Research Article

Study On Threats To Correct Password Errors Focused On Facebook Cases

Won-chi Jung and Namje Park *

Department of Convergence Information Security, Graduate School, Jeju National University, 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
*Corresponding author.; Email address: namjepark@jejunu.ac.kr

Article History:Received:11 november 2020; Accepted: 27 December 2020; Published online: 05 April 2021

Abstract: Recently it has been discovered that login is possible even if there is a typo in ID or password on Facebook. Facebook explained, "For the convenience of users, we allow some level of error in ID or password." In addition, "Security issues such as hacking are safe because they are strictly limited in the scope of typos and identify password entry methods rather than simple typographical errors." In this paper, We want to confirm Facebook's claim. We can analyze the type of typos of users and guess these effects. And We want to check the problem of the function that allows typos. Facebook is used by many people in many countries. That is also being serviced in Korea. Allowing typos means that Facebook save password in plain text. The Korean Privacy law enforces one-way encryption of passwords. When personal information is leaked, there is a lot of problem. Among them, the password has a large extent of damage. because many people use the same ID/password on various sites. The hacker who hacked into one site will attempt to steal information from other sites with the same ID and password. Therefore, the password should store the hash value.

Keywords: Facebook, One-way password, privacy, password, login authentication.

1. Introduction

Facebook is a representative social network service, with more than 2 billion users. People upload their daily photos to personal data on Facebook. In addition, it is used as a messenger. Facebook's security policy will require thoroughness. But recently it has been discovered that login is possible even if there is a typo in ID or password on Facebook. Facebook's users and some experts have expressed concern, but Facebook's official statement said that it is a function for user convenience and is perfectly safe. There are three main types of Facebook cases that have been known to date that allow typos. We don't know why this is safe or not. Because Facebook didn't disclose the algorithm. Although we have also looked at research on "How to securely correct user typos" in various studies. As shown in Figure 1, That means safety under certain circumstance. That is only Internet users and Service providers exist[1-4].

Many governments are monitoring Facebook. Also, if you look at Facebook's "data policy," it is said that we can provide your information at the request of an investigative agency. One of the things to keep in mind is that because of Facebook's open nature, your security or privacy is significantly affected by your friends' security/privacy settings. So, even if you follow the guidelines here, the effects will be halved if your friends don't. So, for your security and for the security of your friends, it is very important to spread these guidelines to your friends as well. Many people use Facebook groups for communication and organization. While Facebook provides the ability to create "secret" groups, it recognizes that the information shared within it is not only shared among members of the group, but can also be provided to third parties such as Facebook and government agencies. Should be. Also, always keep your Facebook privacy settings up to date. The settings described here will help keep your Facebook account more secure. However, we recommend that you always refer to the official Facebook help page to make sure there are no changes to your privacy and security settings. Also see the Facebook Terms of Service and Data Policy.

According to Developers have a website called 'How to Geek', Allowing typos is only applicable for keystrokes entered, and not allowed in notepad or clipboard formats. In order to hack using this type of typographical error, the hacker must already know the correct password. Also, as shown in Figure 2, we can see that we define typos that occur when we know the password correctly[5-13].

***Corresponding author:** Namje Park
Department of Convergence Information Security, Graduate School, Jeju National University, 61 Iljudong-ro, Jeju-si, Jeju Special Self-Governing Province, 63294, Korea
Email address: namjepark@jejunu.ac.kr

