ASH1925008M

by Iftekhar Efat

Submission date: 13-Mar-2022 01:01AM (UTC-0500)

Submission ID: 1782977957

File name: ASH1925008M.pdf (342.86K)

Word count: 2199

Character count: 11673

Strengths and weakness of current authentication methods

Md. Al-Amin
ASH1925008M

March 13, 2022

Report submitted for **SE2206: Information Security** under BSc. in Software Engineering Program, Institute of Information Technology (IIT), Noakhali Science and Technology University

Project Area: **Information Security ....**
Project Supervisor: **MD. IFTEKHARUL ALAM EFAT**
Assistant Professor
Institute of Information Technology (IIT)
Noakhali Science and Technology University

In submitting this work I am indicating that I have read the University's Academic Integrity Policy. I declare that all material in this assessment is my own work except where there is clear acknowledgement and reference to the work of others.

I give permission for this work to be reproduced and submitted to other academic staff for educational purposes.

OPTIONAL: I give permission this work to be reproduced and provided to future students as an exemplar report.

Abstract

The process of allowing a user access to an information system is known as authentication. Passwords, personal identification numbers (PIN), and personal information such as tokens, smart cards, and biometrics are the three types of authentication techniques now in use. The purpose of this study is to discuss the strength and weakness of current authentication techniques.

1 Introduction

The process of authenticating a user's identification is known as authentication. Various authentication systems are used to identify users. The authentication process in a security system compares the information provided by the user to the database. The user is permitted access to the security system if the information matches the database information.

There are three types of authentication mechanism used[1]. Validation is the first step in the access control process, and it involves three common variables: something you know, something you have, and something you are. Something you know usually necessitates an individual entering a login and password to have access to the system. You may have a situation where the user authenticates with a smart card. Something you are is a situation in which the user uses biometrics to get access control.

Authentication systems allow users to gain access to the system in various ways, but they all work in different ways. Access control verifies various login credentials, such as usernames and passwords, PINs, biometric scans, and security tokens, to identify users. Multifactor authentication (MFA), a method that needs multiple authentication methods to validate a user's identity, is included in many access control systems.

Once a user is authenticated, access control then authorizes the appropriate level of access and allowed actions associated with that user's credentials and IP address. Access control keeps confidential information such as customer data, personally identifiable information, and intellectual property from falling into the wrong hands.

There are many authentications methods developed for users to gain access to the system.Some methods are simple, cheap and easy to implement. Some are more complex to implement, hard to crack and provides better user experience. Main Goal of all authentication method is to provide better security and user experience.

2 Types of authentication

2.1 Password Authentication

A password is a string of characters used to verify the identity of a user during the authentication process. Passwords are typically used in tandem with a username; they are designed to be known only to the user and allow that user to gain access to a device, application or website. Passwords can vary in length and can contain letters, numbers and special characters.

2.1.1 Strengths of Password Authentication

1. Password authentication is the most widely used authentication system. Because they are simple, inexpensive and convenient mechanisms to use and implementation.

2. One of the strength is that longer password is very difficult to break. 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.

2.1.2 Weakness of Password Authentication

1. As user need remember there password. So they prefer to use a simple person. The more simple the password, the easiest it is to guess. Also there are 26 letters, 10 digits and 40 symbols. So the limitation of choice of alphabet makes the password breakable.

2. If user write down there password for remembering it in the long run, there is high chance the password maybe stolen.

3. Users may willing or unwillingly share his/her password which increases the risk of password being public or go to wrong hand.

4. User may forget his/her own password.Because it is too long or complex or the user have not used the password for long time.

2.2 Smart Card Authentication

A smart card is a credit-card sized card that has an embedded certificate used to identify the holder. The user can insert the card into a smart card reader to authenticate the individual, Smart cards are commonly used with a PIN providing multi-factor authentication.

Figure 1: Smart card

2.2.1 Strengths of Smart Card Authentication

1. Smart cards provide different ways to securely identify and authenticate the holder and others who want to gain access to the card safely through A PIN code or biometric data.
2. The smart card was programmed to be read flexibly and easily by a wide range of devices and readers or by multi-technology readers and in various expandable locations by adding new control panels and readers.
3. 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.
4. It is portable and can be easily carried by users.
5. The smart card is locked if Pin is entered incorrectly after number of attempts. Smart card prevents dictionary attacks.

