International Journal of Current Research in Science and Technology
Volume 3, Issue 5 (2017), 1–4.
ISSN: 2394-5745
Available Online: http://ijcrst.in/

International Journal of Current Research in Science and Technology

Analysis of Security Schemes

Research Article

Alok Sharma[1], Nidhi Sharma[1]* and Ankit Kumar[1]

1 Department of Computer Science, Baba Mast Nath University, Rohtak, Haryana, India.

Abstract: In todays scenario, internet is used daily for communication as well as data sharing which increase the chance of licking of personal information. This security is normally provided by some authentication process. Password security is a major issue for any authenticating process and different researches in past have proposed different techniques which we will analyze in present paper.

Keywords: Login, authentication, hashing, password security.

© JS Publication.

1. Introduction

Authentication is one of the most important requirements to secure information. There exist various methods for authentication like passwords, PINs, Steganography etc. [1] Steganography is one way to hide the information in such a way that no one expects the desired recipient can get to know about the existence of communication. It is an art and science of hiding the existence of communication. Such information may be communicated in the form of texts, binary files. Steganography includes the concealment of information with in computer files. Password based systems are also used for authentication. But to store user passwords within databases as plaintext or only with their unsalted hash values is a blunder mistake of application developers. Many successful hacking attempts that enabled attackers to get unauthorized access to sensitive database entries including user passwords have been practiced in the past [1]. Revealing of password files is a serious security problem that has affected many users and companies like Yahoo, LinkedIn, eHarmony and Adobe [2], [3], since revealed passwords cause many possible cyber-attacks. These recent crisis has indicated that the weak password storage methods are currently in place on many web sites. For example, the passwords in the eHarmony system were stored using MD5 hashes without salt and also the LinkedIn passwords were also stored with unsalted hash values by using SHA-1 algorithm [6]. According to this, there are two issues that should be acknowledged to control these security problems: First is passwords must be protected by taking relevant providence and storing with their hash values enumerated through salting mechanisms. Then, it must be hard for attacker to reverse hashes to acquire plaintext passwords. And another is that a secure system should detect whether a password file is revealed or not to take relevant actions [8].

2. Symmetric Key Encryption (Public Key)

Symmetric key encryption uses same key, called secret key, for both encryption and decryption. Users exchanging data keep this key to themselves. Message encrypted with a secret key can be decrypted only with the same secret key. The

* *E-mail: nidhisharma1725@gmail.com*

algorithm used for symmetric key encryption is called secret-key algorithm. Since secret-key algorithms are mostly used for encrypting the content of the message they are also called content-encryption algorithms. The major vulnerability of secret-key algorithm is the need for sharing the secret-key. One way of solving this is by deriving the same secret key at both ends from a user supplied text string (password) and the algorithm used for this is called password-based encryption algorithm. Another solution is to securely send the secret-key from one end to other end. This is done using another class of encryption called asymmetric algorithm, which is discussed later. Strength of the symmetric key encryption depends on the size of the key used. For the same algorithm, encrypting using longer key is tougher to break than the one done using smaller key. Strength of the key is not liner with the length of the key but doubles with each additional bit. Following are some of popular secret-key algorithms and the key size that they use.

3. Asymmetric Key Encryption (Private Key)

Asymmetric key encryption uses different keys for encryption and decryption. These two keys are mathematically related and they form a key pair. One of these two keys should be kept private, called private-key, and the other can be made public (it can even be sent in mail), called public-key. Hence this is also called Public Key Encryption. A private key is typically used for encrypting the message-digest; in such an application private-key algorithm is called message-digest encryption algorithm. A public key is typically used for encrypting the secret-key; in such an application private-key algorithm is called key encryption algorithm [4].

4. Hashing Technique

The aim of hashing is :

1. Map an extremely large key space onto a reasonable small range (of integers)
2. Such that it is unlikely that two keys are mapped onto the small integer

Only a small fraction of key is used, i.e., $\mid K \mid << \mid U \mid$. That implies with direct addressing most of the direct address table T is wasted. A hash function maps a key onto an index in the hash table T, $h : U \rightarrow \{0, 1, \ldots, m-1\}$ where m is the table-size and $\mid U \mid = n$. Hash collsions, i.e., $h(k) = h(k')$ for $k \neq k'$, raise the issues:
–how to obtain a hash function that is cheap to evaluate and minimizes collisions?
–how to treat hash collisions when they occur? [5]

5. Steganographic Techniques

In order to embed secret data into a cover message, the cover must contain a sufficient amount of redundant data or noise. This is because in the embedding process Steganography actually replaces redundant data with the secret message. This limits the types of data that we can use with Steganography. There are basically three types of steganographic protocols used. They are Pure Steganography, Secret Key Steganography, and Public Key Steganography. Pure Steganography is defined as a steganographic system that does not require the exchange of a cipher such as a stego-key. This method of Steganography is the least secure means by which to communicate secretly because the sender and receiver can rely only upon the presumption that no other parties are aware of this secret message. Secret Key Steganography is defined as a Steganographic system that requires the exchange of a secret key (stego-key) prior to communication. Secret Key Steganography takes a cover message and embeds the secret message inside of it using a secret key (stego-key). Only the parties who know the secret key can

reverse the process and read the secret message. Unlike Pure Steganography where a perceived invisible communication channel is present, Secret Key Steganography exchanges a stego-key, which makes it more susceptible to interception. The benefit to Secret Key Steganography is even if it is intercepted; only parties who know the secret key can extract the secret message [7].

