Ticket Based One Time Password Client-Server Authentication Scheme

Aye Aye
Ph.D (IT) candidate
University of Computer Studies, Mandalay
Mandalay, Myanmar
ayeayeucsm@gmail.com

Tin Mar Kyi
Department of Physics
University of Computer Studies, Mandalay
Mandalay, Myanmar
tinmarkyi@gmail.com

***Abstract*—Password authentication is a subject of great interest in client-server system. One Time Password (OTP) scheme becomes popular today in client-server authentication for the insufficiencies of static passwords. The purpose of OTP is to make the attackers more difficult to gain unauthorized access to restricted resources. Leslie Lamport proposed one-time password scheme using hash function in his paper "Password Authentication with Insecure Communication". But the four main shortcomings of Lamport's protocol are (1) weak password strength or suffering from guessing attack (2) suffering from replay attack (3) lack of mutual authentication (4) high hash computation. The existing one-time password authentication schemes are not secure at registration phase because only encryption algorithms and hash functions are used. Therefore, any intruder can impersonate as the authenticated user and can access the service of service or resource. The proposed scheme focuses on Ticket instead of password in registration phase. Ticket based authentication protocol proposed in this paper is intended to overcome the problems of Lamport's scheme and to support stronger confidentiality than traditional password authentication protocols. The security of proposed scheme will be proved by using Markov model and Time Variation model.**

***Keywords*—One Time Password, guessing attack, replay attack, mutual authentication, hash complexity, Ticket**

I. INTRODUCTION

Authentication based on cryptographic techniques is a great challenge research area in client-server system. Password authentication is one of the simplest and the most common authentication mechanism over an insecure channel. It provides the legal users to use the resources of the client-server systems. Many researchers proposed several password authentication schemes for secure registration and login process. However, the current Internet environment is vulnerable to various attacks such as replay attack, guessing attack, modification attack, and stolen-verifier attack. In 1981, Lamport proposed a one-time password authentication scheme using cryptographic hash functions [1]. The purpose of a OTP is to make it more difficult to gain unauthorized access to restricted resources. Traditionally the static passwords can be more easily accessed by an unauthorized intruder given sufficient attempts and time. This risk can be greatly reduced by constantly altering the password. Dynamic passwords or one-time passwords play an important role in authentication. As the existing one-time password schemes use only encryption algorithm and hash function in registration process, the password is still vulnerable. Therefore, the impersonators may pretend like the authorized users to get the services. This ticket-based one-time password authentication system is more secure than the existing authentication schemes by preventing from guessing attack and replay attack. It is essential property to get the mutual authentication in the registration phase. The ticket supports the server to authenticate the user and the signature response of server also supports the user to authenticate the server. In this proposed scheme, there is no password transmission in registration phase by the use of ticket. The main responsibility of the trusted third party, RC is to generate Ticket to user. The user must use Ticket instead of password in registration process to get the strong confidentiality.

This paper is organized as follows: in Section II, we discuss related work; in Section III the security requirements of password authentication are discussed. We present the Lamport's one-time password authentication scheme and considerations on Lamport's scheme in Section IV. Ticket based one-time password scheme is proposed in Section V and we present the security proof of the proposed scheme in Section VI, finally in Section VII, we conclude about the proposed system.

II. RELATED WORKS

Authentication is the key for information security for the reason that if the authentication mechanism is compromised, the rest of the security measures are by passed as well [4]. One-time password (OTP) schemes, where each password is used only once, offer available alternative or a supplement to traditional password schemes [4]. The approaches [3], [5] designed password authentication schemes to overcome guessing attack and achieve mutual authentication. Lamport [1] introduced the first one-time password authentication scheme. This initial work has been followed by a number of subsequent improvements [6-9]. In 2004, Tsuji-Shimizu proposed 2GR [9] to eliminate a stolen-verifier attack on SAS-2 and a theft attack on ROSI. Lin-Hung showed that the 2GR scheme is vulnerable to an impersonation attack, in which any attacker can masquerade as a legitimate user, without stealing the verifiers [10]. In 2012, T.Tsujii [2] presented the

