A SURVEY ON AUTHENTICATION ATTACKS AND COUNTERMEASURES IN A DISTRIBUTED ENVIRONMENT

Jesudoss A.[#1]
Research Scholar, Faculty of Computer Science and Engineering, Sathyabama University,
Chennai, Tamil Nadu, India[1]
jesudossas@gmail.com, jesudoss.mca@sathyabamauniversity.ac.in[#]

Subramaniam N.P.[*2]
Asst. Professor, Department of EEE, Pondicherry Engineering College,
Puducherry, India[2]
npsubbu@pec.edu, npsubbu@yahoo.com [*]

Abstract

Web applications are not capable of many security attacks. Many attacks needed only minimum effort. In this paper, we analyze different possible attacks on authentication aspects of security and propose various countermeasures for mitigating attacks. This paper enables you to shield your web applications from various attacks on authentication. Different types of authentication mechanisms have also been suggested for different types of attacks.

***Keywords*:** Authentication; Attack; Countermeasures; Vulnerabilities; Threats; Security.

1. Introduction

Due to flaws in many conventional authentication systems, many password attacks have occurred [1]. Determining one's identity helps to maintain their user accounts on online transactions and services. The authentication is essential to avoid identity theft. Authentication is the process of confirming an individual, whether he is the person that he claims to be. Authentication is one important aspect of security that has to be addressed effectively [2]. Otherwise the other aspects of security such as authorization, availability, auditing, confidentiality, integrity and non-repudiation may also be easily compromised. In Paper [2], various authentication methods have been discussed in detail. This paper focuses on various attacks on authentication aspects of security.

It is crucial to understand the differences between Vulnerabilities, Threats and attacks [3]. Vulnerability is a weakness in the system that makes a Threat to occur. It refers to an inability to defy the hostile challenge. The threat represents a potential danger that may occur. It is just a sign for a future attack to come. A Threat represents incessant danger to an asset. A Threat may or may not be intentional and may not cause damage also. I.e. Threat provides a room for an attack. Whereas an attack means any malicious action that exploits vulnerability and destroys or modifies, prevents access to an asset or gain access to an unauthorized asset. An attack has always exploited vulnerability and cause damage to the asset and is quite intentional. An exploit is a tool used by the attacker to cause damage to the asset. Here is an example, "when antivirus is not updated regularly, system may be affected by the virus and cause severe damage". Therefore, the absence of updating antivirus is the vulnerability, the viruses are the threats, and causing damage is an attack.

In this paper, section 2 describes an overview of the taxonomy of authentication attacks & countermeasures. Section 3 discusses about various authentication methods prevailing today. Section 4 provides a comparative analysis of various authentication attacks, countermeasures, authentication mechanism, *etc*.

2. An Overview of the Taxonomy of Authentication Attacks & Countermeasures

In this paper, the various attacks on authentication and its countermeasures have been suggested.

2.1. *Eavesdropping Attacks:*

An attacker taps the information that goes on the wire and uses it for future purpose. It is a kind of replay attack. It may be network eavesdropping or offline eavesdropping. MITM is a kind of eavesdropping attack

Countermeasure:

The message can be encrypted using standard encryption `techniques such as AES 128 bit or RC4 stream cipher. SSL helps to provide the encrypted communication channel. Further Central Authentication Service (CAS), a single sign-on protocol can be used along with SSL. Network eavesdropping can be avoided by using very strong authentication protocols such as Kerberos as it never transmits the password across the network.

2.2. *Man-in-the-Middle Attack:*

MITM is a kind of eavesdropper attack. An attacker comes in between two hosts, i.e. customer and the website (bank or shopping), and all the communication between them goes only through the attacker. So he impersonates both the parties to one another and may copy, alter or delete a portion of the data traffic between them i.e. attack on mutual authentication. MITM may be used to simply monitor the data and may not be reused also. It may be a passive attack or active attack.

Countermeasure:

Brute Force Attack and MITM can be solved by SSL. Using SSL, the traffic is encrypted so it can't be tampered or modified by MITM or brute force attack [4]. There are ways to fake connections (primarily by proxy servers) so that the user believes they have an SSL connection to a site but they may be navigated to a non-SSL site. The actual SSL connection will be from the proxy server to the website and not from the user to the website. The ultimate result is that the proxy may be able to read user's information. Moreover, the parties at both ends can be authenticated mutually to prevent MITM attacks. This mutual trust can be obtained by a certification authority. HMAC (Hashed message authentication code) can be used. If there is any alteration in the data by the attacker, then the computation of HMAC on receiving end may fail.

