Journal of Universal Computer Science, vol. 17, no. 11 (2011), 1623-1633
submitted: 26/3/09, accepted: 30/1/11, appeared: 1/7/11 © *J.UCS*

Security Analysis of Three Password Authentication Schemes

Kyung-Ah Shim
(National Institute for Mathematical Sciences, Daejeon, Korea
kashim@nims.re.kr)

Abstract: In this paper, we show that a verifier-based password authentication scheme and two remote user authentication schemes are insecure against several active attacks. These results demonstrate that no more password authentication schemes should be constructed with such ad-hoc methods, i.e, the formal design methodology using provable security should be employed.

Key Words: Password-based authentication, verifier-based password authentication, remote user authentication, smart card, server-compromise attack.
Category: E. 3, D. 4. 6.

1 Introduction

Two entities, who only share a password, and who are communicating over an insecure network, want to authenticate each other and agree on a session key to be used for protecting their subsequent communication. This is called the *password-authenticated key exchange* problem. The first password-authenticated key exchange (PAKE) protocol, known as Encrypted Key Exchange (EKE), was suggested by Bellovin and Merritt [Bellovin and Merritt 92a]. Using a combination of symmetric and public-key cryptography, EKE resists dictionary attacks by giving a passive attacker insufficient information to verify guessed passwords. The family of EKE protocols represents a strong level of password authentication protocols available. However, EKE still suffers from plaintext-equivalence, requiring that both the client and the host have access to the same secret password or hash thereof. To overcome these flaws, verifier-based password authentication protocols have been proposed such as the Augmented EKE(A-EKE) [Bellovin and Merritt 94c], which makes EKE a verifier-based one. Since then, many PAKE protocols that promised increased security have been developed [Boyko et al. 00a],[Bellare et al. 00a],[Jablon 96b],[Jablon 97b],[Steiner et al. 95b],[Wu 98a]. Among them, SPEKE [Jablon 97b], SRP [Wu 98a], PAK [MacKenzie and R. Swaminathan 99] and AMP [Kwon 03b] are being discussed by the IEEE P1363 standards working group for standardization on password-based public key cryptographic techniques [IEEE P1363.2]. From the practical perspective, AMP and SRP are known as the most efficient four-pass PAKE protocols. Kwon [Kwon 03b] submitted a summary of AMP to IEEE P1363.2. His documentation contains four-pass protocols, AMP, AMP2, AMP3 and three-pass protocols:

TP-AMP, TP-AMP2. He argued that the protocols are secure against password-related attacks such as on-line password guessing, off-line password guessing, two-for-one password guessing and server compromise. In this paper, we point out that AMP3 [Kwon 03b] is still insecure against server-compromise attacks.

A number of password authentication schemes with smart cards have been proposed [Chan and Cheng 02b],[Fan et al. 02b],[Lamport 81b],[Shen et al. 03b],[Sun and Yeh 03b],[Yang and Shieh 99b],[Yang et al. 05b],[Yang et al. 04b]. Due to the low cost, the portability and the cryptographic capacity, smart cards have been widely adopted in remote authentication schemes. In this paper, we show that Wang's and Kim *et al.*'s remote user password authentication schemes [Wang et al. 07b],[Kim et al. 05b] with smart cards are vulnerable to an impersonation attack and forgery attacks, respectively.

The rest of the paper is organized as follows. In Section 2, we show that AMP3 [Kwon 03b] is insecure against server-compromiser attacks. In Section 3, we point out security weaknesses of two remote user password authentication schemes with smart cards. Concluding remarks are given in Section 4.

2 Cryptanalysis of Kwon's Verifier-based Password Scheme

We first review AMP3 which is one of lightweight versions of AMP [Kwon 03b]. We assume that A and B are well-behaving legitimate parties. In user-to-server situations, A is a user and B is a server. Let q of the length at least 160 bits and p of the length 1024 bits be primes such that $p = rq + 1$ for some value r co-prime to q. Let g be a generator of G_q, where G_q is an order q subgroup of Z_p^*, the multiplicative group of the integers modulo p. For simplicity, we omit the operation "mod p". Let $h_i : \{0,1\}^* \rightarrow \{0,1\}^n$ $(i = 0, \cdots, 5)$ be one-way hash functions for some n. A function $\texttt{ACCEPTABLE}_2\texttt{()}$ is defined as follows: $\texttt{ACCEPTABLE}_2\texttt{(c)}$=False if c is confined to a tiny subgroup, True, otherwise. Let π be A's password and its verifier $\nu = g^u$, where $u = h_0(id, \pi)$ for an identity id of A. The server B stores ν as A's verifier. AMP 3 is depicted in Figure 1. Its resulting session key is $K = K' = h_5(id, A, B, m, \mu, \alpha) = h_5(id, A, B, m, \mu, \beta)$, where $\alpha = \beta = g^{(x+1)y}$.

