An Efficient Password Authentication Scheme for Smart Card

Rajaram Ramasamy and Amutha Prabakar Muniyandi

(Corresponding author: Rajaram Ramasmay)

Department of Computer Science and Engineering, Thiagarajar College of Engineering
Thiruparankundram, Madurai, Tamil Nadu, India, 625 015, India (Email: rrajaram@tce.edu)

(Received Aug. 27, 2009; revised and accepted Jan. 23 & Apr. 29, 2010)

Abstract

Yang-Wang-Chang proposed an improved timestamp associated password authentication scheme based on Yang-Shieh, who had earlier proposed timestamp-based remote authentication scheme using smart cards. In this paper, we propose an efficient password authentication scheme with smart card applying RSA. The proposed scheme withstands most of the attacks with minimum computational cost.

Keywords: Authentication, password, remote system, RSA, smart card

1 Introduction

Remote user authentication using smart cards is a good solution for many e-based applications. Smart card implementation ensures secure communications. Several schemes using timestamp for remote authentication have already been proposed. However these are vulnerable to certain types of forgery attack. To access resources at remote system, users should have proper access rights. One of the simplest and efficient mechanisms is the use of a password authentication scheme. To access the resources, each user should have an identity (ID) and a password (PW). In the existing traditional set up the ID and PW are maintained by the remote system in a verification table. If a user wants to login to a remote server, he has to submit his ID and password PW to the server. The remote server receives the login message and checks the authenticity of the user by referencing the verification table. If the submitted ID and PW match the corresponding pair stored in the server's verification table, the user will be granted access to the server.

A remote password authentication scheme authenticates the legitimacy of the remote user over insecure channel. In such schemes, the password is often regarded as a secret shared between the authentication server (AS) and the user, and serves to authenticate the identity of the individual login. Through knowledge of the password, the remote user can use it to create a valid login message to the authentication server. AS checks the validity of the login message and provides access right. Password authentication schemes with smart card have a long history in the remote user authentication environment.

This work proposes an efficient password authentication scheme with smart card using RSA. The proposed scheme entails reasonable computational cost. We have done the security analysis of this scheme. Section 2, provides a brief review of related password based authentication schemes. Section 3, proposes an efficient password authentication scheme with smart card. Section 4, discusses the security analysis of the proposed scheme with related schemes. Section 5, provides a computational cost comparison with other related schemes. Section 6, discusses the implementation results. Section 7, gives the concluding remarks

2 Related Work

In 1981, Lamport [19] proposed a remote password authentication scheme using a password table to achieve user authentication. Lamport [19] scheme is not secure, due to some vulnerability. A remote user authentication scheme using smart card was proposed by Hwang-Li [10]. Hwang-Li's scheme is based on ElGamal's [6] public key scheme. This scheme can withstand replaying attack by including time stamp in the login message. Moreover, the remote system does not need to store a password table for verifying the legitimacy of the login users. The system only needs to maintain a secret key, which is used to compute user passwords, based on user submitted parameters during the authentication phase. The strength of the scheme relies on the difficulty of computing discrete logarithms over finite fields. Therefore a user cannot compute the secret key of the system from known information. This scheme is breakable only by a legitimate user. A legitimate user can impersonate other legal users by constructing valid pairs of user identities without knowing the secure key of the system. Later, Shen [24] analyzed impersonation attack of Chan [2] on Hwang Li's [10] scheme, and suggested ways to repulse the attack. Awasthi-Lal [1], presented a remote user authentication scheme using smart card with forward security. Forward security ensures that the previously generated passwords in the system are secure even if the system's secret key is compromised. Yoon-Ryu-Yoo [35] citing Lal [1] proposed a hash based authentication scheme based on the work of Chien et al. [5]. In the authentication phase, the system cannot validate the login request message to compute the password of the user.

Yoo [34], presents an enhancement to resolve the problems in above-mentioned scheme. This scheme enables users to change their passwords freely and securely without the help of a remote server, while also providing secure mutual authentication. But the scheme entails more computational cost.

