A Review on Authentication Methods

Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, Jean-Jacques Schwartzmann

A Review on Authentication Methods

Syed Zulkarnain Syed Idrus[1,2], Estelle Cherrier[2], Christophe Rosenberger[2], and Jean-Jacques Schwartzmann[2]

[1]Universiti Malaysia Perlis, 01000 Kangar, Perlis, Malaysia

[2]Université de Caen Basse-Normandie, UMR 6072 GREYC, F-14032 Caen, France

ENSICAEN, UMR 6072 GREYC, F-14032 Caen, France

CNRS, UMR 6072 GREYC, F-14032 Caen, France

{syed-zulkarnain.syed-idrus,estelle.cherrier,christophe.rosenberger,

jean-jacques.schwartzmann}@ensicaen.fr

Abstract. The Internet has consolidated itself as a very powerful platform that has changed the communication and business transactions. Now, the number of users navigating through the Internet is more than 2.4 billions. This large audience demands online commerce, knowledge sharing, social networks etc., which grew exponentially over the past few years. Thus, it leads to the need for security and enhanced privacy. In recent days, fraud over the Internet constitutes one of the main drawbacks for the widespread of the use of commercial applications. Therefore, the three vital security issues take place every day in our world of transparent fashion, more precisely: *identification*, *authentication* and *authorisation*. An *identification* is a process that enables recognition of an entity, which may be either a human, a machine, or another asset such as a software programme. In security systems, *authentication* and *authorisation* are two complementary mechanisms for determining who can access the information resources over a network. Many solutions have been proposed in the literature, from a simple password to recent technologies based on RFID (Radio Frequency IDentification) or biometrics (Mahier et al., 2008). This paper provides an overview on existing authentication methods, and its pros and cons when designing an online service.

Keywords: Information technology, user authentication, online services, cryptography, biometrics.

1 Introduction

For the past two decades, computer networks have grown at an explosive rate. In a wide range of environments, such networks have become a mission critical tool. Organisations are building networks with larger scales than ever before, and the connectivity with the global Internet has become indispensable. Along with this trend has come an explosion in the use of computer networks as a means of illicit access to computer systems (Goyal et al., 2005; Liao et al., 2009). Internet is known as a very powerful platform that changes the way we communicate and perform business transactions in current technology (Syed Idrus et al., 2008; Syed Idrus, 2008). It has now touches every aspect of our lives along with emerging of newer security threats, ready to embark towards the journey of destructions. According to the Internet World Stats, as of June 30, 2012, over 2.4 billions users are using the Internet, and hence the numbers no doubt will keep on increasing. Thus, the advent of information securities has revolutionised our life particularly with the information that are available, whereby data can easily be accessed and manipulated (Syed Idrus et al., 2009, 2012a). Transmitted information level is becoming more important especially as interactions that used to only be carried out offline, such as bank and commercial exchanges are now being carried out online in the form of Internet banking and electronic commercial exchanges, and damages due to such attacks will be greater (Cha and Kim, 2008; Davaanaym et al., 2009). As increasing amounts of personal information are surfacing on the Web, it is essential to remain wary of the risks surrounding the ease in which our private details can be accessed. Social networking and online profiles contribute to this: giving potential intruders a plethora of sensitive information. Insafe reports that more than a quarter of children in Europe have online networking profiles which can be exposed, and with over 900 million people on Facebook alone the danger is widespread (Parris-Long, 2012).

> *'It is good to be wary about publishing your personal information even if other people are happy to post pictures of their house or their contact details - remember what goes online, usually stays online'* (Parris-Long, 2012).

The aim of this paper is threefold. Section 2 deals with the concepts and definitions of authentication. In Section 3, it is devoted to a survey of some of the existing authentication methods. We make some comparisons between different

authentication methods, discuss in Section 4. In this paper, we are interested to discover the advantages, disadvantages and also an arbitration towards the existing methods but our focus is on biometrics, specifically to keystroke dynamics. We also discuss about the future trends of authentication.

2 Concepts and Definitions of Authentication

Before presenting the different existing methods, we give some definitions and concepts. The concepts listed below are partially based on the result of (Menezes et al., 1996) and (Chabaud and Grumelard, 2006). The authentication process implies different entities:

- The *claimant* is the entity that authenticates to the system, in order to use the services. It could be a person or an Information System (IS);
- The *monitor* is the entity that provides an authentication service. It asserts the identity of a claimant (or reject it in case of a wrong authentication) and checks if it can grant him/her the use of the required service;
- The *Information System* (IS) provides services, such as an access to a computer account, an application, a door unlocking or a network printer, and will let the *claimant* use its services if the *monitor* correctly authenticated it (with a given required level of trust).

  Example: A worker needs to access his/her place of work. The main door is secured with an authentication token. The lock contains a token reader and triggers the unlocking of the door if the token is presented to the reader and if the verification system estimates that this worker is allowed to access. In that case, the claimant is the worker, the monitor is the verification system, and the function provided by the IS is the unlocking of the door.

2.1 The Authentication Concept

'Identification', 'authentication' and 'authorisation' are three interrelated concepts, which form the core of a security system. *Identification* is the communication of an identity to an IS. Before *authentication*, the claimant typically provides the IS an identity anyway (for example, a login or an email address), and the monitor asserts the identity by *authentication* (for example, using a password). An *authentication* is a proof given by a claimant to assert a monitor that he/she really corresponds to the identity he/she provided. The monitor then asserts the IS of the identity of the user. Finally, the *authorisation* is the granted privileges given to the user.

