication request is generated that requires them to authenticate using their U2F security key.
- Use U2F security keys that have been certified to the latest U2F specification version.

[9] Universal Authentication Framework

- Instruct users to report any lost or missing U2F security keys as soon as practical. [4]

3.5 Conclusion

From the above review, it is inferred that the most secure way to use a token is combined with the use of another factor (multi-factor authentication). What is more, the context in which the authentication is performed defines the efficiency of the method.

Whether it is a hardware token or a one-time password generator application, a significant parameter, which cannot be overlooked when efficiency is evaluated, is the analysis of the conditions in which the authentication takes place.

Assistance in meeting the challenges of possession based authentication comes with following authentication protocols such as U2F. FIDO with this protocol addresses many of the concerns [24]:

- Standardizes online crypto and local authenticator interfaces to improve security.
- Promotes better customer experience with authentication.
- Reduces hacking risks.
- Builds on ubiquitous hardware for out-of-band authentication on mobile devices.

4

Biometrics authentication

Apart from knowledge or possession based authentication, inherence based authentication has a big footprint in the field. Based on statistics from Mobile & Wearable Biometric Authentication Market Analysis & Forecasts 2017-2022, conducted by Goode Intelligence, the appetite for biometrics has expanded rapidly:

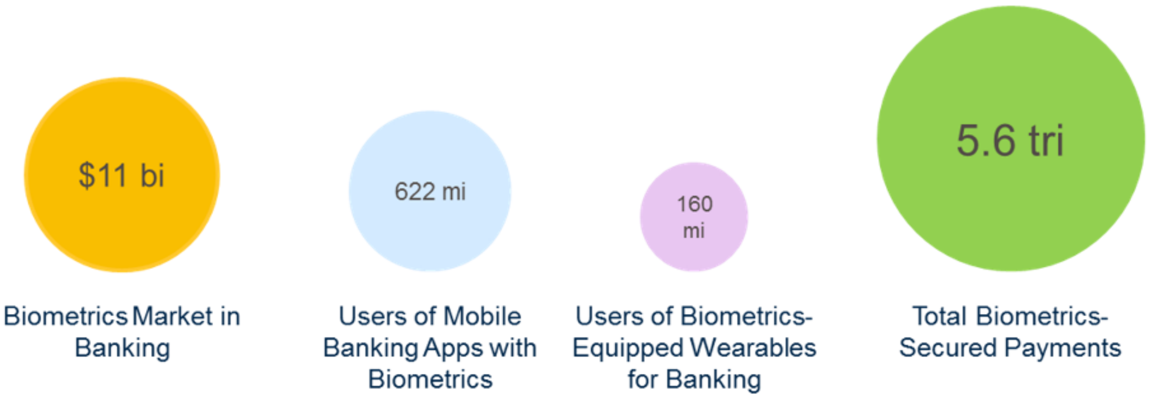


Figure 5 Biometrics in Financial Services by 2020 [25]

In this chapter, initially we try to elaborate the basic differentiating factors of the biometrics credentials versus the KBAs methods

Further, we describe the biometric traits and modes and present the characteristics and there major technological and market maturity aspects. Given the nature of this authentication method category, we shed light on the basic usability, risk and mitigation factors an IS designer should consider, in order to select an authentication method like this and to protect the biometrics credentials.

4.1 Biometric methods Vs non-biometric authentication methods

Biometric authentication methods differ technically from non-biometric authentication methods in two important ways:

- Stochastic Variations [26]: “Biometric comparison is probabilistic, whereas other [orthodox] authentication factors are deterministic” [21]. Unlike, say, passwords or one-time passwords, which are fixed or change in a formulaic way from one time to another, the captured biometric sample data (and thus the derived probe data), varies slightly from one time to another. Thus, probe data will never be an exact match to the reference data held for that person, and authentication depends on how close one is to another. The comparison process is, therefore, a source of errors that impact trust and user experience. In order to deal with the probabilistic nature of the biometric authentication, two indices have been introduced to calculate rejection or acceptance:
    - False Acceptance Rate (FAR): The false acceptance rate is the measure of the likelihood that the biometric security system will incorrectly accept an access attempt by an unauthorized user. A system's FAR typically is stated as the ratio of the number of false acceptances divided by the number of identification attempts [27].
    - False Rejection Rate (FRR): The false rejection rate is the measure of the likelihood that the biometric security system will incorrectly reject an access attempt by an authorized user. A system’s FRR typically is stated as the ratio of the number of false rejections divided by the number of identification attempts [28].

    An accepted authentication verdict is a risk-agreed balance between the FAR and the FRR.

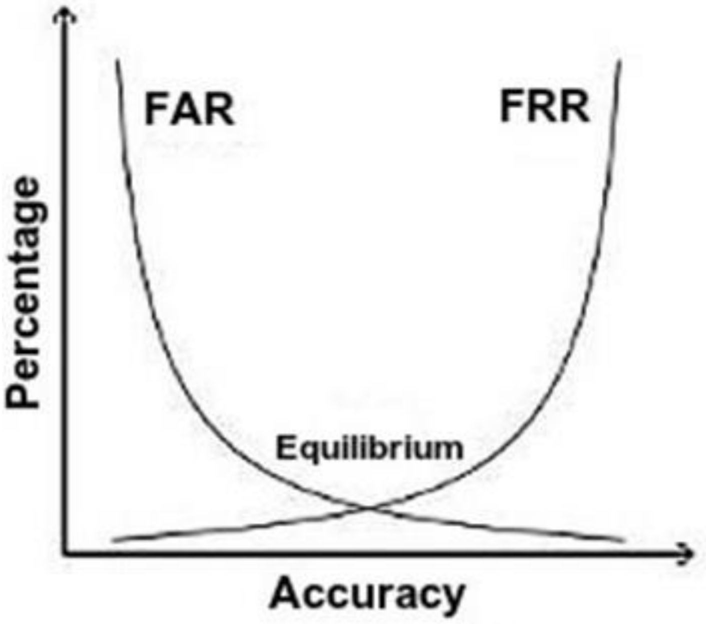


Figure 6 FAR and FRR equilibrium [29]

- No “Shared Secrets” [26]. Unlike, say, passwords and cryptographic keys, biometric traits are not secret and cannot, in principle, be made secret. Thus, biometric authentication cannot and does not depend on the secrecy of biometric traits, but instead relies on the difficulty of impersonating the living person presenting the trait to a capture device (“sensor”). NIST [21] notes that “Biometric characteristics do not constitute secrets. They can be obtained online or by taking a picture of someone with a camera phone (e.g. facial images) with or without their knowledge, lifted from objects someone touches (e.g. latent fingerprints), or captured with high resolution images (e.g. iris patterns). While presentation attack detection (PAD) technologies (e.g. liveness detection) can mitigate the risk of these types of attacks, additional trust in the sensor or biometric processing is required to ensure that PAD is operating in accordance with the needs of the credential service provider and the subscriber”.

This point is not widely known, which leads to some very common misconceptions. For example, a common criticism of biometric authentication is, say, “You can’t reset a fingerprint”. However, this is based on the mistaken notion that the biometric data is just a kind of password or token, and overlooks the importance of live presentation of the fingerprint. In a robust fingerprint method, it should not matter that an attacker can present a facsimile of a person’s fingerprint; anything other than the person’s actual finger (still attached to his or her living body) should not work.

However, this kind of misconception is reinforced by the lack of any liveness testing in biometric enabled consumer devices, and there has been a lot of publicity about successful attacks against Apple Touch ID, Samsung swipe sensors, Android face recognition and so on.

Therefore, a robust biometric authentication method must be able to confirm that the biometric trait is being presented by a living person.

In order to conclude a biometric recognition, the following steps and actions need to be executed [30]:

- Sample acquisition: Collection of biometric data using appropriate sensors.
- Feature extraction: Conversion of biometric data into templates.
- Storage: Storage of templates in appropriate memory, which depends on the application.
- Matching: authentication of user by comparing biometric template of the user with the existing templates stored in the database.
- Decision: Based on the result of the matching, the user will be authorized or denied to access the resources.