A PAKE protocol is said to be secure against a server compromise attack (or a stolen-verifier attack) if, when server's password file is captured and an adversary learns the verifier, it should still not allow the adversary to impersonate the client without an expensive dictionary search. In other words, an adversary, who has compromised a server and could obtain A's verifier ν, should not able to impersonate A without mounting dictionary attacks on ν. Kwon [Kwon 03b] argued that the AMP protocols containing AMP3 are secure against password-related attacks including server-compromise attacks. Now, we show that AMP3 is still vulnerable to the server-compromise attack.

$$
\begin{array}{lcl}
User\ A\ [id, \pi] & & Server\ B\ (id, \nu = g^u) \\
x \leftarrow_R Z_q,\ \ m \leftarrow g^x & & \\
& \xrightarrow{id,\ m} & \\
& & y \leftarrow_R Z_q,\ \ c \leftarrow m \cdot \nu \\
& & \mu \leftarrow g^y \text{ if } \texttt{ACCEPTABLE}_2\texttt{(c)=False} \\
& & \mu \leftarrow c^y \ \ \text{otherwise} \\
& \xleftarrow{\mu} & \\
u \leftarrow h_0(id, \pi) & & d \leftarrow m \cdot g \\
w \leftarrow (x+u)^{-1}(x+1) \bmod q & & \text{abort if } \texttt{ACCEPTABLE}_2\texttt{(d)=False} \\
\alpha \leftarrow \mu^w & & \beta \leftarrow d^y \ \ \text{otherwise} \\
k_1 \leftarrow h_3(id, A, B, m, \mu, \alpha) & & k_1' \leftarrow h_3(id, A, B, m, \mu, \beta) \\
& \xrightarrow{k_1} & \\
& & \text{abort if } k_1 \neq k_1' \\
& & k_2 \leftarrow h_4(id, A, B, m, \mu, \beta) \\
& \xleftarrow{k_2} & \\
k_2' \leftarrow h_4(id, A, B, m, \mu, \alpha) & & \\
\text{abort if } k_2 \neq k_2' & & \\
K \leftarrow h_5(id, A, B, m, \mu, \alpha) & & K' \leftarrow h_5(id, A, B, m, \mu, \beta)
\end{array}
$$

Figure 1: AMP3

• **Server-Compromise Attacks on AMP3.** Suppose that the verifier $\nu = g^u$ is compromised to an adversary E and E wishes to impersonate A to B. $E(A)$ represents E impersonating the client A.

1. First, the adversary $E(A)$ sets m to be $\nu \cdot g^{-2}$ and sends $\{id,\ m\}$ to B impersonating A.
2. After receiving the message, B thinks that the message is from A. Then B chooses $y \in_R Z_q$, computes
$$c = m \cdot \nu = g^{u-2} \cdot g^u = g^{2u-2}, \quad \mu = c^y = g^{(2u-2)y},$$
and sends μ to $E(A)$. Next, B computes
$$d = m \cdot g = g^{u-1}, \quad \beta = d^y = g^{(u-1)y}, \quad k_1' = h_3(id, A, B, m, \mu, \beta).$$
3. On the receipt of the message, $E(A)$ can compute α (which is equal to β) from μ as
$$\alpha = \mu^{1/2} = (g^{(2u-2)y})^{1/2} = g^{(u-1)y}.$$
Then $E(A)$ computes $k_1 = h_3(id, A, B, m, \mu, \alpha)$ and sends it to B.

