

## Multi-factor Authentication and their Approaches



Saroj Singh <sup>a</sup>

### Article history:

Received: 2 November 2016

Accepted: 30 March 2017

Published: 31 May 2017

### Keywords:

*authentication;*

*entropy;*

*inherence;*

*possession;*

*supplemental guidelines;*

### Abstract

A multi-factor authentication is an approach to authentication which requires the presentation of two or more of the three authentication factors: a knowledge factor ("something the user knows"), a possession factor ("something the user has"), and an inherence factor ("something the user is"). Two-factor authentication seeks to decrease the probability that the requestor is presenting false evidence of its identity. In reality, there are more variables to consider when establishing the relative assurance of truthfulness in an identity assertion than simply how many "factors" are used. The U.S. Federal Financial Institutions Examination Council issued supplemental guidance on this subject in August 2006, in which they clarified, "By definition true multifactor authentication requires the use of solutions from two or more of the three categories of factors.

2395-7492© Copyright 2017. The Author.

This is an open-access article under the CC BY-SA license

(<https://creativecommons.org/licenses/by-sa/4.0/>)

All rights reserved.

### Author correspondence:

Saroj Singh,

Department: CSE

Applied College of Management & Engineering Mitrol, Palwal (MDU)

Email address: [sarojraj47@gmail.com](mailto:sarojraj47@gmail.com), [acme.singh10@gmail.com](mailto:acme.singh10@gmail.com)

### 1. Introduction

Ting & LaRoche (2015), Ekstrom & Harman (1976), multi-factor authentication (also Two-factor authentication, TFA, T-FA or 2FA) is an approach to authentication which requires the presentation of two or more of the three authentication factors: a *knowledge* factor ("something the user *knows*"), a *possession* factor ("something the user *has*"), and an *inherence* factor ("something the user *is*").

<sup>a</sup> Department: CSE, Applied College of Management & Engineering, Mitrol, Palwal (MDU)



Singhal (2012), Owen & Shoemaker (2008), two-factor authentication is commonly found in electronic computer authentication, where basic authentication is the process of a requesting entity presenting some evidence of its identity to a second entity.

Using multiple solutions from the same category Two-factor authentication is often confused with other forms of authentication. Two-factor authentication requires the use of two of the three authentication factors. The factors are identified in the standards and regulations for access to U.S. Federal Government systems. These factors are:

- a) Something the user knows (e.g., password, PIN, pattern);
- b) Something the user has (e.g., ATM card, smart card); and
- c) Something the user is (e.g., biometric characteristic, such as a fingerprint).

When a bank customer visits a local automated teller machine (ATM), one authentication factor is the physical ATM card the customer slides into the machine ("something the user has"). The second factor is the PIN the customer enters through the keypad ("something the user knows"). Without the corroborating verification of both of these factors, authentication does not succeed. This scenario illustrates the basic concept of most two-factor authentication systems: the combination of a known factor and a possession factor.

#### 1) Regulatory definition

Details for authentication in the USA are defined with the Homeland Security Presidential Directive 12 (HSPD-12).<sup>[2]</sup> Existing authentication methodologies involve the explained three types of basic "factors". Authentication methods that depend on more than one factor are more difficult to compromise than single-factor methods.<sup>[1]</sup>

#### 2) Limitations

According to proponents, TFA could drastically reduce the incidence of online identity theft, and other online fraud, because the victim's password would no longer be enough to give a thief permanent access to their information. However, many TFA approaches remain vulnerable to man-in-the-browser and man-in-the-middle attacks.<sup>[3]</sup>

Bhargav-Spantzel *et al.*, (2007), in addition to such direct attacks, three aspects must be considered for each of the 2 (or more) factors in order to fully realize the potential increase in confidence of authentication:

- 1) The inherent strength of the mechanism, i.e. the entropy of a secret, the resistance of a token to cloning, or the uniqueness and reliability of a biometric.
- 2) Quality of provision and management. This has many aspects, such as the confidence one can have that a token or password has been securely delivered to the correct user and not an imposter, or that the correct individual has been biometrically enrolled, as well as secure storage and transmission of shared secrets, procedures for

password reset, disabling a lost token, re-enrollment of a biometric, and prompt withdrawal of credentials when access is no longer required.

- 3) Proactive fraud detection, e.g. monitoring of failed authentication attempts or unusual patterns of behavior which may indicate that an attack is under way, and suitable follow-up action.

## 2. Materials and Methods

After explaining research model, theory, technique of collecting the data, technique of analyzing the data, hypothesis research chronological, including research design, research procedure (in the form of algorithms, Pseudocode or other).

