A Secure SCAM (Smart Card based Authentication Mechanism)

Ravi Singh Pippal
Radharaman Institute of Research and Technology, Bhopal, M.P.

Rajesh Ahirwar
Radharaman Institute of Research and Technology, Bhopal, M.P.

Shivpratap Singh Kushwah
Institute of Technology and Management, Gwalior, M.P.

PradeepYadav
Institute of Information Technology and Management, Gwalior, M.P.

ABSTRACT
Recently, Tsai et al. proposed dynamic ID based smart card authentication scheme. This paper demonstrates that Tsai et al.'s scheme fails to provide early wrong password detection, secure password change and protection against insider attack. To overcome, we propose a secure SCAM (Smart Card based Authentication Mechanism) which keeps all previous merits and achieves security and functionality requirements. The performance of both the schemes has been analyzed in terms of various metrics. Comparing with Tsai et al.'s scheme, our scheme provides higher security with nearly same cost. For network where clock synchronization is tough, nonce based scheme is additionally offered.

Keywords
Authentication, Nonce, Password, Security, Smart card.

1. INTRODUCTION
Due to the rapid development of Internet technology, several typical activities are conducted over it. In order to transfer secret information over a public network like Internet, several security issues are there that must be taken into account. Among these, the primary requirement is to confirm the identity of the user who desires to realize access to vital data. Authentication ensures the origin of a message correctly identified and provides an assurance that the identity is not a fake. To avoid issues associated with traditional password based authentication methods, smart card authentication schemes are widely used because of their low computational cost. Smart card is a tamper resistant integrated circuit card with memory to store personal data and a processor capable of performing computations [1]. In smart card based password authentication scheme, server does not maintain database/verification table to verify a user's identity.

Authentication scheme based on smart card is usually consists of three phases namely; registration phase, login phase and verification phase. The registration phase is invoked when a new user desires to register within the server. The user submits his or her credentials to the server. Upon receiving the registration request, server computes necessary parameters using the submitted credentials along with the secret key (maintained by the server instead of verification table) and issues a smart card to user by storing the computed parameters into smart card memory. The login phase and verification phase are invoked when a user needs to access resources from the server. In the login phase, user creates a login request and sends it to server to pass the verification phase. Once the login request is received, server checks the validity of login request and the legitimacy of user.

1.1 Contribution of this Paper
Recently, Tsai et al. [20] proposed a dynamic ID authentication scheme using smart cards. They claimed that their scheme provides security against several potential attacks. This paper first demonstrates that Tsai et al.'s scheme has security vulnerabilities under the assumption that no one can extract data from tamper resistant smart card. These security pitfalls are (i) it fails to provide early wrong password detection and secure password change phase; (ii) it is insecure against insider attack. To beat these weaknesses, this paper proposes a secure SCAM (Smart Card based Authentication Mechanism) which inherits all the previous merits and accomplishes the security and functionality requirements. The security of this scheme relies on the difficulty of breaking one way hash function and solving discrete logarithm problem. The performance of both the schemes has been analyzed in terms of various metrics. Comparing with Tsai et al.'s scheme, our scheme is more robust and gives higher security. A nonce based scheme is also proposed for such networks where clock synchronization is hard to achieve.

The remainder of the paper is structured as follows. Section 2 explores the existing literature related to smart card authentication scheme. Section 3 discusses Tsai et al.'s dynamic ID authentication scheme and its related susceptibilities. The proposed SCAM is described in section 4. Section 5 demonstrates an in-depth security analysis of SCAM. Performance comparison of SCAM with Tsai et al.'s scheme is given in section 6 and a nonce based scheme is also suggested for large networks. Finally, section 7 concludes the paper.

2. LITERATURE REVIEW
Throughout the last two decades, numerous smart card authentication schemes have been proposed [2, 4, 6, 8-13, 15-18, 20, 21]. An ID based smart card authentication scheme using RSA cryptosystem has been given [2] and claimed that the scheme avoids need for verification table and resists replay attack. However, it is proved that the scheme is exposed to impersonation attack [3]. A remote user authentication scheme based on ElGamal's cryptosystem has been proposed [4] and claimed that the scheme is able to resist replay attack and exempt necessity of maintaining verification table to authenticate the legitimate user. Though, it is found that the scheme is at the risk of impersonation attack [5]. To boost efficiency, remote user authentication scheme using one-way hash function has been suggested [6]. However, the scheme has security drawbacks which are (i) user is not allowed to choose and change the password freely. (ii)

absence of mutual authentication. Moreover, the scheme is exposed to offline and online password guessing attacks [7]. To handle these flaws, a remote user authentication scheme using one-way hash function has been proposed [8]. It is claimed that the scheme permits users to choose the password freely and provides mutual authentication between remote user and the server. Nevertheless, it exhibits parallel session attack [7].

