International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 06 | June 2020 www.irjet.net p-ISSN: 2395-0072

Enhancement in Google Two Step Authentication

Prashant Bhosale[1], Harshali Patil[2]

[1]Student, Dept. of Institute of Computer Science, MET College, Maharashtra, India
[2]Assistant Professor, Dept. of Institute of Computer Science, MET College, Maharashtra, India

---

Abstract - *As nowadays an increase in Google user's an increase in attacks on user's emails has been rising rapidly,*

On daily basic and information can be sold by hackers on various platform, as Generated OTP in the second process contains only 6-digit numerical combination can be cracked easily, this paper will help Gmail user's to enhanced, a more secure methodology for authenticating login.

As enhancement in two-step authentications will add one additional security level in the process of login.

However, this paper tries to improve the security process by using IMEI number, last 4-digit of contact number, and QR Code for multiple device accessibility.

This paper helps to increase the security level to keep the user's credentials and data safe. by adding advanced security mechanisms to improve privacy or fraud risk for email account accessibility.

Key Words: **Security enhancement, Advanced Mechanism's, improved privacy, Security levels, Multifactor authentication.**

1. INTRODUCTION

Nowadays almost everyone has their emails which may contain crucial information or data (personal or officials) this data should be kept safe from a third person or hacker by providing high-level security mechanisms. On October 26, 2018, Gmail globally tweets that Gmail has over 1.5 billion active users [1]. Taking into consideration this point number of users is increasing day by day. The number of users using a two-step verification process provided by Gmail to secure each user by sending a security code on verified mobile but Less than 10% of active Gmail users have enabled two-factor authentication, mentioned by Google engineers [2]. As the Verification code is of 6-digit send to user mobile contain only numbers, a hacker can easily crack this code by using number combination. In this paper, a process is derived to make more advance secure two-step verification mechanisms by making use of barcode, IMEI number, and contact number variations.

2. What is Two-Step Authentication

In the two-step authentication process, the user first needs to enter the login credentials such as username, password, and then a unique passcode is sent to the user through email or on a mobile device. User can also able to manually change the second step of authentication if he/she is not comfortable with the passcode generator method. There are various methods that a user can take advantage such as

2.1 Security Key

A small device that will act like a Key that helps to prove it's a genuine user signing in. which can simply connect phones or computers.

2.2 Tap Yes on device

A Pop Up shown on device displaying the yes or no option for verifying authenticate user.

2.3 Offline Security Code

An offline 10-digit security code is present on user mobile device just need to go in Settings-google-security code.

2.4 Verification Code on Google authenticator App

User receive a 6-digit code on authenticator application.

2.5 Verification Code on registered mobile number

A 6-digit verification code is generated and send to the mobile phone.

2.6 Enter one of your 8-digit backup Code

This code is downloadable into devices and each code can use once only, Search in computer or device for "backup-codes-username.txt" with your username [3].

3. Types of 2FA Technology:

PIN from a paper/card (one-time PIN), digital certificate, RSA token code, Verisign token code, PayPal token code, apps like Google Authenticator, Authy, Microsoft authenticator, PIN received by SMS/email, a USB token, A smartcard, 2FA Via Biometric [4].

4. Need for Security Enhancement:

This paper is used to broadly describe the useful need for security enhancement for two-step authentications

The reason behind the updating of the authentication process is because nowadays the number of smartphone and smartphone users is increasing day by day in high amounts and each user is using an email platform most commonly used in Gmail. Yearly analysis of smartphone user worldwide ranging from the year 2016 to 2021,

Is shows that the year 2021 will contain a huge number of smartphone users worldwide which will be around 3.8 billion [5].

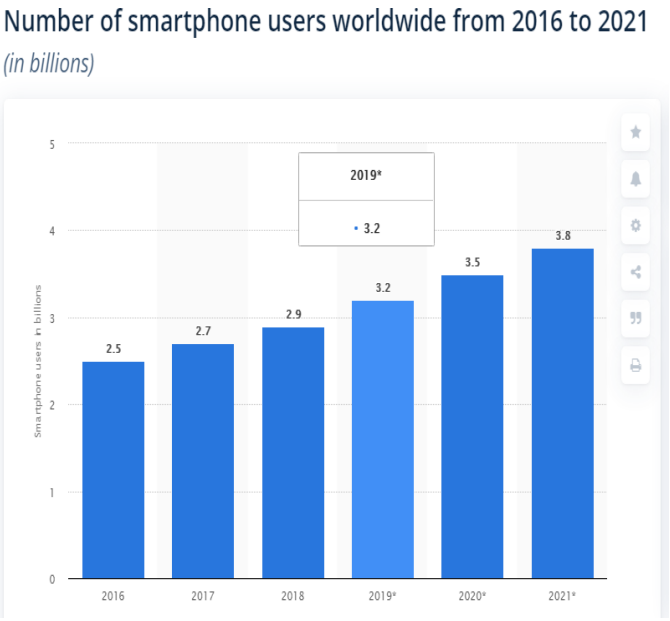

Chart -1: Smartphone user's worldwide

An only password is the actual key of user credentials but many of the users don't keep their password as strong as needed and then the hacker can easily get the advantage of this, Google also rewards for finding software vulnerability through that and also paid 6.5 million dollars [6]. Also, there are fewer amounts of people who use the two-step authentication mechanisms

Looking at the situation of people loosely typed password and not using any security mechanism and after using the 2FA still there password and verification code is get compromised so there should be a private key which should act strong password and only known by the server and user which will provide easy to use mechanisms for every user. One can also check the list of the website who uses two-step authentication methods [7].