4.2 Biometric traits and modes

Biometric authentication uses unique biological or behavioral traits to corroborate users' identities when they access endpoint devices, networks, or mobile, networked, web or cloud applications [26].

Biometric authentication can use:

- A one-to-one comparison mode, where there is an implicit or explicit claim of identity. This is known as (biometric) *verification*. It is the exact parallel to non-biometric authentication methods.
- A one-to-many search mode, when the user simply presents his or her biometric trait and the system determines the user's identity from a range of candidates. This is known as (biometric) *identification*. Authentication (verification) is implicit in this case.
- Identification against a restricted list of candidates, a one-to-few search mode, is known as (biometric) *screening*.

To be useful for authentication (via verification, identification or screening), a biometric trait must be unique, persistent and measurable.

Furthermore, it must be possible to capture a sample (image, recording, etc.) of that trait and to extract identifying data (a feature set) in a way that preserves that uniqueness.

Biometric traits follow the classification below:

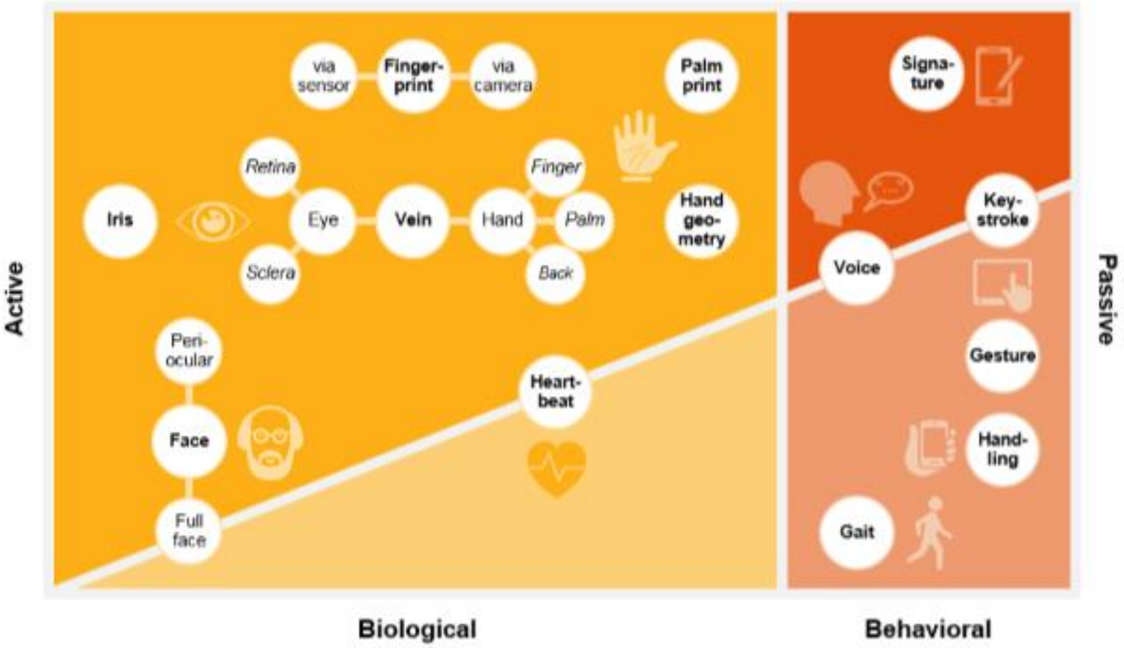


Figure 7 Biometric traits and modes [26]

Biological traits (face, fingerprint, iris, vein, etc.) are unique, measurable physiological attributes. They change very slowly and are unalterable without significant duress or trauma. However, some people find capture to be invasive or find specialized sensors difficult to use.

Behavioral traits (such as gesture, keystroke and voice) are unique measurable actions, and they distinctively incorporate time as a metric. Thus, they are sometimes distinguished as dynamic traits, rather than static biological traits. They are less stable than biological traits, changing over time (thus, biometric reference data needs continual refreshment) and typically requiring multiple profiling events to determine a reliable behavioral baseline. They also change with age, stress, injury and sickness, but extracted features can be relatively invariant.

Methods that incorporate two or more distinct traits (for example, face and voice) are known as *multimodal* methods (in contrast to monomodal or unimodal methods).

Active modes are characterized by discrete enrolment processes and distinct verification steps, which require the user's conscious action and intent. *Passive* modes are characterized by “invisible” enrolment and evaluation that take place continuously during normal user interactions, typically without the user knowing the profiling and analysis is taking place.

Since 2013, when Apple introduced a mobile device with a fingerprint sensor incorporated in the home button, biometric authentication has gained momentum. Many technologies have evolved and struggle for acceptance.

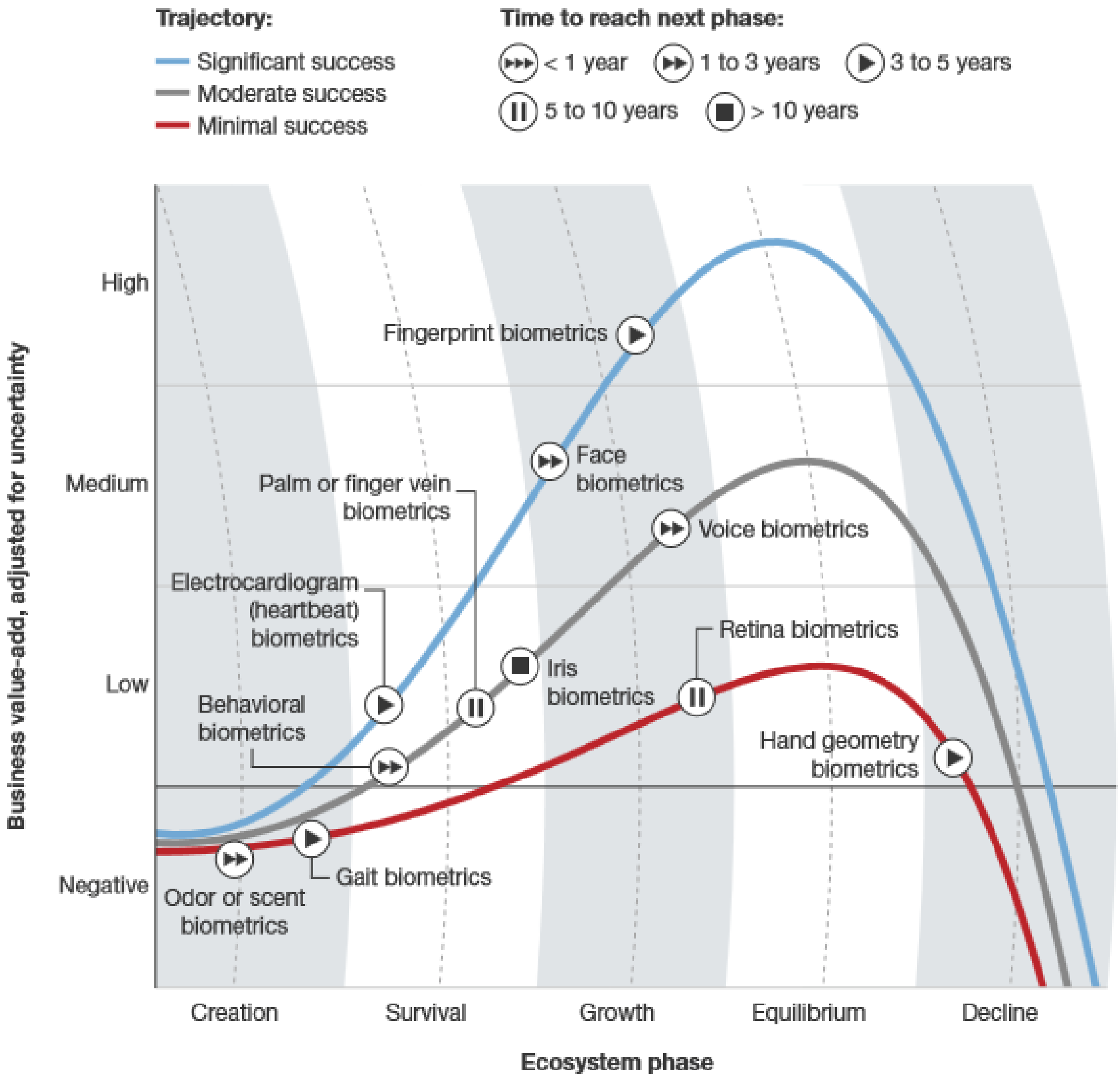


Figure 8 Biometric authentication technologies [31]

4.2.1 Odor or scent biometrics

Odor or scent biometrics (OSB) authenticate users based on the chemical compositions that distinguish their odors. OSB are not ready for adoption. A joint academic-private sector study involving 13 subjects over 28 sessions attributed an over 85% accuracy rate to odor or scent biometrics, but that is the most significant evidence of the biometrics' potential [31]. This biometric trait has rarely made it out of the lab (Mastiff Electronic Systems' Scentinel[10]) [26].

