All rights are reserved and copyright of this manuscript belongs to the authors. This manuscript has been published without reviewing and editing as received from the authors: posting the manuscript to SCIS 2007 does not prevent future submissions to any journals or conferences with proceedings.

SCIS 2007 The 2007 Symposium on
Cryptography and Information Security
Sasebo, Japan, Jan. 23-26, 2007
The Institute of Electronics,
Information and Communication Engineers

Cryptanalysis of ID-Based Remote Authentication with Smart Cards on Open Distributed System from Elliptic Curve Cryptography

Duc-Liem Vo * Kwangjo Kim *

Abstract— Remote authentication is an important mechanism to control user access to remote systems in a way such that only authorized users can be authenticated before being granted services. There are several methods to implement authentication but for human, password authentication is preferred. With advances in elliptic curve cryptography, Wu *et al.* [10] proposed ID-based remote authentication schemes with smart cards. Their schemes do not require the server to store a verification table for authenticating users and let users choose and change password freely. In addition, the remote hosts can be in open distributed networks and require nothing about the secret of the key information center to authenticate users. However, we show that these schemes are insecure by impersonation attacks. With these attacks, any adversary can be successfully authenticated and then use services at no cost. We also suggest a repaired scheme which is more secure than the original scheme.

Keywords: Cryptanalysis, authentication, ID-based, smart cards

1 Introduction

Remote authentication over insecure communication is an important application of cryptographic protocols. The first construction, proposed by Lamport [6] in 1981, can resist replaying attack but it needs a password table for verifying the legitimacy of the login user. However, the system will be vulnerable if the verifier, who is holding password table, is compromised. In ID-based authentication schemes [2, 3, 5, 7, 8], the using password table is eliminated but remote users need to rely on a password generation center for computing their secret key, making the users' inconvenience. Recently, remote password authentication schemes using smart cards are widely introduced due to the advantages in low cost communication, computation and no password table. Some schemes even let users choose password by their choices.

In 2005, Wu *et al.* [10] proposed ID-based remote authentication schemes with smart cards using elliptic curve cryptography. These schemes allow users to choose their password freely and require no password table for verifying the legitimacy of users. The schemes also are flexible in which any distributed remote host can authenticate users without knowing any secret from the key information center. In this paper, we propose an attack on Wu *et al.*'s remote authentication schemes by which an adversary can successfully authenticate himself with the remote server.

The organization of the paper is as follows. In the next section, we brief concepts of bilinear pairings. We review Wu *et al.*'s schemes in the Section 3 and propose attack on these schemes in Section 4. A repaired version of Wu *et al.*'s schemes and its analysis are shown in Section 5. Section 6 closes with concluding remarks.

2 Bilinear Pairings

We summarize some concepts of bilinear pairings using similar notations used by in this section. Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be additive and multiplicative groups of the same prime order q, respectively. Let P be a generator of $\mathbb{G}_1$. Assume that the discrete logarithm problems in both $\mathbb{G}_1$ and $\mathbb{G}_2$ are hard. Let $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ be a pairing which satisfies the following properties:

1. *Bilinear*: $e(aP, bP') = e(P, P')^{ab}$ for all $P, P' \in \mathbb{G}_1$ and all $a, b \in \mathbb{Z}_q^*$.
2. *Non-degenerate*: If $e(P, P') = 1\ \forall\, P' \in \mathbb{G}_1$ then $P = \mathcal{O}$.
3. *Computable*: There is an efficient algorithm to compute $e(P, P')$ for any $P, P' \in \mathbb{G}_1$.

To construct the bilinear pairing, we can use the Weil pairing or Tate pairing associated with supersingular elliptic curves [1, 4].

3 Review of Wu *et al.*'s schemes

In [10], Wu *et al.* proposed a pairing-wise timestamp-based password authentication scheme and its extended version, called pairing-wise nonce-based password authentication scheme, for the network without clocked synchronization. There are four phases in remote authentication schemes, namely initialization phase, registration phase, login phase and authentication phase.

In both schemes, there is a key information center that is responsible for generating keys for all entities, issuing smart cards to new users and serving password-changing request for the registered users.