Another economical remote user authentication scheme has been given [9] and claimed that the scheme permits users to choose and change the password freely, resists replay attack and avoids the necessity of verification table. However, it is found that this scheme fails to resist Denial-of-Service attack and does not offer mutual authentication [10]. An improved scheme has additionally been proposed to overcome these security weaknesses. To defend against insider and reflection attacks, an improved scheme over [8] has been urged [11]. It provides the facility to change the password freely. But, it is weak against parallel session attack and has insecure password change phase. Further improvement has also been suggested [12]. However, the improved scheme remains vulnerable to guessing attack, Denial-of-Service attack and impersonation attack [13]. To remedy these drawbacks, an enhanced scheme has also been presented. Though, the scheme is weak against guessing attack, denning sacco attack and does not offer perfect forward secrecy [14].

A dynamic ID based remote user authentication scheme using one way hash function has been proposed [15]. The authors claimed that their scheme is secure against replay attack, impersonation attack, guessing attack, insider attack and stolen verifier attack. In addition to that, users can choose and change their passwords freely. However, the scheme is weak against guessing attack [16] and insider attack [16, 17]. Additionally, the scheme is password independent [17] and does not provide mutual authentication [16, 17]. An improved scheme has been suggested to beat these flaws [17]. But, the scheme does not provide security against password guessing attack and server masquerade attack [18]. An enhanced scheme has also been given to resist password guessing attack, user masquerade attack and server masquerade attack. Nevertheless, the scheme is exposed to password guessing attack, server masquerade attack and lack of password backward security [19]. Recently, a dynamic ID authentication scheme has been proposed [20] and claimed that this scheme provides security against several potential attacks and satisfies the essential needs of end users. However, it is shown that this scheme is vulnerable to impersonation attack, offline password guessing attack, fails to provide perfect forward secrecy and does not solve time synchronization problem [21].

3. REVIEW OF TSAI ET AL.'S SCHEME

This section briefly reviews Tsai et al.'s [20] dynamic ID authentication scheme and exposes the vulnerabilities present in this scheme. The notations used throughout this paper are summarized as follows.

U_i	:	Remote user
ID_i	:	Identity of U_i
PW_i	:	Password chosen by U_i
S	:	Authentication server
PW_i^*	:	Password guessed by the adversary
x	:	Secret key maintained by S
d	:	Secret number maintained by S
p	:	Large and safe prime number
g	:	Primitive root in Z_p^*
$h(\bullet)$	:	Cryptographic one way hash function
$\|$	:	Message concatenation
$\oplus$	:	Bitwise XOR operation
T_1	:	Current system timestamp generated by U_i
T_2	:	Current system timestamp generated by S
N_1	:	Random nonce generated by U_i
N_2	:	Random nonce generated by S
SK	:	Shared session key between U_i and S

3.1 Tsai et al.'s Dynamic ID Authentication Scheme

This scheme consists of four phases: registration phase, login phase, verification phase and password change phase. In this scheme, (X, Y) means S's secret key and its corresponding public key, where X is stored in S's protected memory and $Y = g^X mod\ p$ is stored in each users smart card. The details of these phases are stated as follows.

3.1.1. Registration phase

In this phase, U_i chooses ID_i and PW_i and then submits $\{ID_i, PW_i\}$ to S over a secure channel. Upon receiving the registration request from U_i, S computes $N_i = h(PW_i \| ID_i) \oplus h(X \| ID_i)$ and issues a smart card over secure channel to U_i by storing $\{N_i, Y, h(\bullet)\}$ into smart card memory.