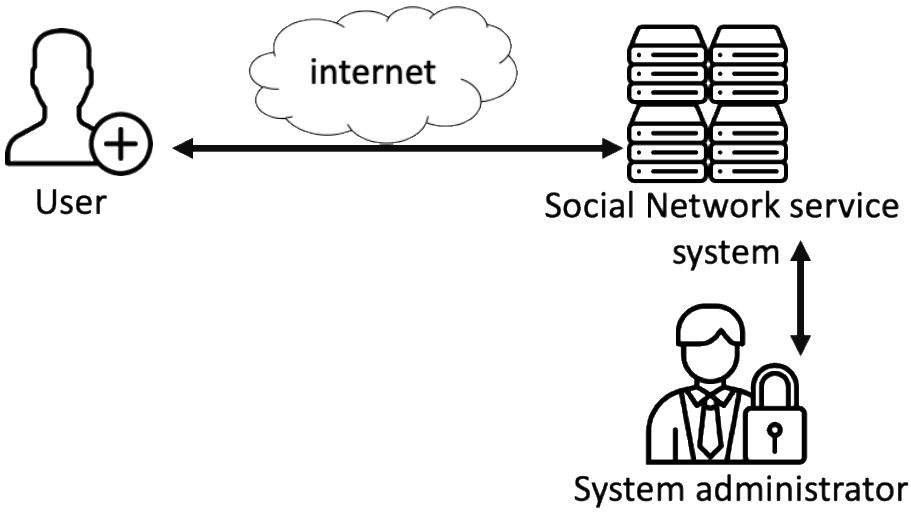

Figure 1 User – System – System Admin relation diagram

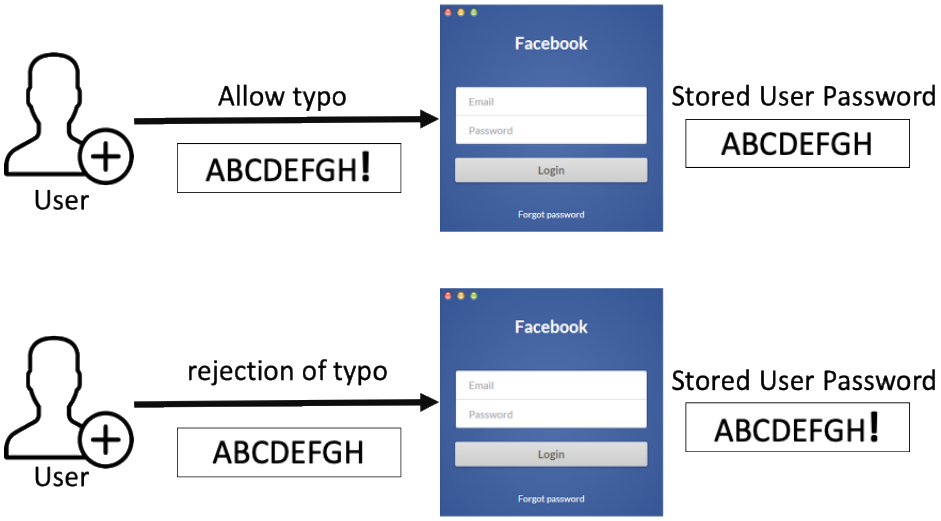

Figure 2 Facebook correct typo Processing

2. Materials and methods

2.1 Related research

You entered the ID incorrectly to log in to Facebook, and the phenomenon of logging in is summarized in Table 1.

Table1 Three major cases of Facebook's allowed password error

NO.	Permitted password errors
Case 1	Capslock key turned on, and Capitalizations are reversed. (e.g) “mypassword”, “MYPASSWORD”
Case 2	Enter an extra character at the beginning or end of a password. (e.g) “mypassword”, “1mypassword!”
Case 3	The first character of the password should be lowercase, but you typed it capitalized. but you typed it capitalized. (e.g) “Mypassword!”, “mypassword!”

This explains that Facebook is a function for user convenience, and it is applied to the ID and password fields. In accordance with the definition of the Guide to Encrypting Personal Information issued by the Ministry of Public Administration and Security and the KISA(Korea Internet Security Agency), “Password” is entered with an identifier when an information subject or personal information handler accesses a system. connected to the information and communication network to identify the presence or absence of access rights.

It is a unique string that must be passed to the system so that it can be done, and it means information that should not be disclosed to others. "Hash function" refers to a one-way function that always converts a message

of arbitrary length into a hash value of fixed length. “One-way (hash function) encryption” means a method that is not decrypted when an encrypted value is generated using a hash algorithm function, etc., and the recommended encryption method is shown in Table 2.

Table2 Safe cryptographic algorithm Standard (example, As of September 2016).

Public institutions	**Permitted password errors**
SHA-224,	SHA-224
SHA-256	SHA-256
SHA-384	SHA-384
SHA-512	SHA-512 Whirlpool etc.

The type and frequency of typos learned from MTurk experiment. Types of typos can be defined as follows Table 3. Through this, We learned that the case of ‘All characters are inverted’ is the most frequent. Most of them, when the Caps lock on the keyboard is activated, it is seen as an attempt to log in without recognizing it

Table 3 The top categories of typos

Typo type	**% of typos**
Case of All characters are inverted	10.9
Case of first letter is reversed	4.5
Case of Add additional characters to first or end	5.9
Case of Missing shift for symbol at end	0.2
Other errors	78.4

2.2 . Proposed Password one-way encryption

The reason for storing the password as a one-way password is that a system that handles personal information will store the information in a database. The data in the database is diverse and accessible to many people. Because of this, various administrators can access values such as querying the DB and entering virtual data. Since most users create and manage accounts with the same ID and password for various services, through this, the developer at Site A tries to log in to Site B with the user's ID and password in the DB. can do. If a one-way password is applied, the one-way password of the password is enforced as a measure of safety because the original password cannot be deduced from the password hashed to the DB even if access to the DB is possible. The following questions are raised in this part of the allowance of Facebook's incorrect password entry.When “mypassword” is hashed to sha-256 The value “ddec437eeb1da25a146a24c432d1165bc646daa7fecc6aa14c636265c83caa14” comes out. “Mypassword1” is hash with sha-256 It is converted to the value “caae1d5e3ee5b5aaffcd8761bf95b63ab5bcc95ccbb8408ae324016718a23445”. “Mypassword” and “mypassword1” have only one character difference, but hash converts them to unrelated strings.

