Journal of Computer Science 7 (8): 1152-1156, 2011
ISSN 1549-3636

A Secure Simple Authenticated Key Exchange Algorithm based Authentication for Social Network

[1]P. Venkateswari and [2]T. Purusothaman
[1]Department of Computer Science and Engineering, Erode Sengunthar,
Engineering College Thudupathi, Erode,
[2]Department of Computer Science and Engineering,
Government College of Technology, Coimbatore, Tamil Nadu, India

Abstract: Problem statement: This study describes about a robust and secured authentication procedure that can be adapted in a private forum within a Social Network Site (SNS) to update its user's profile. **Approach:** The robustness is achieved through combining proven security measures combined with usability aspects. The study demonstrates acceptance of such robustness particularly in a SNS to update user's profile. The study discuss on three related components that were considered for the proposed security measures, namely shared keys based on passwords security methods, personalized questions and one time passwords. The study elaborated shared key for authentication. The keys were calculated based on communication entities at the user's site. Shared key methods have proved to be effective in withstanding general attacks. Most of information security and network security protocols provide security and preserve secrecy based on cryptography techniques. **Results:** While the keys could be generated through conventional password based key generation algorithm, the security can also be enhanced by using personalized questions in addition to the password. The study proposed certain ideal security key that would be generated through socially surveyed personalized questions and password. This key would then become a onetime password for the users for a particular login session. While the keys when generated through highly secured manner and used for mutual authentication, social studies have pointed out to usability weakness. **Conclusion:** This study validated social acceptance in introducing personalized questions that would generate keys for authentication. The study elaborates both authentication technique as well as the social responses on personalized password questions. The personalized password questions have been designed from commonly used security questions like ones that asked to those who have lost their passwords. These questions need to be looked from social angle rather than technical angle. A social survey was conducted restricted to southern India. Based on the responses the questions have been designed and administered in a social network site to generate the keys for authentication purposes. This study elaborates the validity of robustness achieved through this proposed method. The proposed method although proved to be suitable to Southern Indian users of Social Network Site, it can be used for other regions but with personalized questions of that social culture.

Key words: Social network site, password questions, security protocols, dictionary attack, entities identity, economic culture, public keys

INTRODUCTION

Most of the Network Security protocols provide security based on cryptography techniques. The secret key is the most significant data for most of these techniques. The keys should be secretly generated and distributed. Diffie Hellman's (Hussain, 2008; Hsiang and Shih, 2009a) method is a well known key generation and authentication algorithm among public key cryptosystems. Accordingly using senders own private key and partner's public key, the shared session key could be calculated through discrete logarithm. This key could be used for securing further communication between the users. But it is weak in preventing man-in- the middle attack, since the entitie's identity are not included in the message while exchanging public keys (Hussain, 2008; Hsiang and Shih, 2009b).

Corresponding Author: P. Venkateswari, Department of Computer Science and Engineering, Erode Sengunthar, Engineering College Thudupathi, Erode, Tamil Nadu, India

Literature survey: At the same time password and PIN-based user authentication also have numerous deficiencies (Hsiang and Shih, 2009a).

Unfortunately, many security systems are designed in such a way so that security relies entirely on a secret password. Many researchers have shown that people pick random words for guessing passwords. Because of these password cracker programs, users need to create unpredictable passwords, which are more difficult to remember. The human limitation of precise recall is in direct conflict with the requirements of strong passwords. As a result, users often write their passwords down and ”hide” them close to their work space. Strict password policies, such as forcing users to change passwords periodically, only increase the number of users who write them down to aid memorability. Another risk with passwords is that they are easy to write down and to share with others. Some users never bother to reveal their passwords to others. They view this as a feature and not as a risk.

The pure character based password is less secure, since it is easily breakable either by Brute force attack or through Dictionary attack, since passwords are selected in such a way to remember them easily (Aboud, 2010). Mostly it is a combination of alphabet and numerals. Passwords can be revealed by trying through various possibilities in brute force attack. In dictionary attack, crackers can try with any meaningful words of a dictionary. Since performance of security in the conventional password based method depends on the design of the system, to virtually overcome such simple method, another parameter can be added in addition to the password while authenticating the user. The second factor could be a privacy based questions (Berkeley, 2008). Today’s personal security questions owe their strength to the hardness of an information-retrieval problem. But, serious usability and security weaknesses have been reported in personal banking network system (Berkeley, 2008). Still personal security questions form a fall back way of authentication in addition to the passwords, they suffer through various practical difficulties.