Authentication systems provide the answers to both questions: *(i) who is the user?* and *(ii) is the user really who he/she represents himself/herself to be?* Hence, *authentication* represents one of the most promising way concerning trust and security enhancement for commercial applications. It also denotes a property of ensuring the identity of the previously mentioned entities (Kotzanikolaou and Douligeris, 2007). Besides, *authorisation* is a process of giving individuals an access to the system objects based on their identity. *Authorisation* systems provide the answers to the three questions: *(i) is user U authorised to access resource R?*; *(ii) is user U authorised to perform operation O?*; and *(iii) is user U authorised to perform operation O on resource R?*

There is often a confusion between 'identification', 'authentication' and 'authorisation'. These words/terms do not have the same meaning at all. Each of these concepts requires an enrolment step. Enrolment is the 'registration' of a new user, including the emission of tokens and credentials. Enrolment is a major concern and should also be carefully handled. In the rest of this paper, we will consider the IS has already registered the claimant.

Example: Let us consider the same example as the previous one. When the user authenticates himself with his token, he provides his identity by putting his card, which contains an identification number linked to his account. The system does not need to know the full description of the worker, so a simple identification number is enough. Then, the card authenticates to the reader (for example, by a symmetric cryptographic protocol), to prove the authenticity of the provided identity. Finally, the authorisation will be given to the user to go through the door, if he has the right to do it.

Having said that, we then need to have a link between both the claimant and the monitor. 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. The authentication goal is to assert an identity, but the scope of authentication methods is very large and it can vary in many ways. Below is a list of some of the common authentication methods:

- An ID (IDentification)/password: to open a session on a computer or to authenticate on Internet;

- A PIN (Personal Identification Number) code: to unlock a smartcard;
- An RFID card: for accessing a building;
- A fingerprint: to unlock a door;
- A facial recognition system with a webcam: to open a session on Internet;
- A USB token;
- A one-time password token;
- *etc...*

Each one of the authentication methods has a specific use and inherent drawbacks. Tokens can be stolen, facial recognition systems can be broken by presenting a photo of the genuine user... It concerns the *trustability* of the authentication method. In consequence, 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 (see Figure 1).

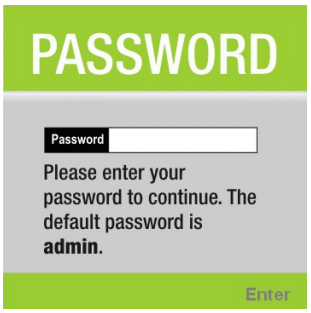

Figure 1: An authentication system seen on a Wi-Fi router that clearly indicates an attacker, which password to try first.

2.2 Basic Steps For Authentication

The common basic steps for authentication are:

1. *Initial step*: the claimant is unauthenticated.
2. *Connection step*: the claimant requires to the IS the use of a function that requires an authentication. The IS asks the monitor to authenticate the claimant.
3. *Authenticated step*: the claimant is authenticated and a session is opened. The IS provides the user the required functions.
4. *Disconnection step*: the user disconnects or is disconnected from the monitor and the state returns to the *initial step*. This step can be initiated on a time out or by an action of the user.

An IS may require different levels of authentication, for example, a level for the administrators and a level for the users. In such a system, the level of authentication is graduated on a scale: level *0* for an unauthenticated user with the lowest rights in the system; level *N* for the administrator with full rights; and one or multiple levels between *0* and *N*. Here, the scheme is that an authentication could be required to switch to a higher level of trust in the claimant by the IS. The provided security of an authentication method depends on usability and acceptability. If the usability is bad, the users will rapidly find ways to bypass the authentication steps for a convenient use. This will lead inevitably to a failure of the system, so it should be considered as a critic.

> *Example 1: In a facility, the door of the warehouse is unlocked by a token associated with a PIN. In this scheme, users that constantly carry heavy packages will rapidly put a piece of cardboard to block the door open.*

> *Example 2: A user of an enterprise has to open a session on his/her computer. The administrator has set the inactivity timeout before unlocking it in two minutes and has imposed highly secured passwords (minimum sixteen characters, changes every week). An average user will rapidly stick a post-it with his/her password on the top of his/her computer.*

The authentication process can be based on a combination of one or more authentication factors. The four (widely recognised) factors to authenticate humans are:

1. ***Something the user knows***: a password, a passphrase, a PIN code, the mother's maiden name...
2. ***Something the user owns***: a USB token, a phone, a smartcard, a software token, a navigator cookie...
3. ***Something that qualifies the user***: a fingerprint, DNA fragment, voice pattern, hand geometry...
4. ***Something the user can do***: a signature, a gesture...

But now, perhaps we could include a 'fifth' authentication factor:

"***Somewhere the user is***: a current location/position, a current time information... "

2.3 Authentication Factors and Strengths

Using more than one factor to authenticate a user is sometimes related as a strong authentication, but the strength of the authentication is more related to the strength of underneath authentication methods, to be more precise: "Two-Factor Authentication" (TF-A). For example, a TF-A implies to a navigator cookie (what you own) and the ability to provide the mother's maiden name (what you know) is a TF-A, but is not a strong authentication, as both authentication methods can be easily compromised. Another alternative factors could be:

- A *spatiotemporal authentication*: the user can be given access to his/her work place only at some predefined times and locations;
- A *web of trust*: a reputation could be a factor for authenticating in some cases;
- A *Turing test* (Turing, 1950) could be considered as an authentication as a human instead of a computer (a CAPTCHA is an example of a Turing test).

An authentication and an electronic signature (or Message Authentication Codes (MACs)) are nearby notions. An electronic signature is nothing else but the authentication of the source of a message. The main difference resides in the fact that authentication is related to a timestamp, as it authenticates the presence of the identified user trough a channel, the fact that it is by nature and not definitive. Moreover, authentication messages generally concerns the claimant identity and not necessarily any other meaningful message, whereas electronic signatures are directly related to a message.

