Dynamic Id Based Remote User Authentication In Multi Server Environment Using Smart Cards: A Review

Shanu Gaharana
Uttar Pradesh Technical University,
Lucknow, India
Email: shanugaharana@gmail.com

Darpan Anand
Hindustan Institute of Technology and Management, Agra
Uttar Pradesh Technical University
Email: darpan.anand.agra@gmail.com

Abstract: Authentication refers to the process of ensuring confidentiality of data. It basically involves verifying a user's identity for accessing a system or service. There are three ways of authentication- i)using something that a user knows eg password ii)using something that a user has eg smart card or identity card iii)using something that a user is or does for example face, finger print ,voice etc. To overcome the risk of partial information leakage from static id based algorithms. Dynamic id based schemes have been proposed. In this paper, we analyzed four dynamic id based remote user password authentication schemes for multi server environment using smart card. All the schemes are vulnerable to the denial of service attack.

Keywords: Authentication, Confidentiality, Algorithm, denial of service

I. INTRODUCTION

We are living in the era of internet and technology and with the rapid development in technology, we are moving towards the concept of Internet of Things (IoT). With the rapidly growing implementation of technologies in the area of e-commerce, e-governance, m-commerce, m-governance etc, security has become a big concern. Security involves ensuring confidentiality, integrity and availability of data.
The process of ensuring the confidentiality of data is known as authentication. Basically in authentication an entity proves itself to be the one it actually claims to be. The most classic password based technique of authentication using a one way hash encryption function, was proposed by Leslie Lamport [1] in 1981.however, the scheme could not resist interpolation attack. To overcome the weakness of maintaining verification table, in 1991, Chang and Wu[2] presented a new remote user password authentication scheme by using smart cards. This scheme eliminated the need of maintaining verifier table. several schemes and improvements have been proposed but the schemes were based on static login identity. The use of static login identity was found to be leaking some partial information in many applications and it is necessary to protect the partial information because an attacker may use this information to launch an attack. In 2004, M.L. Das et al [3] presented a new concept of dynamic ID based remote user authentication scheme and later many schemes were developed that were based on the concept of dynamic identity [4][5][6]. In traditional user authentication schemes, user not only needs to log into various remote servers with repetitive registration, but also needs to remember the various user identities and passwords. In 2000, Lee and Chang[7] proposed a user identification and key distribution scheme based on the factorization difficulty and hash function for multi server environment. In such schemes, the user is registered at registration server once and can use the all the permitted services at remote servers using single id and password.In 2009, Liao \& Wang [8] proposed a dynamic Id based remote user authentication scheme for multi server environments where the user's identity changes dynamically in each session and this scheme was claimed to resist various attacks and achieves mutual authentication. In 2011, Cheng Chi Lee et al[11],proposed a scheme with anonymity that can resist several attacks but it was lacking in mutual authentication. In 2012, Xiong Li et al presented a scheme which was designed in order to protect the user from being tracked [12]. In 2013, Kaiping Xue et al[13] proposed dynamic pseudonym identity based authentication and key agreement scheme that provides traceability and identity protection. In 2014,Leu and Hsieh[14] presented a comparatively more secure and practical scheme that uses few hashing operations in its implementation.

In this paper, we analyze a set of security requirements and goals for dynamic id based remote user password authentication schemes for multi server environment using smartcard.

II. SECURITY REQUIREMENTS AND GOALS

There are some requirements that an ideal password authentication scheme should withstand.

- **Identity protection and user anonymity:** to protect user id from malicious attackers. For this purpose, a concept of dynamic id [3] or pseudonym identity[13] is used.
- **Traceability:** To extract users' real identities and link them with protected pseudonym and dynamic identities, while providing the function of anonymity between the user and the service providing server.
- **Mutual authentication:** refers to a two way authentication where a client must prove its identity to server and server must prove its identity to the client.
- **Session key agreement:** to ensure the security of a communication session be between a user and server, a symmetric key is randomly generated for encryption and decryption of messages exchanged.

978-1-5090-0076-0/15 $31.00 © 2015 IEEE
DOI 10.1109/CICN.2015.212

- **Password updating/changing:** change or update user's password whenever he/she wishes to.
- **Resistance of insider attack:** an insider attack is intentional misuse of computers or networks by authorized persons such as administrators.
- **Resistance of stolen smart card attack:** a stolen smart card can help an attacker to break into the system. an algorithm must be designed in such a way that an attacker might not be able to derive secret information from smart card.
- **Resistance of replay attack and Denial of Service attack:** Replay attack involves intercepting the previous messages and then replaying them to the intended entity(e.g. a server) with a intent to be considered a legitimate user. with this attack, a user can easily impersonate a legitimate user. Denial of service attack prevents the normal operation of a server. It involves flooding the server with several packets so that it becomes busy in handling them leading to denial of service to normal operations.
- **Resistance of eavesdropping attack:** interception of messages exchanged between communicating parties from communication channels.
- **Resistance of masquerade attack:** An efficient scheme must resist masquerade attack, it i s a man in the middle attack.
- **Masquerade attack:** involves intercepting the messages between communicating parties and then recording them for replay and after recording it may or may not alter the messages. It is an attack on confidentiality of data.
- **Replay attack:** It is retransmission of messages that were intercepted or recorded during a communication session between user and server by an attacker to the server.

