ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 12(43), DOI: 10.17485/ijst/2019/v12i43/145555, November 2019*

Password Less Authentication

Riya Sandhu*

Department of Computer Science and Engineering, Manav Rachna University, Faridabad, India; sandhuriy55@gmail.com

Abstract

Background/objectives: Passwordless authentication is one of the most highlighted developments. It has gained much attention recently. **Methods/findings:** Social media and use of internet has been growing day by day, which further needs the security of that level. Security is an important part of the internet world. It is a huge responsibility to provide a level of security for each user. In this study, we aim to a general process of passwordless authentication, we explore some real life cases for a better view of the topic as well as we introduce the techniques of passwordless authentication and the biometric authentication like fingerprint sensors, face recognition, iris recognition, etc. **Improvements/applications**: This initiative, which includes many methods of overcoming the flaws of attacks done by hackers. These authentication techniques are adopted by many companies and are used in android smartphones and many more.

Keywords: Authentication, Security, Multi Factor Authentication, Usability, Magic Link, Mechanism

1. Introduction

Security is very important and vital part of a software development. In so many years, the developers have looked upon various strategies for handling this authentication in such a way that the users get maximum security. This kind of authentication is where the user is not required to login with passwords, so the developers have come across different ways like logging in simply with the help of the magic link, fingerprint, or using an otp or token that would be send to the registered email address or phone number. This is practiced because in today's world customers are having so many passwords, complex passwords, or same passwords which makes it easy for hackers to hack the accounts and misuse them.[1,2]

As by today, we have been going through a lot of stolen and hacked cases. The internet, passwords have posed an increasing risk to web security. We hear all the time, so many social media accounts have been hacked and made publicly available online.

When we talk about authentication, level of assurance is one of the most important topics related to it. The European Union and others have maintained a score card according to which authentication is measured. The highest rating has device is the most secure one.[3]

2. Real Life Cases

So many cases such as the yahoo data breach which said that several years ago, technology giant yahoo announced that the names, email addresses, passwords, and security question answers of over 500 million users were stolen in 2014 breach, dropbox user account leak and LinkedIn data breach had to do with having several passwords leaked.

Earlier this year, 427 million My Space passwords were posted on the dark web for sale, stolen by the same cybercriminal who was selling the data of more than 164 million LinkedIn users just one week prior. A difficult truth to face: chances are that your credentials are out there in a database controlled by an attacker.[4]

Moreover, new platforms and applications are developed every day and users have to sign up and make new passwords for each of them. It is very difficult for the users to keep up, thus encouraging them to use the same password for several applications. This is a very common

*Author for correspondence

occurrence. Now, if the user will have the same password for several applications so if hacker would the password for one application then he could have access to all your accounts. So, with this degradation in security of the user it was thought that what if there were no passwords anymore?[1,4]

Now if we continue this practice of authentication, it would benefit the user in many ways:

1. The user would be able to sign in faster to the desired account and use the service, the more user would love your application. Earlier user's need to get through to the signup forms which included the not much needed information, so eliminating those five extra minutes, we all know how precious the time is.
2. Obviously, the security would increase once you login through password less process, there would be no passwords to be hacked.

2.1. Password Authentication Threats

So, as we have discussed earlier authentication is one of the oldest problems of the information security, and it is always a living matter. Getting a password of a user is the simplest way to gain access to critical systems, steal confidential information, and much more. This is the reason why attackers are really interested in stealing passwords. The evolution of the info security brought several ways to improve the protection and security of user authentication systems, but at the same time attackers are also as brainy as we are so, they also improved their techniques and tools to steal valuable information. The most latest way of stealing a password from a user is asking him/her. This is the reality. The social engineering technique evolved during the time, and nowadays the attackers are becoming smart, asks the user for password to complete his work, or fix the broken thing.

There are attacks which the software experiences and had to deal with it.

