SOME REMARKS ON THE SECURITY VULNERABILITIES OF A HASH BASED STRONG PASSWORD AUTHENTICATION SCHEME

Manoj Kumar

Department of Mathematics
Rashtriya Kishan Post Graduate College
Meerut Karnal Road Shamli, Utter Pradesh.-India- 247776

Abstract- To serve the purpose of user authentication for network security, many strong password authentication schemes have been proposed. W. C. Ku also proposed a hash based strong password authentication scheme and claimed that the proposed scheme withstands to all possible security attacks. In this paper, we analyzes W. C. Ku's scheme and proved that the proposed scheme does not support essential security requirements. In addition, in W. C. Ku's scheme, the remote user is not able to change his/her password freely. This paper also show that proposed scheme is still vulnerable to inside attack, man in the middle attack, password guessing attack, replay attack, impersonation, stolen verifier attack and denial of service attack.

Index Terms: **Login, server, access system, mutual authentication, session key, network security.**

I. INTRODUCTION

The fast growing development of client- server network authenticates a valid remote user online and provides facilities to their users. This network consists of a remote authentication server (*AS*) and a number of users wants to login on the server. The *AS* always has own secret key, which is never exchanged with a remote user, while on the other side, the user has also a secret piece of information, called as user password (*PW*).

Actually, a password based remote user authentication scheme uses a two-way handshake to perform authentication. When the communication link is established between remote user and authentication server, the user sends his/her username and password to the remote authentication server. The remote server has an authentication scheme and user database to authenticate the remote user and if the authentication is found valid, the remote authentication server sends an acknowledgment message to the remote user and in this way remote user gets access to the remote authentication server. In order to provide the security to remote user authentication schemes and to exchange password during the authentication process, a number of techniques have been developed to securely exchange the password over the network [3, 4, 5, 6, 8, 9, 10, 11, 13].

To serve the purpose of user authentication for network security, many strong password authentication schemes have been proposed. W. C. Ku [13] also proposed a hash based strong password authentication scheme and claimed that the proposed scheme withstands to all possible security attacks. In this paper, we analyzes W. C. Ku's scheme and proved that the proposed scheme does not support essential security requirements. In addition, in W. C. Ku's scheme, the remote user is not able to change his/her password freely. This paper also show that proposed scheme is still vulnerable to inside attack, man in the middle attack, password guessing attack, replay attack, impersonation, stolen verifier attack and denial of service attack. The remainder of this paper is organized as follows. Section 2 reviews the W. C. Ku's scheme. The security vulnerabilities and attributes of W. C. Ku's scheme are analyzed in section 3. Finally, comes to conclusion in the section 4.

II. Review of W. C. Ku's Scheme

This section is about W. C. Ku's scheme [13]. W. C. Ku's scheme has two phases: the registration phase and the login phase.

2.1 Registration Phase

In this phase the user *U* initially registers or re-registers to server *S*.

1. User *U* sends his registration request to server *S*.
2. The server *S* sets *T* as current time. If this is *U*'s initial registration, *S* sets $N = 1$, otherwise *S* sets $N = N + 1$. *S* sends a random nonce *r*, *N* and *T* to *U* via insecure channel .
3. User *U* sends $h_2(S \parallel PW \parallel N \parallel T)$ to the server *S* via secure channel. Here $h_2(m) = h(h(m))$ means the message *m* is hash twice.
4. *S* computes the user storage key $K_U^{(T)}$ and the sealed verifier $sv^{(N)}$, as,
$$K_U^{(T)} = h\big(U \parallel h(X_S \parallel T)\big) \text{ and } sv^{(N)} = h_2(S \parallel PW \parallel N \parallel T) \oplus K_U^{(T)}$$
5. *S* stores $sv^{(N)}$, *N* and *T* in the password file.

2.2 Login Phase

Whenever *U* logins to *S*, the following steps involved:

1. *U* sends his login request to *S*.
2. *S* sends a random nonce *r*, *N* and *T* to *U* via insecure channel.
3. *U* computes c_1, c_2, c_3,as,

$$c_1 = h_2(S \| PW \| N \| T) \oplus h(S \| PW \| N \| T),$$
$$c_2 = h(S \| PW \| N \| T) \oplus h_2(S \| PW \| N + 1 \| T),$$
$$c_3 = h(h_2(S \| PW \| N + 1 \| T) \| r)$$

4. *S* computes $K_U^{(T)} = h\big(U \| h(X_S \| T)\big)$.
5. S computes $h_2(S \| PW \| N \| T) = sv^{(N)} \oplus K_U^{(T)}$.
6. *S* computes u_1 and u_2 , as,

$$u_1 = c_1 \oplus h_2(S \| PW \| N \| T) \text{ and } u_2 = c_2 \oplus u_1$$

7. If the equalities $h(u_1) = h_2(S \| PW \| N \| T)$ and $h(u_2 \| r) = c_3$ hold, then *S* authenticates *U*, otherwise, *S* rejects *U*'s login request and terminates this session.
8. After successful authentication, *S* computes a new sealed-verifier using $sv^{(N+1)} = u_2 \oplus K_U^{(T)}$, and replaces $sv^{(N)}$ with $sv^{(N+1)}$, and sets N = N + 1 for *U*'s next login. The value of *T* is unchanged.

