http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (18): 4513-4516, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.4513.4516

Cryptanalysis of Kim et al's Two Password Authentication Schemes

[1]Jiping Li, [1]Zenggang Xiong, [2]Yaoming Ding and [3]Shouyin Liu
[1]School of Computer and Information Science,
[2]School of Physics and Electronic Information Engineering,
Hubei Engineering University, Xiaogan, 432000, China
[3]Department of Electronic and Information
Engineering, Central China Normal University, Wuhan, 430079, China

Abstract: Password authentication has been adopted as one of the most commonly used solutions in network environment to protect resources from unauthorized access. Due to its significance in building a secure communication channel, a number of password authentication protocols have been suggested over the past years. Among these schemes, Kim et al.'s schemes are very novel. In the current work, we are concerned with the security of Kim et al.'s schemes. We show that Kim et al.'s schemes are vulnerable to a forgery attack in which an attacker can easily construct a forged login message to impersonate the legal user.

Key words: Authentication, security, smart card, forgery attack, password guessing attack

INTRODUCTION

With the large scale development of network technology, remote user authenti-cation in e-commerce and m-commerce has become an indispensable part to access the precious resources. Remote authentication is a mechanism to authenticate remote users over insecure communication network. User authentication should be offered to protect the important data and to prevent non-authorized users from gaining profit from data. During the past two decades, password-based remote authentication schemes have been widely deployed to verify the legitimacy of the remote users. Since Lamport (1981) proposed his remote authentication scheme, in which the remote server could authenticate the remote user based on identity and password over an insecure network in 1981, many schemes (Fan *et al*., 2002; Kim *et al*., 2005; Shen *et al*., 2003; Sun and Yeh, 2003; Yang *et al*., 2004; Hwang *et al*., 2013; Cui *et al*., 2013; Yang *et al*., 2012; Chen *et al*., 2010) have been proposed to improve the authenti-cation scheme' s security, the cost or the efficiency.

Yang and Shieh (1999) proposed the first password authentication scheme using smart cards (Yang *et al*., 2005). Since then, many password authentication schemes using smart cards have been proposed (Fan *et al*., 2002; Kim *et al*., 2005; Shen *et al*., 2003; Sun and Yeh, 2003; Yang *et al*., 2004, 2005). Among these schemes, the Kim et al.'s schemes are very novel. In the current work, we are concerned with the security of the protocol. We found that Kim et al.'s schemes are still not secure against a forgery attack. The present work reports this new security problem with Kim et al.'s two password authentication schemes.

REVIEW OF KIM-JEON-YOO SCHEMES

In this section, we review in brief Kim et al.'s two authentication schemes, nonce-based password authentication scheme and timestamp-based password authentication scheme. There are three participants in the two schemes: A Key Information Center (KIC), a server S and a user U. The both two authentication schemes involve three phases, the registration phase, the login phase and the authentication phase.

Nonce-based password authentication scheme

Registration phase: Before the remote user logins to the server S, the user U needs to perform the following steps to initially register with the key information center KIC.

Step 1: U chooses his ID_u and PW_U, then sends them over a secure communi-cation channel toKIC

Step 2: KIC generates two large prime number P and Q and computes $N = P \cdot Q$ and $\phi(N) = (P-1)(Q-1)$

Step 3: KIC chooses a prime number e as public key and computes the private key d, such that $e \cdot d \equiv 1 \bmod \phi(n)$

Corresponding Author: Yaoming Ding, School of Physics and Electronic Information Engineering, Hubei Engineering University, Xiaogan, China, 432000

Step 4: KIC chooses a primitive element g in both F_p and F_q.

Step 5: KIC generates the identifier CID_U of a smart card for the user and computes $S_U = ID_U^{CID_U \cdot d}$, $h_U = g^{PW_U \cdot d}$

Step 6: Now KIC finishes the registration procedure by delivering the completed smart card with the secure information (n, e, g, ID_U, CID_U, SU, hU) to U

Login phase: In this phase, the user U sends a login request message to the server S whenever U wants to access some resources upon S. Whenever the user U wants to login to the remote server S, he/she must perform the following steps.

Step 1: U inserts his smart card, CARD, into a smart card reader and then inputs his ID_U, PWU

Step 2: The U's smart card sends the request message $M_1 = \{M_1 = ID_U, CID_U\}$ to the server S

Step 3: Upon receiving the message M_1, S checks if ID_U, CID_U are correct or not. If not, S rejects the user U's login request. Otherwise, S randomly generate a nonce N and sends message $M_2 = \{n\}$ to the U's smart card

Step 4: Upon receiving the message M_2, theU's smart card randomly generates a number rU and computes $X_U = g^{PW_U \cdot r_U \cdot e}$ and $Y_U = h_U^{r_U} \cdot S_U^N$

Step 5: The U's smart card sends $M_3 = \{X_U, Y_U, n, e, g\}$ to the server S

Authentication phase: In this phase, the server S verifies the authenticity of the login message requested by the user U.Upon receiving the message M_3, S checks whether the following equation holds or not:

$$Y_U^e \equiv X_U^d \cdot ID_U^{CID_U \cdot N} \bmod n$$

If not, S rejects the user U's login request, otherwise, S accepts the user U's login request.