4. After receiving k_1, B checks whether $k_1 = k_1'$ holds or not. In fact, it holds, because α computed by E is equal to β as $g^{(u-1)y}$. Then, B computes $k_2 = h_4(id, B, m, \mu, \beta)$ and sends it to $E(A)$. Next, B computes the session key $K' = h_5(id, A, B, m, \mu, \beta)$.
5. On the receipt of the message, $E(A)$ verifies k_2, and computes the session key $K = h_5(id, A, B, m, \mu, \alpha)$. Finally, E succeeds in impersonating A to B as well as knowledge of the session key $K = K' = h_5(id, A, B, m, \mu, g^{(u-1)y})$.

By using the verifier ν, the adversary can compute the first transmitted message m to confine the shared secret to a predictable value from the received message μ computed by the legitimate server B. By fabricating the message from the compromised verifier, the adversary can impersonate A and compute the shared secret, $\alpha = \beta = g^{(u-1)y}$ established between $E(A)$ and B without the knowledge of the password π. Therefore, AMP 3 is insecure against the server-compromise attack.

3 Cryptanalysis of Two Remote User Password Schemes

3.1 Wang *et al.*'s Authentication Scheme

In 2000, Hwang and Li [Hwang and Li 00b] proposed a new remote user authentication scheme using smart cards. In 2002, based on Sun's scheme [Sun 00b], Chien *et al.* [Chien et al. 02b] proposed a most cost-effective remote user authentication scheme that achieves mutual authentication, freely choosing password, no verification table, and involving only few hashing operations instead of the costly modular exponentiations. Later, Ku *et al.* [Ku and Chen 04b] pointed out that Chien *et al.*'s scheme is vulnerable to reflection attacks, insider attacks and password guessing attacks. Subsequently, Yoon *et al.* [Yoon and Ryu 04b] showed that Ku *et al.*'s scheme is insecure against parallel session attacks and also proposed an enhanced version to overcome the attacks. Recently, Wang *et al.* [Wang et al. 07b] showed that Ku *et al.*'s scheme and Yoon *et al.*'s scheme are vulnerable to password guessing attacks, forgery attacks and Denial of Service (DoS) attacks. They also proposed an improved scheme to overcome the attacks. In this section, we show that their improved scheme is insecure against impersonation attacks, i.e., it does not achieve mutual authentication as intended.

• Wang *et al.*'s Password Authentication Scheme.
[**Registration.**] This phase is invoked whenever a user U (with an identity ID and a password PW) initially registers to a remote server S.

1. U selects a random number b, computes $h(b \oplus PW)$ and sends $\{ID,\ h(b \oplus PW)\}$ to S via a secure channel.
2. On the receipt of the message, S computes $p = h(ID \oplus x)$, $R = p \oplus h(b \oplus PW)$ and $V = h_p(h(b \oplus PW))$, where x is the permanent secret key of S.

3. The server S sends a smart card containing $\{R,\ V,\ h(\cdot),\ h_k(\cdot)\}$ to U via a secure channel, where $h(\cdot)$ and $h_k(\cdot)$ are a cryptographic hash function and a keyed hash function with a secret k, respectively.
4. U enters b into its smart card so that it does not need to remember b anymore.

[**Login.**] When U wants to login on the server,

1. U inserts its smart card into the card reader, and then enters ID and PW.
2. Smart card computes $p = R \oplus h(b \oplus PW)$ and checks whether $h_p(h(b \oplus PW)) = V$ holds or not. If not, smart card terminates this session.
3. Smart card generates a random number r, and computes $c_1 = p \oplus h(r \oplus b)$, $c_2 = h_p(h(r \oplus b) \oplus T_u)$, where T_u denotes U's current timestamp. Then U sends $M = \{ID, c_1, c_2, T_u\}$ to S.

[**Verification.**] Upon receiving the login request $M = \{ID, c_1, c_2, T_u\}$, the remote system S performs the following steps:

1. Check either if ID is invalid or $T_u = T_s$, where T_s is the current timestamp of S, then rejects the request. If $(T_s - T_u) > \Delta T$, where ΔT denotes the expected valid time interval for transmission delay, then S rejects it.
2. The server S computes $p = h(ID \oplus x)$ and $c_1' = p \oplus c_1$, then checks whether $h_p(c_1' \oplus T_u) = c_2$ holds or not. If holds, S computes $c_3 = h_p(c_1' \oplus T_s)$ and then sends $\{c_3, T_s\}$ to U. Otherwise, S rejects it.
3. Upon receiving the message $\{c_3, T_s\}$, U verifies either T_s is invalid or $T_s = T_u$, U terminates this session. Otherwise, U computes $c_3' = h_p(h(r \oplus b) \oplus T_s)$ and compares $c_3' = c_3$. If they are equal, then U believes that S is authenticated and the mutual authentication between U and S is completed, otherwise U terminates the session. In addition, $c_1' = h(r \oplus b)$ shared between U and S can be used as the session key for subsequent private communications.

