A Study on the Security of Authentication Systems

Otuekong Umoren, Hector Marco-Gisbert
School of Computing, Engineering and Physical Sciences
University of the West of Scotland
High St, Paisley PA1 2BE, UK
Email: {Otuekong.Umoren,Hector.Marco}@uws.ac.uk

***Abstract*—In the age of digitalization, passwords play a significant role to protect user information. The growing number of data breaches has become a major problem allowing unauthorised parties to access confidential data. Over the years, passwords have been the first factor of authentication that is used in various segments, such as web applications, banking, e-commerce, and applications for authentication, etc. In most cases, the passwords are usually assigned to or created by the authorized user, and must be kept secret to keep unauthorized users from having access to information it is meant to protect. However, recent attacks have shown that these passwords are vulnerable to attacks such as, the dictionary, brute force, man in the middle, traffic interception, social engineering, and key logger attack, etc. In this paper, we discuss different types of passwords that prevent unauthorised access to protect users' information. We analyze various attack techniques that are leveraged in many ways to obtain passwords. We also discuss the available protection techniques that aim to protect passwords. However, our analysis reveals that the protection techniques are not sturdy and fail to provide enough protection against the most utilised attack techniques, hence, requiring to have more advanced techniques in place.**

Keywords–graphical password; cryptographic key; password authentication; graphical authentication; biometric.

I. INTRODUCTION

The use of passwords to authenticate users has been a common practice all over the world. The username and password best describes the single-factor authentication [1], these passwords, which are usually what the authorized user knows and are mainly used by Automated Teller Machine (ATM), web applications, mobile applications, computers, automobiles, etc. The passwords serves as a layer of protection for user information and other valuable data. The best way to secure a piece of information is to allow access to only the authorized user [2]. However, passwords have several issues, one of those is the limitations of humans to recall alphanumeric passwords, as a good password should be easy to remember by the authorized user and hard to guess by an unauthorized user [3] [4]. Users hardly select passwords that are easy to recall and difficult to guess, Yan et al. in their publication identified the limitations of human memory as one of the issues of password authentication [5]. If users were not needed to recall passwords, a password that is difficult with long characters and strings to be used as long as the system permits it.

The words that most users can recall are usually names or short dictionary words, which makes these passwords vulnerable to dictionary attacks [6]. Some users often have this false idea that using popular slangs and keyboard layout or arrangement like "QWERTY" constructs strong passwords because those words cannot be found in the dictionary. An incident occurred on a social web application "rockyou.com", where there was a security breach and users' credentials that were stored in plaintext were compromised. The poor password policies were major vulnerabilities in their system [2]. Some passwords use words or names in users' native language that are easy to remember but are also vulnerable to dictionary attacks, while other passwords are difficult to recall and secure against guessing. In order to have a strong password in place, the user might want to write the password in a secure place but that could also lead the password to be compromised [5]. The users can set complex text-based passwords, which can be difficult to remember as well as difficult to break, whereas simple passwords can be easily remembered and it may not take much effort to compromise [7]. Despite their vulnerabilities, passwords still have an important role in users' experience on the web application, mobile application, and many other areas where security is needed [8]. Hence, it is very important to have a proper security measure in place to have a sturdy password.

This paper is organized as follows: In Section II, we discuss different aspects of currently implemented passwords types. Section III reviews various security threats that can be executed to compromise user passwords. In Section IV, we talk about the current protection techniques that are in place to provide security. Section V analyses the major authentication techniques in terms of security, vulnerability, and possible attacks. Finally, the concluding Section VI discusses the accomplishments from this research work. It also indicates the future work to be initiated to meet the current challenges revealed through this research.

II. BACKGROUND

In this section, we discuss various aspects of the passwords that are utilised in the current digital format. Our discussion includes reviewing the basic features and also weaknesses of the password types to determine their robustness.