III. REVIEW OF DYNAMIC ID BASED SCHEMES FOR MULTI SERVER ENVIRONMENTS

The general notations used in this paper are described as in the table 1:

A. Review of Cheng Chi Lee Scheme (2011):

In this scheme[11], three entities are involved: the user(U_i), the service providing server(S_j) and registration center(RC).RC chooses the master key x and a secret number y to compute h(x‖y) and h(y) and then shares them with Sj through a secure channel. Only RC knows the master secret key x and secret number y. The scheme is explained in Figure 1 and the parameters used in figure are:

N_i , N_j= nonce (generated at user and server side respectively)

$$CID_i = h(b \oplus PW_i) \oplus h(T_i \parallel A_i \parallel N_i) \quad (1)$$

$$P_{ij} = T_i \oplus h(h(y) \parallel N_i \parallel SID_j) \quad (2)$$

SYMBOL	DESCRIPTION
ID	User's ID
PW	User's password
h(.)	One way hash function
⊕	Bitwise XOR computation
‖	Concatenation operation
y	Secret value of server(to be stored on smart card)
x	Secret value of server
SID_j	Server identity

TABLE 1

$$Q_i = h(B_i \parallel A_i \parallel N_i) \quad (3)$$

$$M'_{ij} = h(B_i \parallel N_i \parallel A_i \parallel SID_j) \quad (4)$$

$$M''_{ij} = h(B_i \parallel N_j \parallel A_i \parallel SID_j) \quad (5)$$

B. Review of Xiong Li, Jian Ma et al Scheme (2012):

In this scheme[12], three participants are involved: the user (U_i), the service providing server (S_j) and registration center(RC).RC chooses the master key x and a secret number y to compute h(x‖y) and h(SID_j‖h(y)) and then shares them with S_j through a secure channel. and a secret number y to compute h(x‖y) and h(SID_j‖h(y)) and then shares them with S_j through a secure channel. The scheme is explained in Figure 2 and the parameters used in figure are :

$$A_i = h(b \oplus PW_i) \quad (6)$$

$$P_{ij} = E_i \oplus h(h(SID_j \parallel h(y)) \parallel N_i) \quad (7)$$

$$CID_i = A_i \oplus h(D_i \parallel SID_j \parallel N_i) \quad (8)$$

$$M_1 = h(P_{ij} \parallel CID_i \parallel D_i \parallel N_i) \quad (9)$$

$$M_2 = h(SID_j \parallel h(y)) \oplus N_i \quad (10)$$

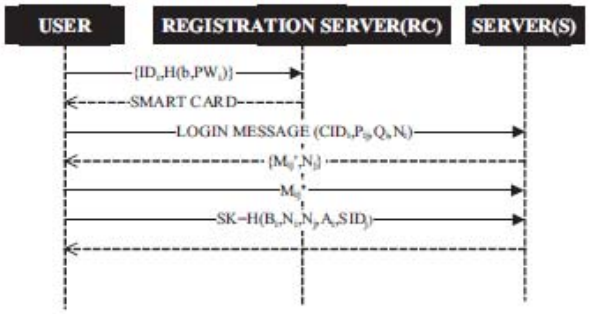

Fig. 1. Cheng Chi Lee Scheme

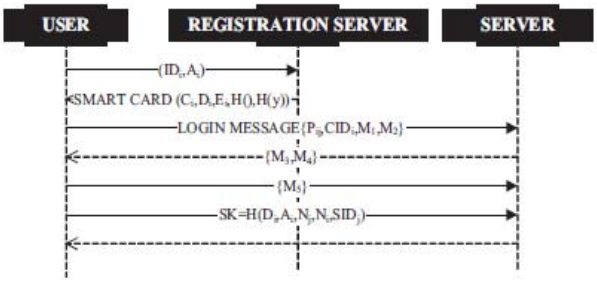

Fig. 2. Xiong Li, Jian Ma et al Scheme

$$M_3 = h(D_i \parallel A_i \parallel N_j \parallel SID_j) \quad (11)$$

$$M_4 = A_i \oplus N_i \oplus N_j \quad (12)$$

$$M_5 = h(D_i \parallel N_i \parallel A_i \parallel SID_j) \quad (13)$$

C. Review of Kaiping Xue et al Scheme (2013):

In this scheme[13], three participants are involved: the user(U_i), the service providing server(S_j) and control server(CS).The scheme is explained in Figure 3 and the parameters used in the figure are :