2.2.2 Weakness of Smart Card Authentication

1. User may find it difficult to remember the PIN. Also he/she may enter wrong PIN.
2. The card is small and light-weight. So the user may lose his card because of carelessness or the card maybe stolen by attacker. A attacker can easily break security using card.
3. There are some users who frequently use their card on various online site. Using card on unsafe site, A user may be the victim of Phishing.[3]
4. Sometimes PIN can be known by shoulder surfing

2.3 Biometric Authentication

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. Fingerprints and handprints are the most widely used biometric method in use today.[2]

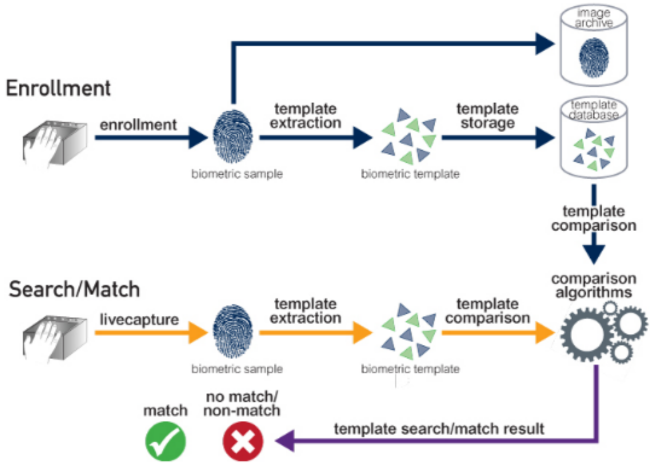

Figure 2: Biometric Authentication Process

2.3.1 Strengths of Biometric Authentication

1. Relieve user of difficult task of recalling passwords. There is no necessity to long and complex password.
2. For each individual Biometric factors are unique and is simple.
3. It is Very difficult to replicate biometric feature.
4. Biometric characteristics an individual inherits into himself.SO Biometric characteristics cannot be lost.
5. Biometric is used at major places such as at airports, immigrations purpose and at prisons.
6. Fingerprint scan is small and inexpensive.
7. Can be used over the phone lines.
8. Eye scan are accuracy in identifying users.

2.3.2 Weakness of Biometric Authentication

1. 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.

2. Biometric systems typically can be adjusted for sensitivity, but the sensitivity affects the accuracy.
3. 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.

3 Background

3.1 Password Authentication

In 1961, MIT was designing computers for multiple users. It was around this time that innovators at MIT, Bell Labs and Unix (then Unics) started thinking about the value of being able to have systems verify that users are who they say they are, which led to the birth of authentication. Also in 1961, the first known breach occurred when a researcher printed out passwords and gave them to other users. And then, in 1962, a software bug infected the system's master password profile, making everyone's passwords available to anyone who logged in. At this early stage in password history, hackers were more interested in exploring and testing computer systems than in criminal activity.

3.2 Smart Card Authentication

Integrated circuit cards were invented by Jürgen Dethloff a German engineer with the help of his associate Helmut Grötrupp in 1968. In 1992 the patent was registered and approved by the relevant authorities. The initial public use of smart cards was basically for telephone bill payments in France in 1983. In 1974 a French discoverer Roland Moreno decided to patent his first idea of the memory card. This was followed by Michel Ugon a scientist from Honeywell Bull inventing the first microprocessor smart card in 1978. The device a self programmable one chip microcomputer (SPOM) defined the essential structural design to program the chip. The manufacture and production of the smart card increased immensely in 1977. Manufacturers SGS Thomson, Bull CP8 and Schlumberger led the mainstream use of smart cards. Schlumberger bought the CP8 patent form Bull then later combined its own internal smart card unit with CP8 to come up with Axalto. Gemplus the world's number one smart card manufacturer merged with Axalto the world's number two smart card manufacturer and became Gemalto. Motorola company used the CP8 patent almost three years later to develop the first secure single chip microcontroller. The highlight of smart card use came in 1984 when the French Postal and Telecommunications services experimented successfully ATM bank cards with chips. This prompted the installation of microchips in to nearly all French Debit cards in 1992. By the start of 1984, MasterCard, Europay and Visa had a common accord with regards to the EMV system that addressed aspects on expanding the specifications that enable the use of smart cards in banking. Today the use of smart cards has developed being used in various activities like identification making phone calls and even for ATM withdrawals.

3.3 Biometric Authentication

While the earliest accounts of biometrics can be dated as far back as 500BC in Babylonian empire, the first record of a biometric identification system was in 1800s, Paris, France. Alphonse Bertillon developed a method of specific body measurements for the classification and comparison of criminals. While this system was far from perfect, it got the ball rolling on using unique biological characteristics to authenticate identity. Fingerprinting followed suite in the 1880s, not only as a means of identifying criminals but also as a form of signature on contracts. It was recognized that a fingerprint was symbolic of a person's identity and one could be held accountable by it. Through there are debates on who exactly instigated fingerprinting for identification, Edward Henry is denoted for the development of a fingerprinting standard called the Henry Classification System. This was the first system for identification based on the unique architectures of fingerprints. The system was quickly adopted by law enforcement replacing Bertillon's methods becoming the standard for criminal identification. This began a century's worth of research on what other unique physiological characteristics could be used for identification.

