A Proposed Approach for Multiserver Authentication and Key Agreement with User Protection and Security

Amita Jangid[1], Er. Akhil Pandey[2], Vishal Shrivastava[3]

[1] M.Tech scholar, Dept. of CSE, Arya College of Engineering & Information Technology SP-42 RIICO Industrial Area Kukas, Jaipur Rajasthan,India
[2] HOD, Dept. of CSE, Arya College of Engineering & Information Technology SP-42 RIICO Industrial Area Kukas, Jaipur Rajasthan,India
[3] Professor, Dept. of CSE, Arya College of Engineering & Information Technology SP-42 RIICO Industrial Area Kukas, Jaipur Rajasthan,India

Abstract:-Use of smart card makes remote user verification and key agreement easy, elastic to making a secure scattered system environment. It is very important to provide user privacy protection in authentication phase. In this paper, we are describing the performance comparison of Jung approach for multiple server authentication and key agreement schemes with user protection in network security with our proposed approach. First we are describing the juang approach then overview of our approach with comparison. All the areas those can be improved by us are also defined. Our approach is works for single server as well as multi sever environment. According to our analysis the juang approach is open to the element, leak-of-verifier attack and session key discovery attack and smart card loss attack. We are saving data into the server table in form of digital identity, smart card is removed by us, and so the new approach is safe from smart card loss attack.

Keywords: *user verification, session key, comparison, key size, smart card, network security.*

*****

1. Introduction

The user must login to access the services provided by the server. For login user send his username and password to the server through a protected path. In this case for to check the authenticity of the user sever reads the message send by the user and verifies his identity and password, if the identity and password matches then server gives rights to access all services provided by itself otherwise user not allowed to access the services. In previous paper we study the Juang approach for multi server authentication and key agreement problem and we figure out its limitation and improvement areas. In previous paper we study the Juang approach for multi server authentication and key agreement problem and we figure out its limitation and improvement areas. So in this paper we shall describe the step by step implementation of our proposed approach. Juang scheme is efficient for authentication and key agreement but the drawback of the scheme; it has no ability of anonymity for the user. We can make it more secure and cost effective. The following points must be considered for user authentication and key conformity phase.

a. **Confidentiality shelter**: in the phase of authentication the opponent can not constrain the identity of the user.
b. **Generously choose password:** All uses are free to change password and select his password by himself.
c. **Less communication and computation cost:** The smart card is costly and it is not offers a powerful computation capability so we are removing the smart card from our approach.
d. **Mutual authentication:** Server authenticate user mutually.
e. **Session key contract:** Each server and user must establish a session before communication [7, 8].

Usually in all scheme each user needs to register many servers and memorize more than one identities and passwords. This is not convenient way for the users. To make it easy to use many approaches are proposed for multi server authentication. In these entire new schemes only one time login works for many severs. User need not to register on all the servers. These are the following criteria for security of the session key generation phase.

a. **Session key safety**: Session key must be shared with the user and server only securely
b. **Forward confidentiality**: Session key must have some time out feature. The long driven session key is unsecure that is used before for other sessions. For each new session new key must be generate.
c. **Known-key security:** the old session key can not determine the new session key.

2. The Proposed Scheme

Juang approach is smart card based approach for remote logins to multi server environment. This approach is weak beside smart card lost problems, leak-of-verifier attack. To remove all recognized security terrorization in their mechanism, we shall propose an improved version this approach.

Description of proposed improvements in Juang user authentication and key agreement scheme. In place of one simple hash function we are using 3DES which is more secure and required less memory block size. It provides addition security and control over user credentials. User identities saved into the sever tables securely in the form of digital identity.

2.1 Notations

Let “A → B: C” denote A is sender B is message and C is receiver, E y(c) denote that secure key y is used to encrypt the chipper text c. D y(m) denote the secrete key y is used to decrypt the plaintext m corresponding symmetric cryptosystem[13], “&” denote the string concatenate operator and XOR denote the bitwise exclusive-or operator. h denote the hash function.