integration of image based authentication and HMAC based one time password to achieve high level of security in authenticating the user over the internet but this authentication scheme didn't offer mutual authentication. The author [16] proposed an improvement to withstand the impersonation attacks and achieve Wu and Chieu's claimed security requirements. In [18], Yang and Shieh proposed two methods to prevent replay attack. However, two papers [16, 17] pointed out that Yang and Shieh's schemes have a drawback in that an intruder is able to impersonate a legal user by constructing a valid login request from an intercepted login request.

III. SECURITY REQUIREMENTS OF PASSWORD AUTHENTICATION

In this section, we define the security requirements an ideal password authentication scheme should satisfy. In addition, we shall also introduce all of the attacks that an ideal password authentication scheme should withstand. We sort them as follows [15]:

SR1. Forgery Attacks (Impersonation Attacks)
An attacker attempts to modify intercepted communications to masquerade the legal user and login to the system.

SR2. Mutual Authentication
The user and the server can authenticate each other. Not only can the server verify the legal users, but the users can also verify the legal server. Mutual authentication can help withstand the server spoofing attack where an attacker pretends to be the server to manipulate sensitive data of the legal users.

SR3. Password Guessing Attacks
Most passwords have such low entropy that it is vulnerable to password guessing attacks, where an attacker intercepts authentication messages and stores them locally and then attempts to use a guessed password to verify the correctness of his/her guess using theses authentication messages.

SR4. Replay Attacks
Having intercepted previous communications, an attacker can impersonate the legal user to login to the system. The attacker can replay the intercepted messages.

SR5. Stolen-verifier Attacks
An attacker who steals the password-verifier (e.g., hashed passwords) from the server can use the stolen-verifier to impersonate a legal user to login to the system.

IV. LAMPORT'S ONE TIME PASSWORD SCHEME

In 1981, Lamport [1] proposed a password authentication scheme to authenticate the legitimacy of remote users over an insecure channel. In Lamport's scheme, passwords are stored only on the user side and intercepting a password sent from user to the system would not lead to an impersonation [4]. Lamport's authentication is based on computing the sequence $\{x, F(x), F^1(x), F^2(x),\ldots, F^M(x)\}$on the user side, where x is an arbitrary value chosen by the user and kept secret, M is the number of authentications to be performed and may be also chose by the user, F is a known one way function (this means that by giving x it is easy to compute $F(x)$ but by giving $F(x)$ it is infeasible to compute x). At the beginning the system must know $F^M(x)$ and then when the user needs to authenticate for the first time to the system ($i=1$) he will present $F^{M-1}(x)$ as the first one-time password. At the i^{th} authentication the user will prove its identity by sending $F^{i-1}(x)$ and the system will simply verify this by computing $F(F^{M-i}(x))$ and also checking that $F(F^{M-i}(x))= F(F^{M-i+1}(x))$, where $F(F^{M-i+1}(x))$ is the previous authentic one time password.

There are four drawbacks inherent in registration process of Lamport's scheme as follows. Firstly, there is no strong password strength in registration process. Secondly, it suffers from replay attack. Thirdly, there is no mutual authentication between user and server. Finally, the hash complexity problem is occurred in Lamport's scheme.

The registration phase of Lamport's scheme [4] is described in Figure 1.