III. Security Vulnerabilities and Attributes of W. C. Ku's Scheme

3.1 Man in the Middle Attack

In man in the middle attack (often abbreviated MITM) the antagonist intercepts the insecure network. Man in the middle attack is also known as fire brigade attacks. The eavesdropper applies a program that appears to be the server to the client and appears to be the client to the server. In this way, the attacker must be able to intercept all messages going between the server and user and inject himself. The attack may be used simply to gain access to the message or enable the attacker to modify the message before retransmitting it. This attack can only be successful when the eavesdropper can impersonate each endpoint to the satisfaction of the other. In the following discussion, we shall prove that how an malicious user *A* can mount MITM attack on W. C. Ku's hash based strong password authentication scheme, whenever the user *U* sends his login request to *S*.

1. *U* sends his login request L_U to *S*. Malicious user *A* intercept the login request L_U and replace the login request L_U with own valid login request L_A.
2. *A* sends his login request L_A. to *S*.
3. *S* sends a random nonce *r*, *N* and *T* to *U* via insecure channel. Malicious user *A* intercept *r*,*N*, *T* and replace these values with r_A, N_A, T_A.
4. *U* computes c_1, c_2, c_3,as,

$$c_1 = h_2(S \| PW \| N \| T) \oplus h(S \| PW \| N \| T),$$
$$c_2 = h(S \| PW \| N \| T) \oplus h_2(S \| PW \| N + 1 \| T),$$
$$c_3 = h(h_2(S \| PW \| N + 1 \| T) \| r)$$

The malicious user *A* replaces c_1, c_2, c_3 with c_1^A, c_2^A, c_3^A and sends to the server, where

$$c_1^A = h_2(S \| PW_A \| N_A \| T_A) \oplus h(S \| PW_A \| N_A \| T_A),$$
$$c_2^A = h(S \| PW_A \| N_A \| T_A) \oplus h_2(S \| PW_A \| N_A + 1 \| T_A)$$
$$c_3^A = h(h_2(S \| PW_A \| N_A + 1 \| T_A) \| r_A)$$

5. S computes $K_A^{(T_A)} = h(A \| h(X_S \| T_A))$.
6. S derives $h_2(S \| PW_A \| N_A \| T_A) = sv_A^{N_A} \oplus K_A^{(T_A)}$.
7. *S* computes u_1^A and u_2^A ,as,

$$u_1^A = c_1^A \oplus h_2(S \| PW_A \| N_A \| T_A),$$
$$u_2^A = c_2^A \oplus u_1^A$$

9. Obviously, the equalities $h(u_1^A) = h_2(S \| PW_A \| N_A \| T_A)$ and $h(u_2^A \| r_A) = c_3^A$ holds truely, therefore *S* authenticates *A* in place of *U* and starts a session. In this way, the malicious user *A* records all the confidential communication.

3.2 Insider Attack

In an organization's client server computer network, there is a possibility of insider attack. In most of the organizations, the malicious attack is planted by someone who has been entrusted with authorized access to the organization's computer network. This

insider may have knowledge of its architecture therefore insider attack is the primary threat to computer networks in a client server network. This setting allows an insider to browse the sensitive data at the server. Furthermore, as they have already user accounts and corporate e-mail addresses, they likely have access to company data. As usual, if user *U* uses the same password to access other servers for convenience, the insider at server *S* can impersonate the user *U* to access other services. In this way, an insider can also affect all components of organization's computer network and its security on behalf of user *U*. Since, the insider at the server has a legitimate access to the organization's computer network; therefore he will be able to create the following destructive attacks of his choice on behalf of user *U*. If, we observe W. C. Ku's hash based strong password authentication scheme, then it is clear that the insider at server *S* is in possession of the following information.

• Password file of user *U* containing the current *N*, *T*.
• The value $h_2(S \parallel PW \parallel N \parallel T)$.
• All past records about the values *r*, *N*, *T*.
• The login request records c_1, c_2, c_3.
• The verification records u_1 and u_2 .

Since the insider can manipulates these recorded information, in this way, the insider at server will be able to mount an attack of his choice without knowing the related password of a valid user. The insider at the server will be able to mount stolen verifier attack, denial of service attack, password guessing attack, impersonation attack, replay attack etc. Thus, in W. C. Ku's scheme, the insider is a strong antagonist. Beside the above vulnerabilities, the insider will be able to do the following malicious activity.