2.3. *Replay Attacks:*

An attacker copies the message, data, user credentials or key information transmitted between two hosts and then uses it for a nefarious purpose [5]. Replay attack is a specific category of MITM attack. This attack is absolutely intentional. Masquerading or impersonation is a type of attack in which the attacker impersonates a user. Whereas in replay attack, the attacker just sends the same data packet to some user assuming to have the same effect. For e.g. when the user says "no" for a file deletion, the attacker captures it and modifies it as "yes". In fact, replay attack is a specific type of masquerading attack. Thus, replay attack can be used to impersonate a user or entity. Also, sometimes, replay attack may not relate to impersonation at all. Like password, even a cookie can be replayed. The attacker may capture the cookie sent to the user and replay it for gaining unauthorized access with false identities.

Countermeasure:

Timestamp can be utilized along with security tokens. OTP can be applied. The nonce can be generated. SSL helps to eliminate replay attacks and is essential in case of cookie replay attack. Hence both the parties exchange some random number and use it for all encrypted transactions between them. By setting the cookie timeout value for a short period, the replay attack can be prevented as it gives only a short time for the attacker to play.

2.4. *Phishing Attacks:*

The phishing is a type of an attack in which the attacker impersonates the website, email or phone call for nefarious purpose. It is an intentional theft of user credentials [6]. Phishing attacks are usually attempted to steal credit card information, email, password, or any other sensitive information. The attacker creates a website similar to the original website, such as banking website. DNS cache poisoning enables the user to navigate to the attacker's fake website automatically.

Countermeasure:

Digital certificates can be used to avoid phishing attacks. 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. Click the unknown hyperlinks in the emails also leads to a phishing attack. The email attachments should not be downloaded unless it is from reliable sources. The padlock icon in the URL bar can be clicked to verify the identity of the website. The HTTPS protocol must be used in the URL instead of normal HTTP. i.e. https://www.somesite.com.

2.5. *Brute Force Attacks:*

It is generally difficult to protect against brute force attack. Hence, brute force attack attempts on a huge number of key combinations on trial-and-error basis [7]. Unlike dictionary attack, it targets even on unknown combinations. Passwords can be broken up easily when the key size is 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. The computer configuration must be high to perform a brute force attack much faster and efficiently. It starts from the single digit password to the multiple character password and tries out all the keys available on a keyboard.

Countermeasure:

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. This method will exhaust the server resources. Instead, honeypot mechanism can be implemented when the number of consecutive login attempts was failed. Today, most of the online websites, especially banking and financial websites deploy CAPTCHA (Completely Automated Public Turing test) mechanism for avoiding brute force attacks [8]. CAPTCHA is a computer program which generates images randomly and invites the user to enter the same in the given textbox. Based on the input given, it determines the user is a human being or streaming bot. Human beings have the ability to read and understand any distorted text, whereas computers cannot read or understand.

2.6. ***Dictionary Attack:***

A dictionary attack is an attack attempted on authentication data by trying all the possible words in a dictionary. Dictionary attack attempts only to a targeted list of weak passwords or attempts on a limited number of key combinations that has a high possibility of getting succeed [9]. Hence the dictionary attack is always faster than brute-force attack. A dictionary attack is easy when the password chosen is short, weak or common and it becomes very complicated and does not give result when any special characters are included as passwords. Dictionary attack is the first choice of the attacker before trying the brute-force attack. Some examples of software used for dictionary attack are Metasploit, Passcape, Brutus, Cain & Abel, etc.

Countermeasure:

Dictionary attack can be avoided by selecting a strong password. A strong password is the one created with the combination of alphabets both uppercase and lower case, numbers, and special characters. It must not be a word in a dictionary. Broadly speaking, the plaintext or encrypted passwords are not used on the database system. Because compromising a key would open the door for the hacker to see the entire password in a database. Hence, password can be hashed combined with a salt value and then it can be stored on a database.

2.7. ***Insider Attack:***

The Insider attack is a type of malicious attack attempted intentionally within an organization [10]. 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.

Countermeasure:

Intrusion Detection System (IDS) helps to mitigate such attacks. Access control mechanism, monitoring and logging must be strictly maintained.