4.2.2 Behavioral biometrics

Behavioral biometrics (BB) enables both initial authentication and continuous authentication of users once they have already logged in to their accounts. BB watches a user's behaviors (e.g. mouse, movement, screen swipes and taps, typing speed), builds a profile of the user's behavior and interaction with the device, then identifies anomalies from that profile (typically when a hacker takes over a legitimate user's account). Behavioral biometrics is also implicit, does not affect the user experience (in fact, you may have to explain to your users that it is their behavior that authenticates them), and requires minimal extra instrumentation. Forrester [31] sees BB as one of the fastest growing biometric modalities. The relative immaturity of the non-keystroke analysis components of the technology currently limits the business value of BB.

The most frequently cited vendors in the area are BehavioSec[11], BioCatch[12], KeyTrac[13], and NuData Security[14].

Under the behavioral biometrics, the following traits are available:

- Gait biometrics (GB) capture identifying elements of a user's gait (stride length, joint action, foot pressure, etc.) via camera, accelerometers and gyros. This is "passive historic", corroborating the identity of the person carrying the device in an arbitrary period prior to the moment of access.

  Gait biometrics provide no advantage over other forms of biometrics. A user wearing or using a mobile-phone integrated sensor for gait biometrics could also be wearing an ECG sensor, with technology that is more mature. Firms or governments hoping to identify civilians based on gaits would be better served by using face biometrics technology, which is more

[10] http://www.mastiff.co.uk/index.html
[11] https://www.behaviosec.com/
[12] https://www.biocatch.com/
[13] https://www.keytrac.net/
[14] https://nudatasecurity.com/

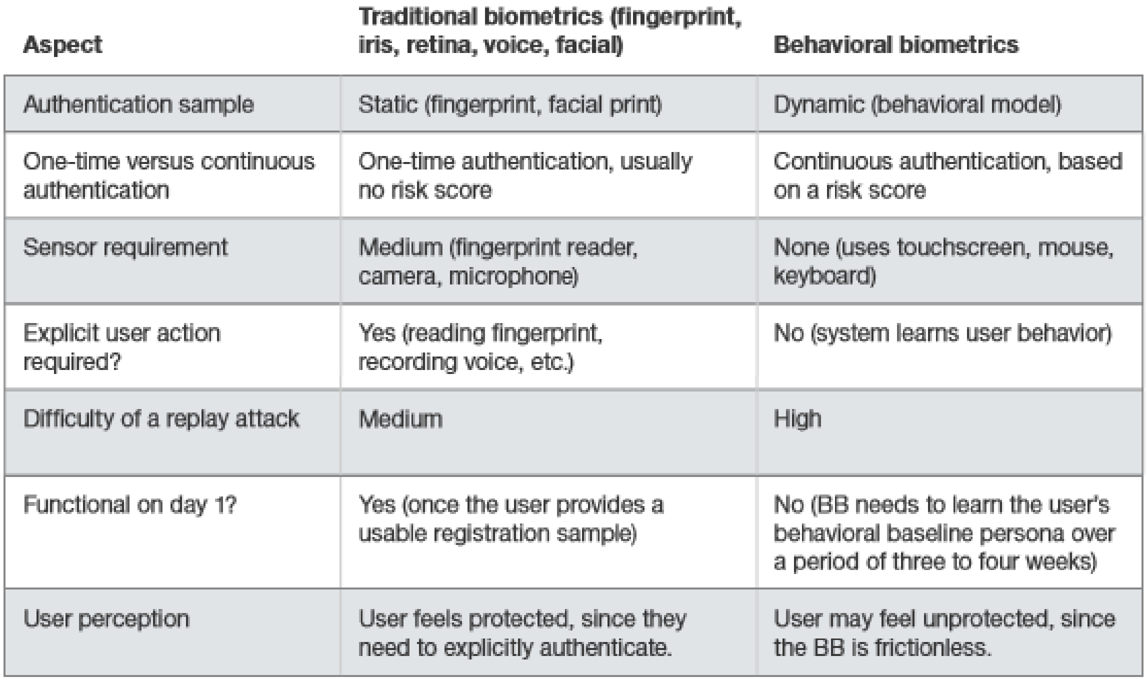
mature. The gait itself could enable continuous authentication during a physical session in a monitored environment, but that is a limited use case relative to other biometrics.

- Gesture. Gesture dynamics, GUI interactivity. Uses pointing devices (mice, trackpads, etc.) or touchscreens. Often combined with handling and keystroke.
- Handling. Handling dynamics, motion, and motion dynamics. Uses accelerometers and gyros. Often combined with gesture and keystroke.
- Keystroke. Keystroke dynamics, keyboard dynamics, and typing rhythm. Uses a physical or virtual keyboard. This can be active, typically in conjunction with typing a password. In passive mode, often combined with gesture and handling.
- Signature. Signature dynamics. Uses a specialized tablet (pad) and stylus or a touchscreen (with or without a stylus). Typically active, but could be effectively passive when a signature image is being captured. Rarely used for authentication, but can be used for electronic signature and non-repudiation in fraud prevention. Important features include stroke order, the pressure applied, the pen-up movements, the angle the pen is held, the time taken to sign, the velocity and acceleration of the signature. Some systems moreover compare the visual image of signatures; however, the focus in signature biometrics lies on writer-specific information rather than visual handwritten content.
- Voice. Voice recognition, voiceprint, speaker recognition, speaker verification (not to be confused with speech recognition, although it may be implemented in conjunction with that). Uses mainstream microphones. They can be influenced by factors such as age, illnesses, mood, conversational partner or surrounding noise. It uses a voiceprint that analyses how a person says a particular word or sequence of words unique to that individual. Voice biometrics adoption is still growing, although not at earlier rates. It is among the most proven and trusted biometric modalities [31].

The most frequently cited vendors in the area are Agnitio[15], Daon[16], NICE Systems[17], Nuance Communications[18], SpeechPro[19], and VoiceVault[20].

[15] http://www.agnitio-corp.com/
[16] https://www.daon.com/
[17] https://www.nice.com/
[18] https://www.nuance.com/
[19] http://speechpro-usa.com/
[20] http://voicevault.com/

Although today, BB is the least mature authentication solution, it holds a lot of promise and is quite different from physical biometrics such as fingerprint, voice, and facial biometrics. The key benefit of BB is that it is much harder to attack with stolen credentials. In fact, session replay is much harder or impossible. On the other hand, BB authentication decisions are always nondeterministic and require time to build a baseline persona profile. To build robust behavioral biometrics-based websites and mobile applications, security professionals need to pay attention to BB's key capabilities and how they differ from that of physical biometrics.



Aspect	Traditional biometrics (fingerprint, iris, retina, voice, facial)	Behavioral biometrics
Authentication sample	Static (fingerprint, facial print)	Dynamic (behavioral model)
One-time versus continuous authentication	One-time authentication, usually no risk score	Continuous authentication, based on a risk score
Sensor requirement	Medium (fingerprint reader, camera, microphone)	None (uses touchscreen, mouse, keyboard)
Explicit user action required?	Yes (reading fingerprint, recording voice, etc.)	No (system learns user behavior)
Difficulty of a replay attack	Medium	High
Functional on day 1?	Yes (once the user provides a usable registration sample)	No (BB needs to learn the user's behavioral baseline persona over a period of three to four weeks)
User perception	User feels protected, since they need to explicitly authenticate.	User may feel unprotected, since the BB is frictionless.