* International Research center for Information Security (IRIS), Information and Communications University (ICU) 103-6 Munji-dong, Yuseong-gu, Daejeon, 305-732, KOREA (vdliem,kkj@icu.ac.kr)

Prior to accessing the remote system, a new user registers by submitting his identity and password to the key information center, and the key information center will issue a smart card for the new user. In the login phase, the user inserts his smart card to the input device terminal and enter his identity and password. Then the terminal sends a login request message to the remote distributed host. In the authentication phase, the remote distributed host verifies the correctness of the submitted message and decides to accept the login request or not.

3.1 Pairing-wise timestamp-based password authentication scheme

Initialization Phase: The key information center selects an elliptic curve E with order q and a base point P as public parameters. Then the key information center chooses a secret $s \in \mathbb{Z}_q^*$, and computes $P_{pub} = sP$. P_{pub} is sent securely to distributed remote hosts for using in the authentication phase.
Registration Phase: The user i submits his identity id_i and his chosen password $pw_i \in \mathbb{Z}_q^*$ to the key information center for registration request. The submission is done over secure channel or in person. The key information center processes the registration request by the following steps:

1. Compute the public key of the user i:

$$Q_i = H_1(id_i),$$

where $H_1(\cdot) : \{0,1\}^* \rightarrow \mathbb{G}_1$ is a public one-way hash function.

2. Compute the secret key of the user i:

$$X_i = pw_i Q_i \oplus sQ_i,$$

where the notation $\oplus$ is the corresponding coordinate exclusive-OR bit operation.

3. Personalize the user's smart card with the data $\{id_i, E, q, P, H_1(\cdot), h(\cdot), X_i\}$ and issue the card to the user i. Here, $h(\cdot)$ is a public one-way hash function.

Login Phase: If the user i wants to login the remote system, he attaches his smart card to the input device terminal, then keys in his identity id_i^* and password pw_i^*. The smart card performs the following operations:

1. Check the validity of the id_i^*. If id_i^* does not match with id_i in the smart card, the login process will be aborted.

2. Calculate:

$$\begin{array}{rcl} A_i & = & rP \\ B_i & = & h(T)(pw_i^* Q_i \oplus X_i) + rQ_i, \end{array}$$

where r is a random number selected by the smart card, T is the current date and time and is used as a timestamp of the input device terminal.

3. Send a message $m_1 = \{id_i^*, T, A_i, B_i\}$ to the remote host.

Authentication Phase: Receiving the message m_1 at the time of T', the remote system authenticates the user using the following steps:

1. Verify the format of id_i^*. If the format of id_i^* is not correct, then the system rejects the login request.

2. Verify the validity of time interval between T and T'. If $(T' - T) \geq \Delta T$, where ΔT denotes the expected valid time interval for transmission delay, then the remote system rejects the login request.

3. Check whether the following equation holds or not:

$$\hat{e}(B_i, P) = \hat{e}(Q_i^*, h(T)P_{pub} + A_i).$$

Here $Q_i^* = H_1(id_i^*)$. If the above equation holds, it indicates that the password pw_i^* is equal to pw_i and id_i^* is equal to id_i. Then the system accepts the request of login, otherwise rejects it.

3.2 Pairing-wise nonce-based password authentication scheme

A nonce-based password authentication scheme is used for the networks without clocked synchronization. The initialization and registration phases are the same as the timestamp-based authentication scheme above. The login phase and authentication phase are described bellow repspectively:
Login Phase: If the user i wants to login the remote system, he attaches his smart card to the input device terminal, then keys in his identity id_i^* and password pw_i^*. The following steps will be performed:

1. Check the validity of the id_i^*. If id_i^* does not match with id_i in the smart card, the login process will be aborted, otherwise, the smart card sends the identity id_i^* to the remote system as a request of remote login.

2. Upon receiving the identity id_i^* of the user i, the remote host verifies the validity of the format of id_i^*. If it is legitimate, then the remote host selects a number n randomly as a nonce, and sends it back to the smart card.

3. Receiving the nonce, the smart card calculates:

$$\begin{array}{rcl} A_i & = & rP \\ C_i & = & n(pw_i^* Q_i \oplus X_i) + rQ_i, \end{array}$$

where r is a random number selected by the smart card.