We omit the [**Password Change**] of Wang *et al.*'s scheme.

• **Impersonation Attacks on Wang** ***et al.*****'s Scheme.** Suppose that an adversary E wants to impersonate a user U to a server S.

1. First, E eavesdrops U's login session and stores its all transcription (c_1, c_2, T_u). Next, E computes $\bar{c}_1 = c_1 \oplus T_u \oplus \bar{T}$, $\bar{c}_2 = c_2$, where $\bar{T}$ is a current timestamp. Then E sends $\bar{M} = \{ID, \bar{c}_1, \bar{c}_2, \bar{T}\}$ to S impersonating U.
2. On the receipt of $\bar{M}$, S checks the validity, $\bar{T} \neq T_s$ and $(T_s - \bar{T}) < \Delta T$, where T_s is the current timestamp of S. Then S computes $p = h(ID \oplus x)$, $\bar{c}_1' = p \oplus \bar{c}_1$, then check whether equation $h_p(\bar{c}_1' \oplus \bar{T}) = \bar{c}_2$ holds or not. In fact, it holds since $\bar{c}_1' = p \oplus \bar{c}_1 = p \oplus (p \oplus h(r \oplus b) \oplus T_u \oplus \bar{T}) = h(r \oplus b) \oplus T_u \oplus \bar{T}$ and $h_p(\bar{c}_1' \oplus \bar{T}) = h_p(h(r \oplus b) \oplus T_u \oplus \bar{T} \oplus \bar{T}) = h_p(h(r \oplus b) \oplus T_u) = \bar{c}_2 = c_2$. Thus $\bar{M} = \{ID, \bar{c}_1, \bar{c}_2, \bar{T}\}$ satisfies the verification equation. Finally, E succeeds in impersonating U to S.

This result demonstrates that the scheme does not achieve the user authentication, i.e., mutual authentication. Therefore, the scheme is totally broken.

We make a suggestion for improvements without any proofs. The weakness of Wang *et al.*'s scheme is due to the fact that the exclusive-or of two same values vanishes completely. Thus, to prevent the attacks, it should be designed to destroy such a relationship. To overcome the weakness, we replace the transmitted message in the [**Login**] phase and [**Verification**] phase as:

[**Login.**] When U wants to login on the server, the smart card generates a random number r, and computes $c_1 = p \oplus h(r \oplus b)$, $c_2 = h_p(h(r \oplus b)||T_u)$, where T_u denotes U's current timestamp. Then U sends $M = \{ID, c_1, c_2, T_u\}$ to S.

[**Verification.**] Upon receiving the login request $M = \{ID, c_1, c_2, T_u\}$,

1. The remote system S checks the validity of ID and T_u. If they are correct then S computes $p = h(ID \oplus x)$ and $c'_1 = p \oplus c_1$, then checks whether $h_p(c'_1||T_u) = c_2$ holds or not. If holds, S computes $c_3 = h_p(c'_1||T_s)$ and then sends $\{c_3, T_s\}$ to U. Otherwise, S rejects the login request.
2. Upon receiving the message $\{c_3, T_s\}$, U verifies the validity of T_s. If it is correct then U computes $c'_3 = h_p(h(r \oplus b)||T_s)$ and compares $c'_3 = c_3$.

By replacing the exclusive-or operation with a simple concatenation, we can prevent the impersonation attacks.