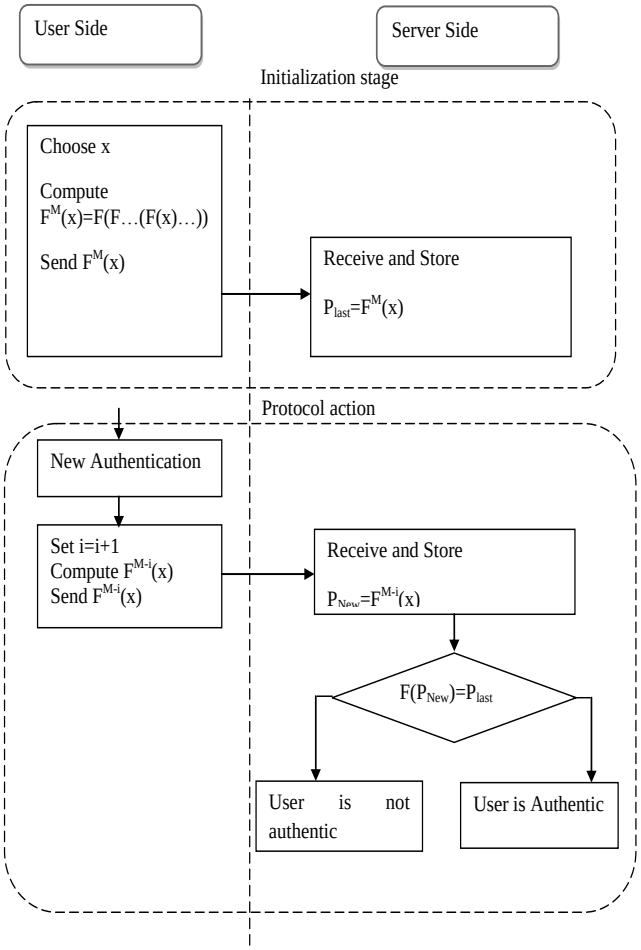

Figure 1. Lamport's one-time password scheme

A. *Considerations on Lamport's scheme*

The following issues may be viewed as security constraints of using hash functions on Lamport's scheme.

1) There is no strong password strength.

At the registration phase, the user chooses the password (x) randomly. The use of hash algorithm only cannot support strong password in registration phase.

2) There is no resistance to replay attack.

The attackers may intercept the authorized user and replay the messages to gain the services in Lamport's scheme. As there is no life-time validation in Lamport's scheme, this scheme suffers from replay attack.

3) There is no authentication process in registration phase.

The attackers may impersonate like the authorized user and try to register to server. After the registration process completes, the intruder can access the service of server. Similarly, the forged server may be registered by the legal user. Therefore, there is no authentication in registration between user and server.

4) There is hash complexity problem at user side.

At the initialization phase or registration phase, the user needs to compute $F^{M}(x)$ and $F^{M-i}(x)$ iteration for protocol action or login phase. Therefore, M^{th} times of hash at user side causes hash complexity problem. For example if $M=2^{20}$ we will need to compute more than one million compositions and time or space can became a problem if computational resources are limited.

V. THE PROPOSED ONE TIME PASSWORD SCHEME

There are processes which may happen for (1) weak password strength or guessing attack, (2) replay attack (3) lack of mutual authentication and (4) hash complexity problem in Lamport's scheme. In the real world, it is essential to be secure registration process to prevent from the assessments of unauthorized users. Thus, the weak points of Lamport's scheme claim the more secure registration process. For these reasons, the proposed scheme is designed in Figure 2.

The main purposes of this purposed scheme are to (1) get strong password or prevent guessing attack, (2) prevent replay attack, (3) get the mutual authentication and (4) reduce hash complexity problem. To generate the strong password strength and prevent from guessing attack, Diffie-Hellman key exchange protocol will be used. To prevent from the replay attack, the life-time based ticket will be generated. To get mutual authentication, the trusted third party (RC) will be designed between user and server. To reduce hash complexity, the existence of time of ticket will be limited not only the number of login (n) of Lamport's scheme but also the time-stamp (T) of ticket. Markov model will be used to prove the password strength. Time validation formula will be applied to check the replay attack.

