INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH VOLUME 5, ISSUE 11, NOVEMBER 2016 ISSN 2277-8616

# A Review Of Authentication Methods

Nilesh A. Lal, Salendra Prasad, Mohammed Farik

**Abstract:** Authentication is process of granting a user access to an information system. There are three main types of authentication mechanisms – password entry, smart card, and biometric. Each authentication mechanism functions differently and has their strengths and weakness. In this paper we review different types of authentication mechanisms, their vulnerabilities, and recommend novel solutions.

**Index Terms**: authentication, biometrics, password, smart card, vulnerabilities

## 1 Introduction

Authentication is process of validating the user's identity. Users are identified using different authentication mechanisms. In a security system the authentication process checks the information provided by the user with the database [1], [2]. If the information matches with the database information, the user is granted access to the security system. There are three types of authentication mechanism used. Validation is the initial phase in access control, and there are three regular variables utilized for verification – something you know, something you have, and something you are [2]. *Something you know* mostly requires individual to get access to the system by typing the username and password. *Something you have* is where the user uses smart card for authentications [1] [2]. *Something you are* is where the user using biometrics methods to get access control. All types of authentication mechanisms allows user to get access to the system however they all work differently. There are many authentications methods developed for users to gain access to the system. In password authentication, there are two forms – weak password and strong password authentications. *Access control* allows the user to log in into the trusted sites of an organization [1]. Every access control has four processes – identification, authentication, authorization, and accountability. The identification is when the user enters the ID and ID is checked with the security system. Some security system generates random IDs to protect against the attackers. There are three authentication processes. Authorization is checking and matching the authenticated entity of information with access level. The authorization process is handled three ways – authorization is performed for authenticated user, authorization is performed for members of the group, authorization is performed across the multiple systems, and accountability is a process keeping system logs. Systems logs keep track of all successful and unsuccessful logins [1], [2], [3].


- *Nilesh Arvind Lal is a postgraduate student in Information Technology in University of Fiji. E-mail: nileshlal@rocketmail.com*
- *Salendra Prasad is a postgraduate student in Information Technology in University of Fiji. E-mail: salen_prasad@yahoo.com*
- *Mohammed Farik is a Lecture in Information Technology in the School of Science and Technology at the University of Fiji Email: mohammedf@unifiji.ac.fj*


## 2 Types of Authentications

### 2.1 Password Authentication

This type of authentication requires the supplicant recall what he knows. There are two parts in this method. First, the supplicant enters the username and second, the password. The password is the secret combination of words and numbers which the supplicant knows.

#### 2.1.1 Strength of Password Authentication

One of the strength is that longer password is very difficult to break. At the point when utilizing passwords, it's imperative to utilize solid passwords. A solid secret key has a blend of capitalized, lower case, numbers, and unique characters. Now security administrators recommend 12 characters passwords. A 12 characters password with 94 cardinality and 78.7 bits entropy will take 55 days to crack using super computers. And using PC it will take 3018 years to crack. Online site such as *PasswordStrengthCalculator.org* can be used to test the strength of a password [4].

#### 2.1.2 Password Authentication Vulnerabilities

Password sniffing is the biggest problem since when the user enters the password (Fig.1). An attacker can sniff the password at different stages of communication. Even if the password is strong, it can easily be known to the attacker [3]. A key problem with user name and password, the human factor [2]:

- passwords are easy to guess or search if easy to remember
- passwords are easily stolen if written down
- users may share passwords
- passwords can be forgotten if difficult to remember

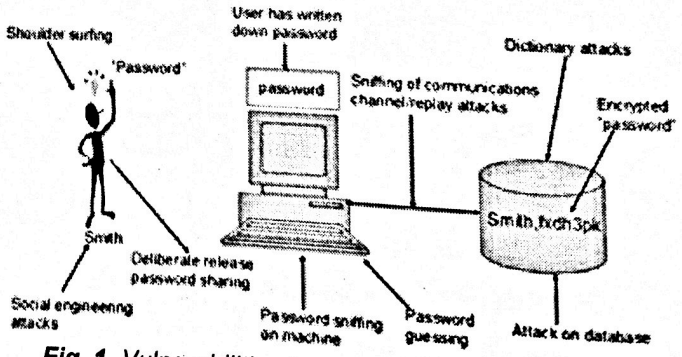


*Fig. 1. Vulnerabilities in password authentication [2]*

With weaker password, the attackers will be able to hack the system easily using the brute force method. Most access control accepts the password of eight character length. There