Figure 9 Behavioral Biometrics vs Traditional Biometrics [32]

4.2.3 The electrocardiogram (ECG)

The electrocardiogram is a graphical depiction of the heart's electrical activity over time. No two electrocardiograms taken from the same subject will be identical, but each person has a unique pattern to his or her heart's electrical activity, which firms can use to differentiate and authenticate distinct users. Also known as electrocardiograph, ECG, EKG and cardiac pulse. The potential business value, which is substantial, of the technology depends on:

1. Users' receptiveness to using ECG as an authentication factor and,
2. Its interoperability with other systems.

There is no evidence that the technology seamlessly integrates into corporate IT and physical access environments right now, nor that users will happily authenticate using their heartbeats.

The most frequently cited vendors in the area are B-Secur[21] and Nymi[22].

4.2.4 Iris biometrics

Iris biometrics (IB) authenticate users based on the unique structure of their irises, which are fully formed within a year of birth. Iris scanners isolate the user's iris, store its unique melanin structure as mathematical code, and then compare future scans during access requests to the stored template to authenticate. Uses a variety of camera technologies, including those that are commonplace in consumer endpoint devices, as well as the infrared cameras required for Windows Hello's face modes. The predominant use cases of IB are for physical rather than logical access, which limits the amount of value the category can create. IB still add value, as the iris is a complex, unique identifier that enables strong 1-to-1 or 1-to-N matching, and users are more familiar with iris scanning than newer biometric solutions such as behavioral or face solutions.

The idea of distinguishing an individual by using iris patterns was suggested by an ophthalmologist in 1936. Later, the idea appeared in some action movies, including 1983's James Bond "Never Say Never Again", nonetheless at that time it remained science fiction. In 1994, the first automated iris pattern recognition algorithm was proposed by physicist and computer-vision expert John Daugman and patented, and continue to be the basis of all current iris recognition systems and products. These have been used to confirm a person's identity by reading the arrangement of blood vessels in the retina or patterns of color in the iris. It is very reliable technique and difficult to map by forgers [30].

The most frequently cited vendors in the area are Crossmatch[23], EyeLock[24], Iris ID[25], IriTech[26], and Safran Identity & Security[27].

[21] http://www.b-secur.com/
[22] https://nymi.com/
[23] https://www.crossmatch.com/
[24] https://www.eyelock.com/
[25] http://www.irisid.com/
[26] http://www.iritech.com/
[27] https://www.morpho.com/en/about-us

4.2.5 Vein biometrics

Vein structure, vein geometry, vein pattern recognition:

- In the hand and finger - palm vein, finger vein. The veins in the back of the hand can also be used, but the term “back-of-hand vein” is rarely used. Uses specialized capture devices with infrared imaging.
- In the retina - Retina, retina scan, retinal pattern (seldom “retina vein”, as the technology predates other vein modes). Uses a variety of camera technologies, including those that are commonplace in consumer endpoint devices. Retina biometrics authenticate users based on the structure of the capillaries that supply blood to the retina. The structural patterns of human retinal capillaries are unique and remain constant from birth to death. Retina scans flood the retina with imperceptible low-energy light, record the pattern the light traces on retinal capillaries, and stores the pattern as mathematical code against which to compare future authentication attempts.

  Retina biometrics have been around for a while, although adoptions and applications have lagged behind those of other older modalities such as fingerprint, face, and voice biometrics. Right now, the only applications for true retina biometrics are for high-security physical access control scenarios.

- In the whites of eyes (sclera) - Eye vein, scleral vein. Uses mainstream camera technologies.

Vein biometrics are currently a strong authentication factor for physical access control. An individual’s vein pattern is unique, remains stable throughout his or her life, and is very difficult to spoof; collection is also nonintrusive and relatively frictionless — users place their palm on or in front of a reader for a few seconds.

The most frequently cited vendors in the area are Fujitsu, Hitachi, and “Safran Identity & Security”.

4.2.6 Face biometrics

Face biometrics authenticate users based on unique features of their faces. 2D facial recognition technology compares the relationship between nodal points on a face in a stored template and image taken during an authentication attempt, while 3D facial recognition technology compares the facial topography (eye socket depth, curves of jaw, nose, chin contours, etc.) in a stored template and subsequent impression to authenticate. Periocular (or circumocular) modes focus on the face structure around the eyes, rather than the full face. It uses a variety of camera technologies, including those that are commonplace in consumer endpoint devices, as well as the infrared cameras required for Windows Hello's face modes. It can be passive (although often with active enrolment). Face biometrics currently serve a critical role in domestic law enforcement and government surveillance. Retailers and physical security departments also employ face biometrics for loss prevention and property protection. The technology is improving, although industrywide accuracy does not yet instill confidence, and accuracy varies widely by vendor.

The most frequently cited vendors in the area are Cognitec Systems[28], Daon[29], FacePhi[30], Gemalto[31], NEC[32], “Safran Identity & Security”, and Sensory[33].

4.2.7 Fingerprint biometrics

Fingerprint biometrics (FB) authenticate users based on the minutiae (Galton ridge structure) of their fingerprints, which are captured in various ways including ultrasonic, light, and capacitive (electricity) sensors. Among all the biometric techniques, this is the oldest method, which has been successfully used in numerous applications. For example, fingerprint scan use in forensic for criminal identification, use in attendance system. FB already provide high business value. Their applications for device access and mobile payment authentication in particular already remove friction from daily consumer activities - no other biometric can claim that.

4.2.8 Hand geometry biometrics

Hand geometry biometrics use length, width, surface area, depth, or other geometric elements of a person’s hand or knuckle to authenticate users. Hand geometry biometrics do not offer notable advantages over other forms of biometrics. The geometries they measure are not unique identifiers, and they