2.8. ***Keylogger Attack:***

Keylogger is a computer program or software that captures the keystrokes of the user for stealing his password. Keylogger need not be software always. It can be a hardware device also [11]. Aside from stealing passwords, it can be used for enterprise security, parental control, etc.

Countermeasure:

The keylogger attack can be avoided by using the virtual keyboard in which the position of characters will change randomly. OTP (one-time password) can be used to avoid keylogger attacks. For Instance, when Gmail account is configured with two-step authentication, OTP sent to the mobile is required to login. OTP can be obtained in special devices such as SafeNet eToken NG-OTP, RSA SecurID tokens. Antilogger such as Zemana, sandboxie, keyscrambler can be used to avoid keylogger attacks.

2.9. ***Malicious Code Attack or Script Kiddie:***

Basic Key logger program to advanced malicious Trojans may be used to gain control over the user's computer system. Some of the malicious codes are Viruses, Worms, Trojan Horses, Script Kiddie, Java applet Attacks, ActiveX Controls, etc. Some of the examples of malicious code are Melissa, Love Bug, Happy99, Code Red, SirCam, Nimda, Slammer, Back Orifice, Sub7, Explore.zip, etc. This attack cannot be easily detected [19]. The malicious code is normally hidden in email, website, file downloads, Java applet and ActiveX content.

Countermeasure:

Software and Operating system patches and antivirus need to be regularly updated.

2.10. ***Session Hijacking:***

Session Hijacking attack is a type of attack in which the attacker exploits the TCP session between a Web server and a Web browser and steals the session token to gain the unauthorized access [12]. A session token is a token sent by the Web server to the Web browser for as a sign of authentication. It may be available

in http request header. This attack is common in Web applications. The attackers usually steal the cookies for hijacking an authenticated session.

Countermeasure:

SSL combined with cookie management system. Some IdP (Identity Providers) such as Shibboleth provides such facility. Switches can be preferred over hubs for avoiding this attack. Secure protocol or cryptography helps to mitigate such attacks. The incoming connections and remote connections can be minimized as to mitigate attacks.

2.11. *Shoulder surfing attacks:*

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.

Countermeasure:

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. When the transaction is over at an ATM counter, all the 10 keys from 0 to 9 can be pressed in order to confuse the attacker. Similarly, while entering your password on a keyboard, type some unwanted characters in between and use backspace to delete and then proceed with actual characters. This may also mislead the attacker.

2.12. *SQL Injection Attack:*

SQL Injection Attack is a code injection technique used to attack websites and login with administrator privileges. The poorly designed websites are the victim of this attack. The attacker can inject SQL commands and gain access to obtain the data from the database [14]. Firewalls or IDS cannot protect the data against the SQL injection attack.

Countermeasure:

Patches for OS, softwares, 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.

3. Authentication Methods

3.1. *Conventional Password Method:*

The traditional password authentication method can be easily compromised. It is vulnerable to various attacks and hence it is not recommended. The advantage in this scheme is it is simple, easy to remember, easy to use, no additional hardware or software or specialized personnel required. The disadvantage is that it is vulnerable to shoulder surfing attack, keyloggers, and spoofed login and phishing attacks.

3.2. *Public Key Cryptography:*

The password can be encrypted to avoid eavesdropping attacks and other attacks. Public key cryptography is also known asymmetric cryptography. It generates two mathematically related keys, public key and private key. The message may be encrypted using public key or private key and decrypted using its corresponding private key or public key. It provides confidentiality of the message. It is used for creating digital signatures.

3.3. *Keystroke Dynamics:*

Keystroke dynamics is a biometric solution in which the users rhythmic typing on the keyboard and the timing between the key pressed is used as an authentication technique [15]. The following information is recorded along with the conventional password.

a) The time taken between a key press and a key release

b) The time taken between two consecutive keys pressed.

The advantage is it requires no extra hardware and programming skill is enough. It prevents from shoulder surfing, keyloggers, phishing, etc. Even with the password the attacker cannot access the system. The disadvantage is high rejections occur due to different typing speed of users. It is difficult to identify even the legitimate user

3.4. *Click Pattern:*

Click Pattern provides strong password rather than text-based password [16]. The click area contains different colour or combination of different symbols. The user click rhythm is also maintained along with click patterns. The advantage is it does not require any extra hardware and prevents from shoulder surfing attack, keyloggers, phishing, etc. It is difficult to compromise even the password is known. The disadvantage is it may have more rejections due to different mental levels of users.