3 A Survey of Existing Authentication Methods

A person's authentication can be the means of accessing a computer or a software on computers or websites. For example, he/she may be asked by the system to provide their username and password (Obaidat and Sadoun, 1998; Bours and Barghouthi, 2009). The most common solution for today's electronic authentication is the use of a username and password (Davaanaym et al., 2009). In order to get some money out, say, from the Automated Teller Machine (ATM), we need a bankcard and a personal identification number (PIN). Besides, some airports have imposed fingerprints or iris scans for authenticating passengers (Bours and Barghouthi, 2009). For traveling security purposes, most countries have now compelled biometric in their passports, and Malaysia was the first country in the world to issue and implement biometric passports, also known as an e-passport in 1998, after a local company, IRIS Corporation, developed the technology (Wikipedia, 2011b).

The well-known ID/password is far the most used authentication method. It is widely used despite its obvious lack of security. This fact is due to the ease of implementation of this solution, and to the instantaneous recognition of that system by the users that facilitates its deployment and acceptance. However, there are several existing password-based authentication schemes that have been introduced and the earliest was by (Lamport, 1981).

Some authentication methods rely on concepts defined by cryptography, however this is not a general rule. Authentication is a critical function in IS as it gives access to the services provided by the IS. The whole security of a system depends on the level of guarantee provided by the authentication method in place. There are no perfect authentication methods, as they are subject to antagonist needs: security, usability, acceptance, cost... The usability and the cost of the provided authentication methods are major concern, as 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.

There are various different authentication methods. But in this paper, we present an (almost) complete overview of some of the available authentication methods discuss in Subsection (3.1) to (3.5) namely static authentication by a shared secret; one-time password token; cryptographic challenge-response based authentication; radio frequency identification; and biometrics. We also elaborate further about their use, limitations and potential benefits, and drawbacks.

3.1 Static authentication by a shared secret

The static authentication is best known through its major implementation: the ID/password form based authentication, as it is a commonly used solution to verify the identity of a demander (see Figure 2). In the general scheme of static authentication, the claimant proves the monitor he/she knows a shared secret, generally by revealing it to the monitor. The monitor then compares it to a value stored in a verification table to reveal if it is the right value. A shared secret can be:

- A *password*: a list of characters, either meaningful or not, generally between six and ten characters in length;
- A *passphrase*: often used very similarly as a password, but as it is longer it maximises the key space, providing a better security;
- A *pass code*: it is a purely numeric password, often used to authenticate the holder of a smartcard (PIN code);
- A *non-text based pass*: graphical passwords (Suo et al., 2005), mouse-movement based... ;
- A *big number or an array of randomly chosen bytes*: for machine to machine authentication.

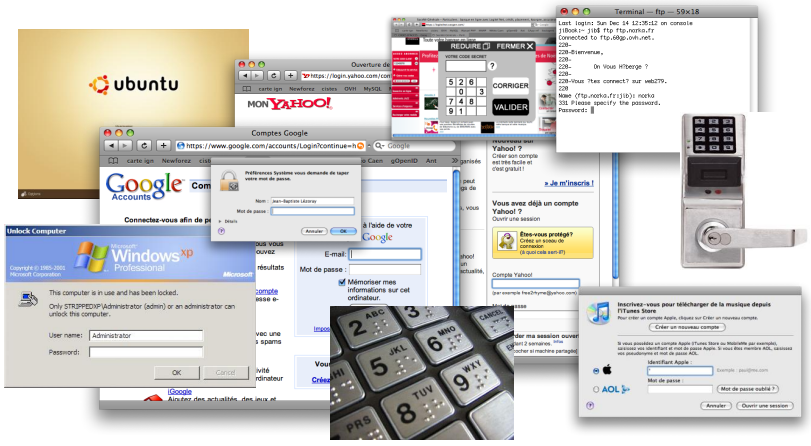

Figure 2: The shared secret is far the most employed method of user authentication.

Static authentication suffers from many drawbacks as it is considered as a low-security solution when used on its own or without precaution:

- Password can be stolen online by an eavesdropper and used in order to gain access to the system (replay attack);
- Physical attacks can easily be done, by a camera recording a PIN sequence as it is being typed, or by a keylogger (either software or hardware) to record a password on a computer;
- Passwords are also vulnerable to guessing attacks, like brute force attacks or dictionary attacks. However, it is possible to limit the scope of these attacks by adding a delay of about one second before entering the password and after entering a wrong password;
- A stolen password hash could sometimes be reverted, for example, by using a list of precomputed hashes of the most common passwords or more sophisticated attacks like using rainbows-tables;
- Passwords can easily be revealed by a user to another (but most authentication methods can also be shared).

Increasing the password strength is a solution to avoid dictionary attacks or to make brute force attacks infeasible. 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. In (Burr et al., 2006), the authors provide a further discussion on password entropy, and the feasibility of such attacks on passwords. For example, a user choose, say, a password of seven characters is said to provide between sixteen and twenty eight bits of entropy.

A password transmitted from the demander to the monitor, without any encryption is considered as a *clear password*. Despite it is widely used, this technique suffers from an obvious lack of security. An eavesdropper can intercept the password (for example, on Internet or intranet), and easily replay it in order to gain access to the IS.

Therefore, the main concern about passwords is the lack of security of their transmission over a channel, the best way to overcome this problem is for the claimant to prove that he/she knows the password without having to send it over the channel. Next, we introduce about one-time passwords (OTPs), which are an evolution of the ID/password system.