are three factors that determine the strength of the password – length, cardinality and entropy. A cardinality of 94 means the password has been created from a pool of 94 characters including uppercase, lower case, numbers and special characters. Entropy is the calculated strength of the password in bits. For example, a password of eight character length, with a cardinality of 94 is equivalent to entropy of 52.4 bits. A normal PC will able to crack the 94 cardinality password in 20 minutes using brute force. Using super computers, it will take 0.07 seconds to crack. Hence a entropy of 52.4 bits or 8 character length is a weak password. Social engineering is another drawback since it lures users to another site where the attackers collect personal information including the passwords and username [3].

#### 2.1.3 Recommended Solution

The best recommendation is to use stronger password. The users need to enter stronger password that is 12 character-length, with 94 cardinality. The users should be careful not to enter personal information or a word from the dictionary. For shoulder sniffing, shield paperwork or your keypad from view by using your body or cupping your hand. To avoid social engineering, avoid suspicious unsolicited phone calls and emails. Pay special attention to suspicious URLs. Install antivirus software's and firewalls. Another solution could be using graphical password which will be more secure compared to text based password. In text based password, the user attempt to memorize the password. Graphical password authenticate is done by selecting series of images [2], [3], [4]. For better security, number of attempts in password entry should be restricted.

### 2.2 Smart Card Authentication

#### 2.2.1 Strength of Smart Card Authentication

Smart Card authentication is *'something a user has'* factor. A smart card is a credit-card sized card that has an embedded certificate used to identify the holder (Fig. 2.). The user can insert the card into a smart card reader to authenticate the individual [2], Smart cards are commonly used with a PIN providing multi-factor authentication. In other words, the user must have something (the smart card) and know something (the PIN) [2], [5].

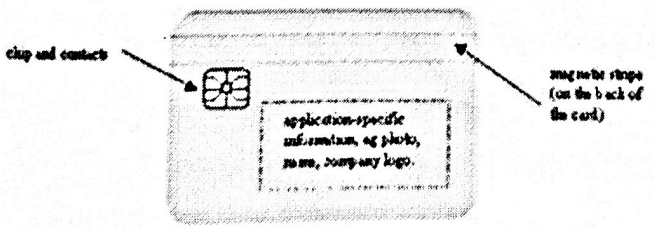

*Fig. 2. Credit card size hardware token [2]*

One of the strength with smart card is that it comes with two varieties. Firstly it comes with memory card with store data with provides two factor authentication. Secondly it comes with microprocessor making it stronger two factor authentication. The smart card with microprocessor stores public and private key certificate. The smart card is locked if Pin is entered incorrectly after number of attempts. Smart card prevents dictionary attacks. It is portable and can be easily carried by users [2], [6].

#### 2.2.2 Vulnerabilities with Smart-Card Authentication

Some of the draws using the smart card is that some users find it difficult to remember the PIN and they enter the Pin at the back of the card. If the card is stolen it can easily be attacked. Smart card can be locked after certain number of incorrect attempts. Since it is portable it can also be stolen. Some users who frequently purchase online can be victim of Phishing. Sometimes PIN can be known by shoulder surfing [1], [7], [4] .

#### 2.2.3 Recommended Solution

The solution to the above problem could be the card must be kept at close hand and not to be shared with others. For shoulder sniffing, shield paperwork or your keypad from view by using your body or cupping your hand. The best way to avoid phishing is not to reveal secrets [6] Turn on SSL client authentication to prevent phishing. Educate users to check for the SSL lock and not accept unrecognized certificates—but don't rely on education alone to solve the problem Another solution could be combining smart cards with RFID (Radio Frequency Identification). Also, combing two-factor authentication (smart cards and biometrics) enhance security [2]. Number of PIN entry attempts should be restricted.