A. Text-based passwords

Text-based passwords are the most implemented and widely adopted passwords in various segments. While humans find it difficult in recalling complicated passwords, various schemes are available to assist users to keep multiple passwords secure. The major problems associated with passwords are memorizing strong passwords and also they are vulnerable to various pernicious attacks. Text-based passwords have been considered insecure for long, and mostly replaced by graphical passwords that can be considered to have improved security and usability [9]. In most cases, a strong password should comprise upper and lower case characters (a-z, A-Z), numbers,

 ISBN: 978-1-61208-811-2

and special characters. They should not be based on language, names, slangs, and must not contain meaningful information, and also must not be written down [10]. Users tend to use different passwords for different networks. In most cases, the password that is being used less, often difficult to remember when having many passwords [3]. The use of a text-based password on multiple platforms or password reuse is often not advisable, because if the password is compromised on one platform, it could be used on another platform or account by the attacker.

B. Graphical Passwords

Graphical passwords are authentication systems that authenticate users through the selection of images or locations on images [11]. It is an authentication scheme where the authorized user is authenticated or the identity of the authorized user is verified through their knowledge on images or graphical objects. This authentication method is often considered as a very secure authentication method. It has its strengths and advantages, such as reduced spoofing attacks. However, like any other authentication methods, it also has weaknesses. One of the major disadvantages is the usability issue [12]. Graphical authentication is categorized into three parts, these are cued recall, recognition, and recall-based authentications. In the recognition-based authentication, the user must recognize and choose images seen previously, while in the recall-based authentication, the user must choose spots on the images [3]. The server requires to store the images and prepare one or more challenges for users for every round of the authentication. Like other authentication systems, graphical authentication has it's vulnerabilities, the most common and obvious is the shoulder surfing attack.

C. Biometric

This authentication method of biometric works with recognition. Unlike graphical passwords where the recognition process is carried out by the user, the task of recognition is carried out by the biometric authentication system. In this scheme, the user's biometrics, such as fingerprint recognition, face recognition, signature verification, are processed and stored in the database, and those data are matched to authenticate user [12]. Although, the unique nature of some of these biometric features serve as advantages for this authentication method, the cost, and difficulty of implementation can be a major disadvantage.

Biometric authentication techniques use features that cannot be forgotten or misplaced. Such secure authentication approaches are the major features of this authentication system [13]. There are different biometric features used in biometric authentication, these are facial recognition, IRIS technology, hand geometry, retina geometry, voice recognition, etc [14].

1) Finger Print Technology: The fingerprint is described as the impression of the friction edges of the part of the human finger, this comprises of connected ridge units of friction ridge skin [14]. To capture these fingerprints, a fingerprint reader or scanner must be in place. The fingerprint scanners are based on thermal, optical, silicon, or ultrasonic principles. The optical fingerprint scanners are the most common, work by capturing the reflection changes on the areas where the fingers touch on the surface of the scanner. They are based on a source of light, a light sensor, and a reflection surface that changes reflection as the pressure changes.

2) Facial Recognition: The facial recognition technology uses a computer application and camera, digital image, or video to identify and verify a person. It is categorized into two parts; the facial metric relies on both the position and distances of the facial features, and the eigenface, which is based on a fixed set of eigenfaces [14].

3) IRIS Technology: IRIS technology uses a video-based image acquisition system to obtain the unique patterns of the iris of the eye. This iris pattern is captured by a grayscale camera within a distance of 10 to 40 centimeters of the camera. When the grayscale image of the iris is captured, the computer application attempts to locate the iris in the image, and creates a net of curves if the iris is found [14].

III. Security Threats

Password vulnerability is not restricted to platforms, operating systems, web applications, or devices such as routers. Attackers use different methods to steal passwords, sometimes with the help of bugs and outdated or insecure firmware. In this section, we analyze various attack techniques that are executed to steal users' passwords.