Questions themselves are inapplicable in nature to various type of users. The answer to these questions are not memorable, ambiguous, guessable and easily attackable. Thus at most care must be taken while framing these security questions. Sample questions could bé:

- What was your dream job at your childhood
- What is the name and colour of your teenage motorcycle
- Which school did you studied in Ninth Standard

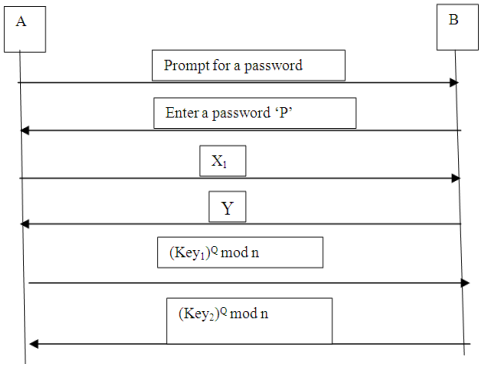

Fig. 1: Generation of Keys between users A and B

However, these types of questions may deeply depend on the of the users local or regional socio economic culture of the users. A combination of password and social questions for calculating shared keys would be more acceptable in SNS.

To enhance the security, the secret key can be calculated from the password. It was described in the Simple Authentication Key agreement algorithm (Aboud, 2010).Here having password as a base, algorithm tried to calculate keys and authenticate the users. The keys can be used to secure the further transmission. This algorithm was DH based algorithm.

The procedure to generate keys from the password (Cheng *et al*., 2010) is explained below through Fig. 1.

The system prompts user A to enter his password; A enters his password ‘ P’. The system then calculates two integers namely Q and Q^{-1} mod n-1 from the password P, where ‘n’ is a large arbitrary prime number. Q has been calculated by some pre defined calculations like:

Q = Sum (ASCII valued of character in the password) mod n-1

$Q\tilde{Q}^{1}$ = 1 mod n-1

User A chooses a random large integer ‘a’ and calculates $X_1= g^{aQ}$ mod n and sends to B. Similarly B chooses a random large integer ‘b’ and calculates $Y_1= g^{bQ}$ mod n sends to A.System then computes $Y = Y_1^{Q1}$ mod n, $Key_1 = Y^a$ mod n from the above inputs. System also computes $X= X_1^{Q1}$ mod, $Key_2 = X^b$ mod n In order to verify the keys calculated are the same at different ends, the system compares uniformly follow keys by mutually exchanging the values $(KEY_1)^Q$ mod n, $(KEY_2)^Q$ mod n.

The security analysis of Simple Authenticated Key Exchange Algorithm (SAKA) was carried by Cheng *et al*., 2010).This algorithm is susceptible to masquerade attack, dictionary attack and thus cannot

provide perfect forward secrecy. To enhance the security and to overcome the vulnerabilities stated above, some modification has been made by Hwang's model (Cheng *et al*., 2010).

In addition to X_1 and key_2 another Key namely K_1 is calculated as under:

$$K_1 = Y^{\tilde{Q}1} \bmod n$$

Similarly from X_2 and Key_1, another key namely K_2 is calculated as under:

$$K_2 = X^{\tilde{Q}1} \bmod n$$

Both these additional keys are exchanged between the users.

To verify the keys received ,instead of applying $\tilde{Q}^1$ on the values received, the receiver calculates key with his private key as follows and compares it against the value received from the system. Once again A computes

$K_2 = (g^a)^{\tilde{Q}1} \bmod n$ and compares it with K_2 as received from the system. Similarly B computes $K_1 = (g^b)^{\tilde{Q}1} \bmod n$ compares it with K_1 as received from the system.

If the keys found are correct, then the authentication is cleared. If not the system will not provide connections between A and B. In the above method masquerade attacks can be prevented as the process takes large random numbers for both the users.

In addition, finding out the of $\tilde{Q}^1$value requires cumbersome procedure for the cracker. Since Q and $\tilde{Q}^1$ are calculated from the password in a predetermined way, even if a password is guessed through the dictionary method, the function through which it is calculated is not known publically. Since the functions should be of such a nature that no two passwords can generate the same Q and $\tilde{Q}^1$.Hence this methodology (Cheng *et al*., 2010) is demonstrated to be effective. It also provides Perfect Forward Secrecy (PFS). A cryptanalysis of Security Enhancement with modified Authentication and Key agreement algorithm is however still suffers by replay and offline password guessing attacks.

Even with the keys are verified, if it is found correct, User A could still be fooled with a wrong session key. The replay attack still possible by intercepting X_1 a cracker eve can impersonate B and send $Y_1' = X_1$ to A. On receipt of it Y_1', A can calculate the key as:

$$Y = Y_1^{Q-1} = g^a \bmod n$$

MATERIALS AND METHODS

Proposed algorithm: The proposed method described in this article explains how it can withstand all such attacks mentioned earlier and how the computational cost is reduced. It also explains how it reforms that would meet the expectation of today's Social Networks. The authentication methodology adopted in social network sites especially for updating the user profile is briefed below through Fig. 2.