### 2.3 Biometric Authentication

#### 2.3.1 Strength of Biometric Authentication

Biometric methods provide the *something you are* factor of authentication (Fig. 3.). Biometrics user authentication is a method that identifies a user and/or verifies their identity based on the measurement of their unique physiological traits or behavioral characteristics. Physiological biometrics is fingerprint, facial recognition, iris-scan, hand geometry, retina scan. Behavioral biometrics is voice recognition, gaits, keystroke-scan, and signature-scan (Fig.4.) [2], [8]. Fingerprints and handprints are the most widely used biometric method in use today. Many laptops include fingerprint readers and fingerprint readers are also available on USB flash drives.

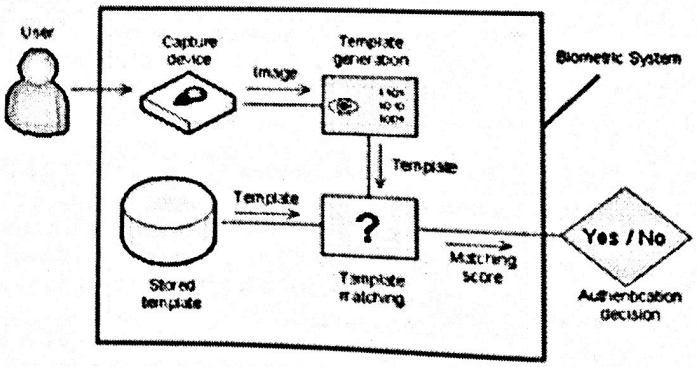


*Fig. 3. Biometrics processes [2]*

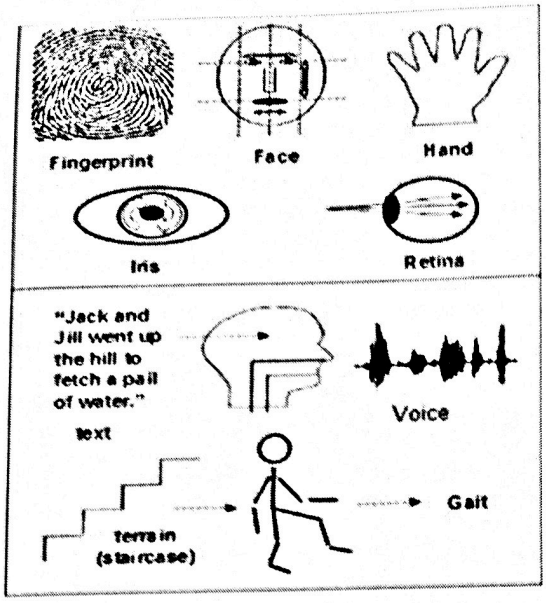


*Fig. 4. Different Biometrics Authentications [2]*

Biometric authentications are widely used and have much strength:

- Relieve user of difficult task of recalling passwords.
- Biometric is unique and is simple.
- Very difficult to replicate biometric feature.
- Biometric characteristics cannot be lost.
- Biometric is used at major places such as at airports, immigrations purpose and at prisons.
- Fingerprint scan is small and inexpensive.
- Can be used over the phone lines.
- Eye scan are accuracy in identifying users [2], [8].

The most common biometric is finger print scanner (Fig. 5.). The fingerprint scanner identifies the image on the user's finger and then matches with the data in the database. Every user has different finger pattern characteristics. When the user's finger-print pattern is saved in the database, the system covert it to into binary [2], [6], [8].

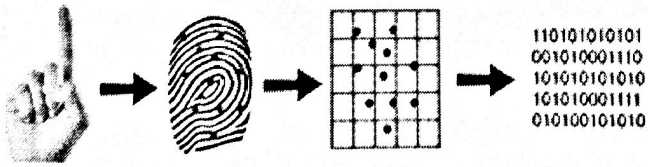


*Fig. 5. How the finger print scanner works [8]*

### 2.3.2 Vulnerabilities with Biometric Authentication

A fingerprint scan is very secure since it's hard to guess the fingerprint pattern. While biometrics does provide the strongest authentication, it is susceptible to errors. A false rejection error (also called type 1 error) occurs when a system falsely rejects a known user and indicates the user is not known [2]. A false acceptance error (also called a type 2 error) occurs when a system falsely identifies an unknown user as a known user. Biometric systems typically can be adjusted for sensitivity, but the sensitivity affects the accuracy. Another problem is no real standard because of vendor specific formats. Also there are user acceptance problems since user may feel criminal when their fingerprint scan is taken. Also injury on fingers can interfere with the scanning process [2].