Then, in order for Facebook to allow the user's password error, the user's password must be stored without one-way encryption, to compare the similarity of the decryption values, or to store all the hashed values in all cases that may be wrong. In the latter case, it is a situation where the last letter does not know which letter is to be entered, and even if the case is reversed, at least several hundred password hash values must be stored.

2.3 . Criteria for encryption of personal information

In the standard for measures to ensure the safety of personal information (Ministry of Public Administration and Security Announcement No. 2019-47), Article 7 (Encryption of Personal Information) No. 2, “Personal information controllers must encrypt and store passwords and bio information. However, if the password is stored, it must be stored in one-way encryption so that it cannot be decrypted. ” Is stated. In other words, the principle is to store the password by one-way encryption. Facebook doesn't have an official position on how to store passwords, but it's likely that it wasn't encrypted and stored. In other words, it did encryption, but it would have gone through an encryption process that could be decrypted. The reason for guessing is that even an account without a history of changing the password several years ago is logged in with a wrong input password. This seems to be evidence that the password was stored in decryptable encryption, and it cannot be considered that the standards for securing personal information have been implemented. It must be managed securely to protect the information of the object.

2.4 . Secure password management

According to data distributed by the Korean government (KISA), secure passwords cannot be easily guessed by third parties, and hacking user information stored in the system or information transmitted over the Internet cannot be found or found. Even if it means a password that requires a lot of time. Among them, the secure password creation tip section requires different passwords for each site. For example, assuming that the A site is hacked and all the member information has been robbed, the hacker has the ID and password information of the member collected from the A site, and logs into another site to log the second and third valuable information. And the method of attack that takes monetary gain is called credential stuffing. If the passwords for Site A and Site B are different, of course, the damage would have stopped at Site A. The proposed method is a method of reflecting a part of the URL of the site in the password Figure 3.

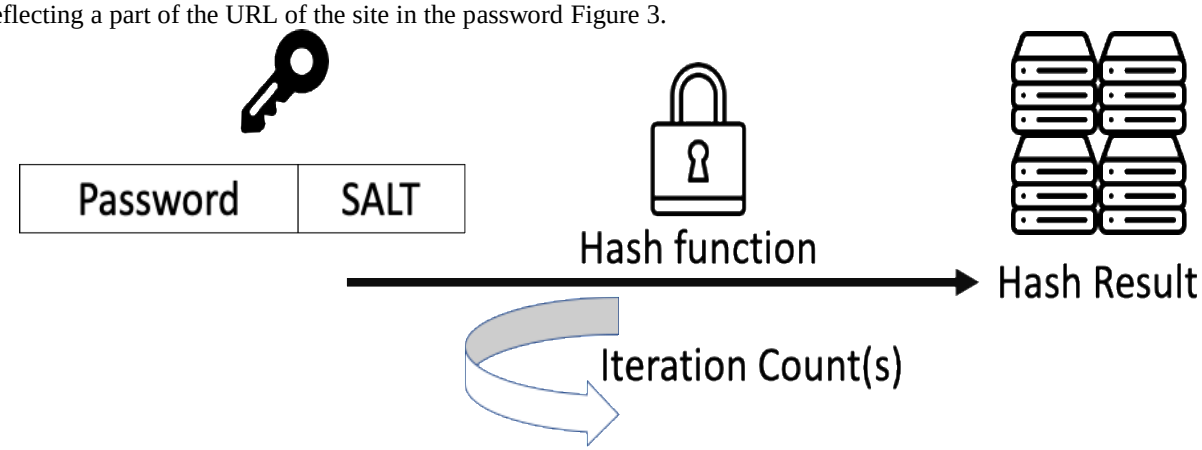

Figure 3 hash-function-based password management

The proposed method is a method of reflecting a part of the URL of the site in the password. Refer to Table4 for details.

