Password Security: Best Practices and Management Strategies

Mohammed Hasan
Faculty of Engineering and Informatics
University of Bradford
Bradford, UK
mhasan2@bradford.ac.uk

***Abstract*—Due to the rapid increase in the desire to use online technology, the use of password security has become vital for users worldwide to protect their sensitive data or accounts by implementing a password key only known to them in order to access their personal data. Throughout the years, as data has become more involved with being stored online, the creativity of different strategies of passwords has also increased as certain data may only be accessed through unique methods such as fingerprint scan. One of the major types of services that require users to protect their details is online banking such as PayPal or NatWest where users would provide a stronger password compared to an account with low value such as a mobile phone game. This report will go in depth on the best practices and strategies that derive from password security.**

I. Introduction

Password security is very common within applications that include personal information or communication such as through messaging or using online banking to perform money transfers which may require security to prevent abuse or misuse by unwanted hackers. However, despite this many users fail to provide a secure password to keep their information safe from hackers by using a very simplistic password [1]. The intention for this report is to discover and analyse the different practices and strategies for password security. To start, the report will consist of the origin of password security as well as its current state. The report will also provide a thorough analysis of the password security problem and will be giving well-reasoned conclusions as well as include discussion, opinion and evaluation to support the theories. Therefore, for each of the practices/strategies, a relevant argument and analysis will be provided.

II. Origin of Password Security

The origin of the first password to be used is during 1961 where the institute of technology by Massachusetts implemented a login command for their operating system called CTSS (Compatible Time-Sharing System) which contained a username and a password. Passwords were then later used through cryptography in the 70s by 'Robert Morris' for his UNIX operating system where numerical values were provided within the passwords to give a higher number of options when implementing a password [4]. However, fast forwarding to the early 2000s, the general password security was on the decline as organisations looked to other options to provide a stronger and safer alternative for protection since the old method was too basic and vulnerable such as by using a 2 factor authentication as the standard of technology had also increased throughout the years [2].

As for the current state of password security, it has been improvised and developed by a large margin since its origin as the use of passwords were deemed to be useless by many enterprises as they were easily exploited or bypassed by intruders to access sensitive information therefore the methods of providing security for users had become more reliable by using different methods such as authentication, sensors, encryption etc. [6]. These methods are more secure compared to the old method and is also easier to use making it more reliable and stronger.

III. Two Factor Authentication

If a victim's biometric data is discovered by an attacker, they could potentially use that information to masquerade the victim or be able to watch their everyday activities. This is a big risk because once a user's biometric data is located, it is compromised as it cannot be changed. However, to avoid this unwanted invasion a two-factor authentication is implemented [3].

Two factor authentication works by containing two separate factors in order to access the personal data. For example, an ATM (Automated Teller Machine) consists of two-factor authentication as it requires a card as well as a PIN (Personal Identification Number) [9]. Since passwords are very vulnerable to hackers, a method to combat weak security is two-factor authentication which banks are looking towards to provide protection for their customers as well as their employees [5, 7]. The two-factor authentication provides and extra layer of security for the user by asking for a PIN number despite having entered the username and password initially in case an intruder already has access to that information [10]. However, from a personal perspective, two-factor authentication is not the most secure and reliable method of password security as mentioned by [8], "It won't defend against phishing. It's not going to prevent identity theft. It's not going to secure online accounts from fraudulent transactions". This is a major factor as phishing is a continuously rising common problem which two-factor authentication does not tackle.

IV. Multiple Passwords

Users may have multiple passwords for different services which despite seeming secure due to keeping each password unique, can be a problem as users may eventually forget many of their unique text passwords overtime [12, 13]. Therefore, to avoid this problem user tend to use the same password for every account which is a security risk as if a hacker is able to locate the password from malicious methods, they will have access to every account of the user with the same password.

Due to a large number of passwords, users may write down their passwords on a physical or software notepad which may be exploited by hackers through either phishing, XSS (Cross site scripting) or by having legitimate access to the notepad [11, 14]. Therefore, having multiple passwords as a method of security is not ideal as it contains many factors of security breach that are previously mentioned such as trouble with remembering many passwords or containing the same password for multiple accounts which can be exploited.

