International Conference on Academic Research in Engineering and Management
IETE, Lodhi Road, Delhi, India (ICAREM-17)
30th April 2017, www.conferenceworld.in ISBN: 978-93-86171-43-6

A SURVEY ON VARIOUS ATTACKS POSSIBLE IN AUTHENTICATION

Tushar R. Mahore[1], Prof. A.V.Deorankar[2]

[1,2] *Computer Science and Engineering, Government College of Engineering, Amravati, India*

ABSTRACT

Internet now a days is one of the most important part of human being, every day with the increase of various web-applications, the security issues is also getting increased. Authentication is one of the common process in allowing a particular user to use the services provided by the web-applications service providers. Authentication requires user's credentials, which may include some personal information, which if goes in wrong hand can be used against the user. So, with the increase of web-application the security is also getting important. In this paper various kinds of attacks are given and how to avoid those attacks some countermeasures are also given. In every web-application not all the security issues are covered. This paper focuses on the attack models which takes very less effort to attack the security of the authentication and focuses on those attacks also which requires little bit more effort but gives accurate results.

Keywords: Graphical Password Authentication; BruteForce Attack; MITM (Man-in-the-Middle attack); Biometric Authentication

I. INTRODUCTION

In the world of internet there are various conventional authentication systems present, in the initial stages of the development of the authentication processes, various flaws has occurred which is responsible for the development of the attack models [1]. On the other hand due to the different attacks, day by day the authentication process gets more secured. Authentication is the process of identifying particular individual, which in result allows the user to gain access to the services provided by the web-application service provider. Authentication is one the most important aspect of the security that has to be addressed effectively [2]. If the security of the authentication is not taken into consideration and can be easily cracked then the other aspects of the security can also be easily compromised. The other aspects of security includes authorization, auditing, confidentiality etc. To protect overall web-application security aspects we have to focus on the authentication security. Various types of authentication methods are present in the world which are discussed in [2]. With all the different types of authentication processes various attacks has also comes into focus which are supposed to be taken into consideration.

Before we take a look on various types of attacks, let's take a look on the different parts of the definition of the attack. It is important to understand the difference between threats, vulnerabilities, and attacks [3]. If there is a weakness in the system it is referred to be as the vulnerability, we can say that is the opening from where the attack is possible. Vulnerability can be occurred because of the weak programming of the application, which gives an opening to the attacker to attack. Threat is the potential danger that may occur. It is just a sign of the

future attack to come. The threat represent incessant danger to an asset. A threat may or may not be intentional and may not cause damage also. On the other hand the attack is the actual damage to an asset, or an unauthorized access to the asset, attack can destroy or modify the asset.

Rest of the paper is arranged in the following way, section 2 describes various authentication methods, section 3 discusses different types of attacks and their countermeasures, and finally section 4 concludes the paper.

II. AUTHENTICATION SCHEMES

Various Human Authentication Techniques are present in Computer World, they are:

1. What you know (Knowledge base authentication)
2. What you have (Token base authentication)
3. What you are (Biometrics base authentication)

The above mentioned authentication processes are currently in use, in different ways at different places. Each and every of them have some advantages and disadvantages.KBA is further classified into two types, (i) Textual Passwords and (ii) Graphical Passwords.

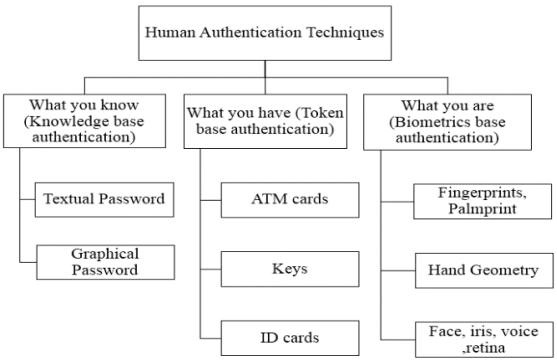

Fig. 1. Taxonomy of Human Authentication Techniques.

2.1. Knowledge Based Authentication

Knowledge based authentication also known as the KBA is the most widely used authentication technique. Near about every web application we see uses the KBA. As the name indicates the KBA requires knowledge of the private information of the individual to show that the person providing the information is the one who is the owner of the identity. In KBA the user has to answer at least one “secrete” question. There are some criteria for the good question in KBA, (a) the question should be appropriate for the large segment of population, (b) the answer is supposed to be easy for remembrance, (c) the question must have only one answer, (d) the answer should be difficult to crack or guess. KBA is further classified into two types, (i) Textual Passwords and (ii) Graphical Passwords.