3.1.2. Login phase

Whenever U_i wants to access S, U_i inserts the smart card to the card reader and keys in ID_i and PW_i. The smart card extracts $h(X \| ID_i)$ by computing $N_i \oplus h(PW_i \| ID_i)$ and computes dynamic ID $CID_i = ID_i \oplus h\left((Y^k mod\ p) \| T_1\right)$, $C = g^k\ mod\ p$ and $B = h(CID_i \| C \| h(X \| ID_i) \| Y \| T_1)$, where '$k$' is a random integer. Then, sends the login request $\{CID_i, B, C, T_1\}$ to S.

3.1.3. Verification phase

Upon receiving the login request $\{CID_i, B, C, T_1\}$; S first checks the validity of T_1 to accept/reject the login request. If not, S rejects the login request otherwise extracts ID_i by computing $ID_i = CID_i \oplus h\left((C^X mod\ p) \| T_1\right)$, $B' = h(CID_i \| C \| h(X \| ID_i) \| Y \| T_1)$ and compares the computed B' with received B. If they are equal, S accepts the login request otherwise rejects it. Then S computes the session key $SK = h(h(X \| ID_i) \| T_1 \| B \| CID_i \| T_2)$, $D = h(SK \| h(X \| ID_i) \| T_1 \| T_2)$ and sends $\{D, T_2\}$ to U_i. After receiving, U_i checks the validity of T_2. It holds, computes the session key $SK = h(h(X \| ID_i) \| T_1 \| B \| CID_i \| T_2)$, $D' = h(SK \| h(X \| ID_i) \| T_1 \| T_2)$ and compares the computed D' with the received D. If it holds, mutual authentication is achieved. After authenticating each other, U_i and S use the same session key $SK = h(h(X \| ID_i) \| T_1 \| B \| CID_i \| T_2)$ to encrypt/decrypt all communication messages between them.

3.1.4. Password change phase

When U_i wants to change the old password PW_i to the new password PW_{inew}, U_i inserts the smart card to the card reader. The smart card computes $h(X \| ID_i) = N_i \oplus h(PW_i \| ID_i)$, $N_i^{'} = h(PW_{inew} \| ID_i) \oplus h(X \| ID_i)$ and stores $N_i^{'}$ instead of N_i in the smart card memory.

3.2 Security Pitfalls in Tsai et al.'s Scheme

This section provides security flaws in Tsai et al.'s scheme. They are (i) exposed to Denial-of-Service attack due to lack of early wrong password detection prior to login request creation (ii) vulnerable to insider attack (iii) insecure password change phase. It is assumed that the attacker is able to intercept all the messages exchanged between U_i and S.

3.2.1 Slow wrong password detection

To check whether or not the requested user is a legitimate bearer of smart card, entered password must be verified at the smart card level before login request creation [10]. In Tsai et al.'s scheme, if user enters a wrong password by mistake, this wrong password is going to be detected by remote server in verification phase. Therefore, Tsai et al.'s scheme is slow to detect the user's wrong password.

Further, attacker is in a position to create invalid login request by entering wrong password which will be detected solely at the server side not at the user side. The similar process can be replicated endlessly to overload the server which limits the server accessibility for the other valid users and leads to Denial-of-Service attack. Thus, Tsai et al.'s scheme shows inadequacy to resist Denial-of-Service attack. This attack can be avoided by verifying the entered password at the user side prior to compute the login request.

3.2.2 Insider attack

Any insider of server system can acquire user's password during the registration phase and then purposely leaks the secret information or impersonate the legitimate user to access different servers [11]. In this scheme, PW_i is sent to S during the registration phase. So, any insider of S can easily get U_i's PW_i and can use it for some personal benefit.

3.2.3 Insecure password change phase

In this scheme, the correctness of old password is not verified before the update of new password either at the server or at the smart card side. Nonexistence of wrong password detection leads to Denial-of-Service attack during password change phase [10]. Old password check at the user side strengthens the security.

4. PROPOSED SCAM

This section describes the proposed smart card authentication scheme. The scheme consists of four phases: Registration phase, Login phase, Verification phase and Password change phase. Registration phase is invoked whenever new user registers in the server. Upon receiving the registration request, server issues a smart card to user by storing essential parameters into smart card memory. The login phase and verification phase are invoked at any time user login into the server. After receiving the login request, server checks the validity of the login request to authenticate the user.