V. Password Encryption Key

A PEK (Password Encrypted Key) is a generated password supplied by the user to provide an extra layer of security for the user's password. This is done by using the password the user inputted and storing it into a server or record. Then once the user attempts to login, the password entered would make an encryption key which will then be compared to the key that was stored onto the server through decryption to ensure its legitimacy which will allow the login to be complete [15]. This method of password security is used to provide a stronger base of security during login as a user provided password key may not be enough protection against future threats such as from phishing methods.

A PEK consists of 2 separate keys to create a encrypt the data for the user which are the data key and the user key. The data key is randomly generated strong key whereas the user key derives from the password that the user inputted so that when the password is inputted by the user, the user key is decrypted which then decrypts the data key to allow access to the data for the user [16]. This means that the data is provided with more protection compared to a user provided password and the password can be changed without having to access the file itself [17]. This is an effective method of protecting data that especially is on the move such as through messages into an insecure channel without allowing exploitation during the process.

VI. Paraphrases

Paraphrases a form of practice for password security as using the standard mix up of letters and numbers when creating a password has become too simple to trick the potential threats from hackers as they are able to identify switch ups such as replacing an 'E' with a '3' or an 'A' with a '4'. Therefore, users are able to use paraphrasing by constructing a long sentence with a switch up of many numbers and letters in order to make it difficult for the attacker to be able to decode the password using a third-party software. This is an efficient method to give lower risk accounts with a login password a strong sense of security but may not be suitable for high risk accounts such as for banks or organisations as it is mentioned by [18], unauthorised access to systems and theft is due to hackers being able to crack the passwords through social engineering therefore organisations are looking more towards security authentication instead of passwords to provide a stronger layer of security for their employees or their clients which paraphrasing does not fulfill [19].

The following table is the statistics from 'LinkedIn' containing the 10 most common passwords after 117 million user passwords were stolen:

Table 1: Data obtained from statista.com

No.	Password	Number of people
1	123456	753,305
2	linkedin	172,523
3	password	144,458
4	123456789	94,314
5	12345678	63,769
6	111111	57,210
7	1234567	49,652

This proves that the average user does not have high value for password security as the most popular passwords are very easy for hackers to guess due to their simplicity.

VII. Facial Recognition

Facial recognition is a recently developed method of security mainly popular from use on smartphones as for the facial recognition to function, all it requires is an camera to detect and store the biometric verification of the user in order to provide a facial ID password before being allowed to unlock the phone. Due to the increase of smartphone usage, the need to protect the data has also increased therefore using the standard numeric or typed password may not be a strong enough solution as it is time consuming and troublesome to remember [20, 22]. The facial recognition method is a very efficient advanced authentication practice of password security as it requires to obtain the shape and location of the user's features such as their nose, eyebrows, chin, lips etc. This means that the need for user interaction with the device is very limited making it a popular method as it is very easy to use and cannot be bypassed with ease compared to a traditional password technique [24, 26]. However, despite its strong features, facial recognition also requires a large memory usage as well as processing power making it difficult to be used consistently in the security management for devices therefore smartphones usually are only able to store 1 facial ID as a password protection at a time compared to other methods such as fingerprint scan which can be stored with multiple entries [21]. The following list is the method used to provide facial recognition as a password protection method for mobile devices:

1) Smartphone captures facial features through biometric data using its front camera.
2) The facial image captured by the smartphone is then processed to allow facial recognition.
3) After it has been processed, the image is then stored into the facial database for it to be accessed when the user requires to login using facial ID [27, 29].

Overall, facial recognition proves to be a very strong and secure method of security especially combined with the two-factor authentication to provide an extra layer of security for not only mobile devices but for other purposes such as gaming or airport travelling [23]. This will help prevent the mitigation of attacks from hackers who intend to steal or misuse the private user data.

VIII. Anti-virus Software

Anti-virus software is a method of password security practice as it provides protection from malicious scripts such as worms, trojans or zombies from phishing attackers by detecting potential threats delivered by them. An example of an antivirus is CMIT Marathon which helps detect any malicious scripts within Java, Chrome, Firefox etc to prevent the hackers from gaining access to personal data or to bypass the victim's password for their accounts [31, 32]. However, antivirus software is mainly catered to computing and is not suitable to mobile devices due to power constraints [34]. The antivirus software may also cost a significant amount to implement it into the computer system which can be a problem for users who may not have the funds to buy it.