- ✓ Insider at the server can steal valuable propriety information of the company's network.
- ✓ Insider at the sever can plant Trojan horses or browse through the file system.
- ✓ Insider at the server can affect availability by overloading the system's processing or storage capacity or by causing the system to crash.

3.3. Off-line Password Guessing Attack

To recover one or more plaintext passwords from hashed password is known as password guessing attack. Off-line password guessing attack is the process of recovering password from data that has been stored in or transmitted by a computer system. A common approach is to repeatedly try guesses for the password. Since, in W. C. Ku's scheme, the user is not free to change his password, therefore an adversary can set a off-line password guessing attack. This section shows that W. C. Ku's hash based strong password authentication scheme [13] cannot withstand password guessing attack. For the success of password guessing attack, an adversary will perform the following operations. The adversary intercepts the login phase and records the following insecure phase.

S→ $U: r, N, T$

U→ S: c_1, c_2, c_3, where,

$$c_1 = h_2(S \parallel PW \parallel N \parallel T) \oplus h(S \parallel PW \parallel N \parallel T),$$
$$c_2 = h(S \parallel PW \parallel N \parallel T) \oplus h_2(S \parallel PW \parallel N + 1 \parallel T),$$
$$c_3 = h(h_2(S \parallel PW \parallel N + 1 \parallel T) \parallel r)$$

After the above setting, to guess a valid password via c_1 , the adversary performs the following steps.

1. Set the value *N*, *T* for the server *S*.
2. Guess a password *PWi*.
3. Computes $c_i = h_2(S \parallel PW_i \parallel N \parallel T) \oplus h(S \parallel PW_i \parallel N \parallel T)$.
4. Check, whether $c_i = c_1$, if it holds, it means the adversary has managed to guess a valid password, otherwise go to step-2 and set a different password *PWi*.

In the similar way, the adversary can guess a valid password via c_2, c_3.

IV Conclusion

This paper analyzes W. C. Ku's scheme and observed that the proposed scheme neither provide mutual authentication between the user and server, nor establish a common session key to provide message confidentiality. In W. C. Ku's scheme, the remote user is not free to change his password. Due to these deficiencies, W. C. Ku's scheme is vulnerable to insider attack, stolen verifier attack,denial of service attack, impersonation attack, MITM attack,off-line password guessing attack etc.

References

[1] Chang C. C. and Hwang K. F., 2003. Some forgery attack on a remote user authentication scheme using smart cards. *Informatics*, 14-3, pp. 189 - 294.
[2] Chen, C.M. and Ku, W.C., 2002. Stolen-verifier attack on two new strong-password authentication protocols. *IEICE Transactions on Communications*, E85-B (11),pp. 2519-2521.
[3] Han C. H. , Shih W.K., 2009. Weaknesses and improvements of the Yoon Ryu Yoo remote user authentication scheme using smart cards, *Computer Communications*, Volume 32- 4,pp. 649-652.
[4] IEEE P1363.2-D13, 2004. Standard Specifications for Password-based Public Key Cryptographic Techniques. *IEEE P1363 working group.*
[5] Jia Y. L. An-Min Zhou, Min-Xu Gao, 2008. A new mutual authentication scheme based on nonce and smart cards. *Computer Communications*. Volume 31, Issue 10, , pp. 2205-2209.

[6] Lamport L., 1981. Password authentication with insecure communication. *Communication of the ACM*, 24, 11: pp. 770-772.
[7] Mitchell C. J. and Chen l.,1996. Comments on the S/KEY user authentication scheme. *ACM Operating System Review*, vol. 30, No. 4, pp. 12-16.
[8] Shen Z. H., 2008. A new modified remote user authentication scheme using smart cards.*Applied Mathematics*, Volume 23-3, 371-376.
[9] Tsai C. S., Lee C. C. and Hwang M. S., 2006.Password Authentication Schemes: Current Status and Key Issues. *International Journal of Network Security*, Vol.3, No.2, pp. 101 115.
[10] Wang Y.Y., Liu J. Y., Xiao F. and Dan J., 2009. A more efficient and secure dynamic ID-based remote user authentication scheme, *Computer Communications* ,Volume 32, Issue 4, P.P. 583-585.
[11] Yen S. M. and Liao K. H., 1997. Shared authentication token secure against replay and weak key attack. *Information Processing Letters*, 78-80.
[12] Ku W. C., Tsai H. C., and Chen S. M., 2003 Two simple attacks on Lin-Shen-Hwang's strong-password authentication protocol," *ACM Operating System Re view*, vol. 37, no. 4, pp. 26-31, Oct 2003.
[13] Ku W. C., 2004, A hash-based strong-password authentication scheme without using smart cards," *ACM Operating System Review*, vol. 38, no. 1, pp. 29-34.