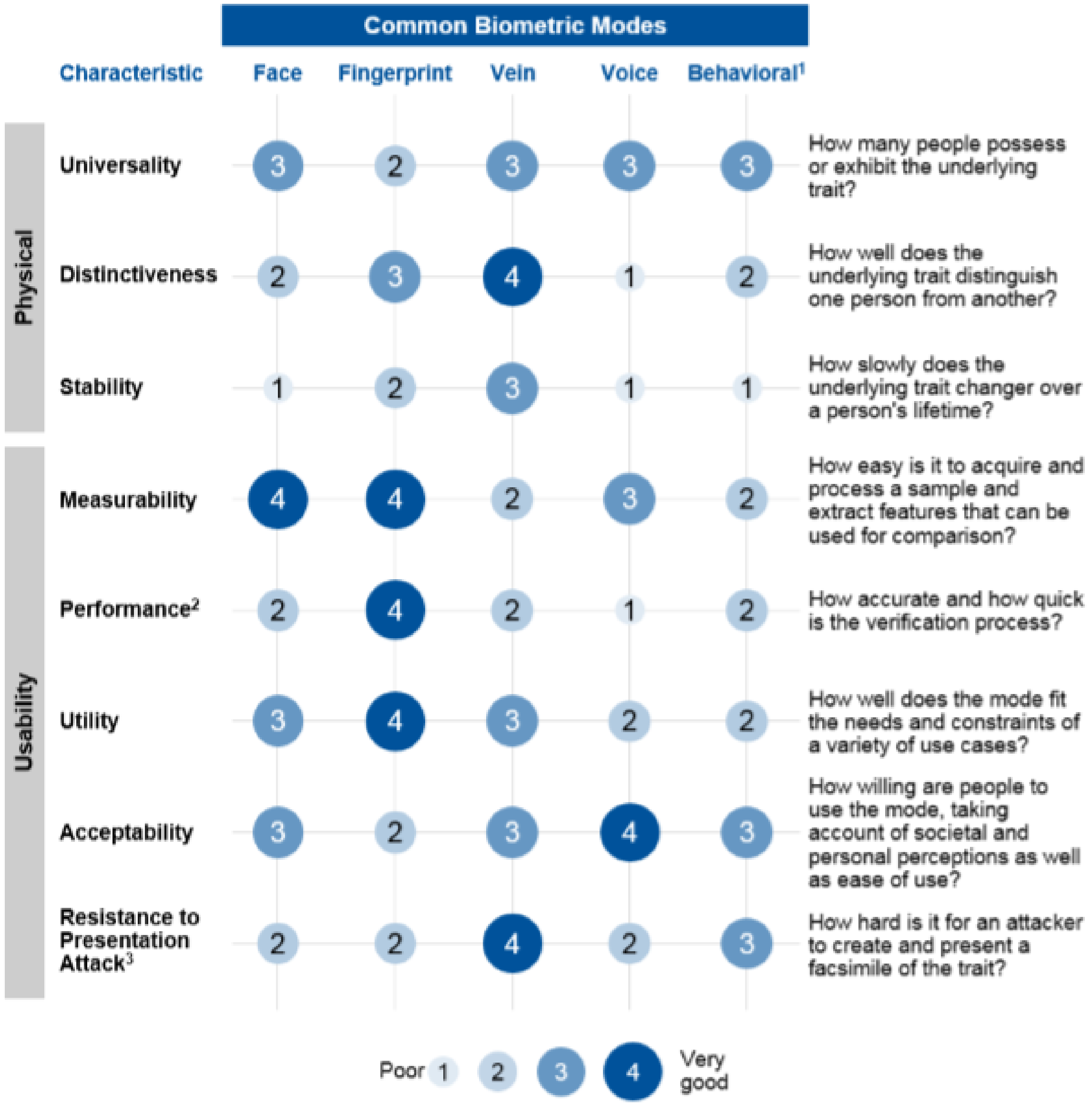
[28] http://www.cognitec.com/
[29] https://www.daon.com/
[30] http://www.facephi.com/en/
[31] https://www.gemalto.com/govt/biometrics
[32] http://www.nec.com/en/global/solutions/safety/Technology/FaceRecognition/index.html?
[33] http://www.sensory.com/

require a physical mount to take a reading. Firms considering biometrics that require users to provide a hand for scanning more often opt for fingerprint or palm/finger vein biometrics, which authenticate based on unique identifiers using a similar or smaller amount of hardware to do so. Hand geometry biometrics will become less appealing as biometrics for unique identifiers (ECG, fingerprint, iris, etc.) proliferate. Investment in hand or finger geometry biometrics will only become more difficult to justify [31].

4.2.9 Combination of Biometrics authentication modes

Selecting a biometrics authentication mode depends on the available budget, the desired user experience and the accepted risk appetite.

In addition, we can combine multiple authentication methods, either synchronous (for example, face and voice simultaneously) or asynchronous (for example, face, followed by voice if and only if face resulted in a match). Synchronous methods are potentially quicker, but some combinations of modes can create poor user experience. A combined method's potential improvement in assurance and accountability, compared with either mode used alone, is generally realized. However, it is not necessarily so; Professor John Daugman of the University of Cambridge has shown [33] that combining two different biometric modes can, in some instances, yield a method that is actually weaker than the stronger unimodal method.



Common Biometric Modes

	Characteristic	Face	Fingerprint	Vein	Voice	Behavioral[1]	
Physical	Universality	3	2	3	3	3	How many people possess or exhibit the underlying trait?
	Distinctiveness	2	3	4	1	2	How well does the underlying trait distinguish one person from another?
	Stability	1	2	3	1	1	How slowly does the underlying trait changer over a person's lifetime?
Usability	Measurability	4	4	2	3	2	How easy is it to acquire and process a sample and extract features that can be used for comparison?
	Performance[2]	2	4	2	1	2	How accurate and how quick is the verification process?
	Utility	3	4	3	2	2	How well does the mode fit the needs and constraints of a variety of use cases?
	Acceptability	3	2	3	4	3	How willing are people to use the mode, taking account of societal and personal perceptions as well as ease of use?
	Resistance to Presentation Attack[3]	2	2	4	2	3	How hard is it for an attacker to create and present a facsimile of the trait?

Figure 10 Characteristics of common biometrics modes [26]

4.4 Privacy risks and mitigation approaches

The use of biometrics authentication methods has raised concerns which are most commonly associated with privacy issues. This is a well-discussed issue in public fora and legislation in many countries. The legislation initiatives will be presented in Chapter 5, whereas here, in the following paragraphs, we try to approach the technical means to protect the biometrics credentials. In order to mitigate this risk, biometric template protection schemes have been introduced as well as other methods described in the paragraphs ahead. In addition, a risk that jeopardizes the efficiency of employing biometrics methods is error-related, and therefore is addressed with the use of error correction techniques.

4.4.1 Biometric template protection

Most existing privacy-preserving biometric authentication approaches focus on storing and transmitting a modified version of the original biometric templates in order to avoid the danger of eavesdropping sensitive data or the case of compromised databases. One direction in order to combat the privacy issues associated with biometric authentication is the employment of biometric template protection schemes such as cancellable biometrics and biohashing. Although biohashing offers low error rates while guaranteeing a quick authentication phase, biohashing schemes are vulnerable to several attacks [34].

4.4.2 Error correcting based methods

The use of error correction codes is an attractive mitigation to the inherently noisy nature of biometric traits. Error correction, indeed, would automatically decode small perturbation of a template into the template itself, solving the problem of noisy data. In this way, the systems can get error-free biometric templates and thus successfully use cryptographic primitives that will not affect the matching biometric process.

However, given that the biometric templates are not uniformly random, and practical error correcting codes do not have high correction capability, the theoretical security is not achievable in practice. It has been shown, indeed, that fuzzy commitment schemes leak private information [34].

4.4.3 Cryptographic primitives

The direct employment of cryptographic primitives seems the most robust approach so far to tackle the challenging problem of privacy-preservation. Most of the state-of-the-art cryptographic protocols, however, were not designed taking into consideration the inherent variability of biometric data. In fact, cryptography tends to amplify small differences and it is not error-tolerant (e.g. hashing, AES, RSA). The main cryptographic tools used to combat the leakage of private information during biometric authentication are [34]:

- Secure multi-party computation (SMPC).
- Verifiable Computation (VC).
- Bloom Filters.

4.4.4 Other non-cryptographic approaches

Given that Oblivious Transfer is a well-established countermeasure against user traceability and distinguishability attacks, most non-cryptographic tools for privacy-preserving Biometric Authentication Systems focus to combat template and sample recovery attacks [34].

Another alternative is to generalize the comparison process to include multiple distances. More precisely, if the matching process relies on such a mechanism that, at each authentication attempt, a distance is randomly selected from a pre-defined set of distances. Thus, the attacker could not gain any information about the stored template without knowing first which distance has been used.

Similarly, changing the value of the threshold τ used for the matching process at each authentication attempt renders harder the implementation of the center search attack. However, such approaches may have a negative impact on the accuracy of the biometric authentication and may increase the false acceptance and/or false rejection rates.

Finally, one could consider combining Differential Privacy (DP) with biometric authentication, in order to achieve privacy preservation. Intuitively, DP allows users to query a database and receive noisy answers, so that no information in leaked about the data stored in the database. Although this combination of DP with biometric authentication could possibly give an end to template recovery attacks (i.e. center search attacks), it could also have an impact on the accuracy of the authentication process.

5

Regulatory Framework

Authentication and authentication methods are an important aspect in the design and the operation of the information systems. Therefore, this function could not be devoid of regulation attempts and initiatives.

In this chapter we present the major current regulatory initiatives in the area, signifying the importance of authentication and the efforts those bodies put stress upon.

5.1 General Data Protection Regulation (GDPR)

The privacy concerns associated with the use and the misuse of the biometrics traits have triggered the European Union in including that authentication means in the General Data Protection Regulation (GDPR), effective May 25, 2018[34].