### 2.3.3 Recommended Solution

Biometrics authentication reduces human factors. But still it has Error 1 and Error 2 authentication problems. The best solution could be combining different biometrics will solve the authentication problems. Also DNA identification could be another solution [2].

## 2.4 Digital Certificate Authentication

### 2.4.1 Strength of Digital certificate Authentication

A digital certificate is an encryption technology that works similar to the Internet version of a passport [9]. Using public key and private key information, digital certificates essentially ensure to the recipient of a message that the message is coming from a specific person [2]. The digital certificate authenticates the identity of the sender to ensure safer communication and prevent fraud on the Internet. The biggest advantages of digital certificate-based authentication are privacy-based [2]. By encrypting your communications — emails, logins or online banking transactions — digital certificates protect private data and prevent the information from being seen by unintended eyes. Digital certificate systems are also user-friendly, usually working automatically and requiring minimal action or involvement from either senders or recipients [2].

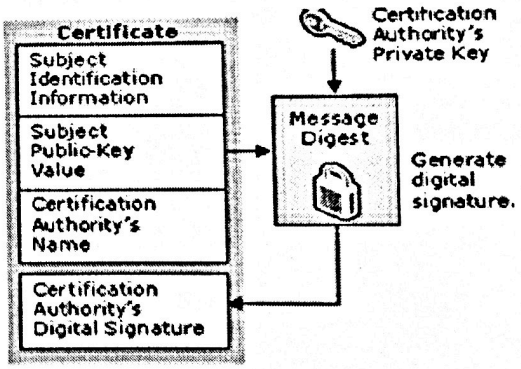


*Fig. 6 Digital Certificate authentication [6]*

### 2.4.2 Vulnerabilities with Digital Certificate Authentication

The authorities that issue digital certificate are attacked by intruders and the certificate information is changed. Attackers create a phishing site and send emails and web sites that look like original and pass the verification test [9], [2].

### 2.4.3 Recommended Solution

The best solution is that the Digital Certificate authorities need to update their software to keep the security threat to minimum. Also placing digital certificate on token will provide stronger security [2].

## 3 Conclusion

Authentication, whether it is password, smart card, or biometric, is an important process in any information system. Password should be at least 12 character long and of 94 cardinality. Smart cards are used together with PIN numbers. Both passwords and PIN should be controlled with limited attempts. Biometrics is the most secured authentication system. Even though fingerprint is very secure, it also has some weakness that need to be addressed in the future. Hence, multiple biometric or a combination of factors can help provide better authentication security. Digital certificates can also be incorporated in today's authentication systems for stronger security.

## References

[1] Webopedia, "Authentication," 2016. [Online]. Available: http://www.webopedia.com/TERM/A/authentication.html. [Accessed 1 Oct 2016].

[2] H. Abie, "semanticscholar," 12 12 2006. [Online]. Available: https://pdfs.semanticscholar.org/3733/2607f7a7ac8284c514845957fd00583e5614.pdf. [Accessed 1 October 2016].

[3] Wikipedia, "Social engineering (security)," [Online]. Available: https://en.wikipedia.org/wiki/Social_engineering_(security). [Accessed 1 October 2016].

[4] M. Farik, "Algorithm to Ensure and enforce Brutce force attack resilient password in routers," Algorithm to Ensure and enforce Brutce force attack resilient password in routers, vol. 4, no. 10, p. 5, 2015.

[5] wikipedia, "Multi-factor authentication," 2005. [Online]. Available: https://en.wikipedia.org/wiki/Multi-factor_authentication. [Accessed 1 October 2016].

[6] B. Schneier, "Schneier on Security," 2010. [Online]. Available: https://www.schneier.com/blog/archives/2010/02/man-in-the-midd_1.html. [Accessed 1 October 2016].

[7] M. McDowell, "US-CERT," 22 October 2009. [Online]. Available: https://www.us-cert.gov/ncas/tips/ST04-014. [Accessed 3 October 2016].

[8] bioelectronix, "Biometric Security," [Online]. Available: http://www.bioelectronix.com/what_is_biometrics.html. [Accessed 1 October 2016].

[9] H. Spector, "Techwalla," 2016. [Online]. Available: https://www.techwalla.com/articles/what-are-the-advantages-disadvantages-of-a-digital-certificate. [Accessed 1 October 2016].