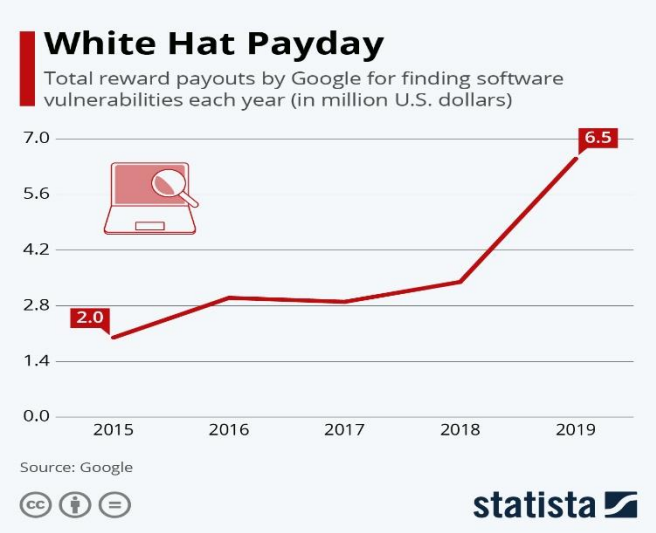

Chart -2: White Hat Payday

Earlier, some research studies based on two-step verification/authentication and purposed a generalized process which is used by many user's; however, past literature has not included all alternate option for second step authentication.

5. Methodology & approach:

5.1 User Registration Process

1. When User visit First time on website for registration Server check the device i.e. (mobile or laptop).
2. According to the device access to registration page process.
3. If the device is a Laptop or computer,
   i) User needs to enter his/her mobile number.
   ii) The user needs to scan the barcode (which is displayed on laptop/computer) with any barcode scanner and with the help of that the mobile IMEI number will be fetched automatically then the registration will be successful.
4. If the device is Mobile,
   i) User needs to enter his/her mobile number
   ii) If User is accessing the page through Web Browser then User needs to scan the barcode (which is displayed on laptop/computer) with any barcode scanner and with the help of that the mobile IMEI number will be fetch automatically or it will automatically

fetched that mobile IMEI Number then the registration will be successful.

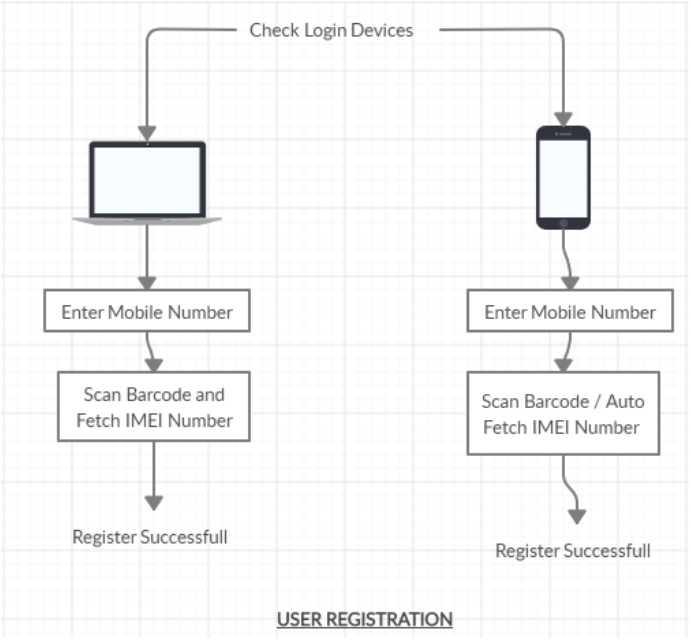

Fig-1: User registration Process

1. When Users visit the First time on the website for registration Server will check the Corresponding device i.e. (mobile or laptop or Computer) and then the user needs to enter the Username and Password and click on the process for 2nd Step.
2. Second Process,
   i) If User is accessing the page through Web Browser then User needs to scan the barcode (which is displayed on laptop/computer) with any barcode scanner and with the help of that the mobile IMEI number will be fetched automatically Or If accessing the page through mobile it will automatically fetch that mobile IMEI number. A User can also give access to multiple devices by Generating a barcode from an already registered mobile device.
   ii) With the addition to barcode user also needs to enter the last 4-digit of registered mobile number then the Login will be successful.