Table 4 Combining your own string and part of site URL

Web Site	Password generation rules
Google.com	“mypassword” + “G”
Naver.com	“mypassword” + “N”
Daum.net	“mypassword” + “D”

Facebook's friendly login policy, even if you set a different password for each site, increases the likelihood that Facebook will be compromised by a credential stuffing attack if one site is compromised.

3. Results

Many countries that Facebook serves have laws for privacy each. Korea also has the Privacy law and the Information and Communication Network law. The laws define the password management. If threats increase for convenient services, measures are needed to counter them.

Facebook's internal policy that try to reduce the threat is unknown, but it is true that threats are increasing.

4. Discussion

In Korea, there are rules to follow for the safe management of passwords. Because there have been many cases of personal information leakage in Korea, and some cases are still being sued. Therefore, many Koreans are interested in personal information protection, and many regulations have arisen. The use of personal information requires protection first.

5. Conclusions

It seems like a big problem to have more than one password and a policy that allows you to log in with a range of errors. This policy checks the similarity of ID, so the range allowed for similar input is quite wide. Due to the similarity of ID, it is of great concern whether there is a way to block access to other people's accounts. Facebook has leaked up to 50 million personal information in 2018, and there have been many other big and small problems related to personal information. Despite Facebook's voice to strengthen personal information, anxiety arose as a user on Facebook who chose convenience over security. Several circumstances have been shown that it is difficult to observe the one-way encryption of the Privacy Law. Facebook is said to be a bona fide function for the convenience of users, but in order to provide domestic services, please pay attention to and comply with domestic privacy laws.

6. Acknowledgements

This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2019S1A5C2A04083374).

7. References

1. R. Chatterjee, A. Athayle, D. Akhawe, A. Juels and T. Ristenpart, pASSWORD tYPOS and How to Correct Them Securely. 2016 IEEE Symposium on Security and Privacy (SP), San Jose, CA, 2016, pp. 799-818, doi: 10.1109/SP.2016.53.
2. Ghacks.net [Internet].: Amazon Login May Accept Password Variants [updated 2018 January 4; cited 2020
3. October 3]. Available from :
4. https://www.ghacks.net/2011/01/31/amazon-login-may-accept-password-variants/.
5. How-To-Geek.com [Internet].: Facebook Fudges Your Password for Your Convenience [updated 2019 January 24; cited 2020 October 3]. Available from :
6. https://www.howtogeek.com/402761/facebook-fudges-your-password-for-your-convenience/ .
7. Biryukov, D. Dinu, and D. Khovratovich. Argon and argon2: password hashing scheme. Technical report, Tech. Rep., 2015
8. Namje Park, Jin Kwak, Seungjoo Kim, Dongho Won, Howon Kim. WIPI Mobile Platform with Secure Service for Mobile RFID Network Environment. LNCS, Advanced Web and Network Technologies and Applications, 2016, Vol.3842, pp.741-748.
9. xkcd.com [Internet].: Password strength [cited 2020 October 3]. Available from : https://xkcd.com/936/
10. Jung W, Oh S, Park N. A study on Facebook's allowed password error. ICICT2020, 2020
11. Donghyeok Lee, Namje Park. Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance. International Journal of Supercomputing, Vol. 73, No. 3, pp. 1103-1118, Mar. 2016.
12. Donghyeok Lee, Namje Park. Geocasting-based synchronization of Almanac on the maritime cloud for distributed smart surveillance. International Journal of Supercomputing, Vol. 73, No. 3, pp. 1103-1118, Mar. 2016.
13. Namje Park and Namhi Kang. Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle. Sensors. 2015 Dec. 16(1): 1-16.
14. Kim J, Park N, Kim G, Jin S. CCTV Video Processing Metadata Security Scheme Using Character Order Preserving-Transformation in the Emerging Multimedia. Electronics. 2019;8(4):412. DOI:10.3390/electronics8040412.
15. Lee D, Park N, Kim G, Jin S. De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment. Peer-to-Peer Networking and Applications. 2018;11(6):1299-1308. DOI:10.1007/s12083-018-0637-1.
16. Satapathy, S. K., Mishra, S., Sundeep, R. S., Teja, U. S. R., Mallick, P. K., Shruti, M., & Shravya, K. (2019). Deep learning based image recognition for vehicle number information. International Journal of Innovative Technology and Exploring Engineering, 8, 52-55.
17. Satapathy, S. K., Mishra, S., Mallick, P. K., Badiginchala, L., Gudur, R. R., & Guttha, S. C. (2019). Classification of Features for detecting Phishing Web Sites based on Machine Learning Techniques. International Journal of Innovative Technology and Exploring Engineering, volume8 (8S2), 425-430.