GDPR adds special restrictions to biometric data processing. As stated in Paragraph 1, Article 9 of the EU General Data Protection Regulation [35], "[…] the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person […] shall be prohibited". Specifically, processing is prohibited unless people provide explicit consent, the data is processed in establishment, exercise or defense of legal claims, or there are specific provisions in national legislation. The "legal claims" justification includes obligations regarding payment authentication instruments, liability for unauthorized payment transaction, and future obligations based on the revised Payment Services Directive (PSD2).

The main question that one needs to address when designing a privacy-preserving biometric authentication protocol is how to guarantee privacy-preservation without downgrading the accuracy of a biometric authentication system. Among the most challenging problems in designing efficient and privacy preserving biometric authentication systems there are [34]:

[34] https://www.eugdpr.org/

1. The resistance to impersonation attacks.
2. The irrevocability of biometric templates.
3. Guaranteeing that personal information remains private.

5.2 PCI Guidelines

Another area where authentication plays an important role is financial transaction. The PCI Security Standards Council has issued a set of directives governing storing, transmitting and operating data related to cards and payments, and user authentication is among those directives.

According to PCI Guidelines [5], there are some basic principles to protect authentication data from unauthorized parties:

- Passwords and other "something you know" data should be difficult to guess or brute-force, and be protected from disclosure to unauthorized parties.
- Biometrics and other "something you are" data should be protected from unauthorized replication or use by others with access to the device on which the data is present.
- Smart cards, software certificates, and other "something you have" data should not be shared, and should be protected from replication or possession by unauthorized parties.

Where any authentication elements rely on a multi-purpose consumer device—e.g., mobile phones and tablets—controls should also be in place to mitigate the risk of the device being compromised.

5.3 Other initiatives

Seeing the big picture in a relationship with community affairs, as e-government has become an integral part of community operations and public services are accessible to citizens via electronic channels, there is a growing need to enhance trust to the means of authentication. In addition, the interoperability issues, especially in the G2G context, have created the need to adopt similar approach in regards with authentication and security issues, if not common standards.

In this respect, several initiatives have been proposed:

- In 2004, an authentication policy has been produced in the context of IDA[35]. This policy lists four authentication assurance levels. The more severe the likely consequences are, the more confidence in an asserted identity will be required to engage in a transaction. [36]
- ENISA[36] has initiated work on electronic authentication focusing on a "language" allowing an adequate description of the concepts and properties [37]
- EU directive on Electronic Signature provides a framework for a standardization of technological mechanisms that can also be used, in specific contexts, for authentication. [38]
- IDABC (Interoperable Delivery of European eGovernment Services to public Administrations, Businesses and Citizens defined a model, which included levels of authentication. [37]
- Several standardization bodies are working on authentication. E.g., ISO/IEC JTC1 SC27 has produced several standards on entity authentication.
- Federation mechanisms such as Shibboleth and Liberty Alliance provide facilities to put in place an interoperable federated authentication.

[35] IDA is a European Commission driven strategic initiative using advances in information and communications technology to support rapid electronic exchange of information between Member State administrations.

[36] European Network and Information Security Agency

6

Discussion

Having presented in the previous chapters the basic authentication methods and there characteristics, we will try in this chapter to compare, to mix them up, to split them apart, to form a concoction to put it into a blender to see if we can get the perfect authentication method "one-size-fits-all".

6.1 Will biometrics wipe out passwords?

Technological innovation continuously produces tremendous achievements in software and hardware. Optimistically, password elimination sounds attractive and potentially provides a solution to many problems. However, the practical difficulties of achieving this meta-goal have become more apparent over the passage of time. Thus, the following can be concluded [39]:

- Password replacement attempts should consider security risks, usability, cost, demographics, user considerations, economic requirements, etc.
- Replacement attempts spanned over decades are merely reducing, rather than eliminating, user reliance on passwords, because password access always remains as a back-up or recovery option. Accordingly, the distinction between reducing dependency as opposed to eliminating it should be made clear.
- The considerable growth of biometric solutions has decreased password use, but claiming the password is dead is unjustified and does not currently appear practical.

Provision of a password feature in a device, whether as a primary or a secondary source, gives an attacker more liberty to attack - i.e. biometric or password. In such cases, it is just old wine in a new bottle, or even worse.

6.2 Authentication scheme attributes with significant role

Unequivocally, legacy text-passwords present flaws and over the years have been the subject of discussion and research in an attempt to find ways to replace them. Nevertheless, evaluation of all authentication schemes should be derived from unbiased and systematic review of factors asserting appropriability.

There has been extended research over the years focusing on the technical parameters authentication schemes should abide, in order to serve their purpose. However, at the same time researchers have developed conceptual frameworks that help authentication researchers and scheme developers in choosing deliberately between schemes and making clear design choices.

Forget et al. [6] suggest that usability should be placed in the center of the criteria during design, as it is interlinked to securing authentication. Based on this notion, they suggest a framework in which KBA schemes are evaluated in regards to a set of features related with persuasion, memory, input and output and obfuscation. They propose focus on user's experience and underlying psychological parameters which may have been overlooked during the design, a rather than security itself. A poor implementation of a scheme may kill its purpose.

Bonneau et al. [10] in their framework compared multiple authentication methods in terms of reaping the list of twenty-five benefits concerning usability, deployability and security, the latter including privacy. Their study concluded that no scheme is flawless or scores equally high in every important factor, so selecting authentication scheme is a matter of deliberate focus on choosing one set of trade-offs over another.

Other criteria taken into account are those related with cost, which is an integral factor of every Information Security application. In the recent systematic literature review of Authentication schemes and methods [3] the observation was made that most studies in authentication are presented in a specific context, so in spite the fact that is not registered as a criterion it cannot be overlooked as it may be the decisive factor.

Also, the level of satisfaction of the users can impact the correct use of the system. The acceptance of authentication methods is the way it is perceived by the user. All those issues should be evaluated before any deployment of an authentication method. [1]

Picking the appropriate authentication method also depends on the vulnerability they show in certain attacks, the probability of occurrence of such attacks and the tolerance users can show in the context of the applications these authentication methods support. The implementation is also crucial. Even a good authentication technique will not be secured if the implementation allows backdoors.

Not only does no known scheme come close to providing all desired benefits: none even retains the full set of benefits that legacy passwords already provide. In particular, there is a wide range from schemes offering minor security benefits beyond legacy passwords, to those offering significant security benefits in return for being more costly to deploy or more difficult to use.

If an authentication method at any time offers a user the ability to reduce the number of authentication factors to a single factor, it is by definition no longer a multi-factor authentication method. A common example of this is when a user is offered the ability to "remember this computer" for a public web resource. In such a scenario, a user may be authenticated initially using multi-factor authentication but a token is then set on their device such that subsequent authentications use a single factor (usually a passphrase) as long as the token on their device is accessible and valid. In this scenario, the claimant verified by the token is the user's web browser rather than the user. As such, it violates the requirement for two or more authentication factors to authenticate a single claimant to a single authentication verifier. Furthermore, the token has characteristics more akin to a session token than an authentication factor, which makes it unsuitable for the purposes of authentication. [4]

6.3 Evaluating the efficiency of authentication methods

Authentication is the real-time process of corroborating a claimed digital identity with a specified or understood level of confidence, which enables activity to be (equally confidently) attributed to a specific individual and militates against illicit access. It is widely accepted that the strength of an authentication method - a measure of the level of confidence[37] in a claimed identity that the method provides - is directly related to the number of authentication factors used, a notion that is entrenched in many regulations. However, the number of factors is neither the sole basis nor a direct indicator of authentication strength, and finding an authentication method that provides the right strength (that is, what is appropriate to the level of risk in a particular use case) is ultimately more important to an enterprise than the number of factors a method has. What, then, is the significance of authentication factors?