Textual passwords are the most commonly used authentication technique in computer field. In text based password authentication, the user is supposed to select username and the alphanumeric password, and remember both of them. Graphical passwords are much more popular in mobile devices. Lots of graphical authentication schemes are developed in last few decades. Some of them are very popular among users, such as PIN authentication. Various graphical authentication schemes [4], [5], [6], [7] are present in the world, these schemes are developed to overcome the problems associated with text based passwords. In the early days of graphical authentication there are some restrictions, due to the low pixel quality of the devices. The first idea of

the graphical password has been given by Blonder in 1996. Graphical passwords shows most promising results over the text-based passwords.

2.2. Token Based Authentication

In token base authentication system, security tokens are used to prove one's identity electronically. The token is used in the addition or at the place of passwords to identify the particular user. The tokens acts like electronic key to access something. Various types of tokens are available in the market, which are used for the authentication process. Some of them may consists cryptographic keys, some may have biometric data such as fingerprint, and some of them may possess passwords.

ATM cards are the basic example of the token base authentication, it comes under the connected tokens smart card technology. Smart cards can be very cheap and contain proven security mechanism. Similar to the ATM identity cards and keys are also the example of the token based authentication. ID cards are the most commonly used authentication technique in any organization. ID cards are most popular in these sectors, they contains RFID tags, which at the time of inserting authenticates on the unique tag number.

2.3. Biometrics Based Authentication

Biometrics based authentication is again most common in some of the organizations. Biometrics is a technology which uses physiological or behavioral characteristics to identify or verify a person. Most commonly used characteristics for authentication include fingerprint, face, and iris. A conventional biometric authentication system works in two phases: enrollment and verification. In the enrollment phase, a biometric feature set is extracted from user's biometric data and a template is created and stored in the database. During the verification phase, the same feature extraction algorithm is applied to query biometric data, and the resulting query feature set is used to construct a query template. The query template is matched against the stored template(s) for authentication. Various biometrics authentication techniques are present in the market, such as (a) Fingerprint or Palm-print, (b) Hand Geometry, (c) Face, Iris, Voice, Retina Detection.

All of these techniques are developed in various ways, the development in this field leads to the more secured Authentication schemes. Among these techniques fingerprint is the most popular technique, which uses fingerprint scanner for authentication.

III. VARIOUS POSSIBLE ATTACKS IN AUTHENTICATION

3.1. Eavesdropping attack

In this type of attack the attacker taps the information that goes on the wire and uses in the future to harm the user. Eavesdropping attack may be offline or online. The countermeasure for the attack is that the message can be encrypted using various encryption techniques such as AES, DES, etc. The data transmission can be made secure by using the SSL or much stronger protocol i.e. Kerberos.

3.2. Man-in-the-Middle-Attack

MITM is the kind of an eavesdropping attack, in this kind of attack the attacker comes in the middle of the communication and keeps an eye on the data transferred. The attacker can use this data to harm someone or just observe the conversation and gain the private information. To avoid this type of attack we can use the secure transmission channel. The SSL can be used to secure the communication channel. Replay attack is the part of the MITM attack where the attacker copy the data and used for the nefarious purpose [8].

3.3. Phishing Attack

Phishing attack is the type of attack where the attacker creates a copy of the original authentication web-page and gathers the confidential data. It is an intentional theft of user credential [9]. Phishing attack is actually performed for the stealing purpose of the passwords, credit card information etc. To avoid phishing attack digital certificates can be used. Unsolicited emails should not be attended such as emails from banks requesting for username and password. When an URL is misspelled, it may lead to a phishing attack.

3.4. brute force attack

This is one of the kind of attack which cannot be avoided, one cannot protect the system from the brute force attack. Brute force attack tries number of key combinations on trial and error basis [10]. It tries ever combination to gain the particular required information. The password can be broken easily if the length of the password is very small. Brute Force attack consumes time considerably when the key size is large and the password chosen is strong. A computer program or ready-made software is commonly used for implementing brute force attack. Brute force attack does not work for online services. Because when multiple attempts from a particular IP address is tracked, that particular IP will be blocked by the administrator or that account that is used by an attacker may be blocked. Tarpitting is another techniques used for reducing the speed of an attacker. It creates a delay in authenticating which helps to reduce the number of attacks per minute.