Timestamp-based password authenti-cation scheme

Registration phase: The same as nonce-based password authentication scheme, before the remote user U logins to the server *S*, the user U needs to perform the following steps to initially register with KCI.

Step 1: U chooses his ID_U and PWU, then sends them over a secure communication channel to KIC.

Step 2: KIC generates two large prime number p and q and computes $n = p \cdot q$ and $\phi(n) = (p-1)(q-1)$.

Step 3: KIC chooses a prime number e as public key and computes the private key d, such that $e \cdot d \cdot 1 \bmod \phi(n)$

Step 4: KIC Chooses a primitive element g in both F_p and F_q

Step 5: KIC Generates the identifier CID_U of a smart card for the user and computes $S_U = ID_U^{CID_U \cdot d}$, $h_U = g^{PW_U \cdot d}$

Step 6: Now KIC finishes the registration procedure by delivering the completed smart card with the secure information (n, e, g, ID_U, CID_U, S_U, h_U) to U.

Login phase: In this phase, the user U sends a login request message to the server S whenever U wants to access some resources upon S. Whenever the user U wants to login to the remote server S, he/she must perform the following steps.

Step 1: U inserts his smart card, CARD, into a smart card reader and then inputs his ID_U, PWU

Step 2: The U's smart card randomly generates a number r_U and computes $X_U = g^{PW_U \cdot r_U \cdot e}$ and $Y_U = h_U^{r_U} \cdot S_U^T$ where T is the current time stamp.

Step 3: The U's smart card sends $M = \{ID_U, CID_U, X_U, Y_U, e, g, T\}$ to the server S

Authentication phase: In this phase, the server S verifies the authenticity of the login message requested by the user $_U$. Upon receiving the message M, S authenticates the user information as follows.

Step 1: S checks if ID_U and CID_U are valid. If not, S stops the session, otherwise, goes to step 2)

Step 2: S checks that the difference between T and T' is within a valid time interval ΔT for transformation delay, where T' is the current time stamp. If not, S rejects the login request, otherwise goes to step

Step 3: S checks whether the following equation holds or not:

$$Y_U^e \equiv X_U^d \cdot ID_U^{CID_U \cdot T} \bmod n$$

If not, S rejects $_U$'s login request, otherwise, S accepts U's login request.

SECURITY ANALYSIS

This section demonstrates that Kim et al's both two schemes have the vulnerability to forgery attack. We assume that an attacker A has total control over the communication channel between the user U and the remote server S which means that he can insert, delete, or alter any messages in the channel. So, A can get the value of ID_U, CID_U, n, e and g. Then A can carry out the forgery attack on Kim et al.'s schemes as follows.

Forgery attack the nonce-based pass-word authentication scheme: Kim et al's nonce-based password authentication scheme is vulnerable to forgery attack. The forgery attack on nonce-based password authentication scheme is demonstrated in detail as follows.

- The attacker A sends the request message $M_1 = \{ID_U, CID_U\}$ to the remote server S
- Upon receiving the message M_1, S randomly generate a nonce N and sends message $M_2 = \{n\}$ to A
- From the process of the registration phase, we know e is a prime number. So, e is co-prime with $CID_U \cdot N$. There are a, $b \in Z_n$ such that $a \cdot e + b \cdot (CID_U \cdot N) = 1$. A computes the value of A and b using the Extended Euclidean algorithm. Then A computes $X_U = (ID_U^{1-(b+1)(CID_U \cdot N)})^e$, $Y_U = ID_U^a$ and sends $M_3 = \{X_U, Y_U, n, e, g\}$ to the remote server S

Theorem 1: The forged attack allows the adversary to login as user U.

Proof: Since the message $M_1 = \{ID_U, CID_U\}$ and $M_3 = \{X_U, Y_U, n, e, g\}$ are valid login message, the adversary eavesdrops on these message and gets the value ID_U, CID_U, n, e and g of user U. Therefore:

$$\begin{aligned} & X_U^d \cdot ID_U^{CID_U \cdot N} \\ & \equiv [(ID_U^{1-(b+1)(CID_U \cdot N)})^e]^d \cdot ID_U^{CID_U \cdot N} \\ & \equiv ID_U^{1-(b+1)(CID_U \cdot N)} \cdot ID_U^{CID_U \cdot N} \\ & \equiv ID_U^{1-(b+1)(CID_U \cdot N)+CID_U \cdot N} \\ & \equiv ID_U^{1-b \cdot (CID_U \cdot N)} \equiv ID_U^{a \cdot e} \\ & \equiv (ID_U^a)^e \equiv Y_U^e \end{aligned}$$

We can see that the attacker without knowing any secret information can impersonate the user U to cheat the remote server S. Hence, Kim et al's nonce-based password authentication scheme fails to provide the authentication service.