[37] As per [21], authentication strength is often more formally expressed as a level of assurance

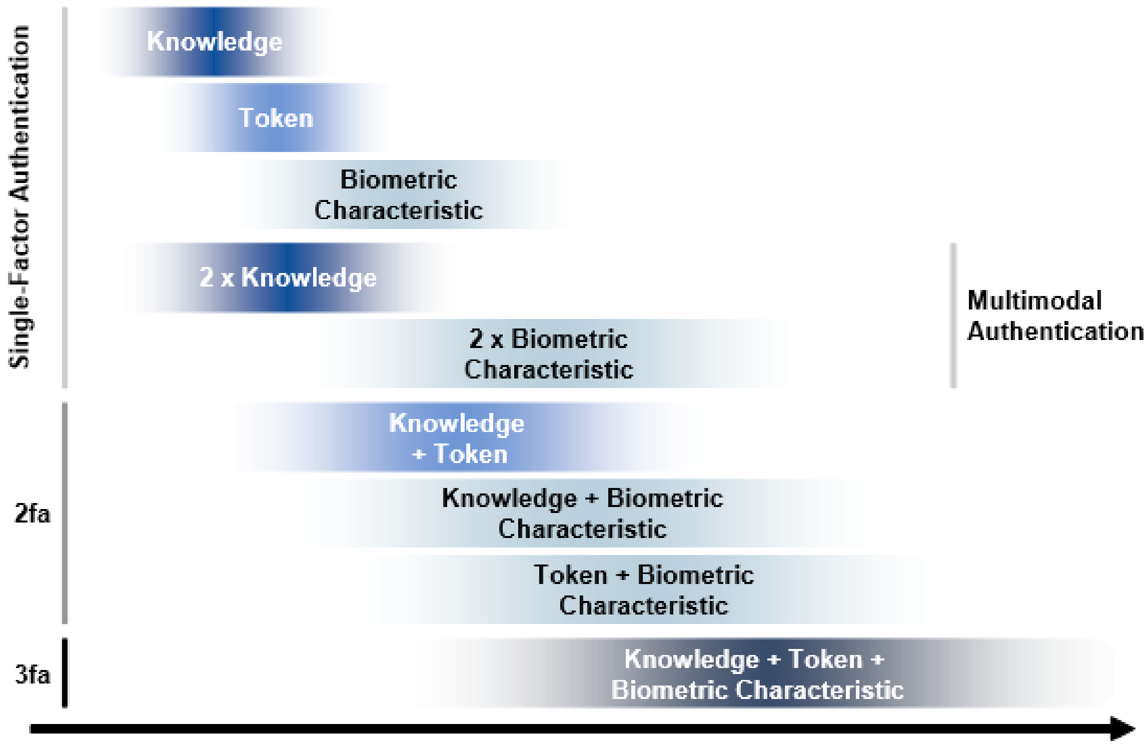

Single-Factor Authentication
Knowledge
Token
Biometric Characteristic
2 x Knowledge
2 x Biometric Characteristic
Multimodal Authentication
2fa
Knowledge + Token
Knowledge + Biometric Characteristic
Token + Biometric Characteristic
3fa
Knowledge + Token + Biometric Characteristic

Figure 11 Notional authentication strength [40]

Although orthodox user authentication methods, based on some kind of credential are widely used, they are not wholly successful in online, mobile and, especially, digital business. There are three key problems [41]:

- Orthodox methods add friction and erode user experience - for example:
    - Longer, more-complex passwords are harder to remember and type accurately (especially on mobile devices).
    - Methods requiring a hardware device can be intrusive.
- Orthodox methods can be strong, but brittle:
    - Once credentials or protocols are compromised, there is no resilience.
    - Some kinds of attack simply bypass authentication, by subverting an already-authenticated session.
- Business moments involve fluid, transient relationships:
    - Familiar people will typically be authenticated using credentials curated by the enterprise.
    - Credential-based methods cannot be used to authenticate total strangers

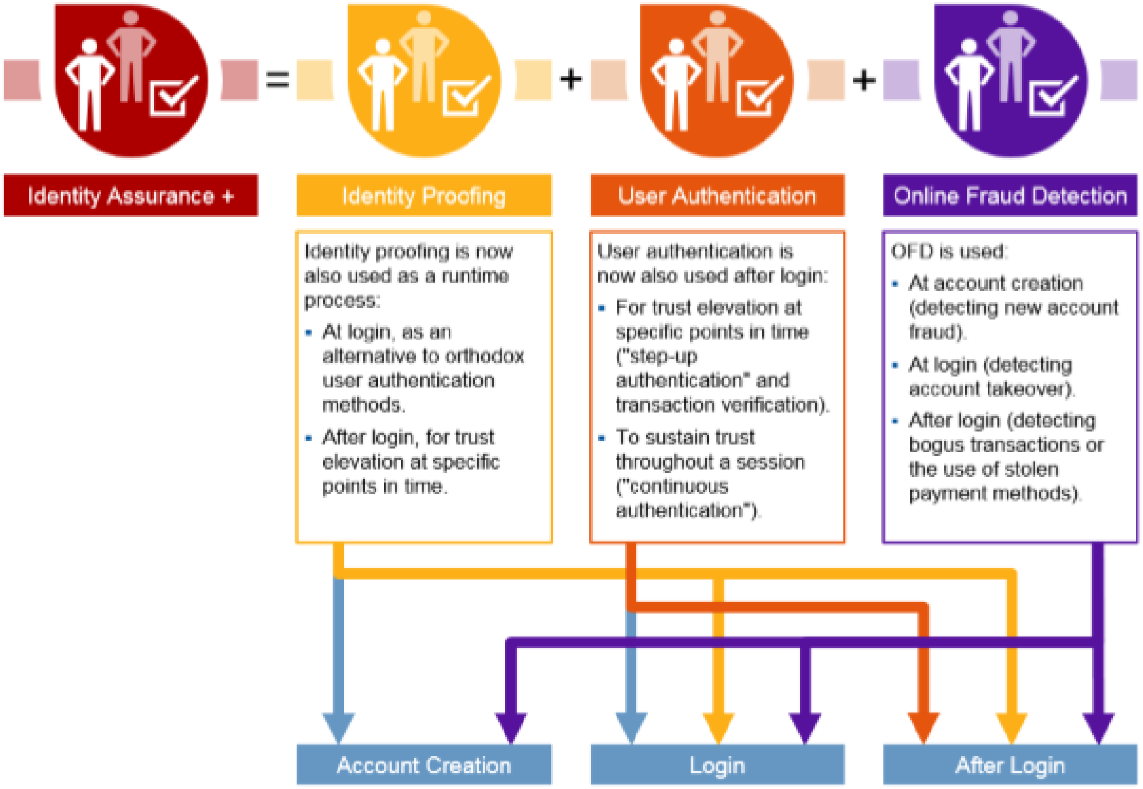

Identity Assurance +
=
Identity Proofing
+
User Authentication
+
Online Fraud Detection
Identity proofing is now also used as a runtime process:
▪ At login, as an alternative to orthodox user authentication methods.
▪ After login, for trust elevation at specific points in time.
User authentication is now also used after login:
▪ For trust elevation at specific points in time ("step-up authentication" and transaction verification).
▪ To sustain trust throughout a session ("continuous authentication").
OFD is used:
▪ At account creation (detecting new account fraud).
▪ At login (detecting account takeover).
▪ After login (detecting bogus transactions or the use of stolen payment methods).
Account Creation
Login
After Login

Figure 12 Building trust [41]

6.4 How to enhance identity trust in authentication

Security and risk management leaders responsible for IAM, fraud prevention and payment security should shift from the paradigm of suspicion to an assumption that the customer has positive intent, by first seeking behavior signals indicating that a user is low risk. This can be achieved through the following [42]:

- Implement bot detection technologies, passive behavioral biometric technologies and behavior analytics to identify and quarantine machine-based attacks with minimal impact to customers and reduced false positives.
- Focus on building an understanding of individual and peer group behavior of legitimate customers, and apply behavior analytics to elevate trust and reduce challenges and step-up requests.
- Implement an adaptive approach to authentication, enabling the selective and intelligent application of friction that is appropriate for the action the user is attempting, thereby reserving high-friction challenges for high-risk activity and providing a seamless experience for most.