A. Brute Force Attack

The brute force attack applies to all the possible password characters and combinations to break encrypted passwords usually when the passwords are saved as encrypted text. This attack technique is also known as an exhaustive key search and can be used on any encrypted data [15]. Although, the attack method is considered to be time-consuming but relatively very effective on passwords that are short [12]. It involves an intensive combination search, similar to a burglar trying all possible combinations on a safe [16]. Brute force attacks can be made more effective through the use of a time-space trade-off, such as Oechslin's rainbow technique, which speeds up the process of breaking passwords [17].

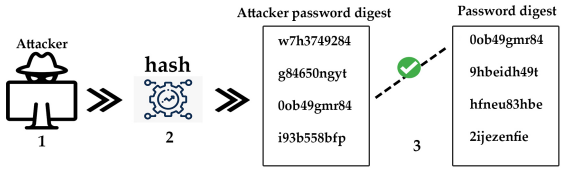

Figure 1. An example of a brute force attack

An authentication system allows unlimited trials; hence, the computational power of the attackers' system plays a vital role for the attack to be successful. In Figure 1, we show that an attacker uses an automated tool. For the attack to be successful, three attacking steps are conducted; 1. Attempt with different password combinations with several trials, the generated passwords are then hashed. 2. The digest requires to be compared to those in the stolen file, and 3. A match is found with the correct password's digest.

B. Dictionary Attack

In a dictionary attack, the attacker uses a combination of meaningful words, mostly daily and occurring words, and tries

to match those words with the password. Many users tend to use names, slang, or their favorite things as passwords, this makes this attack relatively easier than a brute force attack [12]. The dictionary attack checks the words in the dictionary and tries to match the passwords with those words; for instance, English words from the English dictionary, Slang from attackers dictionary, etc.

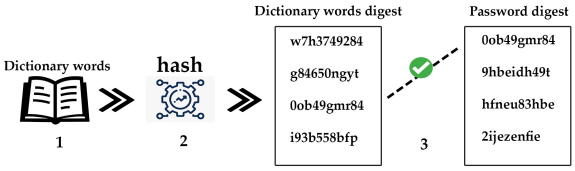

Figure 2. An example of a dictionary attack

An example of a dictionary attack is shown in Figure 2. The attack goes through 3 steps; 1. The attacker generates digests from dictionary words. 2. The digests are then compared to those in the stolen digest file, and 3. The process continues until a match is found.

C. Shoulder Surfing

In this attack, the attacker monitors and observes the victims as they input their password. The attacker usually pays attention to the victim's keyboard to see the combination of keys. There are several ways this attack can be accomplished. The attacker can make use of a hidden Close Circuit TV Camera (CCTV) to observe the victim's activity from another location [12]. Shoulder surfing attack involves an attacker spying on the victim during the user's login activity [18].

D. Phishing Attack

A phishing attack is a web-based attack where the attacker redirects the victim to a legitimate website with the aim of stealing the victim's password [12]. Assume a scenario in which the user needs to visit `www.facebook.com` but is directed to a copy with `www.faceb00k.com` by the attacker. The user unknowingly inputs his login information, presuming that to be a legit website, which is received by the attacker. Once the attack is accomplished, the attacker redirects the victim to the legitimate website.

A phishing attack could be executed by an attacker by masquerading as a known service to trick a user into giving away information. Some users usually fall victim to this because they only depend on visual cues to identify these web applications. A simple execution of this attack would require the attacker to create an identical copy of legitimate websites or an email address similar to a legitimate email address, these looks very convincing to users, especially when the users are not familiar with the browser security indicators and have to depend on what they see for protection [19].

For phishing attacks to be successful, a man-in-the-middle attack must be executed first. An example of a phishing attack is shown in Figure 3. The very first step involves the attacker sending an email with a fake page to Alice. Alice visits the malicious page sent by the attacker. In the next step, any data input by Alice is sent to the attacker. Finally, the attacker uses the credentials to visit the real page.