## 3. Results and Discussions

### 3.1 Knowledge Factors: "Something the User Knows"

Sabzevar & Stavrou (2008), knowledge factors are the most common form of authentication used. In this form, user is required to prove the knowledge of a secret in order to authenticate.

- 1) *Password*

Password is a secret word or string of characters that is used for user authentication. This is the most commonly used mechanism of authentication. Many two factor authentication techniques rely on password as one factor of authentication.

- 2) *PIN*

Personal identification number (PIN) is a secret numeric password and used in ATMs typically.

- 3) *Pattern*

Pattern is a sequence of cells in an array that is used for authenticating the users. e.g. Pattern based authentication is used in Android devices.

### 3.2 Possession factors: "something the user has"

Possession factors have been used for authentication for centuries, in the form of a key to a lock. The basic principle is that the key embodies a secret which is shared between the lock and the key, and the same principle underlies possession-factor authentication in computer systems.

There are several ways of attacking such a system, including:

- 1) An attacker can determine the shared secret, for example by attacking the authenticator or a management system,<sup>[4]</sup> reverse-engineering the possession factor, or intercepting the secret during authentication. In the case of a lock and key, the lock can be picked.<sup>[5]</sup> In an inadequately secured computer system, for example, a database containing the shared secrets can be attacked through **SQL injection**.
- 2) An attacker can steal the possession factor. In the case of a lock and key, the attacker can steal the key and use it before the rightful owner notices the loss and has the lock changed. In the case of a computer system, the attacker can steal the possession and use it before the rightful owner notices and has the device cancelled.
- 3) An attacker can copy the possession factor while it is inadequately safeguarded. An attacker can take an impression of a physical key and make a duplicate; and in the case of computer systems, can clone the possession factor.
- 4) The attacker can intercept the authentication process and masquerade as the authenticator to the party seeking authentication and vice versa, in a **man-in-the-middle attack**. In the case of the lock and key, the attacker can interpose a dummy lock that will allow them to make a copy of the key then later use the copy in the real lock. In the case of a computer system, the attacker can for example interpose a counterfeit authentication interface to intercept the communications and relay the authentication information between the legitimate user and the real authenticator.<sup>[6]</sup>
- 5) The attacker can hijack access after authentication. In the case of a lock and key, the attacker can wait until the owner of a key has opened the lock, and then gain access to the locked facility. In the case of a computer system,

the attacker can for example use **man-in-the-browser** malware, **session fixation**, or **Sidejacking** to gain access to a secured facility as soon as a legitimate user has logged in.

The security of the system therefore relies on the integrity of the authenticator and physical protection of the possession factor. Copy protection of the possession factor is a bonus. This may comprise some form of physical tamper resistance or tamper-proofing, it may use a challenge/response to prove knowledge of the shared secret whilst avoiding risk of disclosure, and it may involve the use of a pin or password associated with the device itself, independent of any password that might have been demanded as a first factor. A challenge/response will not defeat a **man-in-the-middle attack** on the current authentication session but will prevent the attacker from successfully reusing or replaying credentials.

The secret may simply be a number, large enough to make guessing infeasible or it may be a secret key embodied in an **X.509** certificate, supported by a **PKI**.

Many commercial and a few non-commercial solutions are available for providing the possession factor as described in the following sections. The system designer must consider various trade-offs, such as between the costs of deployment and support, usability and user acceptance, and hardware and software requirements. Physical tokens may authenticate themselves by electronic means (e.g. a USB port) or may display a number on a screen, derived from the shared secret and which the user has to type in. In the former case, device drivers may be required which the system designer may or may not be able to rely on if he has no control over the client device (as in the case of authentication to a public website). A one-time pad (such as PPP, described later) is a little different but can still be classed as a possession factor.

#### 1) Tokens with a display (disconnected tokens)



RSA SecurID token

A number of types of pocket-sized authentication token are available which display a changing passcode on an LCD or e-ink display, which must be typed in at an authentication screen, thus avoiding the need for an electronic connection. The number is derived from the shared secret by a cryptographic process which makes it infeasible to work out the secret from the sequence of numbers. Essentially, the secret is hashed or otherwise cryptographically combined with a challenge, and the result is displayed. The same process repeated on the authentication server will yield the same result if the correct secret was used. The challenge can take one of three forms:

- a) In a “sequence-based” token, the token may have a button that is pressed to switch it on and display a new passcode. The cumulative number of button pushes can be used as the challenge. The server, however, must assume that the button may have been pressed a number of times since the last actual use, and attempt the authentication with all likely numbers of button pushes.
- b) In a “time-based” token, the token generally contains a quartz time source, allowing the absolute time to be used as the challenge and a new passcode to be displayed (usually) every 30 or 60 seconds. In this case, the authentication server must allow for a drift in the time source by trying the authentication with a previous and subsequent time as well as the current time. It can hence keep track of the drift in the clock.
- c) The token may have a small keypad on which a challenge can be entered. This may either be a fixed PIN assigned to the user, or a challenge generated by the server and displayed at the authentication screen, or both.