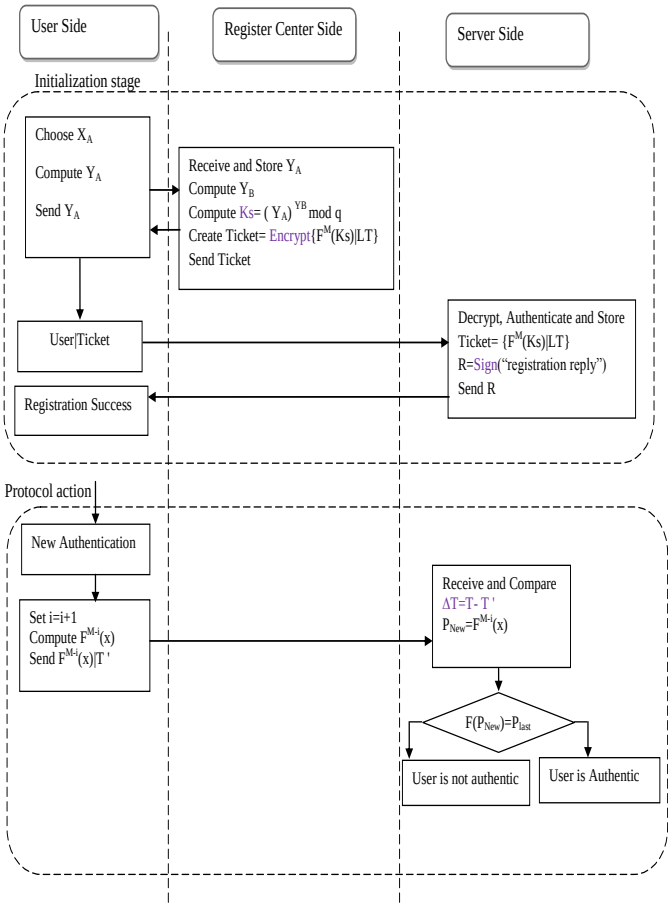

Figure 2. The proposed one-time password scheme

A. *Diffie-Hellman Key Exchange Protocol*

Diffie-Hellman (DH) key exchange protocol is one of the most common or popular protocol for secure key agreement. The DH key agreement protocol allows two users, referred to as Alice (A) and Bob (B), to obtain a shared secret key over a public communication channel. An attacker, eavesdropping at the messages sent by both Alice and Bob will not be able to determine what the shared secret key is. This is an extremely useful primitive because the shared secret can be used to generate a secret session key [11].

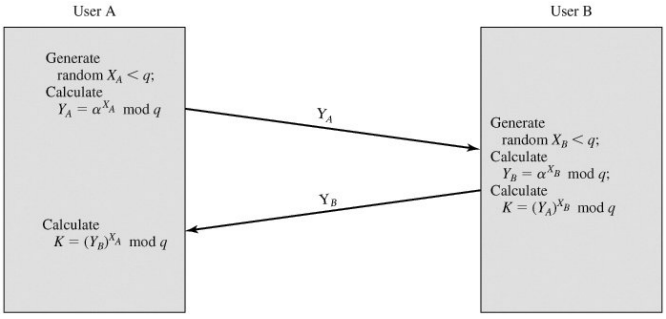

Figure 3. Diffie-Hellman Key Exchange Protocol

Figure 3 shows a simple protocol that makes use of the Diffie-Hellman calculation. Suppose that user A wishes to set up a connection with user B and use a secret key to encrypt messages on that connection.

User A can generate a one-time private key X_A, calculate Y_A, and send that to user B. User B responds by generating a private value X_B calculating Y_B, and sending Y_B to user A. Both users can now calculate the key. The necessary public values q and a would need to be known ahead of time. Alternatively, user A could pick values for q and a and include those in the first message [12]. The use of Diffie-Hellman key exchange protocol can pass the problem of weak password generation step.

B. Time Validation Protocol

Register Center (RC) defines the life-time of Ticket and sends it to user. When the user registers to server, the server stores the life-time of ticket for that user. The server compares and validates the time using the following formula whenever the user logins:

$\Delta T <= T - T'$

If the duration (ΔT) exceeded the limited time, the server will deny the request from user. Therefore, any intruder can't try the replay attack.