7

Conclusions

Authentication is inherent in information systems and services from the first time of their presence. As a result, one would expect authentication to be a weathered and exhausted issue, with technical and operational issues solved.

However, this is not the case. The three pillars of authentication (something you know, something you have, and something you are) evolve as:

- information systems and information technology advance,
- the regulatory frameworks impose new rules,
- marketing needs dictate new user experience and interfaces,
- the distinction between humans and autonomous blurs,
- thread landscape and risk allowances change.

Inherence based authentication remains a widely adopted authentication method, as it is simple to implement and carries great value in most cases. New methods, such as graphical passwords try to cope to new UIs and new threats and prove to be resistant in many cases. On the other hand, the intrinsic friction they launch in user experience is a source marketing complain.

The appliances that support biometrics authentication have evolved over time and the sensors in mobile phones have rendered some biometrics authentication methods almost commodity. Despite that, the stochastic nature of biometric authentication and humane characteristics impersonation have not provided this method a clear win over traditional knowledge based authentication methods.

The technological characteristics of authentication methods have to serve the regulatory directives and have to adapt to the evolving topology of IS, the marketing requests and the threads ecosystem.

Based on the above, identity assurance should be the calculated balance between identity proofing and risk appetite. It seems that, although the identity certainty seems elusive, a continuous combination of user authentication and online fraud detection builds the safest road in the quest of the perfect authentication method.

Although the basic authentication principles (know – have – are) remain the same, the evolution of the technology create new authentication methods, new user needs and new authentication threats. Therefore, the authentication landscape is constantly evolving and the quest for the identity trust in authentication remains open to a future re-evaluation.

Bibliography

[1] S. Idrus, E. Cherrier, C. Rosenberger and J.-J. Schwartzmann, "A Review on Authentication Methods," *Australian Journal of Basic and Applied Sciences,* June 2013.

[2] H. K. Sarohi and F. U. Khan, "Graphical Password Authentication Schemes: Current Status and Key Issues," *IJCSI International Journal of Computer Science Issues,* March 2013.

[3] I. Velásquez, A. Caro and A. Rodríguez, "Authentication schemes and methods: A systematic literature review," *Information and Software Technology,* September 2017.

[4] Australian Government, Australian Cyber Security Centre, "Multi-factor Authentication," September 2017.

[5] PCI Security Standards Council, "Guidance for Multi-Factor Authentication," 2017.

[6] A. Forget, S. Chiasson and R. Biddle, "User-centred authentication feature framework," *Emerald Insight,* 2015.

[7] A. I. Mohd Anwar, "A Comparative Study of Graphical and Alphanumeric Passwords for Mobile Device Authentication," in *Conference: Modern Artificial Intelligence & Cognitive Science Conference*, 2015.

[8] D. Davis, F. Monrose and M. K. Reiter, "On User Choice in Graphical Password Schemes," in *SSYM'04 Proceedings of the 13th conference on USENIX Security Symposium*, 2004.

[9] L. Sobrado and J. Birget, "Graphical Passwords," *The Rutgers Scholar,* 2004.

[10] J. Bonneau, C. Herley, P. v. Oorschot and F. Stajano, "The Quest to Replace Passwords:A Framework for Comparative Evaluation of Web Authentication Schemes," in *Security and Privacy (SP), 2012 IEEE Symposium on*, 2012.

[11] D. Hong, S. Man, B. Hawes and M. Matthews, "A Graphical Password Scheme Strongly Resistant to Spyware," in *Proceedings of the International Conference on Security and Management, SAM '04, June 21-24, 2004, Las Vegas, Nevada, USA*.

[12] "Draw a Secret Scheme," [Online]. Available: https://www.usenix.org/legacy/publications/library/proceedings/sec99/full_papers/jermyn/jermyn_html/node4.html.

[13] S. Chiasson, P. v. Oorschot and R. Biddle, "Graphical Password Authentication Using Cued Click Points," 2007.

[14] A. Nayak and R. Bansode, "Analysis of Knowledge Based Authentication System Using Persuasive Cued Click Points," in *7th International Conference on Communication, Computing and Virtualization 2016*, 2016.

[15] B. B. Zhu, J. Yan, G. Bao, M. Yang and N. Xu, "Captcha as Graphical Passwords—A New Security Primitive Based on Hard AI Problems," *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY,* no. 9, June 2014.

[16] Carnegie Mellon University CyLab, "The reCAPTCHA Project," [Online]. Available: https://www.cylab.cmu.edu/partners/success-stories/recaptcha.html.

[17] "Google introducing reCaptcha," [Online]. Available: https://www.google.com/recaptcha/intro/index.html.

[18] NIST, "Electronic Authentication Guideline," in *NIST Special Publication 800-63-2*, 2013.

[19] L. Lamport, "Authentication with insecure communication," *Communications of the ACM,* November 1981.

[20] "How-to Geek," [Online]. Available: https://www.howtogeek.com/232314/u2f-explained-how-google-microsoft-and-others-are-creating-universal-two-factor-authentication-tokens/.

[21] NIST, "Authentication and Lifecycle Management," in *NIST Special Publication 800-63B Digital Identity Guidelines*, 2017.

[22] M. Bhat and A. Singh, "Innovation Insight for Fast IDentity Online Protocols," Gartner, 2016.

[23] Fido Alliance, [Online]. Available: https://fidoalliance.org/download/.

[24] A. Cser and M. Maxim, "Brief: Don’t Ignore FIDO," Forrester, 2016.

[25] S. Krishnan, "Biometrics and the Era of Sensing Machines," CapGemini, 15 May 2017. [Online]. Available: https://www.capgemini.com/2017/05/biometrics-and-the-era-of-sensing-machines/.

[26] A. Allan and T. Phillips, "Technology Insight for Biometric Authentication," Gartner G00329041, 2017.

[27] "Webopedia," [Online]. Available: https://www.webopedia.com/TERM/F/false_acceptance.html.

[28] "Webopedia," [Online]. Available: https://www.webopedia.com/TERM/F/false_rejection.html.

[29] "Bayometric," [Online]. Available: https://www.bayometric.com/false-acceptance-rate-far-false-recognition-rate-frr/.

[30] O. Kaiwartya, M. Prasad, S. Prakash, D. Samadhiya, A. H. Abdullah and S. O. Abd Rahman, "An Investigation on Biometric Internet Security," *International Journal of Network Security,* pp. 167-176, March 2017.

[31] A. Cser and A. Spiliotes, "TechRadar: Biometric Authentication," Forrester, 2017.

[32] A. Cser and M. Maxim, "Vendor Landscape: Behavioral Biometrics," Forrester, 2017.

[33] J. Daugman, "Cambridge University," [Online]. Available: http://www.cl.cam.ac.uk/~jgd1000/combine/combine.html.

[34] E. Pagnin and A. Mitrokotsa, "Privacy-preserving biometric authentication: challenges and directions," Chalmers University of Technology, Gothenburg, Sweden, 2017.

[35] E. Parliament, "EUR-Lex," 27 April 2016. [Online]. Available: http://eur-lex.europa.eu/eli/reg/2016/679/oj.

[36] Interchange of Data between Administrations, "Basic Policy for establishing the appropriate authentication mechanisms in sectoral networks and projects".

[37] ENISA, *Mapping security services to authentication levels.*

[38] A. Varghese, *eGovernment & CIP Operations.*

[39] K. Siddique, Z. Akhtar and K. Yangwoo, "Biometrics vs passwords: a modern version of the tortoise and the hare," *Computer Fraud & Security,* January 2017.

[40] A. Ant, "Defining Authentication Strength Is Not as Easy as 1, 2, 3; Update," Gartner, 2016.

[41] A. Ant and J. Care, "Take a New Approach to Establishing and Sustaining Trust in Digital Identities," Gartner, 2017.

[42] T. Phillips, "Don't Treat Your Customer Like a Criminal," Gartner, 2017.

[43] "Digital Identity Guidelines, Authentication and Lifecycle Management," NIST, 2017.

[44] G. Kreizman, "Hype Cycle for Identity and Access Management Technologies, 2017," Gartner, 2017.