Most such tokens have at least a basic level of copy protection in that it would take a certain level, perhaps a high level, of sophistication to extract the secret from the chip on which it is stored.

Display tokens have the advantage that no drivers or electronic interfaces are required on the user access device. Often, it is possible to arrange for the passcode from the display to be appended to a password in an existing password field, so that the only modifications required are in the authentication server. A disadvantage in some sectors is that the display is usually small, and may be difficult to read for visually impaired users.

There are several manufacturers of display tokens used to authenticate online transactions. These are generally designed as a key fob to be attached to a key ring or lanyard, or as a device that can conveniently be carried in a pocket or handbag.

Recently, it has become possible to take the electronic components associated with regular keyfob tokens and embed them in a credit card form factor. However, because card thickness (.79mm to .84mm) prevents traditional components or batteries from being employed, special polymer-based batteries must be used which have a much lower battery life than their traditional coin cell brothers, and an **e-ink** rather than LCD display is generally used. Additionally, low-power semiconductor components are necessary to conserve the power used during sleep and/or actual use of the product.

Disconnected tokens are vulnerable to man-in-the-middle attacks by virtue of the fact that they are physically disconnected from the authenticating entity. See Man-in-the-middle vulnerability explained below.

## 2) *Connected tokens*

In a corporate or enterprise environment where the user access device and its capabilities are known and any required device drivers may be deployed, a token with an electronic interface may be more convenient as there is no need to read and type a passcode from the device. The form factor of the electronic interface sets a minimum size, however much of the electronics can be miniaturized, and end-user resistance is not common. Some types require a device reader and maybe special device drivers, whereas others use an interface which is almost universally available such as USB. Even USB, however, may not be available on highly locked-down terminals such as thin clients, pads or kiosk systems.

Like display tokens, connected tokens embody a shared secret (either a long number or in some cases an X.509 certificate). This is normally interrogated by a challenge/response to avoid exposing it. Most types have at least some level of copy protection.

### a) *USB tokens*

A **USB** port is standard equipment on today's computers, and **USB tokens** generally have a large storage capacity for **login credentials**, and perhaps user data as well. However, they may be relatively costly to deploy and support, are vulnerable to theft and fraud, and have met user resistance.

Any USB memory device can be used as a token simply by storing a secret (possibly an X.509 certificate) on it, but then there is nothing to stop it from being copied. This can be prevented if the device is designed to present itself as an authentication device responding to a challenge/response protocol rather than as a storage device. The downside is that a special device driver may then be required.

### b) *Smartcards*

Smart cards are the same size as a credit card. Some vendors offer smart cards that perform both the function of a proximity card physical access device and network authentication. Users can authenticate into the building via proximity detection and then insert the card into their PC to produce network login credentials. In fact, they can be multi-purposed to hold several sets of credentials, as well as electronic purse functionality, for example for use in a staff canteen. They can also serve as ID badges.

In some countries, notably in Europe and Asia, banks and financial institutions have implemented Chip Authentication Program technology which pairs a banking smart card with an independent, unconnected card reader. Using the card, reader and ATM PIN as factors, a one-time password is generated that can then be used in place of passwords. The technology offers some support against transaction alteration by facilitating Transaction Data Signing, where information from the transaction is included in the calculation of the one-time password, but it does not prevent man-in-the-middle attacks or man-in-the-browser attacks because a fraudster who is in control of the user's internet or is redirecting the user to the legitimate website via a hostile proxy may alter the transaction data "in-line" before it arrives at the web-server for processing, resulting in an otherwise valid transaction signature being generated for fraudulent data.

As has already been indicated, there are two kinds of smart card: contact smart cards with a pattern of gold plated contacts, and contactless or proximity cards, with an RFID chip embedded within the plastic. The former is more often used in banking and as a 2nd factor and can be conveniently carried with other credit/debit/loyalty cards in a wallet. They are normally loaded with an X.509 certificate. However, they do need a special reader. Some laptops and thin client terminals have a smart card reader built in, and **PC Card** smart card readers are available which can be kept permanently within the shell of the laptop. Alternatively, USB smart card readers are available which are no more expensive than many display tokens, in fact, some smart cards have an interface which is electrically (but not mechanically) USB, so that the reader needs no intelligence whatsoever and

consequently can be very cheap. Even so, it is less convenient than a built-in or PCCard reader but is a good option for a desktop computer.