3.2 Kim *et al.*'s Password Authentication Schemes

In 1999, Yang and Shieh [Yang and Shieh 99b] proposed two password authentication schemes with smart cards. One is the timestamp-based, and the other is the nonce-based. In 2002, Chan and Cheng [Chan and Cheng 02b] showed that Yang and Shieh's scheme was insecure against forgery attacks. In 2003, Sun and Yeh [Sun and Yeh 03b] pointed out that Chan and Cheng's attack on Yang and Shieh's scheme cannot work, because the attacker forged an invalid identity which does not exist in server's identity table. At the same time, Sun and Yeh [Sun and Yeh 03b] showed that Yang and Shieh's two schemes were vulnerable to forgery attacks, i.e., an adversary can easily find out login request messages to pass server's authentication verification. Later, Shen *et al.* [Shen et al. 03b] and Yang *et al.* [Yang et al. 04b], separately, proposed improved Yang and Shieh's password authentication schemes to withstand known forgery attacks. Recently, Kim *et al.* [Kim et al. 05b] showed that Yang *et al.*'s schemes cannot withstand forgery attacks and then proposed improved schemes to resist the attacks. In this section, we show that Kim *et al.*'s improved schemes are still insecure against forgery attacks. Also, we point out that Kim *et al.*'s forgery attack II on Yang *et al.*'s schemes cannot work. We first review Kim *et al.*'s password authentication schemes: the timestamp-based one and the nonce-based one [Kim et al. 05b]. In the schemes, a Key Information Center (KIC) is responsible for generating key information, issuing smart cards to users and serving password changing request for registered users.

• **Timestamp-based Password Authentication Scheme.**
[**Registration Phase.**] A user U_i sends its identifier ID_i and a password PW_i to the KIC via a secure channel. The KIC card will perform the following steps:

1. Generate two large prime numbers p and q, and compute a composite $n = p \cdot q$. Choose a prime number e and find a corresponding secret key d such that $e \cdot d = 1 \bmod \varphi(n) = (p-1) \cdot (q-1)$. Find a primitive element g in both $GF(p)$ and $GF(q)$, where g is server's public information.
2. Generate a smart card's identifier CID_i for U_i and compute $S_i = ID_i^{CID_i \cdot d} \bmod n$, $h_i = g^{PW_i \cdot d} \bmod n$.
3. Send the smart card, which includes $(n, e, g, ID_i, CID_i, S_i, h_i)$ to U_i.

[**Login Phase.**] If the user U_i wants to login, it inserts its smart card into a card reader and keys in its identity ID_i and password PW_i. The smart card generates a random number r_i and compute $X_i = g^{PW_i \cdot r_i \cdot e} \bmod n$, $Y_i = h_i^{r_i} \cdot S_i^T \bmod n$, where T is a current timestamp. Then it sends a login request message $M = (ID_i,\ CID_i, X_i,\ Y_i,\ n,\ e,\ g,\ T)$ to a remote server S.

[**Authentication Phase.**] Upon receipt of the login request message, S checks whether ID_i and CID_i are correct or not. If not, the login request is rejected. Check whether $(T' - T)$ is within the valid time interval ΔT, where T' is the time S received the message. If not, the login request is rejected. Then S checks whether $Y_i^e = X_i^d \cdot ID_i^{CID_i \cdot T} \bmod n$ holds or not. If it holds, S accepts the login request. Otherwise it rejects the request.

• **Nonce-based Password Authentication Scheme.**

[**Registration Phase.**] It is the same as that of the timestamp-based one.
[**Login Phase.**] If the user U_i wants to login, it inserts its smart card into a card reader and keys in its identity ID_i and password PW_i.

1. The smart card sends a login request message $M_1 = (ID_i,\ CID_i)$ to S.
2. Upon receipt of the message M_1, S checks whether ID_i and CID_i are correct or not. If any one of these two is not valid, the login request is rejected and the connection is closed. Otherwise, S computes a nonce $N = f(r_j)$ and sends it back to the smart card. Note that r_j is a random number and f is a one-way hash function.
3. Upon receipt of the nonce N, the smart card generates a random number r_i, computes $X_i = g^{PW_i \cdot r_i \cdot e} \bmod n$ and $Y_i = h_i^{r_i} \cdot S_i^N \bmod n$, and sends $M_2 = (X_i,\ Y_i,\ n,\ e,\ g)$ to S.

[**Authentication Phase.**] Upon receipt of the login request message M_2, S will check whether $Y_i^e = X_i^d \cdot ID_i^{CID_i \cdot N} \bmod n$ holds or not. If it holds, S accepts the login request. Otherwise, it rejects the login request.

• **Forgery Attacks on the Timestamp-based Authentication Scheme.** An adversary E wants to forge U_i's login request message on the scheme.