1. Brute force attack
2. Password replay attack
3. Man in the middle

2.1.1. Brute Force Attack

This attack is the most simple and common attack used by hackers nowadays. This includes trial and error method in which the hacker tries to get all the patterns or passwords possible for an account to be hacked or any website. By using this repetitive technique of formations of password the hacker tracks down the correct password and misuses the details of the particular individual or identity.[5]

Hackers use super computers for such attack which tries almost 10^9 attempts in one second. This reduces much time and hopefully the attacker gets the password in the first set of attempts. Example: "dictionary attack" this is that we might try all the word in the dictionary.

How to defend against brute attacks?

The users must create more complex passwords. The password length can be limited. The temporary locking out a user who exceeds the attempts of entering the passwords. Nowadays, some programs are introduced which deny the IP address after few wrong attempts.

2.1.2. Password Replay Attack

A replay attack is nothing but a lower form of man in the middle attack. In this the attacker replays the messages or data to get some effective or hash data which I useful to hack another account. This is based on total security and includes fooling the two people having a conversation that they have completed the talk but then the hacker replays the chat and finds out the data in it.[5]

2.1.3. Man in the Middle Attack

This is another technique of hacking which is widely used by hackers. This is mostly used in social networking sites. In this kind of cyber attack, the hacker indulges or includes himself into a conversation with two people and then gets the access to information or data they are sharing. It also allows the third person to intercept and allows him to send data and talk to the other person without telling the truth.

It exploits the security of two people sharing data and it also comes under eavesdropping. The man in the middle attack can also happen in financial sites where the middle person is in between the login and the authentication.[6]

3. Password Less Authentication Adopted by Microsoft

Microsoft has also come to the observation that passwords are no longer enough for today's IT world as well as for security, the password login procedures are predictable and leave users vulnerable to theft. Password

authentication has always been an easy way or has always been the one option to access our accounts.

This is the reason why Microsoft decided to adopt multi-factor authentication (MFA). MFA is nothing but very similar to password authentication; it is basically a method of authentication, which requires more than one step to login into the account. This has many techniques in it, for example:

1) Card swiping and pin generation.
2) Logging into website and getting otp via mail or phone no (Figure 1).
3) Card swiping and fingerprint recognition, and many more.

Microsoft, many years ago adopted MFA with smart cards to secure the identity of employees. Firstly, they started using smart cards to secure, but it was not a great success as it required a card reader in each hardware device which is difficult to implement; moreover, smart cards are prone to be lost or forgotten.

4. Microsoft Adopting Password Less Strategy

Passwordless basically means without the help of passwords. User login to his/her account without the use of passwords. So if a person wants to adopt the passwordless technique then he/she must know some basic steps to do so.

4.1. Choosing the Right Technology

If we want to use passwordless then we first have to highlight upon the disadvantages of having passwords and look upon the advantages of passwordless future. The key steps such as security, precision, and applicability are needed to be taken care of.[7]

Figure 1. Example of getting OTP via phone number.

Microsoft was using windows as the technology and now it used windows hello which gives Windows 10 users another way to log into any device using fingerprint, iris scan, or facial recognition. Windows hello was no doubt a great technology to be used for diminishing passwords out of the IT world.

Moreover, the hardware devices used with windows were FIDO but now as Microsoft has been in touch with other alliance members so, now FIDO2 hardware devices are compatible to log into the services.[8,9]

4.2. Understanding How It Works

Put a light upon the passswordless technologies which are good at their work and how well they cope up with today's IT generation. Therefore, it is important to know how it works and the passwordless technology decreases the threat of security.[7]

Windows hello was basically made for reducing the use of passwords and replace them with MFA authentication. Windows hello is designed to identify person's face, iris, or fingerprint and then log him into their pc. The camera which windows hello uses is not a normal camera; it requires a specific real sense depth camera designed by Intel and infrared sensors.

Windows hello for business is personal, simple and provides a brilliant user experience with high security. In place of directly entering the passwords after entering the username, user receives a notification to verify his presence and the user validates his/her presence by matching the pin number or by fingerprint, face scan, or pin to unlock the device.[8]

FIDO2 also plays an important role in this. Microsoft has been in touch with FIDO2 to invent new technologies and FIDO2 provides it with security devices work on windows.