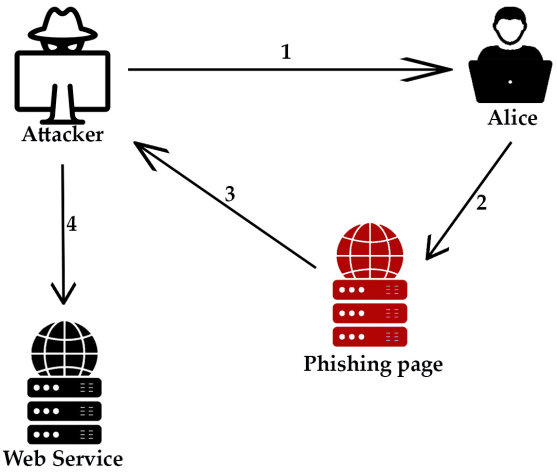

Figure 3. An example of phishing attack

E. Keyloggers

The keyloggers or key sniffers are software programs that are secretly installed on the victim's device [12]. The program monitors the victim's activities by observing and recording the keys pressed by the victim. The keylogger creates a log file of the keys used by the victim and sends this log file to the attacker usually through an email address. Hardware keyloggers are also very beneficial to conduct this attack [20]. The hardware keyloggers are small electronic devices plugged at the end of the cable of the keyboard, inside the keyboard or installed inside the computer. The devices store the keystrokes in their in-built memory after they are attached to the computer, and often remain undetected by the antivirus.

F. Video Recording Attack

In this attack, the victim's password or keyboard activities are recorded using a video recording device such as a cell phone [12]. The attacker monitors the video for the attack to be successful. This attack serves the same purpose as a shoulder surfing attack, and can be very effective if properly executed. An attacker may perform the video recording on-site or prior to executing the attack [21]. Depending on the device used a video usually can be recorded from 2 to 9 meters. Since, many users tend to use similar patterns, the captured data from victim's device can be used to compromise other devices of the victim.

G. Spoofing Attack

In this attack, the victim is presented with a copy of a known legitimate website requiring the victim to input his username and password [22]. Both the username and password are then saved on the attacker's device without the victim being aware of the incident. Any digital medium that is connected through the network can be spoofed, for example, Internet Protocol cameras, wireless networks, etc. The wireless networks are most vulnerable to spoofing attacks as the attack method can result in various other attack techniques [23].

There are various types of spoofing attacks, such as Address Resolution Protocol (ARP), Domain Name System (DNS), and Internet Protocol (IP) spoofing. Figure 4 shows a DNS spoofing attack where the attacker injects a fake DNS

 ISBN: 978-1-61208-811-2

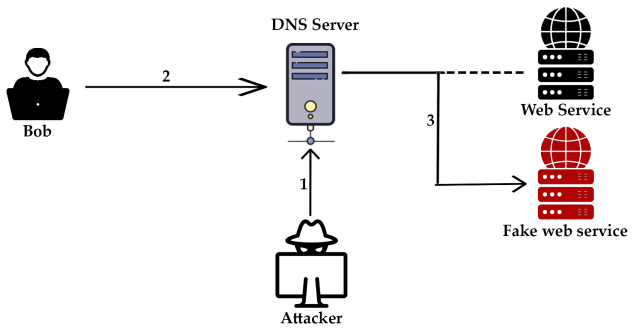

Figure 4. An example of a DNS spoofing attack

entry into the DNS server. BOB sends a request to visit his intended website; however, Bob's request is redirected to the malicious website enabling the attacker to exploit.

H. Sweeper Attack

In this attack technique, the attacker takes advantage of the password autofill function to steal user's login credentials for several websites at the same time without the user having a visit to those websites. This attack method works on password managers that support sync services and the autofill function [24]. It is popularly executed in web browsers through input fields and can be used to harvest users' login details, debit card information, and other personal data.