1. First, E eavesdrops U_i's login phase and stores its login request message

$$M = (ID_i,\ CID_i,\ X_i,\ Y_i,\ n,\ e,\ g,\ T).$$

2. Next, E chooses a current timestamp T'. Then $ID_i^{CID_i \cdot T'} \bmod n$ is relatively prime to n (we denote it $gcd(ID_i^{CID_i \cdot T'},\ n) = 1$, where *gcd* is the *greatest common divisor*). If not, $gcd(ID_i^{CID_i \cdot T'},\ n)$ is a nontrivial factor of $n = p \cdot q$. It contradicts to the infeasibility of the integer factorization problem. Then E can find its inverse $(ID_i^{CID_i \cdot T'})^{-1} \bmod n$. More precisely, $(ID_i^{CID_i \cdot T'})^{-1}$ can be computed as follows: first, E can find integers U and V such that

$$ID_i^{CID_i \cdot T'} \cdot U + n \cdot V = 1 \quad \cdots\cdots \quad (*)$$

by using Euclidean Algorithm [Menezes et al. (96)]. Taking modulo n, E can obtain $ID_i^{CID_i \cdot T'} \cdot U = 1 \bmod n$. Consequently, U is exactly equal to $(ID_i^{CID_i \cdot T'})^{-1}$.

3. The adversary E chooses a random r and computes X_i' and Y_i' as follows:

$$X_i' = [(ID_i^{CID_i \cdot T'})^{-1}]^e \cdot r^{e^2}\ mod\ n, \quad Y_i' = r\ \ mod\ n.$$

Then the above values satisfy the server's verification equation, because

$$(Y_i')^e = r^e\ mod\ n,$$

$$(X_i')^d \cdot ID_i^{CID_i \cdot T'} = [(ID_i^{CID_i \cdot T'})^{-1}]^e \cdot r^{e^2})^d \cdot ID_i^{CID_i \cdot T'}$$
$$= (ID_i^{CID_i \cdot T'})^{-1} \cdot r^e \cdot ID_i^{CID_i \cdot T'} = r^e \quad mod\ n,$$

the verification equation $(Y_i')^e = (X_i')^d \cdot ID_i^{CID_i \cdot T'} \bmod n$ holds.

4. Finally, E sends a login request message $M = (ID_i,\ CID_i,\ X_i',\ Y_i',\ n,\ e,\ g,\ T')$ impersonating U_i. Then, as mentioned above, the server's verification holds. Therefore, E succeeds in impersonating U_i to S without knowing U_i's secret information including the password PW_i.

The same forgery attack can be applied to the nonce-based scheme.

• **Forgery Attacks on the Nonce-based Authentication Scheme.**

1. When a user U_i sends $M_1 = (ID_i, CID_i)$ to a remote server S, an adversary E intercepts the message.

2. The adversary E sends M_1 to S to start the login phase impersonating U_i. Then S sends a nonce N to U_i. Next, E can obtain U such that

$$ID_i^{CID_i \cdot N} \cdot U = 1 \; mod \; n$$

as in (*) by using Euclidean Algorithm since $ID_i^{CID_i \cdot N}$ mod n is relatively prime to n. Then, E chooses a random r and computes

$$X_i' = U^e = [(ID_i^{CID_i \cdot N})^{-1}]^e \cdot r^{e^2} \; mod \; n, \quad Y_i' = r \quad mod \; n$$

and sends $M_2 = (X_i', \; Y_i', \; n, \; e, \; g)$ to the remote server impersonating U_i.

3. As the forgery attack on the timestamp-based scheme, the server's verification for the message M_2 is performed successfully. Consequently, E can impersonate U_i to S without the knowledge of U_i's secret information.

