Security Privilege Using Selective Index In Session Based Password Validation

[1]BALAANAND M, [2]ANITHA D,[3]ANUPRIYA K,
[1,2&3]Department of Computer Science and Engineering
V.R.S College of Engineering and Technology, Arasur, Villupuram-607 107.

Abstract

Textual password and graphical passwords are the most common methods for authentication. But they are vulnerable to eves dropping, shoulder surfing, social engineering and dictionary attacks. To address these problems, the text is combined with the number as an alphanumeric to generate session passwords randomly through Autogen method using RSA algorithm. This method is resistant against shoulder surfing. These are suitable for personal digital assistants. Here, we are utilizing an idea to generate the password as a set of variables for authentication through Autogen method. Such that, a random set of variables has been generated from the password for every session which is registered earlier. Once the user enters for login by giving their identity, the password consisting of random variables are generated and displayed as grid. authenticator has to give the corresponding variables (stored in array address) from their original password which is matched to the variables in the grid. The variables which are shown in the grid is nothing but the array address of the original password stored. After receiving the password from user the system validate it with a database which is encrypted in the server at the time of registration (username & password) then the user is allowed to access for remaining process. If the user does not have enough access, he will be redirected for the login to attempt the next phases.

Keyterms – Rsa Algorithm, Autogen, Keygen, Shoulder Surfing.

1 Introduction

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 re-mote 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 verificationtable. 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 chan-nel. 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 tothe 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, pro-vides 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 overniteelds. 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. Awasthilal [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 Chienet 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 with-out 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. They claimed that their scheme satisfy the following properties: 1) low computation 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 online dictionary attack . The major contribution of fan chan-zhang [7] scheme is a method for preventing the online dictionary attack even if the secret information stored. 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.

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 cans over 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-¯le 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 de¯ne 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] are subject to forgery attacks if the information stored in the smart card is stolen. This violates the \two factor security". 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 wireless authentication protocol and analyze the security of their protocol.

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 re-mote 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 re-play attack and the stolen verifier attack.

Word 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 mini-mum 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

In this paper, we 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 *ui*submits his *idi*and chosen *pwi*to KIC. Key information center (KIC) issues a smart card to user *ui*. 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) Check, whether $t_c \text{¡} t \cdot 4t$, where t_c is the login request received time by server and *4t* is the legal time interval due to transmission delay, if not, then *as* rejects the login request.

3) evaluate the equation

$$Y_i^e = id_i^{cidi} \pounds x_i^{t \pounds tr} \text{mod } n; \ldots (1)$$

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.

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_pandgf_q.

3) Generate the smart card identifier cid_i of u_i and calculate the user' s secret information as $w_i = Id_i^{cidi \pounds d}$mod n.

4) Compute v_i by $v_i = g^{pwi \pounds d \pounds tr}$ mod 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 $x_i = g^{pwi \pounds r}$mod n andy_i=$w_i \pounds v_i^{r \pounds t}$mod n.

2) Send the login request message to s

3.3 AUTHENTICATION PHASE

Server receives the login request and performs the following steps:

1) check whether *idi*is a valid user identity and *cidi*is a legal smart card identity, if not, then *as* rejects the login request.

2) check, whether $tc \text{ ¡ } t \cdot 4t$, where *tc*is the login request received time by server and *4t*is the legal time interval due to transmission delay, if not, then *as* rejects the login request.

3) evaluate the equation *y ei= idcidii £ xt£tri*mod *n;*where*t*is the login request time and *tr*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 pro-posed 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 can-not 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 pro-posed 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 adver-sary cannot create a valid login request with out knowing, pw_i,$tr$and d.

4.3 PASSWORDGUESSING ATTACK

In our paper, 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, and t)* of a useru_i. It is not possible to recover the originalpassword from this login request message.

4.4 IMPERSONATION ATTACK

In this attack, we assume a case given below,Let as assumes in the authentication phase, attackers can sni® the login request messages (id_i, cid_i, x_i, y_i, *n, e, g, and t)*. If 2$cid_i$is a valid*cid*, attackers can send(id_i, 2cid_i, x_i, y_i^2, *n*, *e*, *g*, 2*t*) at 2*t* 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, and then login request is rejected.
2) The login time 2*t* will not satisfy t_c¡t· $4t$, then login request is rejected by server.
3) In the verification phase,

$$Y_i^e = id_i^{2£cidi} £x_i^{2£t£tr} \bmod n \ldots\ldots\ldots\ldots\ldots(2)$$

the equation willnot satisfy.