3.5. *Graphical Passwords:*

Graphical password is an alternative for text-based passwords [17]. Graphical objects are displayed and the user needs to select it. Selected objects are then drawn by user using mouse, touchpad or touch screen. System runs preprocessing on the objects and converts it into hierarchical form. Finally, hierarchical matching is done for user authentication. The advantage is it prevents from shoulder surfing attack. The disadvantage is that the system authenticates the user only if proper sketch is drawn by the user on the touch sensitive screens. The processing time depends on how good the user draws the sketches. Normally it takes longer time for process compared to other schemes.

3.6. *One-Time Password:*

One-time password (OTP) is a password valid for a short period of time and can be used only once. OTP is used for avoiding identity theft. It protects the online transactions from replay attacks, keyloggers, shoulder surfing attacks, etc. An OTP captured by an attacker may be of no use to him. The disadvantage is that it requires some additional technology such as SMS to mobile, or call to mobile for OTP, etc. An OTP may be of random challenge-response type. i.e. prompting for a nonce from the prover. An OTP may also be generated from a password list. Banking and financial companies always use this method.

3.7. *Biometrics:*

Biometric is an image-based authentication system in which finger prints, face, iris, retinal, speech, signature verification are used to verify against the original specimen [18]. The image is preprocessed first and then the classification of images is done. The advantage of this method is that it is real and unique signature and cannot be stolen. The disadvantage is that it is costly and difficult to implement. It is not a completely matured method and it can be easily compromised and is time consuming also.

3.8. *Digital Signatures:*

Digital Signature is a mathematical method that proves the integrity of the document. It assures the recipient that the document has not been altered in transit. It provides integrity, authentication and non-repudiation aspects of security. It is used by companies for distributing their software. The distributor or sender computes the hash for the document and shares it on Web page with the public. The user downloading the software computes the hash and matches against the hash that is available on the Web. If they are same, accept it otherwise reject it. The sender may encrypt the message using public key and the message is decrypted using private key by the recipient. The sender knows that the message can be decrypted only by the particular recipient as he is the only persons having knowledge about the private key. Broadly speaking, a digital signature is a document which is hashed first and then it is encrypted with the private key of the sender and is appended to the original document. The recipients on the other end, decrypts the document using public key so he knows for sure it is send by the particular sender. Then it is hashed by the recipient and he verifies it with the actual hash. Now the verifier or the recipient is able to identify the sender as well as get assurance that the message has not been modified.

3.9. *Authentication Panel:*

In these password schemes, instead of pressing exact button for password, the user is prompted to select the location of the password words from the given panel. Vulnerabilities can be rectified by updating weak components regularly [20]. It prevents from brute force, dictionary and video recording attacks. It does not require extra hardware and it is fast.

3.10. *Zero-Knowledge Proofs:*

In this method, the user can prove his identity to the verifier without revealing the secret that is known only to him. If the secret is revealed to the verifier, he may share it with someone else.

4. Comparative Analysis

The table I given below explains about various attacks, countermeasures, authentication mechanism,

advantages and disadvantages, etc.

Table 1. Comparative Analysis of Attacks, Countermeasures, Authentication Methods - Merits & Demerits