4.1 Registration Phase

In this phase, U_i selects ID_i and PW_i, computes $h(PW_i)$ and submits $\{ID_i, h(PW_i)\}$ to S over a secure channel. Upon receiving the registration request from U_i, S computes $a_i = g^{h(ID_i \| h(PW_i)) \times d} \bmod p$, $b_i = h(ID_i \| x)$ and issues a smart card over secure channel to U_i by storing $\{a_i, b_i, d, p, g, h(\bullet)\}$ into smart card memory.

4.2 Login Phase

Whenever U_i wants to access S, U_i inserts the smart card to the card reader and keys in $ID_i{'}$ and $PW_i^{'}$. The card reader computes $a_i{'} = g^{h(ID_i{'} \| h(PW_i{'})) \times d} \bmod p$ and checks whether computed $a_i^{'}$ equals stored a_i or not. If true, U_i is a legitimate owner of smart card otherwise rejects the login request. The card reader generates current system timestamp T_1, computes anonymous identity $AID_i = ID_i \oplus h(a_i \| T_1)$, $c_i = \left(h\left(ID_i \| h(PW_i)\right) + h(ID_i \| a_i \| b_i \| T_1)\right) \bmod (p-1)$, $d_i = g^{h(ID_i \| h(PW_i))} \bmod p$ and sends the login request $\{AID_i, c_i, d_i, T_1\}$ to S.

4.3 Verification Phase

Upon receiving the login request $\{AID_i, c_i, d_i, T_1\}$; S first checks the validity of T_1 to accept/reject the login request. If not, Srejects the login request otherwise computes $a_i = d_i^d \bmod p$,$ID_i = AID_i \oplus h(a_i \| T_1)$ and checks the validity of ID_i. If holds, S computes $b_i = h(ID_i \| x)$ and checks whether

$$g^{c_i} = d_i \times g^{h(ID_i \| a_i \| b_i \| T_1)} \bmod p \quad (1)$$

holds or not. If eq. (1) holds, requested user is a legitimate user. Subsequently, S generates current system timestamp T_2, computes $H = h(h(ID_i \| a_i \| b_i \| T_1) \| T_1 \| T_2)$and sends the message $\{AID_i, H, T_2\}$ to U_i. After getting the message $\{AID_i, H, T_2\}$ from S, U_i first checks the validity of T_2. If true, computes $H^{'} = h(h(ID_i \| a_i \| b_i \| T_1) \| T_1 \| T_2)$ and checks whether H and $H^{'}$ are equal or not. If holds, S is authentic and mutual authentication is achieved. If not, terminates the session. Both the parties agree upon the common session key $SK = h(ID_i \| a_i \| b_i \| T_1 \| T_2)$.

4.4 Password Change Phase

This phase is invoked when U_i wants to change the password. U_i inserts the smart card to the card reader and keys the credentials, $ID_i{'}$and $PW_i^{'}$. The card reader computes $a_i{'} = g^{h(ID_i{'} \| h(PW_i{'})) \times d} \bmod p$ and checks whether computed $a_i^{'}$ equals stored a_i or not. If true, U_i is prompted to enter a new password. U_i enters a new password PW_{inew}. The card reader computes $a_{inew} = g^{h(ID_i{'} \| h(PW_{inew})) \times d} \bmod p$ and stores a_{inew} instead of a_i in the smart card memory. Thus, U_i can change password without any assistance from S. To resist online password guessing attack, the reader locks the card if U_i enters wrong PW_i more than a limited number of times.

5. SECURITY ANALYSIS

This section provides an in-depth analysis of the proposed scheme in terms of security and functionality properties.

5.1 Impersonation Attack

The login request contains $\{AID_i, c_i, d_i, T_1\}$, where $AID_i = ID_i \oplus h(a_i \| T_1)$, $c_i = \left(h\left(ID_i \| h(PW_i)\right) + h(ID_i \| a_i \| b_i \| T_1)\right) \bmod (p-1)$ and $d_i = g^{h(ID_i \| h(PW_i))} \bmod p$. Therefore, the attacker has

to guess the correct values of ID_i, PW_i, a_i and b_i to masquerade as U_i. Let's assume attacker guesses the password PW_i^*, the correct values of ID_i, b_i and d are still needed to forge the login request. Hence, attacker is unable to forge the login request to impersonate a valid U_i.