MS Windows has smart card authentication functionality built in, allowing authentication against a password and a smart card with no additional software apart from the smart card device driver (if needed). This can be configured to screen-lock the computer if the smart card is withdrawn. If the card also has a contactless chip used for physical access control, the user will be forced to lock his screen by withdrawing his smart card each time he leaves the office.

There have also been smart cards released over the last 5 years which employ a combination of an embedded 2FA token inside a credit card form factor. These "powered" smart cards typically consist of:

- 1] An ISO compliant credit card (ID-1) size
- 2] A flexible display
- 3] A switch-on button.
- 4] An embedded in rechargeable battery.

When the button is pressed, the card displays an OTP value, which is then typed by the user on his PC keyboard. On the remote application side, the OTP number is checked using the authentication server. The OTP number is calculated according to the OATH industry standard and using some secret data securely stored in the device.

Another concern when deploying smart cards, USB tokens, or other TFA systems is the security of the software loaded on to users' computers. A token may store a user's credentials securely, but the potential for breaking the system is then shifted to the software interface between the hardware token and the OS, potentially rendering the added security of the TFA system useless.

The downsides of smart cards include that they are not the smallest form factor (although they do fit conveniently in a wallet) and that the card reader is an extra expense. Another disadvantage is that they are less robust than most other forms of the token. Repeated flexing can damage both contact and contactless smart cards, and adverse climatic conditions can reduce the reliability of contact smart cards.

c) *Audio Port tokens*

Audio port tokens are usually used to provide authentication service for mobile terminals, because many different mobile manufacturers have various own interface, such as stock, micro USB, mini USB and etc. In contrast, the audio port is the most standard port on today's smart mobile terminals, and the audio port can be used for data transfer between authentication tokens and mobile terminals instead of the USB port. An audio port token usually has a built-in battery as a power supply for the tokens. It has the almost the same function as the USB tokens except for mobile terminal support, which is a digital certificate container with on-board encrypt/decrypt and sign/verify function.

d) *Wireless*

Contactless smart cards as described above can be used as a second factor. Other forms of RFID token can be used, as well as Bluetooth.

e) *Dallas iButton*



An iButton is a plastic fob, as used for Istanbul Akbil smart ticket

The Dallas iButton resembles a rather large button cell, with a very robust stainless steel case. It uses the Dallas 1-wire interface in which both power and bidirectional signaling utilize a single connection (together with a ground connection). It only has to be touched momentarily on a receptacle for the host device to read or interrogate it and so has found use particularly in conjunction with retail cash registers, allowing a sales assistant to instantly identify him/herself to the cash register.

Although not commonly used as a second factor in general purpose computer systems, it is offered as an option on the highest security versions of the Eclipt<sup>[7]</sup> self-encrypting hard disk.

f) *CASQUE*

CASQUE is an unusual hybrid connected token with a display. It incorporates a secure chip rated at EAL5+. It has an LCD display on the front and several photodiodes on the back, which are held up against several flashing squares displayed on the log-in screen. A challenge is communicated to the token by the pattern of flashing. This is then combined with a shared secret stored within the token to produce a passcode which is shown on the LCD display, for the user to type in. An advantage is that the challenge is based neither on a time nor a sequence, and so synchronization is not an issue. The Challenge/Response protocol also allows the Token's keys to be changed so resisting Token cloning attempts. The system also allows the User to ask for a specified phrase to be echoed on the Token allowing the User to authenticate the Host and so deny Phishing attempts.

g) *Magnetic stripe cards*

Magnetic stripe cards (credit cards, debit cards, ATM cards, loyalty cards, gift cards, etc.) are easily cloned and so are being or have been replaced in various regions by smart cards, particularly in banking. However, even though the data on the magnetic stripe is easily copied, researchers at Washington University in St. Louis have found<sup>[8]</sup> that the random and unique disposition of the billions of individual magnetic particles on each magnetic stripe can be used to derive a "magnetic fingerprint" which is virtually impossible to clone. This is an example of a physically unclonable function. Special magnetic card readers have been developed and commercialized under the name "Magneprint", which can digitize this fingerprint in order to positively identify an individual card.