3.2 One-time password token

The main drawback of static passwords is their lack of protection against replay attacks, hence, the purpose of the OTP mechanism is to annihilate the replayability of passwords with the generation of a new password for each use. OTP systems can be considered as a bridge between a static password authentication and a better authentication method. It facilitates the migration of legacy applications that were designed to rely only on passwords (mainframes, websites, the IS of an organisation...). The only impacted component is the monitor, and the IS does not need any change. An OTP token generally consists in a device with an LCD (Liquid-crystal Display) screen, which displays alphanumeric characters. It can have a button to generate OTPs, and some are locked by a PIN code (whose keyboard is either directly on the device either on the reader), so they can be considered as TF-A.

As OTP generates a password, the verification requires synchronisation between the token and the monitor. There are several categories of OTP, depending on counter synchronised, time synchronised, involving a secure channel, or with a shared list of passwords.

Figure 3: Left token is a challenge type OTP card with a PIN code (CRYPTOCard©). The one on the right is a counter synchronised OTP token (ZyXEL).

A *counter synchronised OTP*, sometimes also called "Mathematical hash chain OTP" or "Mathematical key chain OTP", often implies to a token with a button on it (see Figure 3). Each press on the button generates a new password that can be used to log on. Most are based on the Leslie Lamport-scheme (Lamport, 1981). Secondly, in a *time synchronised OTP*, the token has an internal clock and so as the monitor (see Figure 3). New passwords are generated from the value of the current timestamp, rather than on a shared secret or a previous password. The value of the generated password usually changes every one or two minutes. Thirdly, an OTP can also be sent to the claimant through *a secure channel*. The claimant has to be authenticated through an unsecured channel, but the monitor could provide the claimant with a random OTP through a third party channel, which is considered as secured, where the claimant is already authenticated. The claimant then sends back the OTP through the unsecure channel to prove his/her identity to the monitor. Finally, with a *shared list of password*, the claimant and the monitor share copies of the same unpredictable list of passwords. If the list is ordered, 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.

Another form of an authentication method is a cryptographic challenge-response based authentication. We discuss about this method in the next subsection as to why this method of authentication is considered as efficient.

3.3 Cryptographic challenge-response based authentication

PAP (Password Authentication Protocol) is a simple protocol for authentication over a network, which sends clear passwords and identifiers over the network. Subsequently, CHAP (Challenge Handshake Authentication Protocol) is an improvement of PAP, but it still requires transmitting a hashed password. The main idea of a challenge-response based authentication is that the claimant proves he/she knows the secret without sending it clear over the channel. Thus, CHAP is a challenge-based authentication protocol, but the transmission of a hashed password is still a problem due to brute force and dictionary attacks (Ratha et al., 2001; Uludag et al., 2004). Besides, hashed passwords still contain a lot of information about the secret password. The main response to solve that problem is the use of cryptography, either symmetric (Daemen, 2012) or asymmetric in order to implement a challenge-response authentication. Generally speaking, a challenge-response authentication system is a system that issues a "challenge" on the client request i.e. challenge in this context: question of identification, and verifies it in the "response" of the claimed identity i.e. response in this context: provide a prove of identification.

In the symmetric case, the monitor sends a challenge to the claimant. The challenge can be a large integer, an array of integers... Generally, the claimant then enciphers the challenge with the shared key and sends the result back to the monitor, which compares the result with the one it has also calculated. In the asymmetric case, the claimant owns a private key associated with a certificate that contains the relative public key. The claimant provides the monitor his/her certificate (and his/her public key). The monitor sends a random number as a challenge, and the claimant uses its private key to sign the challenge (or to encipher it), and sends the result back to the monitor. The monitor then verifies the signature with the public key (or decipher the response) to check the challenge was verified.

The main challenge on the claimant side is to protect the private key (or the shared key) of the user. To do so, a piece of software on the claimant computer can seal the private key with a password or a passphrase on the user's device. Another solution is to use a secure element with a sealed storage of the keys: smart card, USB secured Token, TPM (Trusted Platform Module)... Such hardware components handle the cryptographic computing involving the private key of the user. The authentication of the user to the smartcard can be required to unlock the cryptographic service. It can be done by a PIN code or by biometrics (see Figure 4). Cryptographic challenge-response based authentication is a very efficient and confident authentication method, if implemented correctly. However, on the monitor side, the maintenance of the PKI (Public-key Infrastructure) can be very time, energy and money consuming.

Figure 4: An example of a contactless smartcard for logical access control with an embedded fingerprint sensor for match on card (E-smart Technologies).

Subsequently, a common means of authentication is by using the Radio Frequency IDentification (RFID), which is a technology for transmitting data from devices called RFID tags to a specific reader. In the following subsection, we define how this method can help the users in communication capabilities, especially via Internet.

3.4 Radio Frequency IDentification

The first generation of RFID tags was used in the 1950s for a military purpose, but it was limited to an identification purpose. At that time, their use was limited to the transmission of a serial number wirelessly over radio waves. In the past few years, RFID tags have been a large success in industry, and their use became common. Application range of RFID tags is very large: item identification for inventory data, supply chain management, phones with RFID capabilities, authentication plastic cards... It is said that we rely to an Internet for things, and hence, RFID tags will help moving toward this way by adding communication capabilities to common items. The presence of RFID tags in the everyday life has just begun. For example, a credit card with a built-in RFID system could be debited by a wireless POS (Point of Sale), even if the card is still in the bag of its owner. The classical protection against those attacks is a PIN code printed on the card, which is needed to unlock the chip. So the attacker will need to have the card in hand to read the code. Such a protection is used for RFID passports (biometric passports).

Having mentioned biometrics, we elaborate about this method of authentication and how this technology has a strong link in relation to ourself, in the subsequent subsection. It is considered as a trustable security systems that can be an alternative to password-based security system.