I. Man-in-the-Middle Attack (MITM)

In this attack technique, an attacker monitors communications between users to capture the transmitted data [25]. This attack is usually performed in a Local-Area Network (LAN), and enabling the attacker to perform both DNS spoofing and Denial-of-Service (DoS) attacks [26]. Man-in-the-Middle Attack (MITM) exploits the system where the HTTP server sends a certificate to the web browser using its public key [27]. If the certificate does not come from a trusted source, the communication path becomes vulnerable enabling the attacker to replace the legitimate certificate from the HTTP server with a fake certificate.

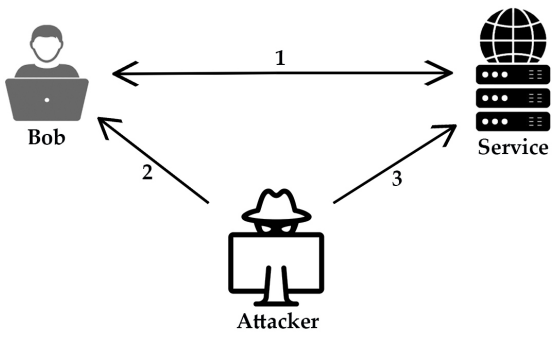

Figure 5. An example of man in the middle attack

A successful MITM permits an attacker a channel to carry out other attacks, such as the phishing attack. An example of MITM is shown in Figure 5. Bob is connected to a website, where the attacker monitors communication between Bob and the service. The attacker is able to capture the transmitted data.

IV. Current Protection Techniques

In this section, we discuss 3 most advanced protection techniques that are available to defend against the attacks discussed in Section III.

A. Graphical Authentication

The concept of graphical passwords works with the user being authenticated with images [28]. Graphical passwords were introduced to remove the burden of human memory, this means by clicking an image or drawing, a complicated password can be created that the user would not memorize. Typically, the user has to select points on the image to get authenticated. The system is built on recognition, whereby the user must recognize previously seen images and choose memorable locations on these images. With the type of graphical password system, the user might be required to perform recall asks and recognition tasks. The graphical password is proposed as an alternative to text-based passwords [7]. Graphical authentication replaces text-based passwords with images since humans can recall details in static pictures better than words. In other words, humans can remember things they have seen for a long time, which makes graphical passwords easy to recall and difficult to guess.

B. Biometric Authentication

Biometric authentication systems validate user's identity through human features, physiological and behavioral traits [14]. These features are unique and provide users with secure and automatic recognition. The system helps overcome the problems and limitations in authentication systems. Biometric system is classified into unimodal and multimodal; the unimodal system uses one biometric feature and the multimodal system uses multiple biometric features. The multimodal system is improved and overcomes the limitations of the unimodal systems that focus on the inaccuracy in the unimodal system.

C. Token-Based Authentication

A token is a string that a server generates for a client and can be passed through an HTTP request [35]. The client's application exchanges authentication credentials for an authentication token and when requested it just sends the token. When the server receives the token, it looks for the credential of the user to determine if the user is authorized to the requested information. Tokens usually have an expiration time, after that they become invalid. However, there is a possibility for tokens to be leaked while they remain valid. A server is able to determine if a token is too old and could reject it if it is invalid [35]. Both hardware and software tokens are utilized. Hardware tokens are usually physical devices, where the software tokens are applications on devices, an example is the Google authenticator application. The tokens display random digits called One-Time Passwords. The One-Time password is a common form of authentication in a multi-factor authentication and are generated randomly by a server. These randomly generated passwords are used once and are resistant to sniffing and replay attacks.

V. Security Analysis

In this section, we analyse the major password-based attacks towards the available protection techniques discussed in

Section IV. Our analysis shows the effectiveness of protection techniques.