The antivirus software is built to filter content the user may run into online or on the internet as that is where the likelihood to run into a malicious script or phishing attempt is at high. Therefore, the antivirus software will help block the potential threats or it will warn the user of a risky webpage before they are accessing it. This means that an antivirus software is vital to have when relating to password security as browsing online allows the user to be victim to numerous methods of phishing attempts which could easily gain access to the user's password [25]. This can happen through methods such as XSS (Cross Site Scripting) or phishing which sends the user to a spoof webpage and trick the user to provide their personal details including their password. Despite its cost, the benefits of installing an antivirus software outweighs the negatives as the benefits such as protecting the password from phishing attempts can potentially save the user more money or damage from the exploits compared to the cost of purchasing and installing the software.

IX. Password Blacklist

A method of password management is password blacklist which consists of a database that contains the most common passwords used by everyday users which hackers may have access to in order to obtain the details of a victim to steal or misuse their data [35]. Therefore, organisations are also compelled to create a password blacklist database for their employees to avoid using the common password for protection on their accounts in order to avoid infiltration by hackers that could use the account for their own profit or to ruin the reputation of the organisation. Organisations can also use the password blacklist method to help identify if the password entered by the user when creating an account on their webpage is too strong or too weak [28]. This is done by comparing the user-entered password to the database containing all the common passwords users tend to use to give a feedback to the user to inform them if the password they had entered is too weak or suitable [31].

Another form of protection provided by password blacklists is that since the attacker is reliant on guessing the password using common passwords, the login feature will have a limit to the amount of entries that the user is allowed to make before requiring a secondary authentication to unlock the account for security purposes. This prevents the attacker from repeatedly attempting to guess the password or using a software application to automatically enter the common passwords continuously until the correct one is inserted [26]. From a personal perspective and from the research conducted, password blacklisting is a vital method for enterprises or users creating a password for financial services as a successful phishing attack on an employee can cause substantial damage to the enterprise as well as the loss of a user's credentials can be a major blowback for the company as well as the user [30]. Therefore, ensuring that creating a password with simple character switch-ups is not ideal for protecting the sensitive data.

X. Password Sharing

Password sharing is a form of password management as enterprises may decide to share the passwords to other employees or databses using software applications such as Excel, Spreadsheet etc. The passwords can also be shared by users to other individuals by using methods such as email or messaging. According to [31], users who consisted of a lack of perseverance on their password security or with high self monitoring tend to share their password to others without much care. [32] conducted an investgation where they had asked the youth if they had shared their passwords with their friends. From this investigation it was determined that 84% of the youth did not share their password and 16% had shared it between 1-2 times or 5+ times. This shows that the youth is unaware of the potential risks of sharing their password to their friends as the password could potentially be misused or shared across by the recipitent of the password. Therefore, enterprises strongly advise their customers not to share their passwords or PIN codes for fiancial banking to other people as they will no longer have the protection of the business for their accounts which in turn makes the customer liable for the damages done without being able to hold the company responsible [34].

From conducted research and personal opinion, password sharing is not recommended to be done through unsafe methods such as in messaging or email as phishing attackers or hackers may be able to gain access to the password using brute force attack so it would be safer to share passwords to another individual face-to-face to avoid a hard copy of the password that can be accessed at any moment [33]. This may apply for companies as the user can provide the password or PIN through the phone instead of using software.

XI. Continuous Backups

Continuous backups are required to ensure that the data that has been infiltrated or misused by hackers after conducting a successful operation in a phishing attempt is retrievable despite being stolen or deleted. Since the rise of phishing attacks and methods as well as the importance of data stored online, computing and wireless devices now contain a facility to be able to backup their data onto another device or within the cloud. Therefore, in the event of a phishing attack if data has been stolen, the user will be able to retrieve the lost data due to backup [35]. However, this process requires the user to complete continuous backups to ensure that the data stored is up to date which can be done by applying a frequency of when to backup the data which can be determined by the convenience of the user or by constantly doing a backup every night for Apple iPhone using the backup feature. This entails that backups are necessary for when the password is breached due to poor password management to minimalise the damage or to readjust the data if possible, to make the stolen data invaluable.