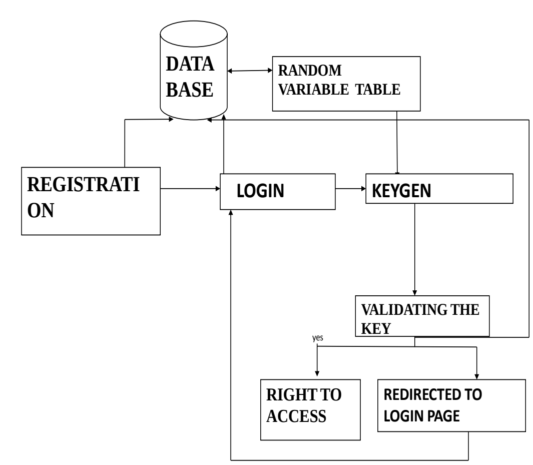

Fig 4.4.0 Architecture Diagram

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 ex-ponentiation operation;
5) $T_{mmul}$is the time taken for executing a modular mul-tiplication operation;

6) $T_h$is the time for executing a one-way hash function;
7) $T_{ck}$is the time for executing a function to generatecheck digit for the registered identity.

Table 1: Computation Cost Comparison Between Proposed Scheme And Related Schemes

6. PERFORMANCE NOTATIONS

1) $T_{mul}$is the time for multiplication;
2) $T_h$is the time for executing hash function;

Schemes	E1	E2	E3
Yang-shieh [33]	2*tmexp* + 1*tmmul*	2*tmexp* + 3*tmmul* + 1*th*	2*tmexp* + 1*tmmul* + *th*
Fan-li-zhu [8]	2*tmexp* + 1*tmmul*	2*tmexp* + 3*tmmul* + 1*th*	2*tmexp* + 1*tmmul* + *th*
Yang-wang-chang [32]	2*tmexp* + 2*tmmul*	2*tmexp* + 3*tmmul*	3*tmexp* + 1*tmmul*
Kumar [17]	$Tmexp+tc_k$	$3t_{mexp} + 2t_h$	$2tmexp + th + tc_k$
Kumar [18]	$Tmexp+tc_k$	2*tmexp* + 1*th*	$Tmexp+th+tc_k$
Our scheme	2*tmexp* + 3*tmmul*	2*tmexp* + 3*tmmul*	3*tmexp* + 2*tmmul*

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 genera-tion.

T_h,t_{exp},t_{mul},t_{inv},t_{kv}, t_{inkv}entail heavy com-putational 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 onthe 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 phaseneed 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 Aesbased on Ecdlp [25], the signature scheme with message recovery, the signature generation. 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. The proposed scheme removes the pitfalls in the above-mentioned schemes. We provide security analysis of the proposed scheme and implementation cost analysis.

Computation Cost Comparison Between Proposed Scheme And Related Schemes

Phase needs t_{ecmul} + t_{mul} + t_h, and the message recov-ery phase has costs 2t_{ecmul} + t_{ecadd} + t_h. In the hsu and wu [2] scheme, the signer generates a signature thatThe computational cost is 3t_{exp} +t_{mul}, and the verifier re-Covers the message which needs 3t_{exp} + (2t+1)*tmul* + ($t_¡$ 1)*tinv*. In Nyang Et Al. [13] scheme, signature generationPhase and verification phase required computational cost2t_{exp}+t_{mul}+t_h and 2t_{exp}+t_{mul}+t_h respectively. Chen et al. [15] scheme, requires the computational cost. Nature 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.

7. CONCLUSION

In this paper, two authentication techniques based on text and numbers are proposed for PDA’S. These techniques generate session passwords and are resistant to dictionary attack, brute force attack and shoulder-surfing. Both the techniques use grid for session passwords generation. Pair based technique requires no special type of registration, during login time based on the grid displayed a session password is generated. For hybrid textual scheme, ratings should be given to colors, based on these ratings and the grid displayed during login, session passwords are generated. However these schemes are completely new to the users and the proposed authentication techniques should be verified extensively for usability and effectiveness.

8. REFERENCES

[1] A. K. Awasthi and s. Lal, \a remote user authenti-cation scheme using smart cards with forward secu-rity," *ieee transactions on consumer electronics*, vol. 49, no. 4, pp. 1246-1248, 2003.

[2] C. K. Chan and l. M. Cheng, \cryptanalysis of a re-mote 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 andmathematics with applications*, vol. 26, no. 7, pp. 19-27, 1993.

[4] C. C. Chang and t. C. Wu, \remote password au-thentication 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 e±-cient 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 sig-nature scheme based on discrete logarithms," *ieeetransactions on information theory*, vol. 31, no. 4,

pp. 469-472, 1985.

[7] C. Fan, y. Chan, and z. Zhang, \robust remote au-thentication scheme with smart cards," *computersand 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," *computerstandards 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," *ieeetransactions 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 au-thentication scheme," *international journal of net-work security*, vol.1, no.2, pp.77-80, sep. 2005.

[13] W. C. Ku, \a hash-based strong-password authen-tication scheme without using smart cards," *acmoperating system review*, vol. 38, no. 1, pp. 29-34,jan 2004.

[14] W. C. Ku, c. M. Chen, and h. L. Lee, \cryptanal-ysis of a variant of peyravian-zunic' s password au-thentication scheme," *ieice transaction on com-munication*, vol. E86-b, no. 5, pp. 1682-1684, may2003.