The brute force attack possesses a high risk to authentication systems. Although the large password space of graphical authentication is robust and effective, it does not offer full protection against brute force [31]. The attackers' chance and ability to break a large password fully rely on the obtained computational power. The biometric authentication's randomly created passwords offer almost similar protection against brute force attacks as graphical authentication; however, the randomly created passwords fail to provide complete protection against brute force attacks [32]. Token-based authentication offers high-level protection against brute force attacks. The short lifetime of the randomly generated passwords makes the token-based authentication somewhat resistant to brute force attacks [32].

Dictionary attack does not pose great risks on the protection techniques as it does with brute force attack. However, it requires a lot of effort on recognition-based graphical passwords than recall-based graphical passwords [29]. The biometric authentication and token-based authentication are both resistant and highly effective against a dictionary attack. The biometrics' data upon its extraction is converted and stored as random digits or random alphanumeric texts. The randomly generated one-time passwords and their short life-time is also very effective against the dictionary attack [32].

Shoulder surfing can be very destructive if executed properly. Graphical authentication cannot be relied on for complete protection against shoulder surfing [29]. The authentication activity carried out on the screen could be exposed to an attacker, thus it does not make graphical authentication effective against shoulder surfing. Biometric authentication is very effective against shoulder surfing. Although, token-based authentication is resistant to shoulder surfing, the possibility of exploitation mainly depends on the short lifetime of the one-time-passwords [32]. A short lifetime makes the system effective, whereas a long lifetime makes it vulnerable.

All the discussed protection techniques are very effective against spyware and malware. Graphical authentication is resistant to spyware as the authentication activity is carried out on screen [11]. The biometric and token-based authentication, on the other hand, may generate some security concerns. The short lifetime of the one-time password makes the token-based authentication resistant to this spyware. Spoofing attacks is a scalable attack, the graphical authentication is effective against this attack. Biometric authentication is vulnerable to a spoofing attack. On the other hand, Token-based authentication is resistant to the spoofing attack. Graphical authentication is very effective against a man-in-the-middle attack, the man-in-the-middle attack is not feasible on graphical authentication. Biometric authentication is vulnerable to this attack, this is possible through a spoofing attack [33], that makes the biometric authentication less effective on this attack.

A combination of two or three protection techniques discussed would mitigate attacks such as the brute force, dictionary, shoulder surfing, man-in-the-middle attack, and spyware, hereby protecting systems. This combination would consist of the graphical authentication and the token-based authentication in a two-factor authentication, with the graphical password as the primary authentication and token-based authentication as the secondary authentication. As shown in Table I, token-based authentication is more effective than other discussed protection techniques. The table highlights notable security features in the protection techniques, their respective vulnerabilities and attacks that would exploit these vulnerabilities. A combination of graphical authentication (knowledge factor) and biometric authentication (inherent factor) would be decent for security and usability. However, the combination of the graphical password (knowledge factor) and token-based authentication (possession factor) in a two factor authentication would be the best combination of the discussed protection techniques to mitigate security threats such as the dictionary, brute force, shoulder surfing, malware and spyware (key loggers), spoofing and phishing attacks.

VI. Conclusion And Future Work

In this paper, we have discussed various passwords types showing their vulnerability by indicating various security threats. We have also discussed the current protection techniques, and outlined the challenges of authentication systems. Our analysis has shown that although traditional attacks, such as spyware, brute force attacks, etc, are difficult to execute on graphical and biometric authentication, graphical passwords make some resistance. However, graphical passwords are not widely used and vulnerable to attacks in different ways. We have also shown that text-based passwords are not secure enough and are vulnerable to major attacks, whereas the biometric, token-based and graphical authentication are making it more difficult to break passwords. Furthermore, we have revealed that all protection techniques fulfill the purpose of security to a minimal extent, but vulnerable to different attacks. Therefore, a robust security technique should be in place.

For our future work, we aim to design a sturdy security technique considering the limitations revealed through this research. The future research work will be an ultimate security approach mitigating the vulnerabilities discussed in this paper.

