Security Gaps In Authentication Factor Credentials

Neeraj A. Sharma, Mohammed Farik

Abstract: Authentication factors refer to user login credentials that a user supplies to an authentication process for it to decide whether to grant or deny access. While two-factor and three-factor authentication generally provides better security than one-factor authentication, the aim of this paper is to review, security in individual authentication factor credentials that are in use nowadays. These credentials will be discussed in factor categories – knowledge factor, possession factor, and inherence factor. The paper details current security gaps and some novel approaches to diminish the gaps in these authentication factors. We believe that our recommendations will inspire development of better authentication credentials and systems.

Index Terms: Authentication, Biometrics, Cards, Passwords, PIN, Retinal Scan

1 Introduction

THE term authentication is the procedure of identifying if someone or something is in fact what they are stating to be [1], [2]. Authentication credentials can be categorized as what you know (knowledge factor), what you have (possession factor), what you are (inherence factor), and the latest, where you are (location factor). 'What you know' factor refers to use of credentials such as passwords, pass codes, and pin numbers. 'What you have' factor refers to credentials you have such as physical keys and cards [1], [2]. 'What you are' factor refers to biometric credentials such as fingerprint, hand- geometry, retina, voice and signature scans. 'Where you are' factor refers to ones' current physical location [1], [2]. It is well known that two-factor and three-factor authentication generally provides better security than one-factor authentication. Our aim in this paper is to review, security of individual authentication factor credentials to improve credentials in whatever factor, they may be used in one-factor, two-factor, or three-factor. These credentials will be discussed in factor categories – knowledge factor, possession factor, and inherence factor. The paper details current security gaps in these credentials and recommends some novel approaches to diminish the gaps. We believe that our recommendations will inspire development of better authentication credentials and systems. So, in section 2, we discuss the types of authentication factors, in section 3, the gaps in authentication credentials, in section 4, novel recommendations, and conclusion in section 5.

2 Types Of Authentication Factors

People use different authentication factors and credentials, which are detailed in this section.

- *Neeraj A. Sharma is currently pursuing Master's Degree program in Information Technology at The University of Fiji. E-mail: neerajs@unifiji.ac.fj*
- *Mohammed Farik is a Lecturer in Information Technology at The University of Fiji. E-mail: mohammedf@unifiji.ac.fj*

2.1 Knowledge Factor

2.1.1 Password

Passwords are words, numbers or a combination of both that is required to access something. In other words, passwords are secrets that are provided by the clients whenever it is requested. This is something that the user knows. Passwords are the most common sort of user authentication and require a high level of memorability from the user to store a combination of the word [3]. For example, TH15@P@55W0RD. Passwords are commonly used to log-on to computers/phones/tablets, and all operating systems have a built-in option that can allow the users to password protect their devices and disallow intruders, hence the easiest option when choosing authentication credentials.

2.1.2 Credit/Debit Card PIN

Credit card and Debit card PINs are important to whoever has these cards. Using the cards, the authorized person can withdraw money from it. Usually, there is a four number PIN, and it is convenient to use and easy to remember the PIN [3]. This is very similar to having a password for a computer/phone/tablet. The authentication process works in such a way that after attempting three wrong PINs the card will be captured and the owner or authorized person him/herself will need to go and retrieve the card from the bank.

2.1.3 Safe Combination

Safe combination is a very common sort of authentication credential where the user has to enter a numeric digit to open the safe and get the contents of the safe. This is very similar to passwords and PINs [3]. Users need to remember the combination codes in order to open the safe successfully.

2.2 Possession Factor

2.2.1 Magnetic Card

Magnetic cards are a type of card that is able to store some data in its iron-based particles also known as magnetic stripes. In order to make this authentication credential work, the users are required to swipe the cards in the card machine to get authorization [4]. This is mostly used in organizations that have office level accesses, some staffs may not be allowed in the next level or floor.

2.2.2 Smart Card

Smart Cards are the new trend of authentication credentials. It has a two-factor authentication process where it stores the

user identity and a PIN. This is physically carried by the user and is a much stronger way to authenticate users. The users are required to place the smart card in the cardholder and then press the PIN in the keypads. Once the user enters the PIN then it will access the stored identity in the card and start the authentication process [4]. Smart cards are portable, easy to use, lightweight, and most importantly, people are used to carrying cards nowadays.

2.2.3 Credit/Debit Card

Credit and debit cards are very similar to the magnetic cards. In order to withdraw money from it, users are required to take the card to the ATM machine and withdraw whatever amount they require. Some credit and debit cards require a PIN number and others do not. Some even allow the users to buy bills and shop online suing these cards [4]. If the PIN number and the card are correct, you will be authorized.