References

[1] Bailey, D.V., Dürmuth, M. and Paar, C., 2014, September. Statistics on password re-use and adaptive strength for financial accounts. In International Conference on Security and Cryptography for Networks (pp. 218-235). Springer, Cham. [Accessed 7 Dec. 2019].

[2] Riley, S., 2006. Password security: What users know and what they actually do. Usability News, 8(1), pp.2833-2836. [Accessed 7 Dec. 2019].

[3] Margaret Rouse - Definition from WhatIs.com (2019). What is password? - Definition from WhatIs.com. [online] SearchSecurity. Available: https://searchsecurity.techtarget.com/definition/password. [Accessed 8 Dec. 2019].

[4] I. Ghafir and V. Prenosil, "Malicious File Hash Detection and Drive-by Download Attacks," International Conference on Computer and Communication Technologies, series Advances in Intelligent Systems and Computing. Hyderabad: Springer, vol. 379, pp. 661-669, 2016.

[5] Das, M.L., 2009. Two-factor user authentication in wireless sensor networks. IEEE transactions on wireless communications, 8(3), pp.1086-1090. [Accessed 11 Dec. 2019].

[6] U. Raza, J. Lomax, I. Ghafir, R. Kharel and B. Whiteside, "An IoT and Business Processes Based Approach for the Monitoring and Control of High Value-Added Manufacturing Processes," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[7] Aloul, F., Zahidi, S. and El-Hajj, W., 2009, May. Two factor authentication using mobile phones. In 2009 IEEE/ACS International Conference on Computer Systems and Applications (pp. 641-644). IEEE. [Accessed 11 Dec. 2019].

[8] Schneier, B., 2005. Two-factor authentication: too little, too late. Communications of the ACM, 48(4), p.136. [Accessed 11 Dec. 2019].

[9] I. Ghafir, V. Prenosil, and M. Hammoudeh, "Botnet Command and Control Traffic Detection Challenges: A Correlation-based Solution." International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 7(2), pp. 27-31, 2017.

[10] Chiasson, S., Forget, A., Stobert, E., Van Oorschot, P.C. and Biddle, R., 2009, November. Multiple password interference in text passwords and click-based graphical passwords. In Proceedings of the 16th ACM conference on Computer and communications security (pp. 500-511). ACM. [Accessed 12 Dec. 2019].

[11] I. Ghafir, J. Svoboda, V. Prenosil, "A Survey on Botnet Command and Control Traffic Detection," International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 75-80, 2015.

[12] Utin, D., Cambridge Interactive Dev Corp, 2013. Password encryption key. U.S. Patent 8,447,990. [Accessed 12 Dec. 2019].

[13] Thomas Pornin - Encrypting With Passwords - Encryption of Key vs. Data 2015

[14] https://security.stackexchange.com/questions/88984/encrypting-with-passwords-encryption-of-key-vs-data [Accessed 12 Dec. 2019].

[15] I. Ghafir and V. Prenosil, "Advanced Persistent Threat and Spear Phishing Emails." International Conference Distance Learning, Simulation and Communication. Brno, Czech Republic, pp. 34-41, 2015.

[16] Adams, A., Sasse, M.A. and Lunt, P., 1997. Making passwords secure and usable. In People and Computers XII (pp. 1-19). Springer, London. [Accessed 13 Dec. 2019].

[17] J. Svoboda, I. Ghafir, V. Prenosil, "Network Monitoring Approaches: An Overview," International Journal of Advances in Computer Networks and Its Security (IJCNS), vol. 5(2), pp. 88-93, 2015.

[18] Table data: https://www.statista.com/chart/4974/social-media_-people-still-use-pathetic-passwords/ [Accessed 13 Dec. 2019].

[19] Ijiri, Y., Sakuragi, M. and Lao, S., 2006, May. Security management for mobile devices by face recognition. In 7th International Conference on Mobile Data Management (MDM'06) (pp. 49-49). IEEE. [Accessed 13 Dec. 2019].