5.2 Replay Attack

An adversary may attempt to act as an authentic user by resending previously intercepted messages. This scheme uses timestamps T_1 and T_2 which are verified at both the ends. As a result, attackers cannot enter the system by resending the previously transmitted messages to impersonate legal users. If adversary desires to alter T_1, he or she needs to recalculate AID_i and c_i which is not possible without knowing ID_i, PW_i, a_i and b_i. Thus, this scheme is able to resist replay attack.

5.3 Password Guessing Attack

In the proposed scheme, $h(PW_i)$ is employed in the calculation of c_i and d_i. Let us suppose that the adversary intercepts login request $\{AID_i, c_i, d_i, T_1\}$ during its transmission from U_i to S. It is hard to guess the all three parameters ID_i, a_i and b_i correctly at the same time to ascertain whether or not each of the guessed passwords is correct. Moreover, to derive PW_i from d_i, adversary has to solve the discrete logarithm problem and break the security of one way hash function. Therefore, the scheme is secure against offline password guessing attack. To resist online password guessing attack, we can limit the number of attempts made by user to some fixed value.

5.4 Stolen Verifier Attack

U_i*'s* secret information stored at S is beneath intensive threat from the attackers. In the proposed scheme, rather than storing passwords of all the registered users in the verification table, S keeps secret key 'x' and secret number 'd' to avoid maintaining verification table used to verify U_i*'s* login request. Hence, the scheme is secure against stolen verifier attack.

5.5 Insider Attack

Many users employ identical password to access different servers for their ease of remembering long passwords. However, a privileged insider of server can get this password and then attempt to utilize it to impersonate a legal user. In our scheme, $h(PW_i)$ is sent to S rather than PW_i to resist insider attack. So, any insider of S cannot get U_i*'s* password PW_i and thus, this scheme is free from insider attack.

5.6 Reflection and Parallel Session Attack

To resist reflection and parallel session attacks, the given scheme employs uneven structure of communicating messages, i.e., $\{AID_i, c_i, d_i, T_1\}$ and $\{AID_i, H, T_2\}$. There is no symmetry in the values of $AID_i = ID_i \oplus h(a_i \| T_1)$, $c_i = \left(h\left(ID_i \| h(PW_i)\right) + h(ID_i \| a_i \| b_i \| T_1)\right) \ mod\ (p-1)$, $d_i = g^{h(ID_i \| h(PW_i))} \ mod\ p$ and $H = h\left(h(ID_i \| a_i \| b_i \| T_1) \| T_1 \| T_2\right)$. Hence, the attacker is unable to launch parallel session attack by replaying server response message as the user login request or reflection attack by resending user login request as the server response message.

5.7 Secure Session Key Establishment

In the proposed scheme, common shared session key $SK = h(ID_i \| a_i \| b_i \| T_1 \| T_2)$ differs among sessions due to the value of timestamps T_1 and T_2. Attacker is unable to seek out the present session key or any of the previously used session keys from the eavesdropped messages because the values of ID_i, a_i and b_i are unknown and it is infeasible to guess these values simultaneously.

5.8 Our scheme provides early wrong password detection

Card holder verification at the user side is very essential to avoid unnecessary burden on the server which leads to Denial-of-Service attack. This scheme quickly verifies the entered password at the user side prior to login request creation by comparing a_i' with the stored a_i. If U_i enters wrong password, the smart card prompt U_i to re-enter correct password. It creates a login request only when smart card finds entered password correct. As a result, Denial-of-Service attack is completely eliminated.

5.9 Our scheme provides anonymity for user's identity

It is better that the user's identity is anonymous from outside the world. It is necessary that an efficient and secure remote user authentication scheme preserves strong anonymity from the eavesdropper. This scheme provides anonymity for the user's identity by sending anonymous identity $AID_i = ID_i \oplus h(a_i \| T_1)$ rather than ID_i, which securely conceals the real identity of the user and the server still recognizes every and every user with its real identity by computing $a_i = d_i^d \ mod\ p$.

6. PERFORMANCE COMPARISON OF SCAM WITH TSAI ET AL.'S SCHEME

In order to measure the security in terms of potential attacks, proposed SCAM is compared with Tsai et al.'s scheme. From Table 1, we can see that SCAM is safer in comparison with Tsai et al.'s dynamic ID authentication scheme. It includes early wrong password detection which resists Denial-of-Service attack either during verification phase or password change phase. Further, it resists insider attack.