3.5. Dictionary Attack

Dictionary attack is an attack based on the similar type of data the attacker gathers from the observation. It is similar to the brute force attack, the only difference is here the attacker knows which kind of combinations he has to try. The dictionary attack can be avoided by using the strong password. The strong password can be created by using the combination of alphabets (lowercase/uppercase), numbers and special characters.

3.6. Insider Attack

The Insider attack is a type of malicious attack attempted intentionally within an organization [11]. The employees of the organization bestowed with more power and knowledge about the environment initiates such an attack. The system administrators or network managers steal the authentication data or exchange keys. Intrusion Detection System (IDS) helps to mitigate such attacks. Access control mechanism, monitoring and logging must be strictly maintained.

3.7. Keylogger Attack

Keylogger is the computer program which keeps the track of keystrokes on the computer [12]. From this application an attacker can get easily the password. The best way to avoid the keylogger attack is to use the virtual keyboard in which the positions of the characters will change randomly.

3.8. Shoulder Surfing Attack

Attacks using social engineering such as monitoring the keyboard entry by the user or collecting his personal information to verify whether it is used as a password or forms part of the password. Shoulder surfing attack can be avoided by providing wrong information for security questions and by providing passwords with spelling mistakes. While entering a PIN at an ATM or typing password on a keyboard, it can be covered so as to prevent this attack.

3.9. SQL Injection Attack

SQL injection attack is performed on the database, in this type of attack the SQL query is fired in the database intentionally to get the passwords. The attacker can inject SQL commands and gain access to obtain the data

from the database [13]. Patches for OS, software's, and antivirus are to be regularly updated. A proper validation of input data can mitigate SQL Injection attack. Access Control permission on the database must be strictly defined.

IV. CONCLUSION

This survey helps us to take in consideration various possible attacks, while designing the authentication system. Form this survey we can say that depending on the nature of application we can design an authentication system which in future can help in avoiding the possible attacks.

REFERENCES

[1] Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider, "A Survey of Password Attacks and Comparative Analysison Methods for Secure Authentication", World Applied Sciences Journal, vol. 19, pp. 439-444, Jan. 2012.

[2] A. Jesudoss and N.P. Subramaniam, "A Taxonomy of Authentication Techniques for Web Services", International Journal of Engineering Research and Technology, Vol. 3 2014, pp. 271-275.

[3] C. Onwubiko and A. P. Lenaghan, "Managing Security Threats and Vulnerabilities for Small to Medium Enterprises", in Proc. IEEE Intellgienc and Security Informatics, 2007, p. 244-249.

[4] R. Dhamija and A. Perrig, "Deja vu: A user study using images for authentication," in Proceedings of the 9th conference on USENIX Security Symposium-Volume 9. USENIX Association, 2000, pp. 4–4.

[5] "Realuser," http://www.realuser.com/.

[6] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proceedings of the 8th conference on USENIX Security Symposium-Volume 8. USENIX Association, 1999, pp. 1–1.

[7] S. Wiedenbeck, J. Waters, J. Birget, A. Brodskiy, and N. Memon, "Passpoints: Design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 102–127, 2005.

[8] Syverson, P, "A Taxonomy of Replay Attacks", in Proc. CSFW7 '94, 1994, p. 187-191..

[9] Chun-Ying Huang, Shang-PinMa, Kuan-TaChen, "Using one-time passwords to prevent password phishing attacks", Journal of Computer and Network Applications, Vol. 34, Issue 4, pp. 1292-1301, Jul. 2011..

[10] Carlisle Adams, Guy-Vincent Jourdan, Jean-Pierre Levac and François Prevost, "Lightweight protection against brute force login attacks on web applications ", in Proc. PST '10, 2010, p. 181-188.

[11] Adrian J Duncan, Sadie Creese, Michael Goldsmith, "Insider Attacks in Cloud Computing", in Proc. TrustCom '12, 2012, p. 857-862.

[12] K. Sapra, Husain, B. ; Brooks, R. ; Smith, M."Circumventing keyloggers and screendumps", in Proc. MALWARE '13, 2013, p. 103-108.

[13] William G.J. Halfond, Jeremy Viegas, and Alessandro Orso, "A Classification of SQL Injection Attacks and Countermeasures", ACM TISSEC, Vol. 13, Feb. 2010.