TABLE I. Authentication techniques and their vulnerability to attacks

Authentication Technique	Security features	Vulnerabilities	Possible Attacks
Graphical Passwords	Large password space [29], Decoys [30] randomly assigned images [31]	User's activity can easily be monitored on screen [29]	Brute force search [31] [29], Guessing [29], Shoulder surfing [29], spyware [29], Dictionary attack [29]
Biometric	Randomly created passwords, Limited attempts [32]	Biometric hardware [33]	Spoofing attack [33] [34], Denial-of-service attack [33], Replay attack [33], Man-in-the-middle attack [33]
Token-based	Short token life time [32], Large entropy [32], One-time password [32]	Difficult to replace [32]	Lost or stolen token [32], Denial of service [32]

 ISBN: 978-1-61208-811-2

REFERENCES

[1] A. Nath and T. Mondal, "Issues and challenges in two factor authentication algorithms," International Journal of Latest Trends in Engineering and Technology (IJLTET), ResearchGate, 2016, pp. 318–327.

[2] T. Touchette, B. Hewitt, and M. Huson, "Password security: What factors influence good password practices," 03 2012, pp. 1–9.

[3] S. Wiedenbeck, J. Waters, J.-C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical passwords: Effects of tolerance and image choice," in Proceedings of the 2005 symposium on Usable privacy and security, 2005, pp. 1–12.

[4] E. M. W. R. Chowdhury, M. S. Rahman, A. B. M. A. A. Islam, and M. S. Rahman, "Salty secret: Let us secretly salt the secret," in 2017 International Conference on Networking, Systems and Security (NSysS), 2017, pp. 115–123.

[5] J. Yan, A. Blackwell, R. Anderson, and A. Grant, "Password memorability and security: Empirical results," IEEE Security & privacy, vol. 2, no. 5, 2004, pp. 25–31.

[6] S. T. Haque, M. Wright, and S. Scielzo, "A study of user password strategy for multiple accounts," in Proceedings of the third ACM conference on Data and application security and privacy, 2013, pp. 173–176.

[7] A. Gokhale and V. Waghmare, "Graphical password authentication techniques: A review," International Journal of Science and Research (IJSR) ISSN (Online Index Copernicus Value Impact Factor, vol. 14, no. 7, 2013, pp. 1–7.

[8] D. Florencio and C. Herley, "A large-scale study of web password habits," in Proceedings of the 16th international conference on World Wide Web, 2007, pp. 657–666.

[9] Z. Li, W. He, D. Akhawe, and D. Song, "The emperor's new password manager: Security analysis of web-based password managers," in 23rd {USENIX} Security Symposium ({USENIX} Security 14), 2014, pp. 465–479.

[10] D. Charoen, "Password security," International Journal of Security (IJS), vol. 8, no. 1, 2014, p. 1.

[11] G. Agarwal, S. Singh, and R. Shukla, "Security analysis of graphical passwords over the alphanumeric passwords," International Journal of Pure and Applied Sciences and Technology, vol. 1, no. 2, 2010, pp. 60–66.

[12] M. Raza, M. Iqbal, M. Sharif, and W. Haider, "A survey of password attacks and comparative analysis on methods for secure authentication," World Applied Sciences Journal, vol. 19, no. 4, 2012, pp. 439–444.

[13] V. Matyáš and Z. Říha, "Biometric authentication — security and usability," in Advanced Communications and Multimedia Security. Springer, 2002, pp. 227–239.

[14] M. C. Debnath Bhattacharyya, Rahul Ranjan and F. Alisherov, "Biometric authentication: A review," International Journal of u-and e-Service, Science and Technology, vol. 2, no. 3, 2009, pp. 13–28.

[15] K. Apostol, "Brute-force attack," 2012.

[16] N. Kumar, "Investigations in brute force attack on cellular security based on des and aes," IJCEM International Journal of Computational Engineering & Management, vol. 14, 2011, pp. 50–52.