An advantage of this system is that a magnetic fingerprint already exists on every magnetic stripe card, being an intrinsic characteristic, and so no cards would need to be re-issued in order to upgrade an existing system. Each swipe of the card provides a correlative number called a dynamic digital identifier that can be scored and "matched" to the originating value to determine the authenticity of the card. Since the number changes each time, it cannot be re-used as long as all processing is authenticated. It does require a special reader that can read the magnetic fingerprint value, but these readers can be swapped out incrementally as old readers wear down. So the actual investment could be incorporated as an incremental increase (due to licensing, increased equipment complexity, etc.) of current business cost expectations.

h) *Virtual tokens*

Virtual tokens are similar to a connected token, but with significant differences. Like connected tokens, virtual tokens are a physical device connected to the authenticating server, however, the connected device is the client computer or mobile device<sup>[9][10]</sup>, not a traditional hardware token. No hardware or software must be distributed to the end user. Virtual tokens use the user's existing device as the possession factor, reducing the costs normally associated with implementation and maintenance of security tokens. Processing occurs "server-side" and facilitates the retrieval of one-time-use digitally-signed keys and other information from a connected device using Internet-standard HTTP/HTTPS delivery methods. The retrieved key is then authenticated against the connecting device's digital fingerprint, the user's account details, and other data. Since the authenticating server is communicating directly with the connected device, the method is not as prone to man-in-the-middle attacks as other methods.<sup>[11][12]</sup>

i) *Soft tokens*

The functionality of any disconnected token can be emulated as a "soft token" on a PC or Smartphone using deployed software, whereupon that device itself becomes the possession factor. This saves on deployment costs, but against that, the secret is vulnerable to an attacker or malware that can gain full access to the device. The Zeus Trojan, which can now infect mobile devices running Android or BlackBerry OS, specifically targets<sup>[13]</sup> banking credentials and may forward them to the attacker at a website set up for the purpose, or by SMS messaging. Note: Soft tokens are fundamentally different from virtual token MFA in that "soft" tokens require the user to install software, while virtual token MFA does not.

The secret may comprise an SSL client certificate which can be used to authenticate the device (PC or Smartphone) on which it is stored, and may be used directly to authenticate the client in an SSL connection. Whilst stored on the device, even if held in a password protected certificate store, it is still potentially vulnerable to theft by malware as the certificate store has to be unlocked to be used. Indeed, the malware might trick the user into revealing the password or steal it by keystroke logging.

Such client certificates can be stored more securely in the TPM chip, fitted to many modern laptops. This is tamper-resistant and requires a password or passphrase to unlock it, and contains a cryptographic processor capable of challenge/response processing without divulging the secret.

### 3) *One-time pads*

A one-time pad is a password used only once. Schemes based on a one time pad have been described<sup>[14]</sup> but are rarely deployed due to the need to supply a new password (or 'pad') for each authentication.

Schemes which use a grid-card are not one-time pads and are akin to requesting a selection of characters from a password *known* by the user (albeit a password written down). As such, they only protect against replay attacks (as the same selection of characters can't be sent) and not against duplication of the entire grid (or the building up of a duplicate answer grid over time).

#### a) *UniOTP*

UniOTP is an event/time-based one-time password token with a robust plastic case. Its dust proof, waterproof, and anti-broken features ensure it can work under adverse circumstances, such as construction, military and etc. By clicking the button, the device will display a serial number as the dynamic password.

### 4) *Mobile phones*

There is presently only limited discussion on using wired phones for authentication; most applications focus on the use of mobile phones instead.

A new category of TFA tools transforms the PC user's mobile phone into a token device using SMS messaging, an interactive telephone call, or via downloadable application to a smartphone. Since the user now communicates over two channels, the mobile phone becomes a two-factor, two-channel authentication mechanism. Newer solutions making use of secret photographs to block phishing introduce a third layer of security, two-way (e.g.: mutual) authentication.

Recent examples include Google's two-step verification option<sup>[15]</sup> and CryptoPhoto.<sup>[16]</sup>

#### b) *Vulnerability to attacking*

Any authentication process which utilizes an insecure out-of-band method such as email data link or phone voice or data link or fails to provide mutual authentication, and is inherently vulnerable to **man-in-the-middle** (MITM) attacks. In a man-in-the-middle attack, a fraudster is actually interacting with the legitimate website, and the victim is interacting with the fraudster's counterfeit website. A victim who is lured to a fraudulent website then triggers the attack by entering the normal login credentials on the counterfeit website. The counterfeit website then transmits these stolen credentials to the legitimate website using scripts or other protocols and the legitimate website then initiates a telephone call to the victim. Believing the website to be legitimate, the victim pushes the appropriate buttons on the phone, not realizing that doing so permits the fraudster to complete entry into the victim's account for complete access.

#### c) *Assignment to the bearer*

One basic limitation associated with relying exclusively on mobile phones for secondary authentication is the fact that the respective user must have access to a mobile phone during authentication. The user may have registered a mobile phone number, for example, and when attempting to authenticate from home, must have access to that registered mobile phone. That converts the mobile phone from an office appliance to a personal appliance for usage out of the premises. However, as soon as the mobile phone gets lost, the bearer loses physical control over the mobile authentication factors.