C. Mutual Authentication

In Lamport's scheme, the user not only cannot authenticate the server but also the server cannot authenticate the user. Therefore, there is no two factors authentication in registration phase of Lamport's scheme. In the proposed scheme, the trusted third party called Register Center (RC) is responsible to get the mutual authentication between user and server. The server can authenticate user for the Ticket generated by RC in registration phase. Moreover, the user can authenticate the server by the verification of registration response of server's signature.

D. Life-Time Oriented Password

To overcome hash complexity problem, the duration of password is limited with not only the number of login (n) but also the life-time of Ticket generated by the trusted third party, RC. According to the main contribution of this scheme is the Ticket based registration, the existence of password depends on the life time of Ticket. Even if the value of M is 220, it is no need to compute more than one million compositions and time or space because the life-time of Ticket will be expired when the limited duration complete. Ticket is composed of the following portions: user name, server name, network address, FM(x), current time and the life time.

VI. SECURITY PROOF OF PROPOSED SCHEME

In this section, the security measure how to resist the guessing attack and replay attack will be evaluated.

A. Guessing Attack Resistance

Measuring the strength of passwords is crucial to ensure the security of password-based authentication. Estimating the strength of passwords as a measure to defend against guessing attacks has a long history. To estimate the password strength generated by the proposed system, Password Strength Estimation algorithm from Markov Models [14] will be used.

1) Markov Models

Over the last years, Markov models have proven very useful for computer security in general and for password security in particular. For example, Narayanan et al. [13] showed the effectiveness of Markov models to password cracking. In an n-gram Markov model, one models the probability of the next character in a string based on a prefix of length n. Hence for a given string $c_1;:::;c_m$ we can write

$$P(c_i \ldots, c_m) = \prod_{i=1}^{m} P(c_i | c_{i-n+1}, \ldots, c_{i-1}))$$

our construction only keeps track of the n-gram counts $count(x_1;:::;x_n)$, and the conditional probabilities can easily computed from these by the following formula:

$$P(c_i | c_{i-n+1}, \ldots, c_{i-1}) = \frac{count\ (c_{i-n+1}, \ldots, c_{i-1}, c_i)}{\sum_{x \in \sum} count(c_{i-n+1}, \ldots, c_{i-1}, x)}$$

2) Password Strength Estimation (PSE algorithm)

The strength of a password $c = c_1;:::;c_m$, where each character c_i is chosen from alphabet ,is estimated as follows:

1. For i =1;:::;m, the following conditional probabilities are computed:

$$P(c_i | c_{i-n+1}, \ldots, c_{i-1}) = \frac{count\ (c_{i-n+1}, \ldots, c_i)}{count\ (c_{i-n+1}, \ldots, c_i)}$$

$$= \frac{count\ (c_{i-n+1}, \ldots, c_i)}{\sum_{x \in \sum} count(c_{i-n+1}, \ldots, c_{i-1}, x)}$$

(If the numerator equals zero we use a small out-of-dictionary probability, to account for unseen n-grams. However, this will almost never happen, due to the added noise.)

2. Finally, the strength estimate f(c) for the password c is:

$$f(c) = -log_{2(} \prod_{i=0}^{m} (c_i | c_{i-n+1}, \ldots, c_{i-1}))$$

3) Calculation of Password Strength

This is the sample calculation for measuring the strength of password.

Example: The probability of the string password (with n =5) is computed as follows

P(password)= P(p)P(a|p)P(s|pa) :::P(d|swor)

Picking one of the elements as an example:

p(o|assw)= count(asswo)/count(assw) = 98450/101485 =0.97.

This results in the overall estimation *P(password)*=0.0016

B. Replay Attack Resistance

A replaying the intercepted login message called replay attack cannot work because it will fail the verification phase

for the time interval (ΔT<=T-T'). In which equation, ΔT means the time interval, T means the registration time and T' means the login time. If the time interval exceeds the limited time interval, the system will deny the login attempt and alarm the replay attack.