Table 2 shows comparative results for Tsai et al.'s scheme and proposed SCAM in terms of computational complexity. From both of these tables, it can be clearly seen that SCAM keeps all the previous benefits, is more secure with nearly same cost in comparison with Tsai et al.'s dynamic ID authentication scheme.

For a large network where clock synchronization is difficult, a nonce based scheme is also proposed which works as follows. The registration and password change phases are same as mentioned above in timestamp based SCAM. The difference is only in login and verification phases. At the time of login, U_i inserts the smart card to the card reader and keys in ID_i' and PW_i'. The card reader computes $a_i' = g^{h(ID_i' \| h(PW_i'))\times d} \ mod\ p$ and checks whether computed a_i' equals stored a_i or not. If true, U_i is a genuine bearer of smart card otherwise rejects the login request. The card reader generates random nonce N_1, computes anonymous identity

Table 1. Comparison between SCAM and Tsai et al.'s scheme in terms of security properties

Security Properties	**Tsai et al.'s Scheme**	**Proposed SCAM**
User is allowed to choose and change the password	Yes	Yes
Provides mutual authentication	Yes	Yes
Provides secure session key generation	Yes	Yes
Resists impersonation attack	Yes	Yes
Resists replay attack	Yes	Yes
Resists guessing attack	Yes	Yes
Resists parallel session attack	Yes	Yes
Resists reflection attack	Yes	Yes
Resists stolen verifier attack	Yes	Yes
Resists insider attack	No	Yes
Provides early wrong password detection	No	Yes
Provides secure change of password	No	Yes

Table 2. Comparison between SCAM and Tsai et al.'s scheme in terms of computational complexity

Authentication Scheme	Phases	One Way Hash Function (H)	Exclusive-or Operation (XOR)	Modular Exponentiation (ME)	Total Number of Operations
Tsai et al.'s Scheme	Registration Phase	**2**	**1**	**-**	**12 H + 4 XOR + 4 ME**
	Login Phase	**3**	**2**	**2**	
	Verification Phase	**7**	**1**	**2**	
Proposed SCAM	Registration Phase	**3**	**-**	**1**	**14 H + 2 XOR + 6 ME**
	Login Phase	**4**	**1**	**2**	
	Verification Phase	**7**	**1**	**3**	

$AID_i = ID_i \oplus h(a_i \| N_1)$, $c_i = \left(h\left(ID_i \| h(PW_i)\right) + h(ID_i \| a_i \| b_i \| N_1)\right) mod\ (p-1)$,

$d_i = g^{h\left(ID_i \| h(PW_i)\right)} mod\ p$ and sends the login request $\{AID_i, c_i, d_i, N_1\}$ to S. Upon receiving the login request $\{AID_i, c_i, d_i, N_1\}$; S computes $a_i = d_i^d\ mod\ p, ID_i = AID_i \oplus h(a_i \| N_1)$ and checks the validity of ID_i. If holds, S computes $b_i = h(ID_i \| x)$ and checks whether

$$g^{c_i} = d_i \times g^{h(ID_i \| a_i \| b_i \| N_1)}\ mod\ p \quad (2)$$

holds or not. If eq. (2) holds, S generates random nonce N_2, computes $H_1 = h(h(ID_i \| a_i \| b_i \| N_1) \| N_1 \| N_2)$ and sends the message $\{AID_i, H_1, N_2\}$ to U_i. After getting the message $\{AID_i, H_1, N_2\}$ from S, U_i computes $H_1' = h(h(ID_i \| a_i \| b_i \| N_1) \| N_1 \| N_2)$ and checks whether H_1 and H_1' are equal or not. If true, S is authentic otherwise terminates the session. Subsequently, U_i computes $H_2 = h(h(ID_i \| a_i \| b_i \| N_1) \| N_2 \| N_1)$ and sends $\{AID_i, H_2\}$ to S. Once the message $\{AID_i, H_2\}$ is received, S computes $H_2' = h(h(ID_i \| a_i \| b_i \| N_1) \| N_2 \| N_1)$ and checks whether H_2 and H_2' are equal or not. If it holds, mutual authentication is achieved. Both the parties agree upon the common session key $SK = h(ID_i \| a_i \| b_i \| N_1 \| N_2)$.