2.2.4 Memory Card

Nowadays, people prefer to keep things backed up in a memory stick or memory card. Some things that people backup are usually PIN numbers, passwords, important account details, etc. [5]. People do this because they tend to forget small things, having a backup is not a bad thing but actually, it is a very good thing, but we also need to keep these things safe.

2.3 Inherence Factor

2.3.1 Fingerprint

To get authorization users need to put one of the fingers, which is already authenticated, on the fingerprint scanner to verify the authentication process [6]. To register the users are required to input a series of three fingers just in case the skin is damaged on any one finger than the user can use the other choices [6]. This is a very secure authentication process since this is based on the user itself and he/she cannot give their authenticator to any other person.

2.3.2 Hand-geometry

Hand-geometry authentication is one of the oldest biometric recognition type and is the easiest to use [7]. The device utilizes a very simple idea of measuring and recording the thickness, length, width, and surface region of a person's hand while guided on a plate. The device captures both the top view and the side view of the hand in a picture format [7]. It is a very straightforward approach, if your hand matches the images of the top and side then access is granted, else, you are not allowed.

2.3.3 Retina

A retinal scan authentication is a biometric technique that uses the retinal pattern that is unique on a person's retina blood vessels [8]. The human retina is a thin tissue made out of neural cells that are situated in the posterior position of the eye. In view of the perplexing structure of the vessels that supply the retina with blood, every individual's retina is unique [8]. The system of veins in the retina is complex to the point that even indistinguishable twins do not share a comparative pattern.

2.3.4 Voice

Voice recognition is the type of an authentication credential that is the identification of a person from characteristics of voices also called voice biometrics. Usually, the users are required to say a common pass phrase or passwords to a microphone that will then try to identify the user [9]. This is another very effective way of authenticating and allowing only the authorized personals to access.

2.3.5 Face

The facial scan also known as face recognition is a kind of authentication credential that uses the spatial geometry to distinguish the features of a person's face. It is in the form of a computer visualization that is used to authentication a person [10]. A digital camera captures the image of a person than software locates the face in the images, which is also called face detection. Once the face is detected the software analyzes the spatial geometry where the features of the face will be extracted, then the system locates for a stored template of that person and tries to match it with that template to see if the features of the face matches or not [10].

2.3.6 Signature

A person's signature is one of the ways to authenticate if he/she is the right person or not. Usually, this type of authentication is used in the banks where users try to take money out and this is only possible if the users write the correct signature, this by far is one of the safest authentications as well as it is hard to guess someone's signature and try to rewrite it yourself [11].

2.4 Other Methods of Authentication

2.4.1 Information about User

Information about the user is another means of authentication where the user is authenticated based on attributes [12]. These attributes can be the hair color, skin tone, eye color, an estimate of weight/height, and the way the person looks.

2.4.2 Location Factor

The term 'where you are' (location factor) is another means of authentication which is new but rarely used and exists in certain companies only [12]. This method uses location-based authentication, where it requires the exact location of users.

3 GAPS

3.1 Knowledge Factor

When it comes to knowledge factor in terms of passwords, PIN numbers, and safe combination people can guess it because people often tend to create weak passwords or bad password management practices could lead to having the password stolen, and having strong passwords doesn't make it any safer because sometimes even strong passwords tend to get stolen [1]. Attacks can use tools such as brute force to figure out the passwords which are less than 12-character long. This is a major gap and to overcome this gap we should address this issue. To get rid of these gaps the users should not use passwords that are less than 12-characters long as this can be easily predicted using the brute force attack tools. Users can use special sites to test and see if their passwords are secure or not. Also use smarter passwords and have a rule that allows a minimum password length. Another way to have a strong

password is to have capital letters, symbols, and digits within your password. In regards to the PIN and safe combination, it is not a good idea to have a birthday, year, or months as your PIN or safe combination. It is a good practice to have random numbers as your PIN or safe combination that way it will be hard to guess and figure out [1].

3.2 Possession Factor

Magnetic cards, smart cards, credit/debit cards, and memory cards are all physical objects that the users carry around with them in their wallets or neck straps. These are highly valuable things and needs to be taken care of as losing these items can be catastrophic [1]. People can steal these and use it for their gains and benefits. In order to protect them always remember to keep it safe as soon as you use them [1]. Try to have regular checks to see if the cards are in place if you find your cards are missing you should directly report this matter to banks and proper authorities so your cards will be temporarily disabled and no one else can use it. A novel approach is to implement a tracking mechanism in the cards so that whenever it gets lost or stolen users or clients can easily retrieve it.