Attack	Countermeasure	Authentication Mechanism	Advantage	Disadvantage	Additional Hardware
Eavesdropping	Encryption	SSL	Secured Online	Costly	No
	Token-based - CAS	RubyCAS, SecurID	Single-Sign on	Less control over navigation control	No
	Authentication Protocols	Kerberos	Single-Sign on, mutual authentication	Migrating users to Kerberos database is difficult	No
Man-in-the-Middle Attack	Encryption	SSL	Confidentiality	Performance	No
	Mutual Trust	CA – Certificates	Speed & Security	Expired & Cost	No
	Hashing	HMAC	No need of SSL	Inconsistent	No
Replay Attacks	Dynamic unique data such as TimeStamp, OTP, Nonce	OTP/NONCE SSL	OTP - Two factor authentication	OTP - dependent on addl technology, spoofable	Yes
Phishing Attacks	Mutual Authentication	Digital Certificates	Protects from Impostor	Vendor support, algorithm strength	No
	Avoid download from unreliable source	Digital Signatures	Non-repudiation, prevents imposter	Compatibility, cost	No
	Check for Padlock icon	HTTPS	Confidentiality	Performance	No
Brute Force Attacks	Tarpitting	Biometric	Unique	Data gets changed	Yes
	IDS	Honeypot	Simplicity	Risk	No
	Test Human	CAPTCHA	Avoids bots	Difficult to read	No
Dictionary Attack	Strong passwords	Hashed with SALT value	Makes guessing harder	Slow	No
Insider Attack	Access Control, Monitoring	IDS	Monitors threats inside & outside	Differentiate friend & foe	No
Keylogger Attack	Virtual Keyboard	Microsfot OSK	save cost, space	slow typing	No
	OTP	SafeNet OTP	security	spoofable	Yes
	Antilogger	Zemana, Sandboxie	Avoid keyloggers	cost & maintenance	No
Malicious Code Attack	Update regularly	Enable auto-update	Automanagement	can be compromised	No
Session Hijacking	SSL with Cookie management	Shibboleth	ACL defined easily	change - restart web server	No
	Secure Protocol	Kerberos	Never sent across	Replay attack	No
	Encryption	Cryptography	Privacy & safe	Consumes time	No
Shoulder surfing attacks	Confuse the attacker	Including wrong information	safe from social engg. Attack	simple	No
SQL Injection Attack	Update regularly	Proper Validation	Defines input	Time consuming	No
		Access Control strictly defined	Protects from Intruders	compromised if rights elevated	No

5. Conclusion and Future Work

This survey helps us to consider various attacks and its countermeasures before designing an authentication system. The appropriate authentication mechanism can be chosen depending on the type and nature of the application. We have provided solutions for both online and offline applications. The advantages and disadvantages in implementing each authentication mechanism also have been discussed.

References

[1] Mudassar Raza, Muhammad Iqbal, Muhammad Sharif and Waqas Haider, “A Survey of Password Attacks and Comparative Analysis on 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] Italo Dacosta, Mustaque Ahamad, Patrick Traynor, "Trust No One Else: Detecting MITM Attacks Against SSL/TLS Without Third-Parties", in Proc. 17th European Symposium on Research in Computer Security, Italy, 2012, p. 10-12..

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

[6] 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..

[7] 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.

[8] Elie Bursztein, Matthieu Martin, John C. M, "Text-based CAPTCHA Strengths and Weaknesses", in Proc. CSS '11, 2011, p. 125-138.

[9] Junghyun Nam, Kim-Kwang Raymond Choo, Juryon Paik, Dongho Won, "An Offline Dictionary Attack against a Three-Party Key Exchange Protocol", IEEE Communication Lett., Vol. 13, pp. 205-207, Mar. 2009.

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

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

[12] Italo Dacosta, Saurabh Chakradeo, Mustaque Ahamad and Patrick Traynor, "One-Time Cookies: Preventing Session Hijacking Attacks with Stateless Authentication Tokens", ACM TOIT, Vol. 12, June 2012.

[13] Manu Kumar, Tal Garfinkel, Dan Boneh, Terry Winograd, Reducing Shoulder-surfing by Using Gaze-based Password Entry, in Proc. SOUPS '07, 2007, p. 13-19.

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

[15] Yu Zhong, Yunbin Deng, Anil K. Jain, "Keystroke Dynamics for User Authentication", in Proc. CVPRW '12, 2012, p. 117-123.

[16] Cheng-Jung Tsai, Ting-Yi Chang, Meng-Sung Wu, and Yu-Chiang Li, "An Approach for User Authentication on Non-Keyboard Devices using Mouse Click Characteristics and Statistical-Based Classification", ICIC International '12, Vol. 8, pp. 7875-7886, Nov. 2012.

[17] Sebastian Uellenbeck, Markus Dürmuth, Christopher Wolf, and Thorsten Holz, "Quantifying the Security of Graphical Passwords: The Case of Android Unlock Patterns", in Proc. CCS '13, 2013, p. 161-172.

[18] Taekyoung Kwon and Jae-il Lee, "Practical Digital Signature Generation using Biometrics", in Proc. ICCSA '04, 2004, p. 728-737.

[19] Elias Levy, Ivan Arce, "Worm Propagation and Generic Attacks", IEEE Security & Privacy, pp. 63-65, Mar-Apr. 2005.

[20] Yen-Hung Hu, Mira Yunt, Debra Tang and Hyeong-Ah Choit, "A Study of Traffic Survivability Under Malicious Attacks", in Proc. IEEE Sarnoff Symposium, 2006, p. 1-4.