2.2 Single Server Authentication Scheme

In this section, we propose an efficient single server user authentication and key agreement scheme with privacy protection using 3DES algorithm. The same concept used in this section will be used in the next section to construct an efficient multi-server user authentication and key agreement scheme with privacy protection. Let UIDi be a unique identification of user i. Also, let s be the master secret key kept secretly by the server S.

2.2.1 Registration Phase

Assume User i submits his identity UIDi and his password PWi to the server S for registration. If S accepts this request, he will perform the following steps:

Step 1: Compute Ui ‘s secret information βi = 3DES(IDi & s) and σi = βi XOR PWi.

Step 2: Store UIDi and σi to the memory of sever as a digital identity and share this identity to the user securely.

2.2.2 User Authentication and Session Key Agreement Phase

After successful registration to the server, Ui can login to the server. When he logins in the server. If Ui wants to login to S. He inputs his identity UIDi and his password PWi to this device. Assume that α1 is a nonce value chosen by Ui and α2 is a nonce value chosen by Sj for freshness checking. Assume that γu is a arbitrary number chosen by Ui and γs is a arbitrary number chosen by Sj for generating the session key value ψi = 3DES (γs & γu & βi). The following protocol is the ith login with sever.

Step 1: Ui → S: α1, UIDi,Eβi (γui, 3DES(UIDi & α1));
Step 2: S → Ui: Eβi (γs, α1 + 1, α2);
Step 3: Ui→ S: Eψi (α2 + 1).

2.3 Multi Server Authentication Scheme

There are three participants in our multi-server protocol: a key distribution centre, service providers (servers) and users. Let RC denote the registration centre, Sj denote server j, and Ui denote user i. Let UIDi be a unique identification of Ui and SIDj be a unique identification of Sj Also, let s be the secret key kept secretly by RC, and σj = 3DES(s & SIDj) be the secret key shared by Sj and RC. The shared secret key σj can be computed by RC and sent to Sj after he registered at RC.

2.3.1 Registration Phase

Ui submits his identity UIDi and his password PWi to RC for registration. RC then performs the following steps:

Step 1: Compute Ui ’s secret information βi =3DES(s & UIDi) and σi = βi XOR PWi.

Step 2: Store UIDi and σi to the memory of the server and share this digital identity to Ui securely.

Step 3: Compute the shared secret key βi,j = 3DES(βi & SIDj) between Ui and Sj , and send the encrypted secret key Eσj (βi,j ,UIDi) to each Sj . Upon receiving Eσj (βi,j ,UIDi), Sj stored it in his encrypted keys table.

2.3.2 Login and Session Key Agreement Phase

After successful registration on registration center, Ui can use it to login into Sj. Assume that α1 is a nonce value chosen by Ui and α2 is a nonce value chosen by Sj for freshness checking. Assume that γu is a random number chosen by Ui and γs is a random number chosen by Sj for generating the session key value ψi = 3DES (γs & γu & βi,j). The following protocol is the ith login with sever.

Step 1: Ui → Sj : α1,UIDi,Eβi,j (γu, 3DES(UIDi & α1));
Step 2: Sj → Ui : Eβi,j (γs, α 1 + 1, α 2);
Step 3: Ui → Sj : E ψi (α 2 + 1).

2.3.3 Shared Key Inquiry Phase

In Step 3 of the registration phase, Registration center will send the encrypted shared secret key Eσj (βi,j ,UIDi) to each Sj . After receiving the shared key each server will save the key in encrypted shared key table. The shared key can be verified by the RC if server doesn’t want to store these keys, it can be fetch by RC. The following protocol can be inserted between Step 1 and Step 2 of the login and session key agreement phase when Sj needs the shared key.

Step 1: Sj → RC : α3,UIDi, SIDj ;
Step 2: Eσ j (βi,j ,α3 + 1).

3. Performance analysis

The comparative results has been shown to compare proposed scheme containing 3DES algorithm with other existing Juang scheme that is using one way hash function only.

TABLE 1 Comparison of performance analysis on basic of different parameters

Algorithm	Block Size (bits)	Security level	Cost	Time consume
3DES	64	High	Less	High
Hash function	128	Less	High	Less

Our approach taking more time than juang approach but the use of 3DES in place of hash function makes our approach more secure. The secure key length size is small than Juang approach so the processing time is less and key is more secure than Juang mechanism. The overall performance of our approach is better than Juang approach with high security and user protection.