[20] I. Ghafir, V. Prenosil, M. Hammoudeh, T. Baker, S. Jabbar, S. Khalid and S. Jaf, "BotDet: A System for Real Time Botnet Command and Control Traffic Detection," IEEE Access (IF=4.098), vol. 6, pp. 1-12, 2018.

[21] Duc, N.M. and Minh, B.Q., 2009. Your face is not your password face authentication bypassing lenovo–asus–toshiba. Black Hat Briefings, 4, p.158. [Accessed 13 Dec. 2019].

[22] I. Ghafir, J. Svoboda and V. Prenosil, "Tor-based malware and Tor connection detection," International Conference on Frontiers of Communications, Networks and Applications. Kuala Lumpur, Malaysia, pp. 1-6, 2014.

[23] Caruso, R.D., 2003. Personal computer security: Part 1. Firewalls, antivirus software, and Internet security suites. Radiographics, 23(5), pp.1329-1337. [Accessed 14 Dec. 2019].

[24] I. Ghafir, M. Husak and V. Prenosil, "A Survey on Intrusion Detection and Prevention Systems," IEEE/UREL conference, Zvule, Czech Republic, pp. 10-14, 2014.

[25] Nie, J. and Hu, X., 2008, December. Mobile banking information security and protection methods. In 2008 International Conference on Computer Science and Software Engineering (Vol. 3, pp. 587-590). IEEE. [Accessed 14 Dec. 2019].

[26] I. Ghafir, V. Prenosil, M. Hammoudeh and U. Raza, "Malicious SSL Certificate Detection: A Step Towards Advanced Persistent Threat Defence," International Conference on Future Networks and Distributed Systems. Cambridge, United Kingdom, 2017.

[27] Florêncio, D., Herley, C. and Van Oorschot, P.C., 2014. An administrator's guide to internet password research. In 28th Large Installation System Administration Conference (LISA14)(pp. 44-61). [Accessed 14 Dec. 2019].

[28] De Carnavalet, X.D.C. and Mannan, M., 2014, February. From Very Weak to Very Strong: Analyzing Password-Strength Meters. In NDSS (Vol. 14, pp. 23-26). [Accessed 14 Dec. 2019].

[29] I. Ghafir and V. Prenosil. "Proposed Approach for Targeted Attacks Detection," Advanced Computer and Communication Engineering Technology, Lecture Notes in Electrical Engineering. Phuket: Springer International Publishing, vol. 362, pp. 73-80, 9, 2016.

[30] Habib, H., Colnago, J., Melicher, W., Ur, B., Segreti, S., Bauer, L., Christin, N. and Cranor, L., 2017. Password creation in the presence of blacklists. Proc. USEC, p.50. [Accessed 15 Dec. 2019].

[31] I. Ghafir and V. Prenosil, "DNS query failure and algorithmically generated domain-flux detection," International Conference on Frontiers of Communications, Networks and Applications. Kuala Lumpur, Malaysia, pp. 1-5, 2014.

[32] Whitty, M., Doodson, J., Creese, S. and Hodges, D., 2015. Individual differences in cyber security behaviors: an examination of who is sharing passwords. Cyberpsychology, Behavior, and Social Networking, 18(1), pp.3-7. [Accessed 15 Dec. 2019].

[33] Meter, D.J. and Bauman, S., 2015. When sharing is a bad idea: the effects of online social network engagement and sharing passwords with friends on cyberbullying involvement. Cyberpsychology, Behavior, and Social Networking, 18(8), pp.437-442. [Accessed 15 Dec. 2019].

[34] I. Ghafir, V. Prenosil, M. Hammoudeh, F. J. Aparicio-Navarro, K. Rabie and A. Jabban, "Disguised Executable Files in Spear-Phishing Emails: Detecting the Point of Entry in Advanced Persistent Threat." International Conference on Future Networks and Distributed Systems. Amman, Jordan, 2018.

[35] Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G. and Furlong, M., 2007, April. Password sharing: implications for security design based on social practice. In Proceedings of the SIGCHI conference on Human factors in computing systems(pp. 895-904). ACM. [Accessed 15 Dec. 2019].

[36] Bloch, S., Demirbasa, S. and Curry, A., Data Transfer and Communications Ltd, 2006. Data security device. U.S. Patent 7,054,594. [Accessed 15 Dec. 2019].