3.5 Biometrics

In computer science, in particular, biometrics is used as a form of identity access management and access control (Yang, 2011; Wikipedia, 2011a). However, biometrics is an ancient Greek word and is the combination of two words (*bio*) means life, (*-metric*) means measurement. According to (Wikipedia, 2011a), biometrics has been around since about 29,000 BC when cavemen would sign their drawings with handprints. In 500 BC, Babylonian business transactions were signed in clay tablets with fingerprints. The earliest cataloging of fingerprints dates back to 1891 when Juan Vucetich started a collection of fingerprints of criminals in Argentina. However, it is said that the history of biometrics techniques originated in China in the 14th century. It was a form of finger printing as reported by the Portuguese historian Joao de Barros. The Chinese merchants were stamping children's palm and footprints on paper with ink to distinguish babies (Bhattacharyya et al., 2009).

Biometrics is a science that consists of methods for uniquely recognising humans based upon one or more intrinsic physical or behavioural traits (Jain et al., 1999; Yang, 2011; Wikipedia, 2011a). It has become one of the popular and trustable security systems that have become an alternative to password-based security system. Biometrics techniques have been developed for a machine-based verification of the identity of a person (Prabhakar et al., 2003). Biometrics characteristics can be divided into three main classes namely 'Morphological', 'Behavioural' and 'Biological' (Yang, 2011). *Morphological* is related to the shape of the body such as retina, voice, prints (finger, thumb, palm), iris, hand geometry, face recognition, ear, height, weight, skin, veins, gender... *Behavioural* is related to the behaviour of a person such as gait, signature, keystroke dynamics, voice, driving, gaming... *Biological* is related to the inner part of a living organism such as heart beat, odour, DNA, blood... (see Figure 5). Voice can be categorised in both *morphological* and also *behavioural* trait because every person has a different vocal tract, but voice recognition is mainly based on the

Figure 5: Characteristics of Biometrics.

study of the way a person speaks, hence commonly classified as *behavioural*. Some researchers have coined the term *behaviometrics* for behavioural class of biometrics (Wikipedia, 2011a).

Biometric recognition is largely studied in computer science. The use of biometric techniques, such as face, fingerprints, iris and ears is a solution for obtaining a secure personal authentication method (Yang and Nanni, 2011). Biometrics uses the authentication factors, which are methods based on something that qualifies the user and something that he/she can do. The main advantage of these authentication methods is that there exists a strong relationship between the individual (user) and its authenticator (biometric data). Furthermore, it is difficult to copy the biometric characteristics of an individual compared to most of other authentication methods. Nonetheless, there is a drawback in biometric authentication, which is the uncertainty of its verification result, for example, in fingerprints authentication; there could be a possible error due to bad positioning of the finger (McQuay and Smari, 2009).

Each time a user authenticates himself/herself, he/she provides a biometric information with its reference. This information is generally similar at each authentication attempt. An attacker could intercept the information and replay it. Therefore, the solutions to this predicament have to be *dynamic*. In (Simske, 2009), the author defined that *dynamic biometrics* is known as a dynamic means of granting access rights that must exist. There are several ways to achieve this such as by defining a generalisation of a challenge-based password for biometrics, one-time password authentication scheme or perhaps free text on keystroke dynamics, and hence to achieve a system with a lighter workload and higher security.

Biometric authentication can be summarised in two steps namely enrolment and authentication. The stage of the enrolment is where the user provide his/her biometric data. The biometric data will be captured and then, the features will be extracted and stored into the database. During the authentication process, the stored features will be compared with the ones currently presented for an access. If it matches, then, an access will be granted. For example, in keystoke dynamics, during the enrolment stage, the users are asked to provide their way of typing i.e. by typing given a password or a passphrase on a keyboard between 5 to 10 times. Because keystroke dynamics is a behavioural biometrics, hence, it has to be done collectively i.e. several number of times because each time, the way the users type a password/passphrase, their typing rythm may differ slightly.

As mentioned by (Simske, 2009), we are proposing keystroke dynamics as a solution, especially for password-based authentication. Keystroke dynamics is an interesting and a low cost biometric modality as it enables the biometric system to authenticate or identify an individual based on a persons way of typing a password or a passphrase on a keyboard. It belongs to the class of behavioural biometrics, in the sense that the template of a user reflects an aspect of his/her behaviour, as mentioned earlier. Generally speaking, the global performances of keystroke dynamics based authentication systems are lower than those of popular morphologic modalities based authentication systems (such as fingerprints, iris, etc...). We use the GREYC Keystroke software (Giot et al., 2009) to capture biometric data as shown in Figure 6.

However, there is no single biometric modality expected to effectively satisfy the needs of all authentication applications (usability, security, cost...). Subsequently, a vast number of biometrics have been proposed, researched, analysed and evaluated (Jain et al., 1999). Thus, each biometric has its strengths and limitations, therefore, the respective biometric invokes to specific authentication applications (Jain et al., 1999; Stallings and Brown, 2008). Although each of these biometric methods, to a certain level, possess the desirable properties and has the potential of becoming a valid biometric technique (Newham, 1995), many of them cannot be acceptable as an indisputable evidence of identity "in the court of law". The acceptability of a biometric system as an application that is often compromises between various perceptions or

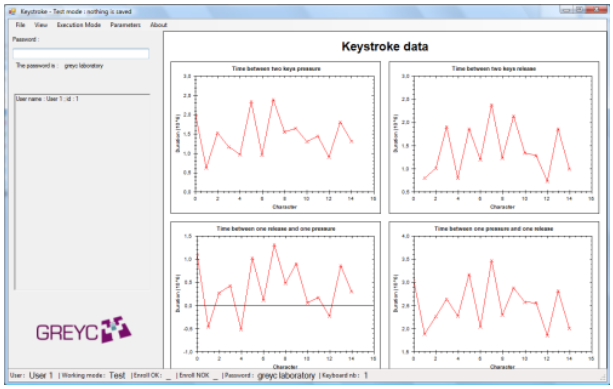

Figure 6: GREYC Keystroke Software

verbotens of community sensitivity and the value or convenience offered by a biometric-based authentication (Jain et al., 1999).