5.2 Two-Step Authentication

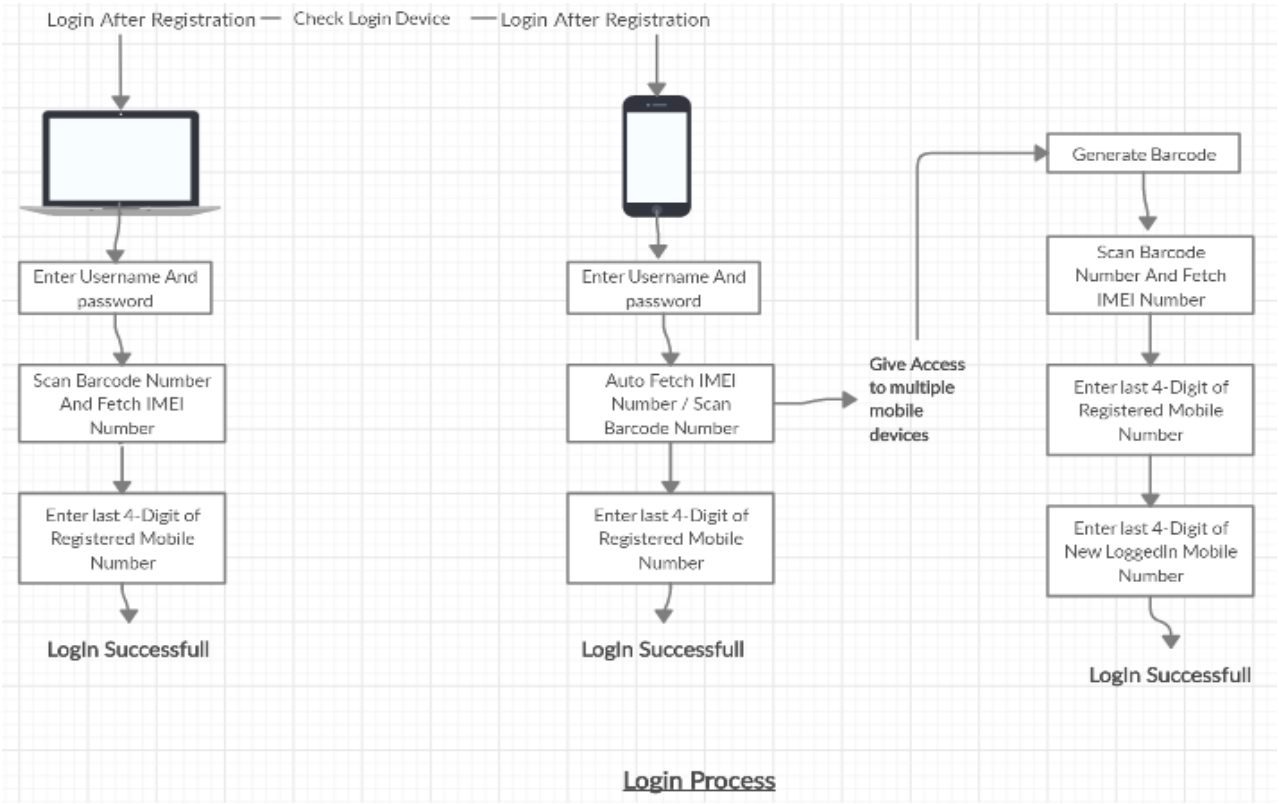

Fig-2: Two-Step Authentication

5.3 Multiple Device Accessibility:

1. Form a computer or laptop to another laptop or computer, a user just needs to enter username, password, and scanning the barcode with entering the registered mobile number.
2. From a mobile device to another mobile device, give access option is provided to Generate a barcode from an already registered mobile device. Then other mobile devices should scan the code and allow for fetching the IMEI number, now user should enter the last 4-digit number of registered mobile numbers and also the last digit of the current mobile number.

6. CONCLUSIONS

This paper broadly defines the way of using two-step authentication and applying the various alternate method of authentication and also there are many other platforms describe but choosing a step of OTP generation can be cracked by a hacker because of its simple combination. To secure the two-step authentication a barcode mechanism will be easy to use and also make a secret key between server and user which will be acting as a password.

REFERENCES

[1] Monika Bhatt, (2019, May 29). Retrieved from https://blog.gsmart.in/how-many-gmail-account-users-in-the-world/

[2] Alison DeNisco Rayome, (2018, January 19). Retrieved from https://www.techrepublic.com/article/google-less-than-10-of-gmail-users-enable-two-factor-authentication/

[3] https://support.google.com/a/answer/175197?hl=enref_topic=2759193&dark=0#keys&prompt&authentic&codes&phone&2sv&security%20

[4] Emiliano De Cristofaro, Honglu Du, Julien Freudiger,Greg Norcie, "A Comparative Usability Study of Two-Factor Authentication," arXiv:1309.5344v2, 2014.

[5] S. O'Dea, (2020, Feb 28). Retrieved from https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

[6] Willem Roper, (2020, January 29). Retrieved from https://www.statista.com/chart/20662/recor-rewards-for-google-researchers/

[7] Josh Davis, (2020, June 24). Retrieved from https://twofactorauth.org/.