In 2004, Kumar [16] proposed a scheme, which is secure against forgery attacks. To ensure security, this scheme suggests some modification in login and authentication phases. This scheme is the modified form of the Shen-Lin-Hwang's [24] scheme and uses one more function C_K to generate the check digit of Kumar [16] for each registered identity. In this scheme, only the AS can generate a valid identity and the corresponding check digit. Fan-Chan-Zhang [7] proposed a robust remote authentication scheme with smart card. They claimed that their scheme satisfy the following properties: 1) low computation for smart cards; 2) no password table; 3) password chosen by the users themselves; 4) no need for clock synchronization and delay-time limitation; 5) withstand the replay attack; 6) server authentication; 7) withstand the offline dictionary attack without smart card; 8) withstand the offline dictionary attack with the smart card; 9) revoking the lost cards without changing the user's identities. The major contribution of Fan Chan-Zhang [7] scheme is a method for preventing the offline dictionary attack even if the secret information stored in a smart card is compromised. The major drawbacks of their scheme are the higher computation and communication costs, because of using Rabin's public-key cryptosystem [28]. Furthermore, their scheme does not provide a function for session key agreement and cannot prevent the insider attack. Ku-Chen [15] proposed an improvement to prevent reflection attack mentioned by Mitchell [22] and an insider attack discussed by Ku-Chen-Lee [14]. In addition, they showed that Chien et al. [5] scheme is vulnerable and can be compromised. Furthermore, Ku-Chen [15] proposed an improvement to Chien et al. [5] scheme to prevent the above-mentioned weaknesses. However, the improved scheme is not only susceptible to parallel session attack proposed by Hsu [9], but also insecure for changing the user's password in password changing phase. Different types of password authentication schemes have been proposed in [1, 2, 3, 4, 5, 8, 9, 20, 26, 31, 33].

In 2004, Yoon et al. [35] proposed a user authentication scheme based on generalized ElGamal signature scheme using smart cards. Wang and Li [29], pointed that Yoon et al. [35] scheme is not forward-secure. In their scheme the previous session keys will be compromised if the secret key of the system is leaked. Wang and Li [29] propose a new scheme which can offer forward secrecy. This scheme is also secure against forgery attack while keeping the merits of the scheme proposed by Yoon et al. [35]. Recently, a hash-based strong-password authentication scheme was described in [13], which withstands several attacks, including replay, password-file compromise, denial-of-service, and insider attacks. However, this protocol is still vulnerable to stolen-verifier, and impersonation attacks described by Kim-Koc [12].

Tsai, Lee and Hwang [28] present the survey of all currently available password-authentication-related schemes and classify them in terms of several crucial criteria. Tsai et al. [28] pointed out, most of the existing schemes are vulnerable to various attacks. They fail to achieve all the objectives that an ideal password authentication scheme should. They also define all possible attacks and goals that an ideal password authentication scheme should withstand and achieve. Tian et al. [27] show that Yoon et al. scheme [34] is subject to forgery attacks if the information stored in the smart card is stolen. This violates the "two factor security" objective of the smart card based remote user authentication schemes. Tian et al. [27] propose an amendment to this problem and propose two new schemes, which are more efficient and secure than Yoon et al.' s scheme. Liu et al. [21] proposed a novel ECC-based wire-less authentication protocol and analyze the security of their protocol.

Yang-Shieh [33] proposed a timestamp based password authentication scheme. This scheme is susceptible to well-known attacks. Fan et al. [8] proposed an enhancement in Yang-Shieh's [33] scheme. The scheme is similar to Yang-Shieh scheme, except it stipulates a strict limit on the user ID selection. Yang-Wang-Chang proposed a scheme [32], which removes the pitfalls present in the Yang-Shieh scheme [33]. Pathan-Hong [23], established that some kind of attacks are possible on Yang-Wang-Chang [32] scheme. Recently, Yang et al. [32] improved Yang and Shieh's [33] two password authentication scheme to withstand Sun and Yeh's [25] forgery attacks. However, Kim et al. [11] pointed out that Yang et al.'s [32] improvements still cannot withstand forgery attacks. At the same time, Kim et al. [11] proposed improved methods. Wang and Yang [30] pointed that Kim et al.'s [11] improvements also cannot resist the forgery attacks.