#### d) *SMS one-time password*

SMS one-time password uses information sent in an SMS to the user as part of the login process. One scenario is where a user either registers (or updates) their contact information on a website. During this time the user is also asked to enter his or her regularly used telephone numbers (home, mobile, work, etc.). The next time the user logs in to the website, they must enter their **username** and password; if they enter the correct information, the user then chooses the phone number at which they can be contacted immediately from their previously registered phone numbers. The user will be instantly called or receive an SMS text message with a



unique, temporary PIN code. The user then enters this code into the website to prove their identity, and if the PIN code entered is correct, the user will be granted access to their account. This process provides an extra layer of online security beyond merely a username and password. These solutions can be used with any telephone, not just mobile devices.

As with any out-of-band authentication method, SMS one-time password methods are also vulnerable to man-in-the-middle attacks. They are also vulnerable to mobile number porting attacks. In this scenario, an attacker tricks a mobile provider into transferring a victim's mobile number to a new account under the attacker's control. Any SMS messages or calls sent to the victim's mobile number will instead be sent only to the attacker. The victim may be unaware of the attack until the victim notices their cell phone is no longer working or is no longer assigned the same mobile number.<sup>[17]</sup>

e) *Smartphone push*

The push notification services offered by modern mobile platforms, such as iPhone's APNS and Android's C2DM/GCM, can be used to provide a real-time challenge/response mechanism on a mobile device. Upon performing a sensitive transaction or login, the user will instantly receive a challenge pushed to their mobile phone, be prompted with the full details of that transaction, and be able to respond to approve or deny that transaction by simply pressing a button on their mobile phone. Smartphone push two-factor authentication has the capability to not only be more user-friendly but also more secure as a mutually-authentication connection can be established to the phone over the data network.

f) *Additional phone token*

There is a newer method of using the mobile phone as the processor and having the Security Token reside on the mobile as a Java ME client. This method does not include data latency or incur hidden costs for the end user. While this method can simplify deployment, reduce logistical costs, and remove the need for a separate hardware token devices, there are numerous trade-offs.

Users incur fees for text/data services or cellular calling minutes. In addition, there is a variable latency involved with SMS services, especially during peak SMS usage periods like holidays. Finally, as with telephone-based processes, these processes are also vulnerable to MITM attacks, such as a victim unwittingly supplying login credentials to a counterfeit website. The counterfeit website passes these to the legitimate website using scripts or other protocols. The legitimate website then initiates an SMS text message delivery of a one-time-password to the victim's mobile device or simply waits for the Java token value to be generated. The victim enters the one-time-password onto the counterfeit website, which then forwards this to the legitimate website, where the waiting fraudster uses it to complete the fraudulent access.

g) *Mobile signature*

Mobile signatures are digital signatures created on a SIM card securely on a mobile device by a user's private key. In such a system text to be signed is securely sent to the SIM card on a mobile phone. The SIM then displays the text to the end-user who checks it before entering a PIN code to create a signature which is then sent back to the service provider. The signature can be verified using standard PKI systems.

Mobile Signature systems have been in use for several years. However, as with magnetic card and client digital certificate solutions, they are vulnerable to malware, are costly to deploy and support, and are strongly resisted by consumers.

h) *Mobile applications*

Smartphones and tablets can use a dedicated mobile device application for secure access to online services. The mobile device application uses the Web browser or Web service capabilities of the device for authentication and subsequent access to the service. This approach allows a cryptographic key to be used to authenticate the user, which protects against a man-in-the-middle attack.

### 3.3 Inherence factors: "something the user is"

1) *Biometrics*



Figure 1. A human thumbprint - a common type of biometric data used in authentication

Biometric authentication also satisfies the regulatory definition of true multi-factor authentication. Users may biometrically authenticate via their fingerprint, voiceprint, or iris scan using provided hardware and then enter a PIN or password in order to open the credential vault. However, while this type of authentication is suitable in limited applications, this solution may become unacceptably slow and comparatively expensive when a large number of users are involved. In addition, it is extremely vulnerable to a replay attack: once the biometric information is compromised, it may easily be replayed unless the reader is completely secure and guarded. Finally, there is great user resistance to biometric authentication. Users resist having their personal physical characteristics captured and recorded for authentication purposes. In short, selection and successful deployment of a biometric authentication system need careful consideration of many factors.<sup>[18]</sup>

For many biometric identifiers, the actual biometric information is rendered into a string or mathematics information. The device scans the physical characteristic, extracts critical information, and then stores the result as a string of data. The comparison is therefore made between two data strings, and if there is sufficient commonality a pass is achieved. It may be appreciated that choice of how much data to match, and to what degree of accuracy, governs the accuracy/speed ratio of the biometric device. All biometric devices, therefore, do not provide unambiguous guarantees of identity, but rather probabilities, and all may provide false positive and negative outputs. If a biometric system is applied to a large number of users - perhaps all of the customers of a bank - the error rate may make the system impractical to use.