Algorithm	**Strength**	**Weakness**	**Analysis**
Secret Key Cryptography	Very fast. Vast quantity of key possible key permutation.	Involves logistics problem of conveying/ distributing symmetric key among the different parties.	The advanced and high performance microprocessors available have made this encryption vulnerable and less secure against brute force attacks.
Public key Cryptography	Public key is shared and privet key is kept secure.	Computational time required for RSA encryption is more. If private key is compromised, then a huge set of user base gets vulnerable.	Widely used in internet environment.
Hash Functions	Fast. Provides integrity of data through Digital Signatures.	Difficulty to find a good hash function that work for a wide set of data. Does not work well with skewed data.	Choice of hashing function depends on input data.
Steganographic Techniques	Existence of secret message is unrevealed	Only image steganography comes out as a technique in which noise level during transmission is negligible.	Techniques available are detectable by bit comparison tools available in market.

Table 1. **Synthesis of different steganographic/cryptographic security techniques**

Lot of work is already defined by different researchers for security. Some of contribution of existing researchers is analyzed in this paper.

The Lucent Personal Web Assistant (LPWA) : applies the latter approach. It operates as an HTTP proxy server that users access with a master username and password. They can then tag web site password fields to be automatically filled in with values derived from a hash-based function of the user's master password and the domain name of the web site [8].

PWDHASH : a recently released utility by Ross et al. applies a similar hash-based technique on the client side. It functions as a web browser plug-in, seamlessly replacing values submitted via web site password fields with hashes of those values and the site's domain name. PwdHash is primarily intended to provide a defense against "phishing" or "spoofing" attacks by linking site passwords to the domain name of the server to which they are actually sent [9].

Password Salting : is adding a random string of characters to passwords before their hash is calculated to make password hashing more secure and it makes them difficult to reverse. The random string of characters can be a combination of letters, numbers and other characters [10].

Password Agent : a new password hashing mechanism that utilizes both a salt repository and a browser plug-in to secure web logins with strong passwords. Password hashing is a technique that allows securing web logins with strong passwords. Password hashing is a technique that allows users to remember simple low-entropy passwords and have them hashed to create high-entropy secure passwords. Password Agent generates strong passwords by enhancing the hash function with a large random salt. With the support of a salt repository, it gains a much stronger security guarantee than existing mechanisms. Password Agent is less vulnerable to offline attacks, and it provides stronger protection against password theft. Moreover, Password Agent offers some usability advantages over existing hash-based mechanisms, while maintaining users' familiar password entry paradigm [11].

Scheme	Strength	Weakness	Analysis
Lucent Personal Web Assistant (LPWA)	This scheme tag the web site password fields to be automatically filled in with values derived from a hash-based function.	Prone to phishing or spoofing attacks	It operates as an HTTP proxy server that users access with a master username and password.
Password Multiplier	generate high entropy password	No advance phishing protection	Password Multiplier uses a strengthened hash function to generate high entropy password Widely used in internet environment.
PwdHash	primarily intended to provide a defense against "phishing" or "spoofing" attacks	No advance Phishing protection	It provides defense against attacks by linking site passwords to the domain name of the server to which they are actually sent.
Salt hash password	Use to store the Password Hash and salt in the database in the user's account to decrypt the password	In case of brute force attack, salt will not provide any security	The attacker will now have to recalculate their entire dictionary for every individual account they're attempting to crack.
Password Agent	allows users to remember simple low-entropy passwords	video recording attacks, spyware	utilizes both a salt repository and a browser plug-in to secure web logins with strong passwords

Table 2. **Synthesis of different Password Security Schemes**

6. Conclusion

In this paper, different Steganographic , Cryptographic Techniques and Password Security Schemes are analysed. The previous researches by Juels and Rivest, Imran Erguler suggested some really effective hashing, salting and honey words techniques which make the security process more secure but combination of salting, hashing and differential masking makes password security scheme more secure and effective and steganographic technique comes out more advanced technique.

References

[1] Emin Islam Tatli, *Cracking More Password Hashes With Patterns*, Department of Electrical and Electronics Engineering, Istanbul Medipol University, (2014).

[2] D.Mirante and C.Justin, *Understanding Password Database Compromises*, Department of Computer Science & Engineering Polytechnic Inst. of NYU, Tech. Rep., (2013).

[3] A.Vance, *If Your Password is 123456, Just Make IT Hackme*, The New York Times, 20(2010).

[4] N.F.Johnson and S.Jajodia, *Exploring Steganography: Seeing the Unseen*, http://www.jjtc.com/pub/r2026.pdf

[5] N.F.Johnson and S.Jajodia, *Steganalysis: The Investigation of Hidden Information*, IEEE Information Technology Conference, (1998).

[6] Stackoverflow,http://stackoverflow.com/questions/244903/why-is-a-password-salt-called-a-salt.

[7] J.Kelley, *Terror groups hide behind Web encryption*", USA TODAY, 06(19)(2001), 50-55.

[8] T.Li Gong, Mark A.Lomas, Roger M.Needham and Jerome H.Saltzer, *Protecting poorly chosen secrets from guessing attacks*, IEEE Journal on Selected Areas in Communications, 11(5)(1993), 648-656.

[9] Blake Ross, Collin Jackson, Nicholas Miyake, Dan Boneh and John C.Mitchell, *Stronger Password Authentication Using Browser Extension*, Supported by NSF through the PORTIA project.

[10] Search Security http://searchsecurity.techtarget.com/definition /salt.

[11] Benjamin Strahs Chuan Yue Haining Wang, *Secure Passwords Through Enhanced Hashing*, The College of William and Mary Williamsburg, VA 23187, USA.