FIDO2 has been the backhand of Google, Microsoft, Mozilla, and other tech giants; moreover, it has come up with webauthn which is a common web application that secures all the web pages.[9]

4.3. User Adoption (Figure 2)

No change is easy. Therefore, this is also not possible to just launch a new technology and expect people or users to start practicing it. People need to gain trust upon the

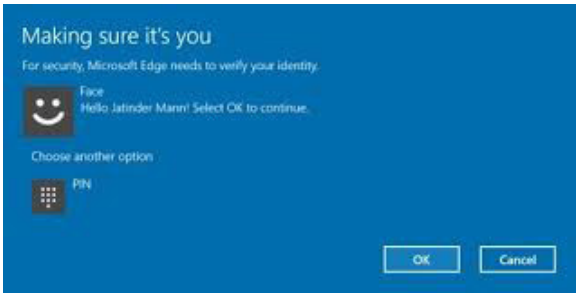

Figure 2. Snapshot.

technologies; moreover, it is very important to change thinking of people and broader their way of thinking.[8]

User adoption can be done by letting users know the advantages of password less authentication over passwords. It is more fast and safer than password authentication. It is cost effective and much more. Telling them the threats about the same. For example, in an industry, people must be given awareness camps regarding the topic in which they should discuss:

- Hackers easily get passwords because of which the data get leaked.
- Company has piles of data and hackers can get information of user and also can get another accounts passwords through it.
- User sometime sign into some fake sites with the same password which gets hacked further.[7]

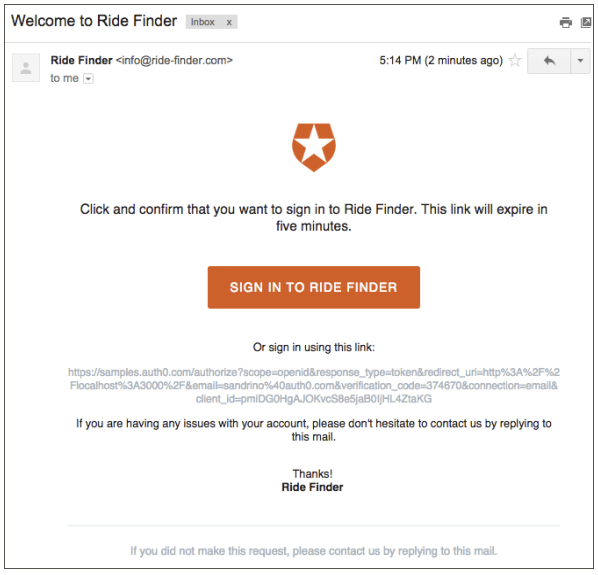

Figure 3. Example of getting magic link at gmail.

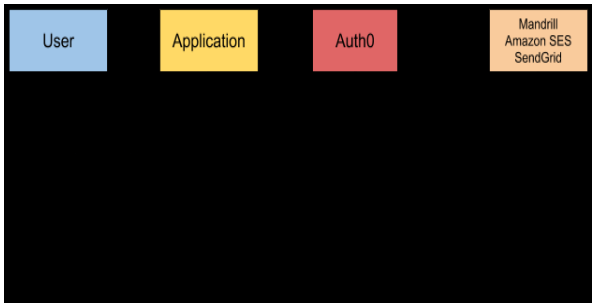

Figure 4. Process of getting magic link via email.