3.3 Inherence Factor

Biometric systems are exposed to two common failures those are false-positive and false-negative. False-positive occurs when a system falsely identifies an imposter as an authentic or valid user. False-negative in when the system fails to make a match between an authentic or valid user with the stored template. Fingerprint, this authentication credential is considered very safe but there is some vulnerability associated with it such as having dummy fingers and dead fingers. It is also not suitable for people with damaged fingerprints due to the daily handling of rough objects and materials [13]. Hand-geometry, this authentication credential is very reliable and safe to use and is suitable for rheumatic hands, meaning it is for people who have strong and firm hands. The gap associated with this is that it is difficult without cooperation. To overcome this gap, you need to place the hands correctly in the machine using the guide plate [13]. Retinal Scans, this authentication credential is the best according to the statistics shown in Tables 1 and 2 as it shows the lowest crossover error rate when compared to other biometric authentication credentials. The gaps associated with this authentication is that it won't work for people who has false eyes, people who use contact lenses, and people who had eye transplants. You cannot really overcome this gap; all you need to do is care for your eye [13]. Voice recognition, this authentication credential is reliable as well but not a lot of people are considering this authentication credential due to some gaps associated with it. People are not considering this credential because of some issues such as unclear voice pronunciation. Users having a cold that could cause a change in the user's voice or speech recognition, and it can also pick up background noise. A person's voice can be easily recorded and used for unauthorized access. To improve these issues, have the installed hardware located at a soundproof place, which will cancel the noise population, and be aware of your surroundings [13]. Facial Recognition is one of the new authentication credentials used to date. There are four gaps associated with facial recognition; these are image quality, image size, face angle, and processing and storing. The image quality will affect how clear the image is, the image size will differ as well in pixels, face angle gap is associated when the user is not standing directly face to face with the camera and is at an angle and processing and storing the image will determine the device capability and storage space itself [14]. Signature, this authentication credential is fairly reliable and easy to authenticate. There are some issues with this authentication as well because some people can easily fake the signature and users can make mistakes as well due to some companies and organizations which are very strict, as they will see the shape and style before accepting. Some users tend to forget their signature styles as well and this can be catastrophic for them. To avoid these issues the best thing to do is to remember the signature style and avoid making mistakes. Overall, the biometric authentication systems need improvement as well. Their authenticating algorithms need to be more precise and accurate. Tables 1 and 2 show the comparison between some of the biometric authentication credentials and looking at Crossover Error Rate (CER), it can be said that ideal authentication credential is retinal scan which has a crossover error rate of 0.0000001% [15], [16], [17], [18], [19]. CER is determined by plotting False Acceptance Rate (FAR) and False Rejection Rate (FRR) wherever they intersect is called the Crossover Error Rate (CER) [15]. The lower the CER, the better the system is performing.

Table 1, *Comparison between Biometric based Authentication*

Characteristic	Fingerprints	Hand-geometry	Retina
Ease of use	High	High	Low
Error Incidence	Dryness, Dirt, Age	Hand Injury, Age	Glasses
Accuracy	High	High	Very High
User Acceptance	Medium	Medium	Medium
Long-term Stability	High	Medium	High
CER	0.2%	0.2%	0.0000001%

Table 2, *Comparison between Biometric based Authentication*

Characteristic	Face	Voice	Signature
Ease of use	Medium	High	Low
Error Incidence	Lighting, Age, Glasses, Hair	Noise, Colds, Weather	Changing Signatures
Accuracy	High	High	Very High
User Acceptance	Medium	High	Medium
Long-term Stability	Medium	Medium	High
CER	2%	2%-5%	2%

4 Recommendations

A few novel recommendations to overcome the gaps in authentication systems are mentioned in this section. First, for passwords, 12 or more characters should be used in a password which should include alphabets (upper and lower case both), numbers, and special characters such as #, @, $, %, etc. Research by Farik and Ali in 2015 show that if a password length is 8, it takes a random computer 44 seconds to guess, whereas if you use a 12 length password it will take a random computer 20 years to guess using the brute force attack tool [20]. There are some websites such as

passwordstrenghtcalculator.org and passwordmeter.com which will advise users on how strong their passwords are and if need be they can randomly generate you a secure password which will take any brute force tools several years to guess [21], [22]. Second, recommendation is for smart cards, credit/debit cards, and memory cards. An organization called TrackR has created a coin-sized device that can track things like keys, phone, wallet, bags, etc. using smartphones to get the location of these items when they are lost [23]. This technique should be implemented in miniaturized version in smart cards, credit/debit cards, and memory cards. Then using mobile app, the card owner can track the location of his/her card. This way lost and stolen cards can be found easily and quickly, and before it is used to launch any attack on a system. Third recommendation is for biometric authentication credentials. Their current algorithms need to be improved so that the crossover error rate could be reduced, together with false acceptance rate and false rejection rate.