4. Send a message $m_2 = \{A_i, C_i\}$ back to the remote host.

Authentication Phase: Receiving the message m_2 the remote system checks whether the following equation holds or not:

$$\hat{e}(C_i, P) = \hat{e}(Q_i^*, nP_{pub} + A_i).$$

Here $Q_i^* = H_1(id_i^*)$. If the above equation holds, it indicates that the password pw_i^* is equal to pw_i, the message m_2 is generated by the user id_i, and the nonce n that the smart card used to calculate C_i is identical to the one generated by the remote host. The message m_2 is fresh and is not a replayed message.

4 Cryptanalysis of Wu *et al.*'s schemes

In this section, we show that both Wu *et al.*'s remote authentication schemes described previously are indeed insecure due to impersonation attacks by an adversary who's knowing P_{pub}. This adversary can be a malicious remote host or co-operates with a compromised remote host. The impersonation attacks on both schemes are done in the same way by the adversary who intercepts the final message sent to remote host. The adversary performs the attacks by acting as the user or intercepting the final message sent to the remote host during user's authentication phase. The other information which the adversary needs to know is the identity id_i of the user i in valid format. This can be done easily when the adversary eavesdrops the previous authentication sessions of the user.

4.1 Attack on timestamp-based password authentication scheme

The adversary wanting to impersonate the user i performs the login phase by intercepting and sending data directly to the remote host without using the smart card.

Login phase: He follows the following steps in the login phase:

1. Select a random number r' and compute:

$$\begin{aligned} A_i' &= r'P - h(T)P_{pub} \\ B_i' &= r'Q_i, \end{aligned}$$

where T is the current data and time.

2. Send the message $m_1' = \{id^*, T, A_i', B_i'\}$ to the remote system.

Authentication phase: Receiving login request from the user i with the message m_1', the remote host performs authentication phase as usual:

1. Verify the format of id^*. This must be valid since it actually is the identity of the user i.

2. Verify the validity of time interval between T and T'. If $(T' - T) \geq \Delta T$, where ΔT denotes the expected valid time interval for transmission delay. This verification also passes since there is no difference between the real user and the adversary in using the transmission line.

3. Check whether the following equation holds or not:

$$\hat{e}(B_i', P) = \hat{e}(Q_i^*, h(T)P_{pub} + A_i').$$

The equation holds and the adversary is successfully authenticated by the remote host. The correctness of the equation is shown bellow:

$$\begin{aligned} \hat{e}(B_i', P) &= \hat{e}(Q_i^*, h(T)P_{pub} + A_i') \\ &= \hat{e}\left(Q_i^*, h(T)P_{pub} + (r'P - h(T)P_{pub})\right) \\ &= \hat{e}(Q_i^*, r'P) \\ &= \hat{e}(r'Q_i^*, P) \\ &= \hat{e}(B_i', P). \end{aligned}$$

4.2 Attack on nonce-based password authentication scheme

Like the previous attack, the adversary wanting to impersonate the user i performs the login phase by intercepting and sending data directly to the remote host without using the smart card.

Login phase: In the login phase, the following steps will be performed:

1. Send id_i^* to the remote host as a request of remote login.

2. Upon receiving the identity id_i^* sent by the adversary, the remote host verifies the validity of the format of id_i^*. This check must be good since the identity is from the real user. Therefore, the remote host selects a number n randomly as a nonce, and sends it back to the adversary.

3. Upon receving the nonce, the adversary selects a random number r' and compute:

$$\begin{aligned} A_i' &= r'P - nP_{pub} \\ C_i' &= r'Q_i, \end{aligned}$$

4. The adversary sends the message $m_2' = \{A_i', C_i'\}$ to the remote system.

Authentication phase: Receiving login request from the user i with the message m_2', the remote host performs authentication phase as usual by checking the following equation holds or not:

$$\hat{e}(C_i', P) = \hat{e}(Q_i^*, nP_{pub} + A_i').$$

The equation must hold since

$$\begin{aligned} \hat{e}(C_i', P) &= \hat{e}(Q_i^*, nP_{pub} + A_i') \\ &= \hat{e}\left(Q_i^*, nP_{pub} + (r'P - nP_{pub})\right) \\ &= \hat{e}(Q_i^*, r'P) \\ &= \hat{e}(r'Q_i^*, P) \\ &= \hat{e}(C_i', P). \end{aligned}$$

Finally, the adversary is successfully authenticated with the remote host since he passes all required authentication checks.