Social Network Sites (SNS) are generally used by likeminded users that would form an online community. User logs into these networks and searches for new like minded users after creating a profile of themselves. Social networks have grown into an explosive proportion in recent years. Social networking sites have become very popular and have become the preferred sites for of communication between the likeminded users. However the popularity of social networks are under a great threats with regard to users personal data. Attackers can gain to the important personal information of the users very easily. But still as SNS likeminded users can form restricted forums within these sites. This study attempts to establish a robustic authentication method especially for such restricted user forums within SNS. Thus the authentication method preferred for social network is demonstrated to withstand at least impersonation attack.

Similarly it was found that eve can guess the password P' and derive corresponding Q' mod n and Q^{-1}mod n. Eve can do the complete derivation and try to match it against the keys calculated from original password. These attacks seriously threaten the security of the protocol.

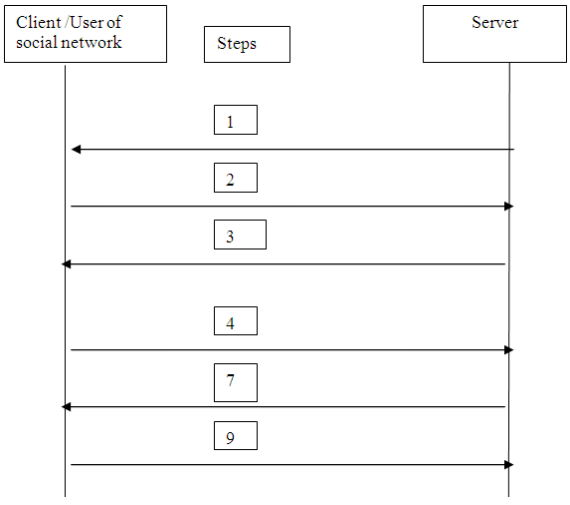

Fig. 2: Message Exchanges in the proposed algorithm

Table 1: User information table that is maintained by the server

User name	Encrypted password	PQ_1	A_1	……	PQ_n	A_n

PQ_1: Personalised Qestion$_1$, A_1: Answer to PQ_1, Q_n and A_n: n^{th} Question and n^{th} answer

$Key_1 = (y^a) \bmod n$

It will become $(g^a)^a \bmod n$.

The procedure to become a member within the restricted forums may be made through two steps:

- Registration phase (Setup)
- Authentication phase (Login)

Getting the credentials of the owner of his profile and try to modify its contents can be secured by verifying his identity before making an attempt to modify it. In this study a novel type of strong authentication method is proposed. To make a more secure key, some factors could be included in addition to the traditional password. These factors may be made so that can be answerable through personalized questions.. To make the keys to be more robust and to make it so unique for each session so that the perfect Forward secrecy would be maintained. These personalized questions, while recorded for the first time during registration phase, will be revoked arbitrarily by selecting with one question at the time of login. This procedure is demonstrated in Fig. 2.

Steps:

Step 1: Prompt the user to enter his User name and to provide his password

Step 2: User enters his authorized name and Password. Server Check it against values stored in the DB (Table 1) by the server

Step 3: User is then prompted with one personalized question, which would be selected randomly from the set of questions by the system and answers provided by the user is checked. It should be noted that this is a part of several personalized answers to questions provided already by the user during the registration phase

Step 4: User has to provide the answer for this social question. As the questions are social in nature , such as date of birth of his close relative, it is likely that the user may remember it and it is also likely to be unique in nature

Step 5: Validate it against the answers stored in the database. If it is correct, then the Server calculates one Time Session Key with the password provided by the user and the answer to the personalized question posted and checked it with the data base .The generation of key is done by using the revised SAKA algorithm

Step 6: Select a random Nonce value and encrypt it with the calculated session key in step5

Step 7: Encrypted nonce value is then transferred to the client

Step 8: The key calculated thus at the client side, will be used to decrypt the encrypted nonce value

Step 9: To authenticate and prove that the keys calculated at the both ends are correct, the client has to take Hash value of decrypted nonce and send it to the Server

Step 10: Server has to calculate the Hash value of the nonce sent and has to compare it against the received hash value. Then the authentication is said to be over and the user will be allowed to update his profile

RESULTS

Security analysis of the proposed protocol: In the proposed method (Secured SAKA for Social Networks) additional features for authentication processes are used for modification. This improvement helps to enhance the security and it becomes more robust.