$$F_i = B_i \oplus N_{i1} \quad (14)$$

$$P_{ij} = h(B_i \oplus h(N_{i1} \parallel SID_j \parallel PID_i \parallel TS_i)) \quad (15)$$

$$CID_i = ID_i \oplus h(B_i \parallel N_{i1} \parallel TS_i \parallel \text{"00"}) \quad (16)$$

$$G_i = b \oplus h(B_i \parallel N_{i1} \parallel TS_i \parallel \text{"11"}) \quad (17)$$

TS_i - current timestamp value

$$J_i = BS_j \oplus N_{i2} \quad (18)$$

$$K_i = h(N_{i2} \parallel BS_j \parallel P_{ij} \parallel TS_i) \quad (19)$$

$$L_i = SID_j \oplus h(BS_j \parallel N_{i2} \parallel TS_i \parallel \text{"00"}) \quad (20)$$

$$M_i = d \oplus h(BS_j \parallel N_{i2} \parallel TS_i \parallel \text{"11"}) \quad (21)$$

$$P_i = N_{i1} \oplus N_{i3} \oplus h(SID_j \parallel N_{i2} \parallel BS_j) \quad (22)$$

$$R_i = N_{i2} \oplus N_{i3} \oplus h(ID_i \parallel N_{i1} \parallel B_i) \quad (23)$$

$$Q_i = h(N_{i1} \oplus N_{i3}) \quad (24)$$

$$V_i = h(N_{i2} \oplus N_{i3}) \quad (25)$$

$$SK = h((N_{i1} \oplus N_{i2} \oplus N_{i3}) \parallel TS_i) \quad (26)$$

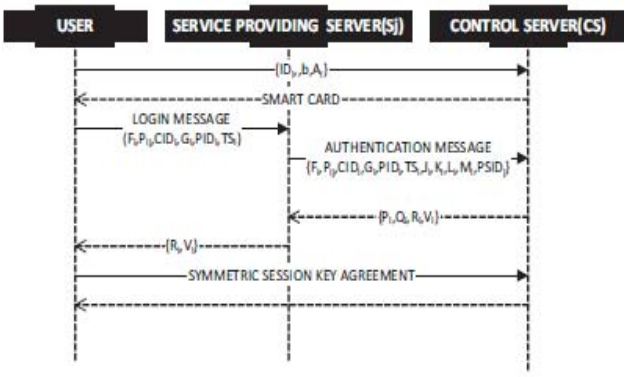

Fig. 3. Kaiping Xue et al Scheme

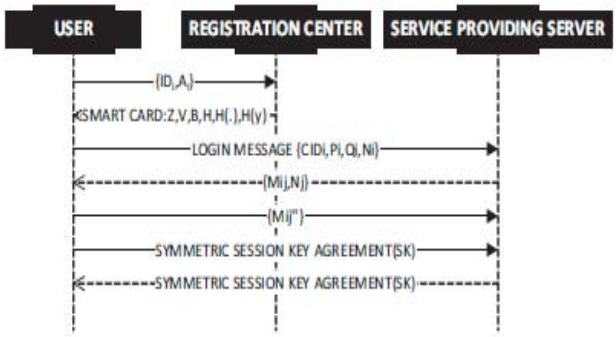

Fig. 4. Leu and Hsieh Scheme

D. Review of Leu and Hsieh Scheme (2014):

In this scheme[14],a random number is used to represent identity indirectly which in turn results in difficulty to guess random number rather than a logic identity. Three participants are involved: the user (U_i), the service providing server(S_j) and Registration server(RC). RC chooses the master key x and a secret number y to compute h(x‖y) and h(y)and then shares them with Sj through a secure channel. The master key x and a secret number y are known to RC only. The scheme is explained in Figure 4 and the parameters used in the figure are :

$$A_i = h(b \parallel PW_i) \quad (27)$$

$$CID_i = h(b \oplus PW_i \oplus R_i) \oplus h(T_i \parallel A_i \parallel N_i) \quad (28)$$

$$P_{ij} = T_i \oplus h(h(y) \parallel N_i \parallel SID_i) \quad (29)$$

$$Q_i = h(O_i \parallel A_i \parallel N_i) \quad (30)$$

N_i , N_j= nonce (generated at user and server side respectively)

$$M_{ij} = h(O_i \parallel A_i \parallel N_i \parallel SID_j) \quad (31)$$

$$M''_{ij} = h(O_i \parallel A_i \parallel N_i \parallel SID_j) \quad (32)$$

$$SK = h(O_i \parallel A_i \parallel N_i \parallel SID_j) \quad (33)$$

IV. CRYPTANALYSIS OF DYNAMIC ID BASED SCHEMES FOR MULTI SERVER ENVIRONMENTS

The analysis of the above discussed schemes is presented in the table 2.