5 Our improvement

5.1 Repair of Wu *et al.*'s schemes

In this section, we propose a repaired version of Wu *et al.*'s remote authentication schemes. The main problem in Wu *et al.*'s schemes is that the random value A_i was an independent element in the verification equation, therefore, an adversary can intercept messages in both cases and authenticate successfully. We modify Wu *et al.*'s schemes to overcome this problem while maintaining the authentication property on distribution network. The repair can be applied to two schemes in the same way. We describe the repaired version of the timestamp-based password authentication scheme bellow.

The initialization and registration phases are the same with the previous schemes except that the key information center can send P_{pub} value to the remote hosts in *public channels* or just simply make it available for everyone. The login and authentication phases are as follows:

Login phase: If the user i wants to login the remote system, he attaches his smart card to the input device terminal, then keys in his identity id_i^* and password pw_i^*. The smart card performs the following operations:

1. Check the validity of the id_i^*. If id_i^* does not match with id_i in the smart card, the login process will be aborted.

2. Calculate:

$$\begin{aligned} A_i &= rP \\ B_i &= h(T, A_i)(pw_i^* Q_i \oplus X_i) + rQ_i, \end{aligned}$$

   where r is a random number selected by the smart card, T is the current date and time and is used as a timestamp of the input device terminal.

3. Send a message $m_1 = \{id_i^*, T, A_i, B_i\}$ to the remote host.

Authentication Phase: Receiving the message m_1 at the time of T', the remote system authenticates the user using the following steps:

1. Verify the format of id_i^*. If the format of id_i^* is not correct, then the system rejects the login request.

2. Verify the validity of time interval between T and T'. If $(T' - T) \geq \Delta T$, where ΔT denotes the expected valid time interval for transmission delay, then the remote system rejects the login request.

3. Check whether the following equation holds or not:

$$\hat{e}(B_i, P) = \hat{e}(Q_i^*, h(T, A_i)P_{pub} + A_i).$$

   Here $Q_i^* = H_1(id_i^*)$. If the above equation holds, it indicates that the password pw_i^* is equal to pw_i and id_i^* is equal to id_i. Then the system accepts the request of login, otherwise rejects it.

The correctness of the verification equation can be easily checked as follows:

$$\begin{aligned} \hat{e}(B_i, P) &= \hat{e}\left(h(T, A_i)(pw^* Q_i \oplus X_i) + rQ_i, P\right) \\ &= \hat{e}(h(T, A_i)(pw^* Q_i \oplus (pwQ_i \oplus sQ_i)) + \\ &\quad +rQ_i, P)) \\ &= \hat{e}(h(T, A_i)sQ_i + rQ_i, P) \\ &= \hat{e}(Q_i^*, h(T, A_i)P_{pub} + rP) \\ &= \hat{e}(Q_i^*, h(T, A_i)P_{pub} + A_i). \end{aligned}$$

For the nonce-based password authentication scheme, we make the similar modification like above. The steps in the login phase are kept the same except the message m_2 is computed by the following equations:

$$\begin{aligned} A_i &= rP \\ C_i &= h(n, A_i)(pw_i^* Q_i \oplus X_i) + rQ_i. \end{aligned}$$

And the verification equation in the authentication phase is changed correspondingly:

$$\hat{e}(C_i, P) = \hat{e}(Q_i^*, h(n, A_i)P_{pub} + A_i).$$

5.2 Discussion

As can be seen, the repaired version of Wu *et al.*'s remote authentication schemes maintains almost the original construction and properties. Firstly, the modification does not change capability of user authentication in open distribution network, that is the remote hosts can be in distributed network and do not need to contact the key information center in order to validate users. The information the remote hosts need to know is just P_{pub} which can be accessed publicly. This is an advantage over the original schemes where the key information center need to send this value to remote hosts through secure channels. Secondly, the modification does not affect to computational complexity of the scheme in timestamp-based approach and just one more hash operation in the nonce-based case. The efficiency of the schemes is maintained.