Kumar proposed a scheme [17] wherein the server and user authenticate one another, and then generate a secret session key for secure communication. In this scheme, the remote user is free to change his/her password without connecting to server. Kumar [18] proposes a secure remote user authentication scheme with smart cards. This scheme not only provides mutual authentication between the user and server, but also establishes a common session key to provide message confidentiality. In addition, this protocol provides the explicit key authentication property for established common session keys. Kumar pointed out that this protocol is provably secure to withstand the replay attack and the stolen verifier attack. In the password change phase of this protocol, each user can change his password without connecting to any server. In this paper, we propose an efficient password authentication scheme with smart card using RSA, which entails minimum computational cost. The proposed scheme removes the pitfalls in the above-mentioned schemes. We provide security analysis of the proposed scheme and implementation cost analysis.

3 Proposed Scheme

This paper, proposes an efficient password authentication scheme with smart card based on RSA. The proposed scheme has three phases, registration phase, login phase, and authentication phase. These phases are explained below.

3.1 Registration Phase

User U_i submits his ID_i and chosen PW_i to KIC. Key Information Center (KIC) issues a smart card to user U_i. Then KIC performs the registration steps:

1) Generate an RSA key pair, namely a private key d and a public key (e, n). KIC publishes (e, n) and keeps d secret.

2) Determine an integer g, which is a primitive in both GF_p and GF_q.

3) Generate the smart card identifier CID_i of U_i and calculate the user' s secret information as $W_i = ID_i^{CID_i \times d} \bmod n$.

4) Compute V_i by $V_i = g^{PW_i \times d \times T_R} \bmod n$, here T_R is the time of registration of the user. This value is unique for every user, and maintained by the server.

3.2 Login Phase

When U_i wants to login to S, he inserts his smart card into a card reader and keys ID_i and PW_i. Then smart card reader will perform the following steps:

1) Generates a random number r and calculate $X_i = g^{PW_i \times r} \bmod n$ and $Y_i = W_i \times V_i^{r \times T} \bmod n$.

2) Send the login request message (ID_i, CID_i, X_i, Y_i, n, e, g, T) to S

3.3 Authentication Phase

Server receives the login request and performs the following steps:

1) Check whether ID_i is a valid user identity and CID_i is a legal smart card identity, if not, then AS rejects the login request.

2) Check, whether $T_c - T \leq \triangle T$, where T_c is the login request received time by server and $\triangle T$is the legal time interval due to transmission delay, if not, then AS rejects the login request.

3) Evaluate the equation
$$Y_i^e = ID_i^{CID_i} \times X_i^{T \times T_R} \bmod n,$$
where T is the login request time and T_R is the registration time of every user.

4) If any one of the above result is negative, then login request is rejected. Otherwise, the login request is accepted.

5) If the login request is rejected three times then automatically the user account is locked and he has to contact server to unlock the account.

4 Security Analysis

This section discusses the security analysis of the proposed scheme.

4.1 Denial of Service Attack

The login request is generated based on password, current time and user's secret information. The login request generation is not based on any previous information; every time it a new one with current time. The attacker cannot create or update the false information for login. DOS attacks might result from the computation consumption also. The attackers might send the forged login request message to S. If ID_i is a valid user identity and T is a valid timestamp, the server S will perform the authentication. The more forged login request messages are sent, the more computation load the server performs. In the proposed scheme, if the login request is rejected three times then automatically the user account is locked and he has to contact server to unlock the account. The proposed protocol overcomes the DOS attack over the computation power of the server.

4.2 Parallel Session Attack

Suppose an adversary intercepts the login request $(ID_i, CID_i, X_i, Y_i, n, e, g, T)$. He cannot create a valid new login request because X_i is calculated using a random number and password PW_i, and Y_i value is calculated using user secret information and current time. The adversary cannot create a valid login request with out knowing, PW_i,T_R and d.

4.3 Smart Card Loss Attack

Suppose user U_i loses his smart card, the adversary cannot use this card without knowing the password of the user U_i. Suppose an adversary wants to change the password, he must know the original password. Thus his attempt to impersonate user U_i fails.

4.4 Password Guessing Attack

In our scheme, the password PW_i is calculated by using certain functions selected by user U_i. Suppose an adversary intercepts the login request (ID_i, CID_i, X_i, Y_i, n, e, g, T) of a user U_i. It is not possible to recover the original password from this login request message.