5 Conclusion

It can be seen that if authentication factor credentials are not improved on an individual basis, there will still be security issues in one-factor, two-factor, and three-factor authentication systems, where each credential will be used. Hence, some novel solutions have been recommended as to how to improve credentials such as passwords, cards, keys, and biometrics. Furthermore, from this research, we can state that the recommended authentication credential to use is retina based authentication as this had a crossover error rate of 0.0000001%. Although some more work may be required to further improve the CER.

References

[1] M. Rouse. "What is authentication? - Definition from WhatIs.com.[online] SearchSecurity. ," 17 Sep. 2016, 2016; http://searchsecurity.techtarget.com/definition/authentication.

[2] *CompTIA Network+*, United States of America: Axzo Press, 2009.

[3] H. Abie. "Different Ways to Authenticate Users with the Pros and Cons of each Method.," 28 Sep. 2016, 2016; http://www.academia.edu/19482213/Different_Ways_to_Authenticate_Users_with_the_Pros_and_Cons_of_each_Method.

[4] Smartcardalliance.org. "Alliance Activities: Publications: Benefits of Smart Cards versus Magnetic Stripe Cards for Healthcare Applications » Smart Card Alliance.," 28 Sep. 2016, 2016; http://www.smartcardalliance.org/publications-benefits-of-smart-cards-versus-magnetic-stripe-cards-for-healthcare-applications/.

[5] Y. Wang. "Password Protected Smart Card and Memory Stick Authentication Against Off-line Dictionary Attacks.," 18 Sep.. 2016, 2016; https://eprint.iacr.org/2012/120.pdf

[6] J. Auth. "Fingerprint authentication | Authasas Advanced Authentication.," 23 Sep. 2016, 2016; http://www.authasas.com/products/diversity-of-supported-authentication-types-and-devices/biometric-authentication/.

[7] S. Xu, Li, M., Ding, J. and Cui, Y., *Personal Identification by Fusing Hand Shape Geometry and Palmprint Features.* , p.^pp. AMM, 278-280, pp.1228-1231., 2013.

[8] J. Trader. "Iris Recognition vs. Retina Scanning – What are the Differences?. [Blog] M2SYS Blog On Biometric Technology. ," 20 Sep. 2016, 2016; http://blog.m2sys.com/biometric-hardware/iris-recognition-vs-retina-scanning-what-are-the-differences/

[9] Wikipedia. "Speaker recognition.," 27 Sep. 2016, 2016; https://en.wikipedia.org/wiki/Speaker_recognition

[10] Biometric-solutions.com. "Face recognition.," 27 Sep. 2016, 2016; http://www.biometric-solutions.com/solutions/index.php?story=face_recognition

[11] K. D. A. S. Syed Navaz, “Signature Authentication Using Biometric Methods,” *IJSR,* vol. 5, no. 1, pp. pp.1581-1584., 2016.

[12] S. Mahnken, *Today's authentication options: the need for adaptive multifactor authentication. Biometric Technology Today.*, p.^pp. pp.8-10, 2014.

[13] Biometrics.pbworks.com. "Biometrics / Advantages and disadvantages of technologies.," 28 Sep. 2016, 2016; http://biometrics.pbworks.com/w/page/14811349/Advantages%20and%20disadvantages%20of%20technologies

[14] J. a. T. Edgell, A. "4 Limitations of Facial Recognition Technology.," 28 Sep. 2016, 2016; http://www.fedtechmagazine.com/article/2013/11/4-limitations-facial-recognition-technology

[15] L. Myers, “An Exploration of Voice Biometrics,” *SANS Institute*, 2004.

[16] S. R. N. Pavešic, D. Ribaric, “Personal authentication using hand-geometry and palmprint features – the state of the art,” 2016.

[17] B. Q. M. Nguyen Minh Duc. "Your face is NOT your password Face Authentication By Passing Lenovo – Asus – Toshiba " 20 Oct, 2016, 2016; https://www.blackhat.com/presentations/bh-dc-09/Nguyen/BlackHat-DC-09-Nguyen-Face-not-your-password.pdf.

[18] D. L. Peter VARCHOL, “Using of Hand Geometry in Biometric Security Systems,” 2016.

[19] A. C. Bichlien Hoang. "Biometrics," 20 Oct. 2016, 2016; https://www.ieee.org/publications_standards/publications/authors/sample_biometrics_pdf.pdf.

[20] M. Farik, S. Ali, “Analysis Of Default Passwords In Routers Against Brute-Force Attack,” *Internation Journal of Scientific & Technology Research,* vol. 4, no. 09, pp. 341-345, 2015.

[21] P. S. Calculator. "Understanding Password Attacks," 19 Oct. 2016, 2016; http://passwordstrengthcalculator.org/.

[22] T. P. Meter. "Test Your Password," 19 Oct. 2016, 2016; http://www.passwordmeter.com/.

[23] TrackR. "Find Lost Items In Seconds," 19 Oct. 2016, 2016; https://www.thetrackr.com/.