Are our current authentication methods safe?

Preetkumar Sandipkumar Patel
Master of Applied Computing, University of Windsor
Windsor, ON, Canada
patel4r4@uwindsor.ca

***Abstract* - In today's era, everything is going online, every single task we imagine can be done within a few clicks. However, the authentication is the only wall that stands between attackers and our ocean of data.**
There are many authentication techniques currently in use, most popular technique is password-based authentication. Which is backed up by multi-factor authentication. Additionally, certificate-based authentication and token based authentication are also making their way into new systems. But how safe are these techniques? Are the current techniques enough? Or do we need an upgrade?
This research-based project focuses on exploring the strong points and weakness of the current authentication techniques as well as the methods which are in development.

1.INTRODUCTION

Authentication is the process or action of proving or showing something to be true, genuine, or valid. In computing, it is the verification of the process or the user. Authentication is most needed now ever than before. Since our everyday tasks can be done using digital means. Authentication is the line of defence between the attacker and our assets. Assets can be our private data or any computer resource.

The Fig.1 shows the number of breaches and the cost of those breaches in millions. The number of breaches and the loss is increasing every year. It calls for our attention to update our authentication methods.

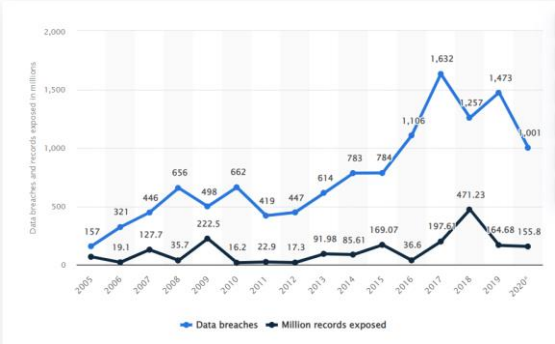

Fig 1. Data breaches and number of records exposed (2005-2020) [1]

Our data is the biggest asset. Nowadays every private data is present on the internet. Whether it may be name, address, mobile number or sensitive information like bank account and medical data. All these data are available on the web and is protected by the security protocols employed by the respective companies.

The main objective of this paper is to Present the detailed description of existing authentication methods, their advantages, and flaws in them. Additionally, this paper is also explores new techniques which are currently under development and have a potential of replacing our current techniques.

2. CURRENT AUTHENTICATION TECHNIQUES

There are various authentication techniques currently in use. The most popular being password-based authentication. Other techniques currently in user are two-factor based authentication, certificate-based authentication.

I. Password-based authentication

Passwords are the most used, in fact "overused" authentication technique. Password is an arbitrary string containing letters, digits, or special characters. Almost every online account we have is protected by some sort of password.

To remember the password easily, almost everyone uses personal information like their name, first name, last name, birthday, etc. However, this feature is an advantage as well as disadvantage of this method. Additionally, passwords are easy to change as well, few clicks and new password is immediately effect.

Passwords are set by user and stored in database. To protect the passwords from attacks on database it is stored in an encrypted form. The passwords are encrypted using hashing algorithms like SHA-256. Since hashing algorithms are on way algorithms it is not possible to crack the password in traditional ways.

Biggest flaw in passwords is that it can be social engineered. Since it is dependent on weakest link of security- humans, it can easily be guessed. Moreover, people tend to set their passwords of small lengths which makes it easier for attacker to crack. [2]

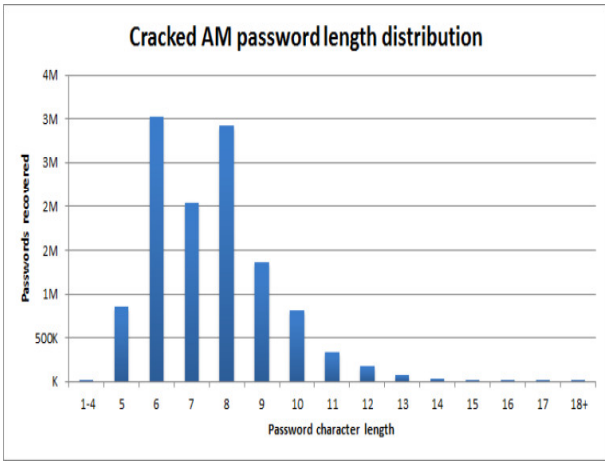

Fig 2. Cracked password length distribution from Ashley Madison breach [3]

Fig 2. Indicates the password length distribution of the cracked password, common length was 6 characters. 6-character passwords are not hard to crack with today's powerful hardware.

Secondly, people tend to keep very common password like the ones indicated in Fig.3. Due to such human error passwords are vulnerable to attacks.

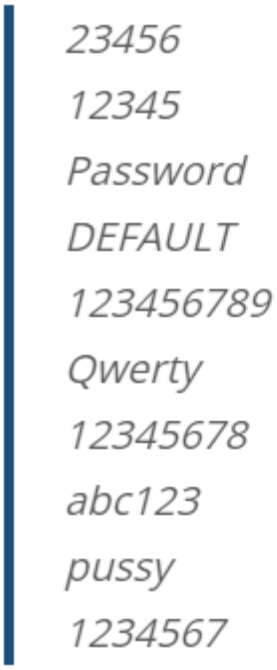

Fig 3. Top 10 passwords from Ashley Madison breach. [3]

However, due to the simplicity to implement as well as to use has kept password in use. But the security that password provides is questionable. Since the assets which it provides requires much more reliability than that.