4.4. Working of Password Less Authentication

As we have already read what password less authentication is and its benefits, now we will study the process of implementing password less authentication in an application. Password less authentication can be implemented in various ways:

- **Authentication from a magic link via email** (Figures 3 and 4): In this form of authentication, user is asked to enter their respective e-mail address. Now, when the user submits the email address, a unique token or code is created and stored which will be generated by the application itself. So then the user receives an email with an URL that contains a unique token that is generated and sent to the user. Now, When the link is clicked by the user, the respective server verifies that the unique token is valid or not and exchanges it for a long-lived token, which is stored in the database and sent back to client to be stored as a browser cookie.[9]
- **Authentication with a one-time code via e-mail:** In this form of authentication, the user is requested to enter their respective email address. Then, an email is sent to the user with a unique, one-time code or password. Once the user enters this code into the application, the app checks whether the code is correct or not, if it is correct, a session is initiated, and the user is logged into the application (Figures 5–7).
- **Authentication with a one-time code via SMS** (Figure 8): In this form of authentication, a user is asked to enter his/her phone number. Then, a unique, one-time password is generated and then sent to the respective phone number. Once the user gets this code he/she enters it into the application, then the app checks whether the code is correct or not and that the phone number exists or not and belongs to a user,

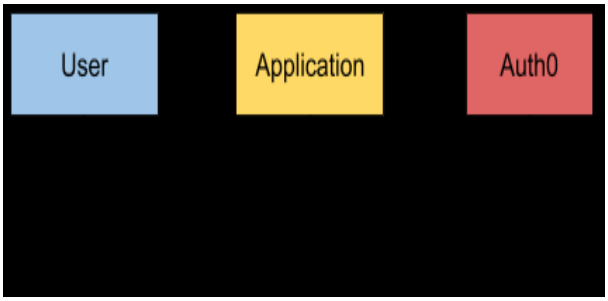

Figure 5. Auth0 sends a clickable link to the use.

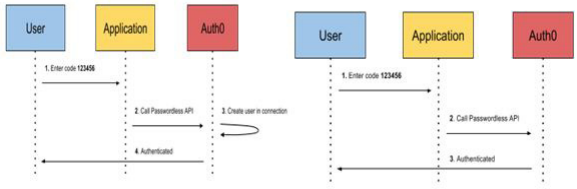

Figure 6. Auth0's one-time code via email and if the email address matches an existing user.[15]

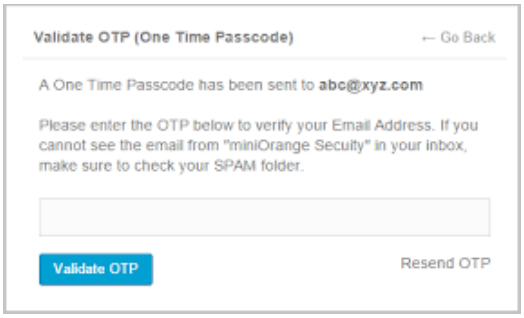

Figure 7. Example of authentication via email.

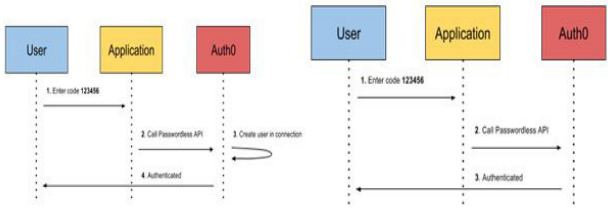

Figure 8. Auth0's one-time code via SMS. So, if the phone number matches an existing user, Auth0 just authenticates the user.[15]

a session is initiated, and the user is logged into the application.[10–12]

- **Authentication with Fingerprint (Figures 9 and 10):** in this form of authentication, a user is asked to place their finger on a mobile device to detect the fingerprint. So, a unique key pair is generated on the device

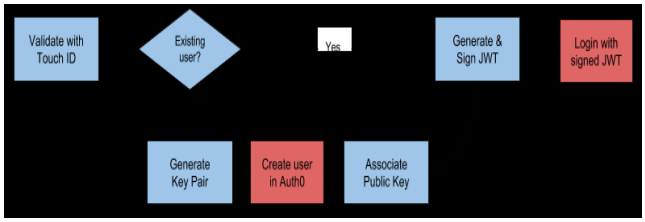

Figure 9. Process of authentication via fingerprint.[15]