4.5 Impersonation Attack

In this attack, we assume a case given below,

Let as assume in the authentication phase, attackers can sniff the login request messages (ID_i, CID_i, X_i, Y_i, n, e, g, T). If $2CID_i$ is a valid CID, attackers can send (ID_i, $2CID_i$, X_i, Y_i^2, n, e, g, $2T$) at $2T$ to login as ID_i.

1) Card identity CID_i is unique identity for every user identity ID_i. The $2CID_i$ is not a valid CID for user ID_i, then login request is rejected.

2) The login time $2T$ will not satisfy $T_c - T \leq \triangle T$, then login request is rejected by server.

3) In the verification phase, $Y_i^e = ID_i^{2\times CID_i} \times X_i^{2\times T\times T_R} \bmod n$, the equation will not satisfy.

5 Cost Analysis

This section, presents the cost comparison of our scheme with other smart card based authentication schemes. Yang-Shieh [33], Fan-Li-Zhu [8], Yang-Wang-Chang [32] and our schemes are based on RSA. Table 1 illustrates the computational cost for each phase. The proposed scheme has high time complexity due to the improved security level from already existing schemes.

Kumar's scheme [17, 18] provides mutual authentication. In the cost analysis part, we omitted the computational cost needed for mutual authentication part.

1) E1 - Computation cost for Registration Phase;

2) E2 - Computation cost for Login Phase;

3) E3 - Computation cost for Authentication Phase;

4) T_{mexp} is the time taken for executing a modular exponentiation operation;

5) T_{mmul} is the time taken for executing a modular multiplication operation;

6) T_h is the time for executing a one-way hash function;

7) T_{C_K} is the time for executing a function to generate check digit for the registered identity.

6 Implementation Results and Discussions

This section, discuses the implementation result of proposed scheme and related schemes. Yang-Shieh [33] scheme needs $2T_{mexp}$+$1T_{mmul}$ computational cost for registration phase, $2T_{mexp}$+$3T_{mmul}$+$1T_h$ for login phase and $2T_{mexp}$+$1T_{mmul}$+$1T_h$ for authentication phase. Fan-Li-Zhu [8] scheme needs $2T_{mexp}$+$1T_{mmul}$ computational cost for registration phase, $2T_{mexp}$+$3T_{mmul}$+$1T_h$ for login phase and $2T_{mexp}$+$1T_{mmul}$+$1T_h$ for authentication phase. Yang-Shieh [33] and Fan-Li-Zhu [8] schemes are need same computational cost. Yang-Wang-Chang [32] scheme needs $2T_{mexp}$+$2T_{mmul}$ computational cost for registration phase, $2T_{mexp}$+$3T_{mmul}$ for login phase and $3T_{mexp}$+$1T_{mmul}$ for authentication phase. Kumar's [17] scheme needs T_{mexp}+T_{C_K} computational cost for registration phase, $3T_{mexp}$+$2T_h$ for login phase and $2T_{mexp}$+T_h+T_{C_K} for authentication phase. Another of Kumar's [18] scheme needs T_{mexp}+T_{C_K} computational cost for registration phase, $2T_{mexp}$+T_h for login phase and T_{mexp}+T_h+T_{C_K} for authentication phase. The proposed scheme needs $2T_{mexp}$+$3T_{mmul}$ computational cost for registration phase, $2T_{mexp}$+$3T_{mmul}$ for login phase and $3T_{mexp}$+$2T_{mmul}$ for authentication phase. Table 2 illustrates the time estimate for various operations. Table 3 illustrates the computational cost for all the phases to the related schemes

6.1 Performance Notations

1) T_{mul} is the time for multiplication;

2) T_h is the time for executing hash function;

3) T_{exp} is the time for exponentiation with mod$P$;

4) T_{inv} is the time for inversion mod$P$;

5) T_{KV} is the time for knapsack value generation;

6) T_{inKV} is the time for inverse knapsack value generation.