IV. CONCLUSION

Security Requirements and Goals	C.C.Lee et al	Xiong Li et al	K. Xue et al	Leu & Hsieh
Identity protection and user anonymity	Yes	Yes	Yes	Yes
Traceability	No	No	Yes	No
Mutual authentication	Yes	Yes	Yes	Yes
Session key agreement	Yes	Yes	Yes	Yes
Password updating/changing	Yes	Yes	Yes	Yes
Resistance of insider attack	No	No	Yes	Yes
Resistance of stolen smart card attack	Yes	No	probable	No
Resistance of replay attack and Denial of Service attack	No	No	Yes	No
Resistance of eavesdropping attack	No	No	No	No
Resistance of masquerade attack	Yes	Yes	Yes	Yes
Masquerade attack	No	No	No	Yes
Replay attack	Yes	No	No	No

TABLE 2

In this paper, we have done the survey of four dynamic Id based remote user authentication schemes in multi server environment. We have discussed the security requirements and goals that an ideal password authentication scheme must satisfy and achieve. Review results are based on cryptanalysis done by other researchers and also done by us. All the schemes provide identity protection, session key agreement and a separate phase for password update or change. Masquerade attack cannot be performed on all the scheme except on the Leu and Hsieh scheme. Replay attack is only possible on the C.C. Lee scheme but rest of the schemes are safe from it as they make use of either timestamps or nonces. Therefore, there is a need to have a look on these goals for future research. Unfortunately, there is no such scheme that meets all the security requirements and attains all the goals. We, therefore, hope that our work will contribute in providing a better idea for figuring out the security challenges of dynamic id based remote user authentication in multi server environment using smart cards and open the new ways for further research in this area.

REFERENCES

1. Lamport L., Password authentication with insecure communication, Commun ACM 1981;24(11):770–2.

2.Chang CC, Wu TC,Remote password authentication with smart card , Comput. Digital Tech., IEE Proc. E 1991;138(3):165–8.

3. Das M L , Saxena A,,Gulati VP,A dynamic ID-based remote user authentication scheme, IEEE Trans Consum Electr 2004;50(2):629–31.

4.JIA-LUN Tsai, Tzong-Chen Wu and Kuo-Yu Tsai, New Dynamic Id Authentication Scheme Using Smart Cards ,Int. J. Commun. Syst. 2010; 23:1449–1462.

5. Fengtong Wen, Xuelei Li ,An improved dynamic ID-based remote user authentication with key agreement scheme, ,Computers and Electrical Engineering 38 (2012) 381–387.

6. Bae Ling Chen, Wen Chung Kuo and Lih Chyau Wuu, Robust Remote Authentication Scheme With Smart Card,Int. J. Commun. Syst. (2012).

7. W B Lee, CC Chang,User identification and key distribution maintaining anonymity for distributed computer networks, ,International Journal of Computer Systems Science \& Engineerin,2000;15(4):211–214.

8. Liao,Y.P. & Wang, S. S, A secure dynamic ID based remote user authentication scheme for multi-server environment, ,Computer Standard & Interfaces, 31(1), 24–29.

9.Kocher, P., Jaffe, J., Jun, B ,Differential power analysis ,Proc. Advances in Cryptology (Crypto'99), Santa Barbara, USA, 1999,pp. 388–397.

10.T.S. Messerges, E.A. Dabbish and Sloan, Examining smart-card security under the threat of power analysis attacks,IEEE Transactions on computers,VOl.51, No. 5, May 2002.

11.Cheng Chi Lee, Tsung Hung Lin, Rui Xiang Chang, A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards, Expert Systems with Applications 38 (2011) 13863–13870.

12.Xiong Li, Jian Ma, W.Wang, Y. Xiong, J.Zhang, A novel smart card and dynamic ID based remote user au authentication scheme for multiserver environments, Mathematical and computer modeling, Vol 58,Issues 1-2, July 2013, Volume 58, Issues 1–2, July 2013, Pages 85–95

13.Kaiping Xue, P. Hong and C. Ma, A lightweight dynamic pseudonym identity based authentication and key agreement protocol without verification tables for multi-server architecture,Journal of Computer and System Sciences 80 (2014) 195–206.

14.Jenq Shiou Leu, Wen-Bin Hsieh, Efficient and secure dynamic ID-based remote user authentication scheme for distributed systems using smart cards,IET Inf. Secur., 2014, Vol. 8, Iss. 2, pp. 104–113