The common problem of personal authentication raises a number of important research issues such as *"which technologies are the most effective to achieve accurate and reliable authentication of individuals?"* Some of these problems are well-known open problems. As examples, in pattern recognition and computer vision, it need a systematic cross-disciplinary effort compared to other authentication methods. Therefore, biometric technology alone may not be sufficient in order to solve these issues effectively, thus the solutions to the outstanding open problems may lie in the innovative engineering designs exploiting the constraints. Otherwise, it would be unavailable to the applications and in harnessing the biometrics technology in combination with other allied technologies (Jain et al., 1999).

In order to prevent information from being accessed by illegitimate or unauthorised users, remote user authentication is certainly one of the most important service (Liao et al., 2009). However, a major concern with the morphological-based biometrics is that if it can be copied by the impostor using, say, deceit or force, the authentic user would be faced with a life-long loss of identity (Woodward, 1997). If this phenomenon ever happens, the consequences could be disasterous.

4 Comparative Study

All authentication methods are different. None of them has the same usage and each one will respond to specific needs. Moreover, different implementations of the same authentication method will provide very different levels of security. For example, even the theoretically strongest authentication method, if the enrolment stage is poor, will likewise provide a poor reliability on the asserted identities. Each authentication method still has intrinsic advantages and problems. Table 1 illustrates a comparative study of general (and generic) authentication methods, on several different criteria. The criteria are:

- The *observed popularity* is the overall proportion of implementations of an authentication method among all implementations of authentication methods;
- The *device cost* is the cost of the per user equipment. It includes, if any, tokens, readers, and their life span;
- The *infrastructure cost* is the cost of the setting up of such an authentication method in an IT architecture, and to maintain the authentication system operational. It includes costs for the user assistance, devices replacement, enrolment of news users, and revocation of users;
- The *ease of use* is the general usability of the authentication method: the user acceptance, the token and its form factor, the potential availability of the system (for example, it could be different for an online or an offline system). Ease of use is a critical criterion as it is commonly the first cause of failure of the establishment of an authentication method in an IT system;
- The *general security* is an evaluation of the security (and of the potential failures) provided by the authentication method, on major cases. It is a very subjective evaluation (but, not the case for cryptography-based solutions), and should be considered as an average for the authentication method.

The comparison points out some interesting facts about authentication processes and deployments as illustrated in Table 1. We can notice that the observed popularity of authentication methods is more related and the low infrastructure costs can also be explained that it is more widespread, than popular. It is likewise, at least for that specific modest set of authentication methods, inversely proportional to the level of security it provides. The direct linkage between popularity and ease of use demonstrates how ease of use is crucial for a deployment of any authentication method. The cost is

Table 1: A comparative evaluation of some authentication methods.

Method	Observed popularity	Average device cost	Infrastructure cost	Ease of use	General security	Disadvantages	Advantages
Simple static password	*** ***	-	*	** **	*	Very low security, usability decreases with multiple passwords.	Very low cost, portability, familiar to users.
Strong static password	** **	-	**	*	**	Usability, still vulnerable to replayability.	Better security than a simple password.
Certificate on a token	** *	**	*** **	** **	** **	Infrastructure costs, cost of the token.	Offline physical authentication.
Synchronised OTP generator token	** *	** *	** *	** **	** **	Device cost, form factor.	Good security, good usability.
Biometrics (Fingerprints)	*	**	**	*** **	*** **	Acceptance, complicated revocation, high cost.	Good general security.

generally proportional with the general security it provides. That implies that it could be a good solution to share strong authentication solutions (monitors) between different Information Systems. (Josang, 2012) also explained how we can protect and when we can use the weak and strong passwords given the levels of authentication assurance in security systems. However, authentication on Internet could be done by using technologies that rely on user centered software solutions.

Authentication of users on web sites is a major concern, as there is no ideal solution to solve it. This problem is due to the underlying protocols and client: HTTP is not adapted to authenticate users, neither is HTML to handle authentication interaction with users. Based on that fact, new solutions began to emerge.

5 Conclusions and Future Trends

The first future trend is of course to increase the security of information systems through a secure authentication of the individual. Meaning that we want to be as sure as possible that the claimant is not an impostor.

The different authentication solutions that could be deployed must be very simple for a client. Authentication is part of the human machine interface for any software applications. The ease of use is important for the logical access control step but also for the enrolment one. As for example, some information systems require a strong password that shall include a combination of uppercase and lowercase letters, numbers, and symbols (see Figure 7). If the password is not strong enough the individual is asked to choose another one. This is generally inconvenient for the user to define such a password and to remember it (Park et al., 2004).

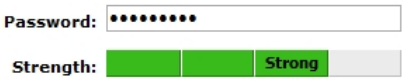

Figure 7: Strong password checking.

Industrial and researchers generally define very efficient and secure authentication solutions as a technical point of view. A good practical solution shall consider some usability aspects during the development step. For many ergonomic or cultural reasons, an authentication method would not be accepted by users. As illustration, even password typing can be reluctant for some users. Human memory is in conflict with most password policies (Mehler and Skiena, 2006). In (Sasse et al., 2001), the authors note usability problems with password authentication, such as the number of passwords a user has to remember, strict password policies, varying systems, and memory demands. Users rarely completely forget a password. Many human factor studies of data entry methods have been realised in the past.