II. Two-Factor Authentication(2FA)

Two factor authentication or 2FA is paired with passwords to provide second layer of protection. As the name suggests, it requires 2 proofs to authenticate the user. It is like protecting the door with two different locks.

Nowadays passwords are paired with 2FA In the form of One-Time Password (OTP). An OTP may be a 4- or 6-digit code which is valid for a very short time. It is generally texted or emailed to user om provided email and phone number. It ensures that even if password is compromised the second layer of protection remains intact.

However, 2FA is very tedious to use. There are many instances where due to slow server or network coverage, the OTP takes longer time to arrive and by the time user gets the OTP it has already been expired. Also, in case of dead device there is no way to receive SMS and hence we are locked out of our own accounts. Lastly, it increases the dependency of system.

Although it is not easy to use, still it is employed by most of the companies due to reliability issues of passwords. Still OTPs are not perfect, the physical device which gets OTP can be stolen.

III. Token-based Authentication

Token-based authentication is a protocol which authenticates using tokens.

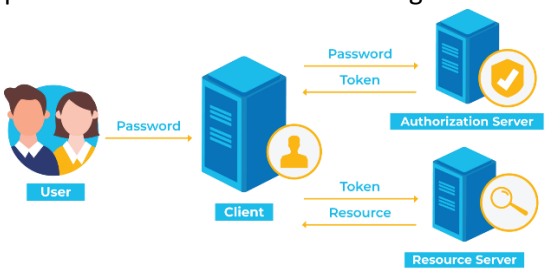

Fig.4 Token-based authentication [4]

Token-based authentication is a protocol which allows users to verify their identity, and in return receive a unique access token. During the life of the token, users then access the website or app that the token has been issued for, rather than having to re-enter credentials each time they go back to the same webpage, app, or any resource protected with that same token. [4]

Auth tokens work like a stamped ticket. The user retains access if the token remains valid. Once the user logs out or quits an app, the token is invalidated. [4]

JWT is widely used token-based authentication method. It is JSON web token. JSON Web Tokens (JWTs) enable secure communication between two parties through an open industry standard, Request for Comments 7519 (RFC 7519). The data shared is verified by a digital signature using an algorithm and public and private key pairing, which ensures optimal security. Furthermore, if the data is sent via Hypertext Transfer Protocol (HTTP), then it is kept secure by encryption. [5]

JWT relies on only one secret key. If in any case, it is compromised sensitive information can be put on risk. Additionally, using web-based tokens increases the data overhead.

Token-based authentication is rapidly gaining popularity and has a potential ton replace traditional methods.

3. AUTHENTICATION METHODS IN DEVELOPMENT

Security in computation world is very critical field and it requires constant development. Researchers are always exploring new and more secure ways to authenticate users. There are many techniques which are in development but still requires some more protection or additional measures to enter the current market.

I. Biometric Based Authentication

Biometrics are body measurements and calculations related to human characteristics. It can be anything like fingerprint, face, DNA, iris etc. Biometrics are unique to each human.

Currently face, iris and fingerprints can be used to authenticate an individual using various sensors. Nowadays face and fingerprints are already being used in smartphones and laptops.

The working of the biometric system is very simple. The capturing device captures biometric information and passes to feature extractor. Feature extractor is an algorithm which extracts biometric features from the captured data. These features are used to authenticate the user. Fig.5 indicates the working of a biometric authenticating system.

Biometric authentication in mobile phones comes with a catch, the biometric data stored in the phone is encrypted with the password of the phone. Also, physical threats can be made to the users to break into biometric authenticated systems. Many instances have occurred where user was

forced to provide their biometrics. Moreover, the sensors which captures the biometric can be meddled with to corrupt or override the detection.

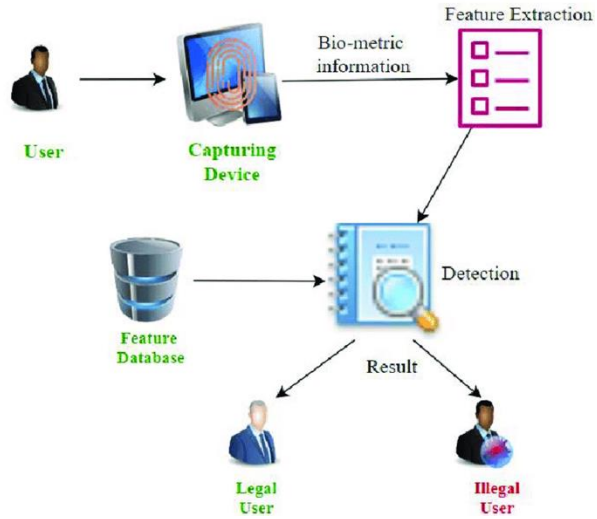

Fig 5. Working of Biometric Authentication

Even though biometric systems are costly to implement, these are very secure and unique. These are rapidly gaining popularity. However, to some users it is a curse as it involves detecting biometrics which are very personal data and can create big privacy concerns if not handled properly. [6]