[17] P. Oechslin, "Making a faster cryptanalytic time-memory trade-off," in Annual International Cryptology Conference. Springer, 2003, pp. 617–630.

[18] S. Man, D. Hong, and M. Matthews, "A shoulder-surfing resistant graphical password scheme - wiw." vol. 3, 01 2003, pp. 105–111.

[19] I. Fette, N. Sadeh, and A. Tomasic, "Learning to detect phishing emails," in Proceedings of the 16th international conference on World Wide Web, 2007, pp. 649–656.

[20] S. Sagiroglu and G. Canbek, "Keyloggers: Increasing threats to computer security and privacy," IEEE technology and society magazine, vol. 28, no. 3, 2009, pp. 10–17.

[21] G. Ye, Z. Tang, D. Fang, X. Chen, W. Wolff, A. J. Aviv, and Z. Wang, "A video-based attack for android pattern lock," ACM Transactions on Privacy and Security (TOPS), vol. 21, no. 4, 2018, pp. 1–31.

[22] G. C. Kessler, "Passwords - strengths and weaknesses," Intemet and Internetworking Security, 1996.

[23] Y. Chen, W. Trappe, and R. P. Martin, "Detecting and localizing wireless spoofing attacks," in 2007 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks. IEEE, 2007, pp. 193–202.

[24] D. Silver, S. Jana, D. Boneh, E. Chen, and C. Jackson, "Password managers: Attacks and defenses," in 23rd {USENIX} Security Symposium ({USENIX} Security 14), 2014, pp. 449–464.

[25] R. Rahim, "Man-in-the-middle-attack prevention using interlock protocol method," ARPN J. Eng. Appl. Sci, vol. 12, no. 22, 2017, pp. 6483–6487.

[26] G. N. Nayak and S. G. Samaddar, "Different flavours of man-in-the-middle attack, consequences and feasible solutions," in 2010 3rd International Conference on Computer Science and Information Technology, vol. 5. IEEE, 2010, pp. 491–495.

[27] F. Callegati, W. Cerroni, and M. Ramilli, "Man-in-the-middle attack to the https protocol," IEEE Security & Privacy, vol. 7, no. 1, 2009, pp. 78–81.

[28] M. Shukran, M. Yunus, K. B. Maskat, W. Shariff, and M. S. B. Ariffin, "Pixel value graphical password scheme-graphical password scheme," Australian Journal of Basic and Applied Sciences, vol. 7, no. 4, 2013, pp. 688–695.

[29] S. S. Biswas and S. Sankar, "Comparative study of graphical user authentication approaches," International Journal of Computer Science and Mobile Computing, vol. 3, 2014, pp. 361–375.

[30] R. G. Rittenhouse, J. A. Chaudry, and M. Lee, "Security in graphical authentication," International Journal of Security and Its Applications, vol. 7, no. 3, 2013, pp. 347–356.

[31] M. D. Hafiz, A. H. Abdullah, N. Ithnin, and H. K. Mammi, "Towards identifying usability and security features of graphical password in knowledge based authentication technique," in 2008 Second Asia International Conference on Modelling & Simulation (AMS). IEEE, 2008, pp. 396–403.

[32] L. O'Gorman, "Comparing passwords, tokens, and biometrics for user authentication," Proceedings of the IEEE, vol. 91, no. 12, 2003, pp. 2021–2040.

[33] M. Joshi, B. Mazumdar, and S. Dey, "Security vulnerabilities against fingerprint biometric system," arXiv preprint arXiv:1805.07116, 2018.

[34] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," IBM systems Journal, vol. 40, no. 3, 2001, pp. 614–634.

[35] J. Kubovy, C. Huber, M. Jäger, and J. Küng, "A secure token-based communication for authentication and authorization servers," in International Conference on Future Data and Security Engineering. Springer, 2016, pp. 237–250.

 ISBN: 978-1-61208-811-2