Thus, a biometric system is essentially a pattern recognition system. Biometric authentication systems necessitate much more operations for the enrolment step than defining a static password as for example. Nevertheless, the verification step is much more convenient for the user as he/she is generally requested to show one morphologic characteristic such as one fingerprint or its face i.e. which makes a personal authentication by determining the authenticity of a specific morphological or behavioural characteristic possessed by the user.

Therefore, for us, the only user authentication method solution is biometrics. We propose to utilise keystroke dynamics in order to avoid password-based authentication problems. The results that we obtained from our previous studies

(Syed Idrus et al., 2012b, 2013) could be used as a reference model to assist the biometric system to better recognise a user by a way he/she types on a keyboard. Hence, it would strengthen the authentication process by hindering an imposter trying to enter into the system. Besides, the main advantage of resorting to keystroke dynamics for authenticating users relies in its low cost. Indeed, no extra dedicated sensor is required. For example, keystroke dynamics is dealt with in the recent papers (Giot et al., 2011; Messerman et al., 2011; Bours, 2012). The fact that the performances of keystroke dynamics are lower than other standard biometric modalities can be explained by the variability of the users behaviour. One solution to cope with this variability is to study soft biometrics, first introduced by (Jain et al., 2004).

Subsequently, we have conducted a couple of research works in biometrics: keystroke dynamics with new approaches using 'soft biometric' and performed several analysis in our recent articles in (Syed Idrus et al., 2012b, 2013). For our soft biometric criteria, we used features such as the way of typing, gender, age and handedness. The outcomes from our analysis have also showed some interesting and promising results. In (Jain et al., 2004), the authors explained about "*soft biometric traits*", which are defined as "*characteristics that provide some information about the individual, but lack the distinctiveness and permanence to sufficiently differentiate any two individuals*". For example Jain *et al.* consider gender, ethnicity, and height as complementary data for a usual fingerprint based biometric system.

Another important trend is the respect of the privacy of users. In order to increase the security of an information system, one could use as many authentication factors as necessary. Even if we do not consider usability and cost aspects, this solution increases also the risk that a hacker could duplicate one authentication data. This could be an important problem for further accesses of the information system. For passwords, if you know a hacker has stolen it, it is quite simple to change it. For a fingerprint, it is not possible to change it (you have to change the used finger), but, there is a cancelable biometrics as alternative solutions. Moreover, most of time, you do not necessary know that your authenticator is compromised.

As a conclusion, all authentication methods such as password, token, biometric features and others have their own advantages and disadvantages. However, biometrics are the solutions the fact that it is the only method to authenticate the user, or the mobile phone's owner. . . .

Acknowledgements

The gratitude goes to The Ministry of Higher Education (MOHE) Malaysia whom had financially supported this work. The authors would also like to express their cordial thanks to GREYC Laboratory, ENSICAEN, France and Universiti Malaysia Perlis (UniMAP), Malaysia for the supports and had made this paper possible for publication.

References

D. Bhattacharyya, R. Ranjan, Farkhod Alisherov A., and M. Choi. Biometric authentication: A review. *International Journal of u- and e- Service, Science and Technology*, 2(3):13–27, September 2009.

P. Bours. Continuous keystroke dynamics: A different perspective towards biometric evaluation. *Information Security Technical Report*, 2012. ISSN 1363-4127. doi: 10.1016/j.istr.2012.02.001. In Press, Corrected Proof.

P. Bours and H. Barghouthi. Continuous authentication using biometric keystroke dynamics. In *The Norwegian Information Security Conference (NISK) 2009*, 2009.

W. E. Burr, D. F. Dodson, and W. T. Polk. Electronic authentication guideline. In *Recommendations of the National Institute of Standards and Technology, NIST SP 800-63, Version 1.0.2*, April 2006.

B. R. Cha and C. W. Kim. Password generation of otp system using fingerprint features. In *2008 International Conference on Information Security and Assurance*, page 243247. Springer, 2008.

F. Chabaud and O. Grumelard. Authentication, a model of human machine authentication. In *workshop European Network and Information Security Agency (ENISA)*, 2006.

J. Daemen. Permutation-based symmetric cryptography, December 2012. Passwords 12 Conference, 3 - 5 December 2012, University of Oslo, Norway.

B. Davaanaym, Y.S. Lee, H.J. Lee, S.G. Lee, and H.T. Lim. A ping pong based one-time-passwords authentication system. In *2009 Fifth International Joint Conference (NCM '09) on INC, IMS and IDC*, pages 574–579. IEEE Computer Society, 2009.

R. Giot, M. El-Abed, and C. Rosenberger. Greyc keystroke: a benchmark for keystroke dynamics biometric systems. *IEEE Computer Society*, 2009.

R. Giot, M. El-Abed, and C. Rosenberger. Keystroke dynamics overview. In Dr. Jucheng Yang, editor, *Biometrics / Book 1*, volume 1, chapter 8, pages 157–182. InTech, July 2011. URL `http://www.intechopen.com/articles/show/title/keystroke-dynamics-overview`.

V. Goyal, A. Abraham, S. Sanyal, and S. Y. Han. The n/r one time password system. In *Proceedings of the International Conference on Information Technology: Coding and Computing (ITCC05)*, volume 1, pages 733–738, 4-6 April 2005.

A. Jain, R. Bolle, and S. Pankanti. *Introduction to Biometrics: Personal Identification in Networked Society*. Kluwer Academic, Boston, MA, 1999.

A.K. Jain, S.C. Dass, and K. Nandakumar. Soft biometric traits for personal recognition systems. In *Proceedings of International Conference on Biometric Authentication,*, 2004.