7. CONCLUSION

In today's era, password based smart card authentication scheme is one amongst the foremost prominent authentication schemes used to verify the legitimacy of remote users. However, most of these schemes fail to provide security against the identified attacks. With the rapid growth of Internet, it is better to design an authentication mechanism by taking smart card as a base. Recently, Tsai et al. proposed a

dynamic ID authentication scheme using smart cards. However, it fails to provide early wrong password detection, secure password change phase and is at risk of insider attack. This paper proposes an extremely secure SCAM (Smart Card based Authentication Mechanism) which has all the previous merits and realizes the necessary functional and security requirements. Its security stands on cracking one way hash function and solving the discrete logarithm problem.

It is proved that the scheme withstands impersonation attack, password guessing attack, replay attack, reflection and parallel session attacks, insider attack and stolen verifier attack. Further, it permits users to choose and alter their passwords freely, provides mutual authentication, early wrong password detection and secure session key establishment. The performance of both Tsai et al.'s scheme and our proposed SCAM has been analyzed in terms of numerous metrics. It is clear that the proposed SCAM is more robust and secure as compare to Tsai et al.'s scheme. For a large network where clock synchronization is hard to achieve, a nonce based scheme is additionally offered. The proposed schemes are better fitted to resource constrained devices and might be simply extended to numerous applications like multi-server authentication, Internet protocol television broadcasting, wireless communication and healthcare applications.

8. REFERENCES

[1] http://en.wikipedia.org/wiki/Smart_card.

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

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

[4] 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.

[5] C. K. Chan, L. M. Cheng, Cryptanalysis of a remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (4) (2000) 992-993.

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

[7] C. L. Hsu, Security of two remote user authentication schemes using smart cards, IEEE Transactions on Consumer Electronics 49 (4) (2003) 1196-1198.

[8] H. Y. Chien, J. K. Jan, Y. M. Tseng, An efficient and practical solution to remote authentication: smart card, Computers & Security 21 (4) (2002) 372-375.

[9] M. S. Hwang, C. C. Lee, Y. L. Tang, A simple remote user authentication scheme, Mathematical and Computer Modelling 36 (1-2) (2002) 103-107.

[10] E. J. Yoon, E. K. Ryu, K. Y. Yoo, An improvement of Hwang-Lee-Tang's simple remote user authentication scheme, Computers & Security 24 (1) (2005) 50-56.

[11] 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.

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

[13] 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 and Interfaces 29 (5) (2007) 507-512.

[14] E. J. Yoon, E. J. Lee, K. Y. Yoo, Cryptanalysis of Wang et al.'s remote user authentication scheme using smart cards, 5th International Conference on Information Technology: New Generations (ITNG-2008) (2008) 575 - 580.

[15] M. L. Das, A. Saxena, V. P. Gulati, A Dynamic ID-based remote user authentication scheme, IEEE Transactions on Consumer Electronics 50 (2) (2004) 629-631.

[16] I. E. Liao, C. C. Lee, M. S. Hwang, Security enhancement for a dynamic ID-based remote user authentication scheme, International Conference on Next Generation Web Services Practices (2005).

[17] Y. Y. Wang, J. Y. Liu, F. X. Xiao, J. Dan, A more efficient and secure dynamic ID-based remote user authentication scheme, Computer Communications 32 (4) (2009) 583-585.

[18] Z. Hao, N. Yu, A security enhanced remote password authentication scheme using smart card, 2nd International Symposium on Data, Privacy, and E-Commerce (ISDPE-2010) (2010) 56-60.

[19] H. Zhang, M. Li, Security vulnerabilities of an remote password authentication scheme with smart card, 2011 International Conference on Consumer Electronics, Communications and Networks (CECNet-2011) (2011) 698-701.

[20] J. L. Tsai, T. C. Wu, K. Y. Tsai, New dynamic ID authentication scheme using smart cards, International Journal of Communication Systems 23 (12) (2010) 1449--1462.

[21] S. Wu, Y. Zhu, Q. Pu, Robust smart-cards-based user authentication scheme with user anonymity, Security and Communication Networks (2011). doi: 10.1002/sec.315