II. Graphic-based authentication

Graphic based authentication employs images instead of using strings as passwords. When a user sets up a password, the user selects points on an image or sets of images that act as unique characters to represent the user. [7]

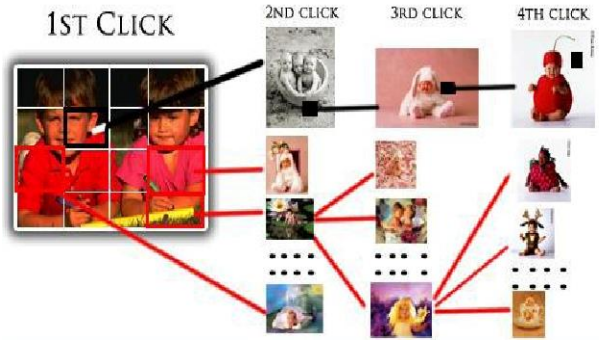

Fig 6. An example of image-based authentication [7]

Fig 6. Shows an example of image-based authentication. It involves selecting specific areas of image(s). According to the areas clicked by the user the authentication is done.

The idea of using image not only increases the storage usage but it also requires more computing power. Graphic based authentication is currently very raw and still needs vast developments.

In Android smartphones, image-based authentication is implemented. It is known as pattern lock; it involves creating a pattern by joining 9 dots in any way user likes. The authentication technique works but is not very popular because simple patterns can be guessed, and difficult patterns are not easy to remember. Additionally, the finger marks on phone screen can also be used to guess the pattern.

The current approaches are very naïve and requires adding some security layers. Even Microsoft tried to include an image-based authentication in Windows. But it was not a complete product as it required the clicks to be very specific and most of the times it did not detect the clicks at correct area and often ended up asking password to unlock the machine.

The current systems are in development, so they ought to have issues. It does not mean that this method does not have a potential to work in current systems. Proper development can create a robust graphic based authentication system.

III. Other methods

Zero knowledge password authentication system. In this protocol the user can provide the authentication server with password without sending any kind of password related data to the server. Thus, user can authenticate him/herself without revealing password to the server. [8]

4.CONCLUSION

In conclusion, the current authentication systems are outdated and still need to catchup. Whether it may be Two-factor authentication or biometric authentication every authentication system in this word is highly relied on passwords. There are multiple reasons why passwords still exist. A major reason for that is simple: Remembering completely random, complex passwords is very difficult. In addition, the average Internet user has at least dozens of online accounts that require a password, and the probability is that the same or a similar password is used across sites [9].

The authentication methods are over relied on passwords. To have a better and safer future we might need to say goodbye to passwords and look for another way which can work as a standalone. Because passwords rely on humans, they are the weakest link in an authentication system.

Currently, there are many potential methods which can replace passwords. In very near future either we will see a goodbye to our passwords or a new system which stands on the base of a password as a secondary authentication system.

REFERENCES

[1] Joseph Johnson*, "Cybercrime: number of breaches and records exposed 2005-2020",* Mar 3, 2021.

[2] Anonymous, "*Most Common Authentication Vulnerabilities*", Teleport, 17 February 2022. [Online]. Available: https://securityboulevard.com/2022/02/most-common-authentication-vulnerabilities/

[3] Luke Payne, "*Statistics on the 11 million cracked Ashley Madison passwords*", Sep 13,2015.

[4] Anonymous Author, "*What is token-based authentication*", Available: https://www.okta.com/identity-101/what-is-token-based-authentication/

[5] Anonymous Author, "*Authentication Token*", Available: https://www.fortinet.com/resources/cyberglossary/authentication-token#:~:text=Token%2Dbased%20authentication%20is%20a,a%20unique%20encrypted%20authentication%20token.

[6] S Harakannavar, Sunil & C R, Prashanth & K B, Raja," *Comprehensive Study of Biometric Authentication Systems, Challenges and Future Trends*",30 November 2018, Available: https://www.researchgate.net/publication/333266096_Comprehensive_Study_of_Biometric_Authentication_Systems_Challenges_and_Future_Trends [accepted: Dec 21,2018]

[7] D.Chakravorty, "*What if we used graphical passwords for authentication?*", UX Collective, 22 December 2020. [Online]. Available: https://uxdesign.cc/graphical-passwords-for-authentication-4e716b94eb47

[8] N Dutta," Zero *Knowledge Password Authentication Protocol*", January 2013. [Online]. Available: https://www.researchgate.net/publication/256374306_Zero_Knowledge_Password_Authentication_Protocol

[9] R Maurer, "The Password Is Slowly Becoming Extinct, but It's Not Obsolete Yet", 30 November 2020. [Online]. Available: https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/the-password-is-slowly-becoming-extinct.aspx#:~:text=A%20major%20reason%20for%20that,password%20is%20used%20across%20sites