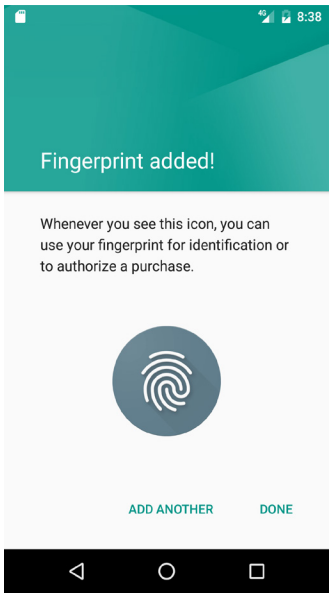

Figure 10. Example of authentication via fingerprint.

and new user is created on the server that maps to the key. Now, a session is initiated and the user is logged into the application.[13–15]

5. Conclusion

In this study, we have studied about the types of hacking and how passwordless authentication techniques help us in overcoming these challenges and how these techniques are useful in proving easy and quick mechanism of authentication. Passwordless authentication has made a great change towards the secure future of cyber crime and hacking. This initiative, which includes many methods of overcoming the flaws of attacks done by hackers. These authentication techniques are adopted by many companies and are used in android smartphones and many more. Moreover, the technology has come so far that people do not have to memorise their passwords, the user can easily login to his/her smart phone by fingerprint or face detection etc.

Acknowledgement

We would like to express our thanks of gratitude to Accendere Knowledge Management Services for providing us a platform and opportunity to pursue the research.

References

1. Yahoo data breach payout blocked by judge. [cited 2019 Jan 29]. https://www.bbc.com/news/technology-47044652.
2. Kalra S. A novel passwordless authentication scheme for smart phones. Adv Eng Int J (ADEIJ). 2016;1(2):11–27.
3. The definite guide on authentication for applications. [cited 2019]. http://www.ubisecure.com/wp-content/uploads/2016/11/The-Definite-Guide-on-Authentication-for-Applications-3.pdf.
4. 500 million users affected by yahoo data breach. [cited 2014]. https://www.pindrop.com/blog/500-million-users-affected-by-yahoo-data-breach/.
5. Ravi SK, Sivadasan ET. Study on framework for password-less authentication. Int J Adv Res Comput Commun Eng. 2016;5(2):642–4.
6. Kamarudin NH, Yussoff YM, Hashim H. Passwordless authentication in mobile e-health using a secure boot non-regenerated unique identity and NFC. Indian J Sci Technol. 2016;9(1):1–9.
7. What is windows hello? Microsoft's biometrics security system explained. [cited 2018 Nov 26]. https://www.computerworld.com/article/3244347/what-is-windows-hello-microsofts-biometrics-security-system-explained.html.
8. Password-less protection. [cited 2019]. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2KEup.
9. Passwordless auth is finally in the horizon. [cited 2018 Dec 27]. https://www.infosecurity-magazine.com/opinions/passwordless-authentication/.
10. Passwordless SMS & email authentication. [cited 2013]. https://auth0.com/docs/connections/passwordless.
11. Passwordless authentication using keystroke dynamics: a survey. [cited 2013]. http://www.rroij.com/open-access/pdfdownload.php?download=password-less-authentication-using-keystrokedynamics-a-survey.pdf&aid=47466.
12. Peyravian M, Zunic N. Methods for protecting password transmission. Comput Secur. 2006;19:466–9.
13. Is passwordless authentication really secure. [cited 2018 Apr 17]. https://www.okta.com/security-blog/2018/04/is-passwordless-authentication-actually-secure/.
14. Kalra S, Sood S. Secure authentication scheme for IoT and cloud servers. Pervasive Mob Comput. 2015;24:210–23.
15. Mobile identity authentication. [cited 2017 Mar]. https://www.securetechalliance.org/wp-content/uploads/Mobile-Identity-Authentication-WP-FINAL-March-2017.pdf.