T_h, T_{exp}, T_{mul}, T_{inv}, T_{KV}, T_{inKV} entail heavy computational cost. T_{ECmul} is used to indicate the time for multiplying a number by a point on the elliptic curve. T_{ECadd} is the time for the adding one point to another on the elliptic curve. Normally, it has minimum computational cost. In this performance analysis, we consider two phases to measure the performance analysis. One could dispute the computational cost over two phases, signature generation phase, and message recovery phase. The signature generation phase of Horster et al. [31] requires $T_{exp} + T_{inv} + 2T_{mul} + T_h$ and the message recovery phase needs $2T_{exp}$+T_h+$3T_{mul}$. The signature generation phase of Wu [14] requires $3T_h + T_{inv} + 2T_{mul} + 2T_{exp}$ and the message recovery phase needs $3T_h$+T_{inv}+$3T_{exp}$. In Tzeng and Hwang AES based on ECDLP [25], the signature scheme with message recovery, the signature generation

Table 1: Computation cost comparison between proposed scheme and related schemes

Schemes	E1	E2	E3
Yang-Shieh [33]	$2T_{mexp} + 1T_{mmul}$	$2T_{mexp} + 3T_{mmul} + 1T_h$	$2T_{mexp} + 1T_{mmul} + T_h$
Fan-Li-Zhu [8]	$2T_{mexp} + 1T_{mmul}$	$2T_{mexp} + 3T_{mmul} + 1T_h$	$2T_{mexp} + 1T_{mmul} + T_h$
Yang-Wang-Chang [32]	$2T_{mexp} + 2T_{mmul}$	$2T_{mexp} + 3T_{mmul}$	$3T_{mexp} + 1T_{mmul}$
Kumar [17]	$T_{mexp} + T_{C_K}$	$3T_{mexp} + 2T_h$	$2T_{mexp} + T_h + T_{C_K}$
Kumar [18]	$T_{mexp} + T_{C_K}$	$2T_{mexp} + 1T_h$	$T_{mexp} + T_h + T_{C_K}$
Our Scheme	$2T_{mexp} + 3T_{mmul}$	$2T_{mexp} + 3T_{mmul}$	$3T_{mexp} + 2T_{mmul}$

phase needs $T_{ECmul} + T_{mul} + T_h$, and the message recovery phase has costs $2T_{ECmul} + T_{ECadd} + T_h$. In the Hsu and Wu [2] scheme, the signer generates a signature that the computational cost is $3T_{exp}+T_{mul}$, and the verifier recovers the message which needs $3T_{exp}+(2t+1)T_{mul}+(t-1)T_{inv}$. In Nyang et al. [13] scheme, signature generation phase and verification phase required computational cost $2T_{exp}+T_{mul}+T_h$ and $2T_{exp}+T_{mul}+T_h$ respectively. Chen et al. [15] scheme, requires the computational cost for signature generation phase of $2T_{ECmul} + T_{ECadd} + T_{mul} + T_h$ and verification phase required $3T_{ECmul} + 2T_{ECadd} + T_h$. The Table 2 illustrates the estimated time for various operations, for the implementation purpose we are taking 128 bit data.

Table 3 illustrates the computational performance analysis for different authenticated encryption schemes with the proposed scheme.

The new scheme has a higher estimated time, compared to the existing schemes. This has to be tolerated due to the higher security it affords, eliminates the verification table of the server and provides mutual authentication between user and the server.

7 Conclusion

Yang-Wang-Chang scheme fails to prevent some tricky forgery attacks. We propose an efficient password authentication scheme using smart card. The proposed scheme restricts most of the well-known attacks with reasonable computational cost. The proposed scheme is based RSA. The server need not maintain password table, instead it maintains only registration time of every user. This will reduce the server over head of maintaining large user data for authentication.

References

[1] A. K. Awasthi and S. Lal, "A remote user authentication scheme using smart cards with forward security," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1246-1248, 2003.

[2] C. K. Chan and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, pp. 992-993, 2000.

[3] C. C. Chang and S. J. Hwang, "Using smart cards to authenticate remote passwords," *Computers and Mathematics with applications*, vol. 26, no. 7, pp. 19-27, 1993.

[4] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," *IEE Proceedings-E*, vol. 138, no. 3, pp. 165-168, 1993.

[5] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card," *Computers and Security*, vol. 21, no. 4, pp. 372-375, 2002.

[6] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, no. 4, pp. 469-472, 1985.

[7] C. Fan, Y. Chan, and Z. Zhang, "Robust remote authentication scheme with smart cards," *Computers and Security*, vol. 24, no. 8, pp. 619-628, Nov. 2005.