Forgery attack the timestamp-based password authentication scheme: Kim et al's timestamp-based password authentication scheme is also vulnerable to forgery attack. The forgery attack on timestamp-based password authentication scheme is demonstrated in detail as follows.

Since e is co-prime with $CID_U \cdot TA$, then A can compute the value of A and b using the Extended Euclidean algorithm such that $a.e + b \cdot (CID_U \cdot TA) = 1$, where TA is the current time stamp. A computes $X_U = (ID_U^{1-(b+1)(CID_U \cdot T_A)})^e$, $Y_U = ID_U^a$ and sends the message $M = \{ID_U, CUDU, X_U, Y_U, n, e, g, TA\}$ to the remote server S.

Theorem 2: The forged attack allows the adversary to login as user U.

Proof: Since the message $M = \{ID_U, CUDU, X_U, Y_U, n, e, g, TA\}$ is valid login message, the adversary eavesdrops on these message and gets the value ID_U, CID_U, n, e and $_{TA}$ of user U. Therefore:

$$\begin{aligned} & X_U^d \cdot ID_U^{CID_U \cdot T_A} \\ & \equiv [(ID_U^{1-(b+1)(CID_U \cdot T_A)})^e]^d \cdot ID_U^{CID_U \cdot N} \\ & \equiv ID_U^{1-(b+1)(CID_U \cdot T_A)} \cdot ID_U^{CID_U \cdot N} \\ & \equiv ID_U^{1-(b+1)(CID_U \cdot T_A)+CID_U \cdot N} \\ & \equiv ID_U^{1-b \cdot (CID_U \cdot T_A)} \equiv ID_U^{a \cdot e} \\ & \equiv (ID_U^a)^e \equiv Y_U^e \end{aligned}$$

CONCLUSION

Smart card-based user authentication technology has been widely deployed in various kinds of applications, such as remote host login, withdrawals from automated cash dispensers and physical entry to restricted areas. In this study, we have demonstrated that Kim et al.'s both two schemes are vulnerable to a forgery attack. So, Kim-Jeon-Yoo schemes are still insecure for practical application and needs to be improved.

ACKNOWLEDGMENT

The authors would like to thank for the support by the Natural Science Foundation of China under the Grant 61370223 and the support by Science Research Project of Hubei Provincial Department of Education under the Grant B2013024. The authors would like to thank to the valuable comments and suggestions of the reviewers.

REFERENCES

Chen, B.L., W.C. Kuo and Y.S. Chu, 2010. Weaknesses of a secure dynamic ID based remote user authentication scheme. Int. J. Converg. Inform. Technol., 5: 84-89.

Cui, J.M., Z.S. Lai and X.J. Zhang, 2013. Cryptanalysis and improvement of a remote user authentication scheme based on dynamic id using smart card. Int. J. Digital Content Technol. Appl., 7: 828-837.

Fan, L., J.H. Li and H.W. Zhu, 2002. An enhancement of timestamp-based password authentication scheme. Int. J. Comput. Secur., 21: 665-667.

Hwang, R.J., F.F. Su and Y.Y. Chen, 2013. A new two-factor dynamic ID-based remote user authentication scheme. Int. J. Converg. Inform. Technol., 8: 837-844.

Kim, K.W., J.C. Jeon and K.Y. Yoo, 2005. An improvement on Yang et al.'s password authentication schemes. Int. J. Applied Math. Comput., 170: 207-215.

Lamport, L., 1981. Password authentication with insecure communication. Commun. ACM, 24: 770-772.

Shen, J.J., C.W. Lin and M.S. Hwang, 2003. Security enhancement for the timestamp-based password authentication scheme using smart cards. Int. J. Comput. Secur., 22: 591-595.

Sun, H.M. and H.T. Yeh, 2003. Further cryptanalysis of a password authentication scheme with smart cards. Int. J. IEICE Trans. Commun., E86-B: 1412-1415.

Yang, C.C., H.W. Yang and R.C. Wang, 2004. Cryptanalysis of security enhancement for the timestamp-based password authentication scheme using smart cards. Int. J. IEEE Trans. Consum. Electr., 50: 578-579.

Yang, C.C., R.C. Wang and T.Y. Chang, 2005. An improvement of the yang-shieh password authentication schemes. Int. J. Applied Math. Comput., 162: 1391-1396.

Yang, F.Y., Y. Li, S.H. Chiu and C.S. Jiang, 2012. Improvements in dynamic ID-based remote user authentication schemes. Int. J. Adv. Comput. Technol., 4: 240-247.

Yang, W.H. and S.P. Shieh, 1999. Password authentication schemes with smart cards. Int. J. Comput. Secur., 18: 727-733.