4 Conclusion

Authentication, whether it is password, smart card, or biometric, is an important process in any information system. Each method follows different methodology to provide security. Each method has its own strengths and weaknesses. We have seen their strength and weaknesses in earlier discussion. In short we can say password is simple and efficient way to provide security whereas smart card and biometric focus more on better security. Finally, we can say every method tries to give better security or better user experience or both.

References

[1] Syed Zulkarnain Syed Idrus, Estelle Cherrier, Christophe Rosenberger, and Jean-Jacques Schwartzmann. A review on authentication methods. *Australian Journal of Basic and Applied Sciences*, 7(5):95–107, 2013.

[2] KHIN SINT SINT KYAW. Analysis on the strength and weakness of current authentication systems to overcome their limitations. 2019.

[3] Sandeep K Sood. Phishing attacks: A challenge ahead. *elearning papers, April*, 2012.

ASH1925008M

ORIGINALITY REPORT

70%	67%	2%	65%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	www.ijstr.org Internet Source	19%
2	www.ukessays.com Internet Source	13%
3	bioconnect.com Internet Source	8%
4	www.hidglobal.com Internet Source	5%
5	arxiv.org Internet Source	4%
6	www.pearsonitcertification.com Internet Source	3%
7	www.vapulus.com Internet Source	3%
8	www.techtarget.com Internet Source	3%
9	Submitted to Bournemouth University Student Paper	2%

10	Submitted to East Carolina University Student Paper	2%
11	Submitted to Wellington Institute of Technology Student Paper	2%
12	global.oup.com Internet Source	2%
13	Submitted to Danford College Student Paper	1%
14	Submitted to Swinburne University of Technology Student Paper	1%
15	www.coursehero.com Internet Source	1%
16	www.researchgate.net Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

ASH1925008M

PAGE 1

Proper Noun If this word is a proper noun, you need to capitalize it.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Article Error You may need to use an article before this word. Consider using the article **the**.

PAGE 2

PAGE 3

Article Error You may need to remove this article.

PAGE 4

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Wrong Form You may have used the wrong form of this word.

PAGE 5

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

Article Error You may need to use an article before this word.

Possessive You may need to use an apostrophe to show possession.

Possessive You may need to use an apostrophe to show possession.

Possessive You may need to use an apostrophe to show possession.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Confused You have used **there** in this sentence. You may need to use **their** instead.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Confused You have used **there** in this sentence. You may need to use **their** instead.

Article Error You may need to use an article before this word.

Verb This verb may be incorrect. Proofread the sentence to make sure you have used the correct form of the verb.

Article Error You may need to use an article before this word.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

Article Error You may need to use an article before this word. Consider using the article **a**.

Article Error You may need to use an article before this word.

Article Error You may need to remove this article.

PAGE 6

Article Error You may need to use an article before this word. Consider using the article **the**.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Prep. You may be using the wrong preposition.

Article Error You may need to use an article before this word.

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word.

Missing "," You may need to place a comma after this word.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Frag. This sentence may be a fragment or may have incorrect punctuation. Proofread the sentence to be sure that it has correct punctuation and that it has an independent clause with a complete subject and predicate.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Confused You have used **A** in this sentence. You may need to use **an** instead.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **the**.

Article Error You may need to use an article before this word.

Proofread This part of the sentence contains a grammatical error or misspelled word that makes your meaning unclear.

S/V This subject and verb may not agree. Proofread the sentence to make sure the subject agrees with the verb.

PAGE 8

Article Error You may need to use an article before this word.

Missing "," You have a spelling or typing mistake that makes the sentence appear to have a comma error.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Missing "," You may need to place a comma after this word.

Missing "," You may need to place a comma after this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Wrong Article You may have used the wrong article or pronoun. Proofread the sentence to make sure that the article or pronoun agrees with the word it describes.

Prep. You may be using the wrong preposition.

Missing "," You may need to place a comma after this word.

PAGE 9

Article Error You may need to use an article before this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

Wrong Form You may have used the wrong form of this word.

P/V You have used the passive voice in this sentence. Depending upon what you wish to emphasize in the sentence, you may want to revise it using the active voice.

PAGE 10

Missing "," You may need to place a comma after this word.

Article Error You may need to use an article before this word.

Article Error You may need to use an article before this word. Consider using the article **a**.

Article Error You may need to use an article before this word.

Garbled Grammatical or spelling errors make the meaning of this sentence unclear. Proofread the sentence to correct the mistakes.

PAGE 11