Biometric information may be mechanically copied and cannot be easily changed. This is perceived as a key disadvantage since, if discovered, the compromised data cannot be changed. A user can easily change his/her password, however, a user cannot change their fingerprint. A bio-identifier can also be faked. For example, fingerprints can be captured on sticky tape and false gelatine copies made, or simple photos of eye retinas can be presented. More expensive biometrics sensors should be capable to distinguish between live original and dead replicas, but such devices are not practical for mass distribution. It is likely that, as biometric identifiers become widespread, more sophisticated compromise techniques will also be developed.

Historically, fingerprints have been used as the most authoritative method of authentication. Other biometric methods such as retinal scans are promising but have shown themselves to be easily spoofable in practice. Hybrid or two-tiered authentication methods offer a compelling solution, such as private keys encrypted by fingerprint inside of a USB device.

A criticism of biometrics for authentication is that whereas it is relatively easy to calculate the strength of a password from its length and composition and hence the time to brute force it, the strength of a biometric is difficult to quantify. There can be no guarantee that a simple attack could not be devised tomorrow, for example by using household chemicals to make an artificial finger from a fingerprint, good enough to be accepted by a fingerprint reader. This is a concern to certain government security authorities where knowing the strength of a security mechanism is considered more important than having a mechanism which might be stronger but whose absolute strength is not quantifiable.

International travelers to many countries are now routinely required to provide fingerprint and/or iris scans to pass. This stockpile of records reduces the strength of biometric-protected resources (for example - those governments can now unlock your PC, decrypt your flash drives, and/or impersonate you).

### 3.4 Challenge questions are not regulatory compliant

Following the U.S. Federal Financial Institutions Examination Council's (FFIEC) publication advising the use of multi-factor authentication, numerous vendors began offering authentication solutions that are not compliant with the FFIEC's definition of "true multifactor authentication". Most notable of these approaches is the challenge/response approach, often coupled with a shared secret image. Soliciting personal information in response to challenge questions simply solicits more of "something the user knows", similar to a login, a password, or a PIN. All are multiple solutions from the same authentication category. Unless these are combined with one of the other two factors (i.e. "something the user has" or "something the user is", it does not constitute multi-factor authentication.

Regulators have repeatedly cautioned against the use of approaches that operate through the solicitation of personal information. On June 17, 2005, the U.S. Federal Deposit Insurance Corporation (FDIC) published supplement guidelines in which it strongly cautioned financial organizations against adopting authentication methods that use personal information for authentication purposes:

"Although consumers are worried about phishing and the trustworthiness of e-mail messages from their banks, they are also concerned about the security of their personal information more generally....When banks consider authentication methods for retail customers, they should be aware that these customers value security and the protection of confidential information... Consumers will require a clear explanation of any security mechanism and the use of any personal information required to implement that security mechanism....limitations on the use of personal information and the existence of privacy safeguards are important elements of consumer acceptance....Consumers are also concerned about the risk associated with large databases of personal information and the potential for the information that is used by authentication methods to be compromised, copied, or imitated. - FDIC"

The FFIEC clarified their position in their August 15, 2006 FAQ Supplement, rejecting such approaches outright: "By definition, true multifactor authentication requires the use of solutions from two or more of the three categories of factors. Using multiple solutions from the same category ... would not constitute multifactor authentication. - FFIEC"

In September 2009, an Illinois district court issued a ruling allowing a couple to sue Citizens Financial Bank alleging that the bank failed to sufficiently secure their account with adequate multi-factor authentication security. (see Wired article) The judge in the case pointed to the FFIEC's guidelines and ruled, "In light of Citizens' apparent delay in complying with FFIEC security standards, a reasonable finder of fact could conclude that the bank breached its duty to protect Plaintiffs' account against fraudulent access."

### 3.5 Cost effectiveness

There are drawbacks to two-factor authentication that are keeping many approaches from becoming widespread. Some consumers have difficulty keeping track of a hardware token or USB plug. Many consumers do not have the technical skills needed to install a client-side software certificate.