[8] L. Fan, J. H. Li, and H. W. Zhu, "An enhancement of timestamp-based password authentication schem," *Computer and Security*, Elsevier vol. 21, pp. 665-667, 2002.

[9] C. L. Hsu, "Security of Chien et al' s remote user authentication scheme using smart cards," *Computer Standards and Interfaces*, vol. 26, no. 3, pp. 167-169, 2004.

[10] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28-30, 2000.

[11] K. W. Kim, J. C. Jeon, and K. Y. Yoo, "An improvement on Yang et al.'s password authentication schemes," *Applied Mathematics and Computation*, vol. 170, pp. 207-215, 2005.

[12] M. Kim and C. K. Koc, "A simple attack on a recently introduced hash-based strong-password authentication scheme," *International Journal of Network Security*, vol.1, no.2, PP.77-80, Sep. 2005.

[13] W. C. Ku, "A hash-based strong-password authentication scheme without using smart cards," *ACM Operating System Review*, vol. 38, no. 1, pp. 29-34, Jan 2004.

[14] W. C. Ku, C. M. Chen, and H. L. Lee, "Cryptanalysis of a variant of Peyravian-Zunic' s password authentication scheme," *IEICE Transaction on Communication,* vol. E86-B, no. 5, pp. 1682-1684, May 2003.

Table 2: Estimated time for various operations

Operations (128 bit)	Estimated Time in ms
T_{mmul}	$\approx$ 1.527932 ms
T_h	$\approx$ 1.513726 ms
T_{mexp}	$\approx$ 2.139810 ms
T_{C_K}	$\approx$ 2.078715 ms

Table 3: Computation cost comparison between proposed scheme and related schemes

Schemes	E1	E2	E3
Yang-Shieh [33]	$\approx$ 5.807552 ms	$\approx$10.377142 ms	$\approx$ 7.321278 ms
Fan-Li-Zhu [8]	$\approx$ 5.807552 ms	$\approx$10.377142 ms	$\approx$ 7.321278 ms
Yang-Wang-Chang [32]	$\approx$ 7.335484 ms	$\approx$8.863416 ms	$\approx$ 7.947362 ms
Kumar [17]	$\approx$ 3.606653 ms	$\approx$8.863416 ms	$\approx$ 7.274389 ms
Kumar [18]	$\approx$ 3.606653 ms	$\approx$5.195674 ms	$\approx$ 5.746457 ms
Our Scheme	$\approx$ 8.863416 ms	$\approx$8.863416 ms	$\approx$ 9.475294 ms

[15] W. C. Ku, and S. M. Chen, “Weakness and improvement of an efficient password based user authentication scheme using smart cards,” *IEEE Transactions on Consumer Electronics*, vol. 50, no. 1, pp. 204-207, Feb 2004.

[16] M. Kumar, “New remote user authentication scheme using smart cards,” *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 597- 600. May 2004.

[17] M. Kumar, “An enhanced remote user authentication scheme with smart card,” *International Journal of Network Security*, vol. 10, no. 3, PP. 175-184, May 2010.

[18] M. Kumar, “A new secure remote user authentication scheme with smart cards,“*International Journal of Network Security*, vol. 11, no. 3, PP. 128-133, Nov. 2010.

[19] L. Lamport, “Password authentication with insecure communication,” *Communication of the ACM*, vol. 24, no. 11, pp. 770-772, 1981.

[20] L. H. Li, L. C. Lin, and M. S. Hwang, “A remote password authentication scheme for multi-server architecture using neural networks,” *IEEE Transactions Neural Networks*, vol. 12, no. 6, pp. 1498-1504, 2001.

[21] Y. L. Liu, W. Gao, H. Yao, and X. Yu, “Elliptic curve cryptography based wireless authentication protocol,” *International Journal of Network Security*, vol. 5, no. 3, PP. 327-337, Nov. 2007.

[22] C. Mitchell, “Limitation of challenge-response entity authentication,” *Electronics Letters*, vol. 25, no. 17, pp. 1195-1196, Aug. 1989.

[23] A. S. K. Pathan and C. S. Hong, “Cryptanalysis of Yang-Wang-Chang’s password authentication scheme with smart cards,” *Proceedings of ICACT 2008*, pp. 1618-1620, Feb. 2008.