VII. CONCLUSION AND FUTURE WORK

One-time passwords have become the central topic in client-server authentication system because they are starting to replace the static passwords in security demand areas such as banks, military, governments and corporate virtual private networks (VPNs) to reduce the effects of password compromise. The proposed scheme not only supports the strong password strength, prevents replay attack and reduces high hash problem but also gives the mutual authentication rather than Lamport's scheme. The life-time based proposed scheme also prevents from guessing attack and replay attack. Future implementation may wish to consider methods to improve the case of usage of the system. For instance, current authentication system requires typing multiple hexadecimal numbers in login phase. Multiple participants who can access multiple services in authenticated way may be additional research.

ACKNOWLEDGMENT

I greatly thankful to my respected supervisor, Dr. Tin Mar Kyi for her excellent guidance, constant help and fruitful discussions throughout the process of writing this paper. I would like to thank Dr. Than Naing Soe for his excellent guidance, where the initial scope of the thesis was defined. The author would like to thank anonymous reviewers for their useful comments.

REFERENCES

[1] L. Lamport, "Password Authentication with Insecure Communication," Communications of the ACM, Vol. 24, pp. 770-772, 1981.

[2] Takasuke TSUJII. "A One-Time Password Authentication Method", January31, 2003

[3] K.Bicakciand N.Baykal: Improving the security and flexibility of one-time password by signature chains. Turk J Elec Engin, (3):1–3, 2003.

[4] Bogdan Groza, Dorina Petrica ," One Time Passwords For Uncertain Number Of Authentications".

[5] C.L. Lin, H.M. Sun, and T. Hwang, "Attack and solutions on strong-password authentication", IEICE Trans. Commun., vol. E84-B, no.9, pp. 2622-2627, Sept. 2001.

[6] T. Tsuji, T. Kamioka, and A. Shimizu, "Simple and Secure password authentication protocol, ver.2 (SAS-2)", IEICE Technical Report, OIS 2002-30, Sept. 2002.

[7] H.Y. Chien, J.K. Jan, "Robust and simple authentication protocol", Comput. J., vol.46, no.2, pp. 193-201, Feb. 2003.

[8] T. Tsuji, A. Shimizu, "One-time password authentication protocol against theft attacks", IEICE Trans. on Commun., vol.E87-B, no.3, pp. 523-529, Mar. 2004.

[9] C.L. Lin, C.P. Hung, "One-Time password authentication protocol against theft attacks", IEICE Trans. on Commun., vol.E89-B, no.12, pp. 3425-3427, 2006.

[10] W.C. Kuo, Y.C. Lee, "Attack and improvement on the one-time password authentication protocol against theft attacks", Proc. of the Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, pp. 19-22, Aug. 2007.

[11] Jean-Fran¸coisRaymond and Anton Stiglic "Security Issues in the Diffie-Hellman Key Agreement Protocol"

[12] William Stallings, "Cryptography and Network Security Principles and Practices, Fourth Edition"

[13] A.Narayanan and V.Shmatikov.Fast dictionary attacks on password susing time-space trade off .In CCS'05: Proceedings of the 12th ACM conference on Computer and communications security, pages364–372,NewYork,NY,USA,2005. ACM.

[14] C.D.Manning and H.Schu¨tze. Foundations of statistical natural language processing. MITPress, Cambridge, MA, USA,1999.

[15] Chwei-Shyong Tsai, Cheng-ChiLee, and Min-Shiang Hwang "Password Authentication Schemes: Current Status and Key Issues" International Journal of Network Security,Vol.3,No.2,PP.101–115, Sept. 2006 (http://ijns.nchu.edu.tw/)

[16] Chien-LungHsu "A user friendly remote authentication scheme with smart cards against impersonation attacks" Applied Mathematics and Computation170(2005)135–143

[17] J.-J.Shen,C.-W.Lin,M.-S.Hwang, Security enhancement for the time stamp-based password authentication scheme using smart cards, Comput.Secur.22(7)(2003)591–595.

[18] W.H.Yang,S.P.Shieh, Password authentication schemes with smart cards, Comput.Secur.18(8)(1999) 727–733