A. Josang. Weak and strong passwords: When to use them, and how to protect them, December 2012. Passwords 12 Conference, 3 - 5 December 2012, University of Oslo, Norway.

P. Kotzanikolaou and C. Douligeris. *Network Security Current Status and Future Directions*, chapter Computer Network Security: Basic Background and Current Issues. 2007.

L. Lamport. Password authentication with insecure communication. *Communications of the ACM*, 24(11):770–772, 1981.

K. C. Liao, M. H. Sung, W. H. Lee, and T. C. Lin. A one-time password scheme with qr-code based on mobile phone. In *2009 Fifth International Joint Conference on INC, IMS and IDC*, pages 2069–2071. IEEE Computer Society, 2009.

J. Mahier, M. Pasquet, C. Rosenberger, and F. Cuozzo. *Biometric authentication*, chapter Encyclopedia of Information Science and Technology. 2nd edition, 2008.

W. McQuay and W. W. Smari, editors. *Security in Computing and Networking Systems: The State-of-the-Art (Textbook)*, chapter 27 - An Overview on Biometric Authentication, pages 1–22. 2009.

A. Mehler and S. Skiena. Improving usability through password-corrective hashing. In *SPIRE 2006, LNCS 4209*, pages 193–204, 2006.

A. Menezes, P. Van Oorschot, and S. Vanstone. *Identification and Entity Authentication*, chapter 10: Handbook of Applied Cryptography. 1996.

A. Messerman, T. Mustafic, S.A. Camtepe, and S. Albayrak. Continuous and non-intrusive identity verification in real-time environments based on free-text keystroke dynamics. In *Biometrics (IJCB), 2011 International Joint Conference on*, pages 1–8. IEEE, 2011.

E. Newham. The biometric report, 1995. URL `http://www.sjb.com`.

M. S. Obaidat and B. Sadoun. *Keystroke Dynamics*, chapter 10 - Keystroke Dynamics Based Authentication. 1998.

I. Park, S. Park, and B. Oh. User authentication protocol based on human memorable password and using rsa. In *A. Lagana et al. (Eds.): ICCSA 2004, LNCS 3046*, pages 698–707, 2004.

A. Parris-Long. Safer internet day: Why every generation has a role to play in keeping the web secure, Retrieved on 10 February 2012. Yahoo! News.

S. Prabhakar, S. Pankanti, and A. K. Jain. Biometric recognition: security and privacy concerns. *IEEE Journals on Security & Privacy*, 1(2):33–42, 2003.

N. Ratha, J. Connell, and R. Bolle. Enhancing security and privacy in biometricsbased authentication systems. *IBM System Journal*, 40(3):614634, 2001.

M.A. Sasse, S. Brostoff, and D. Weirich. Transforming the weakest link ? a human/computer interaction approach to usable and effective security. *British Telecom Technology Journal*, 19(3):122–131, 2001.

S. J. Simske. Dynamic biometrics: The case for a real-time solution to the problem of access control, privacy and security. In *Paper presented at IEEE BIdS Conference*, Tampa, Florida, Sept 22-23 2009.

W. Stallings and L. Brown. *Computer Security: Principles and Practice*. Pearson Prentice Hall, United States of America, 2008.

X. Suo, Y. Zhu, and G. S. Owen. Graphical passwords: A survey. In *21st Annual Computer Security Applications Conference (ACSAC)*, pages 5–9, 2005.

S. Z. Syed Idrus. Database encryption for a web-based claims system. Master's thesis, School of Computer and Communication Engineering, Universiti Malaysia Perlis, Perlis, Malaysia, 2008.

S. Z. Syed Idrus, S. A. Aljunid, S. M. Asi, S. Sudin, and R. B. Ahmad. Performance analysis of encryption algorithms text length size on web browsers. *International Journal of Computer Science and Network Security*, 8(1):20–25, 2008.

S. Z. Syed Idrus, A. Z. Rozali, and H. Desa. The development of a web-based claims system. In *Proceedings of the 2009 International Conference on Computer Technology and Development*, volume 1, pages 317 – 321, Sabah, Malaysia, 13-15 November 2009. IEEE Computer Society.

S. Z. Syed Idrus, S. A. Aljunid, S. Mohd Asi, and S. Sudin. Performance evaluation of encryption algorithms' key length size on web browsers. *IJCSNS International Journal of Computer Science and Network Security*, 12(5):10–13, 2012a.

S. Z. Syed Idrus, E. Cherrier, C. Rosenberger, and P. Bours. A preliminary study of a new soft biometric: Finger recognition for keystroke dynamics. In *9th Summer School for Advanced Studies on Biometrics for Secure Authentication: Understanding Man Machine Interactions in Forensics and Security Applications*, June 11-15 2012b.

S. Z. Syed Idrus, E. Cherrier, C. Rosenberger, and P. Bours. Soft biometrics for keystroke dynamics. In *International Conference on Image Analysis and Recognition (ICIAR)*, June 26-28 2013.

A. Turing. Computing machinery and intelligence. *Journal Mind*, pages 433–460, 1950.

U. Uludag, Pankanti S., S. Prabhakar, and A. K. Jain. Biometric cryptosystems: issues and challenges. In *Proceedings of the IEEE 92*, page 948960, 2004.

Wikipedia. Biometrics, 2011a. URL `http://en.wikipedia.org/wiki/Biometrics`.

Wikipedia. Biometric passport, 2011b. URL `http://en.wikipedia.org/wiki/Biometrics`.

J. D. Woodward. Biometrics: Privacys foe or privacys friend? *Journal of IEEE*, 85(9):1480–1492, 1997.

J. Yang, editor. *Biometrics*. InTech, 2011.

J. Yang and L. Nanni, editors. *State of the art in Biometrics*. InTech, 2011.