As a result, adding a second factor to the authentication process typically leads to an increase in costs for implementation and maintenance. Most hardware token-based systems are proprietary and charge an annual fee per user in the \$50–100 USD range.<sup>[citation needed]</sup> Deployment of hardware tokens is logistically challenging. Hardware tokens may get damaged or lost and issuance of tokens in large industries such as banking or even within large enterprises needs to be managed.

In addition to deployment costs, two-factor authentication often carries significant additional support costs. A 2008 survey of over 120 U.S. credit unions by the *Credit Union Journal* reported on the support costs associated with two-factor authentication. In their report, software certificates and software toolbar approaches were reported to have the highest support costs while Virtual token MFA and geolocation solutions were reported to have the lowest support costs.

### 3.6 Market acceptance

As a result of challenges with integration and user acceptance, true two-factor authentication is not yet widespread, although it can be found in certain sectors requiring additional security (e.g. banking, military). Faced with regulatory two-factor authentication guidelines in 2005, numerous U.S. financial institutions instead deployed additional knowledge-based authentication methods, such as shared secrets or challenge questions, only to discover later that such methods do not satisfy the regulatory definition of "true multifactor authentication". Supplemental regulatory

guidelines and stricter enforcement are now beginning to force the abandonment of knowledge-based methods in favor of "true multifactor authentication".

A 2007 study sponsored by BearingPoint reported 94% of the authentication solutions implemented by U.S. financial institutions to fail to meet the regulatory definition of true multi-factor authentication.

An increasing count of recent undesired disclosure of governmentally protected data<sup>[19][20]</sup> or private data<sup>[21][22]</sup> is likely to contribute to new TF-A requirements, especially in the European Union.

#### 4. Conclusion

Several popular web services employ multi-factor authentication, usually as an optional feature that is deactivated by default.

- a) Two-factor authentication
- b) Many Internet services (among them: Google, Amazon AWS) use open Time-based One-time Password Algorithm (TOTP) to support multi-factor or two-factor authentication.

##### *Conflict of interest statement and funding sources*

The author(s) declared that (s)he/they have no competing interest. The study was financed by the author.

##### *Statement of authorship*

The author(s) have a responsibility for the conception and design of the study. The author(s) have approved the final article.


##### *Acknowledgments*

Nobody can do anything without the grace of God. I thanks to Lord "Krishna" and "OMKAR" who blessed me to achieve my ambition by writing this research paper named "**Multi-factor Authentication and their Approaches**". I am thankful to Almighty God for blessing me with the strength to face my situation with courage and patience. I extended my thanks to my dear husband who encourages me finished the task successfully on time. I also thanks to my parents for their inspiration and blessing.

**References**

- Ting, D. M., Hussain, O., & LaRoche, G. (2015). *U.S. Patent No. 9,118,656*. Washington, DC: U.S. Patent and Trademark Office.
- Ekstrom, R. B., Dermen, D., & Harman, H. H. (1976). *Manual for kit of factor-referenced cognitive tests* (Vol. 102). Princeton, NJ: Educational Testing Service.
- Bhargav-Spantzel, A., Squicciarini, A. C., Modi, S., Young, M., Bertino, E., & Elliott, S. J. (2007). Privacy preserving multi-factor authentication with biometrics. *Journal of Computer Security*, 15(5), 529-560.
- Singhal, T. C. (2012). *U.S. Patent No. 8,090,945*. Washington, DC: U.S. Patent and Trademark Office.
- Owen, W. N., & Shoemaker, E. (2008). *U.S. Patent No. 7,373,515*. Washington, DC: U.S. Patent and Trademark Office.
- Sabzevar, A. P., & Stavrou, A. (2008, November). Universal multi-factor authentication using graphical passwords. In *Signal Image Technology and Internet Based Systems, 2008. SITIS'08. IEEE International Conference on* (pp. 625-632). IEEE.

**Biography of Author**

	<p>BCA MCA A- Level B.tech M.tech</p> <p>Publication:</p> <p>Journals Name &amp; Name of the Publication</p> <p>‘Codes And Ciphers’ (IJARCS)</p> <p>Block Ciphers in Cryptography (IJARCS)</p> <p>Public Key Cryptosystems (IJARCS)</p> <p>System Identification &amp; Clustering (IJARCS)</p> <p>Security-Hash Function – Authentications (IRJEIS)</p> <p>IP Security (IJCU, IRJMIS)</p> <p>Kerberos (IJMRA, IJESR)</p> <p>Security: Telecommunication and Network Architecture (EURO ASIA-IJREAS)</p> <p>Email: <a href="mailto:sarojraj47@gmail.com">sarojraj47@gmail.com</a>, <a href="mailto:acme.singh10@gmail.com">acme.singh10@gmail.com</a></p>
---	--