[24] J. J. Shen, C. W. Lin, and M. S. Hwang, “A modified remote user authentication scheme using smart card,” *IEEE Transactions on Consumer Electronics*, vol. 49, no. 2, pp. 414-416, 2003.

[25] H. M. Sun and H. T. Yeh, “Further cryptanalysis of a password authentication scheme with smart cards,” *IEICE Transactions on Communication*, vol. E86-B, no. 4, pp. 1412-1415, 2003.

[26] H. Tao and C. Adams, “Pass-Go: A proposal to improve the usability of graphical passwords,” *International Journal of Network Security*, vol. 7, no. 2, PP. 273-292, 2008.

[27] X. Tian, R. W. Zhu, and D. S. Wong, “Improved efficient remote user authentication schemes,” *International Journal of Network Security*, vol. 4, no. 2, PP. 149-154, Mar. 2007.

[28] C. S. Tsai, C. C. Lee, and M. S. Hwang, “Password authentication schemes: current status and key issues,” *International Journal of Network Security*, vol. 3, no. 2, PP. 101-115, Sept. 2006.

[29] B. Wang and Z. Q. Li, “A forward-secure user authentication scheme with smart cards,” *International Journal of Network Security*, vol. 3, no. 2, PP. 116-119, Sept. 2006.

[30] R. C. Wang and C. C. Yang, “Cryptanalysis of two improved password authentication schemes using smart cards,” *International Journal of Network Security*, vol. 3, no. 3, PP. 283-285, Nov. 2006.

[31] T. C. Wu, “Remote login authentication scheme based on a geometric approach,” *Computer Communication*, vol. 18, no. 12, pp. 959-963, 1995.

[32] C. C. Yang, R. C. Wang, and T. Y. Chang, “An improvement of the Yang-Shieh password authentication schemes,” *Applied Mathematics and Computation*, vol. 162, no. 3, pp. 1391-1396, 2005.

[33] W. H. Yang and S. P. Shieh, "Password authentication schemes with smart cards," *Computers and Security*, vol. 18, no. 8, pp. 727-733, 1999.

[34] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "Further Improvement of an Efficient password based Remote Authentication Scheme using smart cards," *IEEE Transaction on Consumer Electronics*, vol. 50, no. 2, pp. 612-614, May 2004.

[35] E. J. Yoon, E. K. Ryu, and K. Y. Yoo, "Efficient remote user authentication scheme based on generalized ElGamal signature scheme," *IEEE Transaction on Consumer Electronics*, vol. 50, no. 2, pp. 568-570, May 2004.

R. Rajaram Ramasamy Dean of CSE/IT, Thiagarajar College of Engineering, has BE degree in Electrical and Electronics Engineering from Madras University in 1966. He secured the M Tech degree in Electrical Power Systems Engineering in 1971 from IIT Kharagpur, and the Ph.D. degree on Energy Optimization from Madurai Kamaraj University in 1979. He and his research scholars have published/presented more that 45 research papers in Journals and Conferences. Eight of his scholar secured the Ph.D. degree in computer science and communications areas. Two have submitted thesis and awaiting their results. Six are currently pursuing their Ph.D. research in Anna University with his guidance. His current areas of interest are Mobile Agents, Cryptography and Data Mining. He has published more than 13 text books on Computer languages and Basic Communications. He attended the International Seminar on Solar Energy at University of Waterloo, Canada during 1978. He has served the Makerere University at Uganda during 1977-1978 and University of Mosul during 1980-1981. He secured two best technical paper awards from the Institution of Engineers India and one from Indian Society for Technical Education. He has travelled to Malaysia, London, Paris, Belgium New York, Toronto, Nairobi.

M. Amutha Prabakar received the B. E. degree in Computer Science and Engineering, in 2003; the M. E. in Computer Science and Engineering, in 2005. He had worked as a lecturer in the department of Computer Science and Engineering, R. V. S. College of Engineering and Technology, India from 2004-2007. Now he is doing his Research in the area of cryptography and security under anna university - coimbatore. He worked as a Research Associate in Smart and Secure Environment Lab under IIT, Madras. Now he is working as a Assistant Professor in department of Information Technology, Thiagarajar College of Engineering, Madurai. His current research interests include Cryptography and Security.