Considering security issues, the replaying attack will not be successful. Given that the adversary recorded a messange $m_1 = \{id, T, A_i, B_i\}$ or $\langle n, m_2 = \{A_i, C_i\}\rangle$, if he wants to authenticate at the later time or with other challenged nonce, he needs to recompute value A_i, B_i, or C_i to pass verifying equations. This cannot be done without knowing the secret value X_i, pw_i or r.

For the impersonation attack, if an adversary produces valid message m_1 or $\langle n, m_2 = \{A_i, C_i\}\rangle$, it can be shown that there exists an algorithm can break the Computational Diffie-Hellman problem in the group $\mathbb{G}_1$. Detailed information can be found in [9].

Changing user password is similar to the original scheme. The user needs to bring (or send securely) the smart card to the key information center. The key information center changes information according to the user's request and updated (or issues a new) smart card for the user.

In case of revocation (not mentioned in the previous scheme), the remote hosts need to maintain a blacklist of violated users by themselves. The list just contains the identities of the illegal users and can be published depending on the remote hosts.

6 Concluding Remarks

Remote authentication is an important mechanism to control user access to remote systems in a way such that only authorized users can be authenticated before being granted services. Password authentication is one of preferred methods for remote authentication in which users are verified via their passwords. Wu *et al.* [10] proposed ID-based remote authentication schemes with smart cards using bilinear pairings from elliptic curves. Their schemes do not require the server to store a verification table for authenticating users and let users choose and change password freely. In addition, the remote hosts can be in open distributed networks and require nothing about the secret of the key information center to authenticate users. However, we show that these schemes are vulnerable under impersonation attacks. With these attacks, any adversary can be successfully authenticated with the remote host and then use services at no cost. We also provided a repaired scheme which more secure than the original one while maintaining good properties as well as performance. Our study also is a lesson on designing cryptographic protocols using bilinear pairings, a mathematical technique used intensively these days.

References

[1] Dan Boneh, Matthew Franklin, "Identity-Based Encryption from the Weil Pairing," *Advances in Cryptology - CRYPTO 2001*, Springer-Verlag, pp. 312–229, 2001.

[2] C. C. Chang and S. J. Hwang, "Using smart cards to authenticate remote passwords," *Computers and Mathematical Applications*, Vol.26, No.7, pp.19–27, 1993.

[3] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," *IEE Proceeding-E*, Vol.138, No.3, pp.165–168, 1991.

[4] Steven D. Galbraith, Keith Harrison and David Soldera, "Implementing the Tate Pairing," *Proceedings of the 5th International Symposium on Algorithmic Number Theory*, ANTS-V, Sydney, Australia, pp. 324–337, July 7-12, 2002.

[5] Min-Shiang Hwang and Li-Hua Li, "A new remote user authentication scheme using cards," *IEEE Trans. on Consumer Electronics*, Vol.46, February, pp.28–30, 2000.

[6] L. Lamport, "Password authentication with insecure communication," *Communication of ACM*, Vol.24, pp.770–772, 1981.

[7] E. Okamoto, and K. Tanka, "Identity-based information security managements system for personal computer networks," *IEEE Journal on Selected Areas in Communications*, Vol.7, No.2, 1989, pp. 290–294.

[8] Hung-Min Sun, "An efficient remote use authentication scheme using smart card," *IEEE trans. on Consumer Electronics*, Vol.46, November, pp. 958–961, 2000.

[9] HyoJin Yoon, Jung Hee Cheon and Yongdae Kim, "Batch Verifications with ID-Based Signatures," In *Proceedings of the 7th International Conference on Information Security and Cryptology* - ICISC 2004, Seoul, Korea, LNCS 3506, pp. 233–248, 2005.

[10] Shyi-Tsong Wu, Jung-Hui Chiu and Bin-Chang Chieu, "ID-based remote authentication with smart cards on open distributed system from elliptic curve cryptography," *Electro Information Technology, 2005 IEEE International Conference on*, 22-25 May 2005.