3.3 A Comment on Kim *et al.*'s Attack II on Yang *et al.*'s Schemes

Kim *et al.* [Kim et al. 05b] presented two forgery attacks on Yang *et al.*'s schemes. However, their forgery attack II cannot work. In the attack, an adversary finds a value a such that $a \cdot T' = T$, where T' is adversary's timestamp and T is the timestamp in U_i's past login request message. In fact, finding a in the equation is equivalent to find the solution of the following equation

$$X \cdot T' = T \; mod \; \varphi(n) = (p-1) \cdot (q-1)$$

with unknown X. However, it is infeasible to find the solution without knowing $\varphi(n)$, equivalently, p and q. In other words, its intractability is reduced to the intractability of the RSA problem. If the equation is computed in modulo n and T' is relatively prime to n then the solution X is equal to $(T')^{-1} \cdot T$. But, the equation should be computed in modulo $\varphi(n)$ because the value is used in exponent of the verification equation. More precisely, if $a \cdot T' = T$ mod n is used, the second equality in $(**)$ does not hold:

$$Y_i' = ID_i^{CID_i} \cdot g^{PW_i \cdot r_i \cdot T} = ID_i^{CID_i} \cdot g^{PW_i \cdot r_i \cdot a \cdot T'} \; mod \; n. \; \cdots\cdots \; (**)$$

Thus, their forgery attack II is incorrect.

4 Conclusion

We showed that three password authentication schemes [Kwon 03b],[Kim et al. 05b],[Wang et al. 07b] are insecure against several active attacks. Until now, a variety of password-based authentication schemes have been proposed, However, some of these schemes were subsequently found to be flawed, and then were modified to resist the attacks or were totally abandoned. Also, others only provide informal security analysis, i.e., attack-response heuristic security. However, we cannot guarantee the security of those surviving protocols from this 'attack-response' examination against potential attacks that are not yet reported. So a more formal approach appeared necessary borrowing methods from the theory of complexity. This approach allows a correct specification of the security requirements which in turn can be established by means of a security proof. Since the appearance of such a formal security proof, the methodology of provable security has become unavoidable in designing, analyzing and evaluating new cryptographic protocols. Password authentication schemes are no exceptions. Our results demonstrate that no more password authentication schemes should be constructed with such ad-hoc methods and the formal design methodology using provable security as in [Abdalla and Pointcheval 05a],[Bellare et al. 00a],[Boyko et al. 00a],[Bresson et al. 03a],[Kobara and Imai 02b],[Zhang 04a] should be employed in future design.

Acknowledgement

This work was supported by the National Institute for Mathematical Sciences grant funded by the Korean Government (No. A21103).

References

[Abdalla and Pointcheval 05a] M. Abdalla, D. Pointcheval: "Interactive Diffie-Hellman assumptions with applications to password-based authentication"; Proc. FC'05, LNCS 3579 (2005), Springer-Verlag, 341-356.

[Bellare et al. 00a] M. Bellare, D. Pointcheval, P. Rogaway: "Authenticated key exchange secure against dictionary attacks"; Proc. Eurocrypt'00, LNCS 1807 (2000), Springer-Verlag, 139-155.

[Bellovin and Merritt 92a] S. M. Bellovin and M. Merritt: "Encrypted key exchange: Password-based protocols secure against dictionary attacks"; Proc. IEEE Computer Society Conference on Research in security and Privacy, pp. 72-84, 1992.

[Bellovin and Merritt 94c] S. M. Bellovin and M. Merritt: "Augmented encrypted key exchange: Password-based protocols secure against dictionary attacks and password file compromise"; Technical report, AT&T Bell Lab., 1994.

[Boyko et al. 00a] V. Boyko, P. MacKenzie, S. Patel: "Provably secure password-authenticated key exchange using Diffie-Hellman"; Proc. Eurocrypt'00, LNCS 1807 (2000), Springer-Verlag, 156-171.

[Bresson et al. 03a] E. Bresson, O. Chevassut, D. Pointcheval: "Security proofs for an efficient password-based key exchange"; Proc. The 10th ACM Conference On Computer And Communication Security, ACM Press (2003), 241-250.

[Chan and Cheng 02b] C. K. Chan, L. M. Cheng: "Cryptanalysis of a timestamp-based password authentication scheme"; Computers & Security, 21, 1 (2002), 74-76.

[Chien et al. 02b] H. Y. Chien, J. K. Jan, Y. M. Tseng: "An efficient and practical solution to remote authentication smart card"; Computer and Security 21, 4 (2002), pp. 372-375.

[Fan et al. 02b] L. Fan, J. H. Li, H. W. Zhu: "An enhancement of timestamp-based password authentication scheme"; Computers & Security, 21, 7 (2002), 665-667.