The social responses were obtained through social surveys in South Indian SNS users. The social questions were on the nature of social questions and on the usability of the system. Even though the results of this social survey are the basis for the development of the system, the results and process of the social survey is beyond the scope of this article.

The proposed algorithm can withstand a masquerade attack as user not forge answers to other user's social questions.

Even though the password is easily guessable, the answer to any personalized question is social in nature. Besides out of a few personalized questions one question is selected in a random manner and asked. Therefore the system is highly secured.

DISCUSSION

It should be noted that Till step 5 (Fig. 2.) the server is said to be stateless. The Server is not involved with any valid computation for key generation. Therefore the computation power is not wasted for illegitimate user / attacker. Thus the algorithm is free from Denial of Service (DoS) attack.

Table 2: Comparison between the three methods

Differentiating factor	Simple authenticated and key agreement algorithm	Security enhancement for the simple authentication key agreement algorithm	Proposed algorithm
Mutual authentication	Between peers	Between two users	Between users of restricted user forum and server
Total Message exchanges in one direction	4	4	6
Total computational cost	One Multiplication and (n-1) times of addition where n is no.of characters in the password Besides 8 exponentiations and 10 Modular arithmetic	One Multiplication and (n-1) times of addition where n is no.of characters in the password Besides 10 exponentiations and 12 Modular arithmetic	One Multiplication and (n-1) times of addition where n is no.of characters in the password and the answer Besides 8 exponentiations and 10 Modular arithmetic One Encryption, one Decryption, 2 Hash calculations
Vulnerability	Vulnerable to Masquerade, Dictionary, Replay attack	Vulnerable to Replay and Password Guessing attack	Withstand against all such attacks and provide Perfect Forward Secrecy

Similarly in the key generated out of each login session even though the password may be maintained as a long term secret the answer to the random personalized question makes the key to be socially unique for each session. Therefore this algorithm provides a Perfect forward secrecy.

But however, instead of sending the key itself in any unsecured medium, in the proposed system, basic cryptographic techniques like encryption is used. The keys are then used to encrypt the nonce value. This makes the protocol to be more secured against passive attack like eavesdropping. The eve couldn't predict the key even if the intruder can catch the packet. More over the keys generated as a onetime password process, are not transmitted in the Network as in the earlier algorithms, thus replay attack is still not possible.

In earlier algorithms (Cheng *et al*., 2010) the keys are calculated using exponential and modular arithmetic before verifying the identity of an entity. But in this proposed algorithm, simple symmetric key cryptographic functions and validity through irreversible hash function is used. Thus the system consumes less computational resources.

Because the mutual authentication between the entities are validated by using hash functions.

The comparisons between all the three methods (simple, secured and the proposed) are narrated in Table 2.

CONCLUSION

It is clearly demonstrated that efficiency and usability could be made complementing with each other when security keys are generated through conventional as well as random personalized questions in restricted forum of a SNS.

Even though the user may find it a little cumbersome from the usability point of view, it provides high security and it preserves privacy of the user' profile.

REFERENCES

Berkeley, A.R.U.C., 2008. Personal knowledge questions for fallback authentication: security questions in the era of Face book. Proceedings of the 4th Symposium on Usable Privacy and Security, (SOUPS'08), ACM, New York, pp: 13-23. DOI: 10.1145/1408664.1408667

Cheng, K.M., T.Y. Chang and J.W. Lo, 2010. Cryptanalysis of security enhancement for a modified authenticated key agreement protocol. Inter. J. Network Sec., 11: 55-57. http://ijns.femto.com.tw/contents/ijns-v11-n1/ijns-2010-v11-n1-p55-57.pdf

Hsiang, H.C. and W.K. Shih, 2009a. Efficient remote mutual authentication and key agreement with perfect forward secrecy. Inform. Technol. J., 8: 366-371. DOI: 10.3923/ITJ.2009.366.371

Hsiang, H.C. and W.K. Shih, 2009b. A Secure remote mutual authentication and key agreement without smart cards. Inform. Technol. J., 8: 333-339. DOI: 10.3923/ITJ.2009.333.339 http://www.doaj.org/doaj?func=abstract&id=601121

Hussain, S.M. and H. Al-Bahadili, 2008, A password-based key derivation algorithm using the KBRP method. Am. J. Applied Sci., 5: 777-782. DOI: 10.3844/AJASSP.2008.777.782

Aboud, S.J., 2010. Efficient password-typed key agreement scheme. Int. J. Comput. Sci., 7: 26-31. http://www.doaj.org/doaj?func=abstract&id=495633