[Hwang and Li 00b] M. S. Hwang, L. H. Li: "A new remote user authentication scheme using smart cards"; IEEE Transactions on Consumer Electronics 46, 1 (2000), 28-30.

[IEEE P1363.2] IEEE P1363.2: "P1363.2: Standard Specifications for Password-Based Public-Key Cryptographic Techniques"; availabl at http://grouper.ieee.org/groups/1363.

[Jablon 97b] D. Jablon: "Extended password methods immune to dictionary attack"; Proc. The WETICE'97, Enterprise Security Workshop (1997).

[Jablon 96b] D. Jablon: "Strong password-only authenticated key exchange"; ACM Computer Communication Review, 26, 5 (1996), 5-26.

[Kim et al. 05b] K. Kim: J. Jeon, K. Yoo, "An improvement on Yang *et al.*'s password authentication schemes"; Applied Mathematics and Computation, 170, 1 (2005), 207-215.

[Kobara and Imai 02b] K. Kobara, H. Imai: "Petty-simple password-aAuthenticated key-exchange under standard assumptions"; IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E85-A, 10 (2002), 2229-2237.

[Kwon 03] T. Kwon: "Summary of AMP (Authentication and key agreement via Memorable Passwords)", submitted to IEEE P1363.2, 2003, available at http://grouper.ieee.org/groups/1363/passwdPK/contribut- ions/ampsummary.pdf

[Ku and Chen 04b] W. C. Ku, S. M. Chen: "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards"; IEEE Transactions on Consumer Electronics 50, 1 (2004), 204-207.

[Lamport 81b] L. Lamport: "Password authentication with insecure communication"; Communications of the ACM, 24 (1981), 770-772.

[MacKenzie and R. Swaminathan 99] P. MacKenzie, R. Swaminathan: "Secure Network Authentication with Password Identification"; Submission to IEEE P1363.2, 1999.

[Menezes et al. (96)] A. J. Menezes, P. C. van Oorschot, S. A. Vanstone: "Applied Cryptogarphy"; CRC Press, (1996).

[Shen et al. 03b] J. J. Shen, C. W. Lin , M.S. Hwang: "Security enhancement for the timestamp-based password authentication scheme using smart cards"; Computers & Security, 22, 7 (2003), 591-595.

[Steiner et al. 95b] M. Steiner, G. Tsudik, M. Waidner: "Refinement and extension of encrypted key exchange"; ACM Operating Systems Review, 29, 3 (1995), 22-30.

[Sun 00b] H. M. Sun: "An efficient remote user authentication scheme using smart cards"; IEEE Transactions on Consumer Electronics 46, 4 (2000), 958-961.

[Sun and Yeh 03b] H. M. Sun, H. T. Yeh: "Further cryptanalysis of a password authentication scheme with smart cards"; IEICE Transactions on Communications, E86-B, 4 (2003), 1412-1415.

[Wang et al. 07b] X. M. Wang, W. F. Zhang, J. S. Zhang, M. K. Khan: "Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards"; Computer Standards & Interfaces, 29, 5 (2007), 507-512.

[Wu 98a] T. Wu: "The secure remote password protocol"; Proc. Internet Society Symposium on Network and Distribute System Security, NDSS'99 (1998), 97-111.

[Yang and Shieh 99b] W. H. Yang, S. P. Shieh: "Password authentication schemes with smart cards"; Computers & Security, 18, 8 (1999), 727-733.

[Yang et al. 05b] C. C. Yang, R. C. Wang, T. Y. Chang: "An improvement of the Yang-Shieh password authentication schemes"; Applied Mathematics and Computation, 162 (2005), 1391-1396.

[Yang et al. 04b] C. C. Yang, H. W. Yang, R. C. Wang,: "Cryptanalysis of security enhancement for the timestamp-based password authentication scheme using smart cards"; IEEE Transactions on Consumer Electronics, 50, 2 (2004), 578-579.

[Yoon and Ryu 04b] J. Yoon and K. Y. Ryu,: "Further improvement of an efficient password based remote user authentication scheme using smart cards"; IEEE Transactions on Consumer Electronics 50, 2, (2004), 612-614.

[Zhang 04a] M. Zhang: "Password authenticated key exchange using quadratic residues"; ACNS'04, LNCS 3089, Springer-Verlag (2004), 248-262.