4. Computational complexity our proposed approach

To compute the complexity of each algorithm we identify total number of encryption, decryption and hash functions used in scheme. Following are notation used in complexity computation:

- H means One Way Hash Function
- Ey means Symmetric Encryption
- Dy means Symmetric Decryption

Our approach requires four encryptions operations in registration phase, four encryptions and four decryptions in login phase. In Juang approach [8], four hash functions and one encryption in registration phase, only three encryptions, four decryptions and five hash functions needed in login and authentication phase. So we are describing the comparison results of computational complexity in below table.

TABLE 2 Complexity Analysis

Scheme	Registration Phase	Login & Authentication Phase	Total
Juang	3H + 1Ey	5H + 3Ey + 4Dy	8H + 4Ey + 4Dy
Proposed	4Ey	4Ey+4Dy	8Ey+4Dy

5. Conclusion

We estimate the competence of our scheme and Juang's scheme. Juang's scheme is based on the hash function, and our scheme is based on the 3DES cryptosystem so the performance of our approach is better than Juang approach. In our scheme secrete key length is less than Juang scheme. For compute the computation cost of registration phase we can see the Juang approach [8], needs only one hash function and in our scheme one 3DES function needed that makes secrete keys more secure and less memory size required. The computation cost is base on the aggregation of encryption and decryption operations. Our approach requires four encryptions and four decryptions in login phase. In Juang approach [8], only three encryptions, four decryptions and five hash functions needed. We have removed the smart card also saving all the data on sever in form of digital signatures securely which is cost effective and safe from smart card loss attack.

6. Future work

In the future, we can implement this scheme using smart card to prove that our authentication mechanism is secure and discuss the security issue in detail. Moreover, we will build a more secure, efficient and cost effective extends our scheme for multiserver authentication environment.

7. Reference

[1] S. Bellovin and M. Merritt, "Encrypted key exchange: Password-based protocols secure against dictionary attacks," in Proceedings of IEEE Symposium on Research in Security and Privacy, pp. 72-84, 1992.

[2] M. Burrows, M. Abadi, and R. Needham, "A Logic of Authentication," ACM Transactions on Computer Systems, vol. 8, no. 1, pp. 18-36, 1990.

[3] Y. Chang and C. Chang, "Authentication schemes with no verification table," Applied Mathematics and Computation, vol. 167, pp. 820-832, 2005.

[4] W. Diffie and M. Hellman, "New directions in cryptography," IEEE Transactions on Information Theory, vol. IT-22, no. 6, pp. 644-654, 1976.

[5] C. Fan, Y. Chan, and Z. Zhang, "Robust remote authentication scheme with smart cards," Computers & Security, vol. 24, pp. 619-628, 2005.

[6] M. Hwang, C. Lee, and Y. Tang, "A simple remote user authenticationscheme," Mathematical and Computer Modelling, vol. 36, pp. 103-107,2002.

[7] T. Hwang and W. Ku, "Repairable key distribution protocols forinternet environments," IEEE Transactions on Communications, vol. 43, no.5, pp. 1947-1950, 1995.

[8] W. Juang, "Efficient password authenticated key agreement using smart cards," Computers & Security, vol. 23, no. 2, pp. 167-173, 2004.

[9] W. Juang, "Efficient multi-server password authenticated key agreement using smart cards," IEEE Transactions on Consumer Electronics,vol. 50, no.1, pp. 251-255, 2004.

[10] Juang and W. Nien, "Efficient password authenticated keyagreement using bilinear pairings," in the 16th Information SecurityConference, pp. 214-221,Taichung, Taiwan, June 2006.

[11] L. Lamport, "Password authentication with insecure communication,"Communications of the ACM, vol. 24, pp. 770-772, 1981.

[12] A. Lenstra, E. Tromer, A. Shamir, W. Kortsmit, B.Dodson, J. Hughes,and P. Leyland, "Factoring estimates for a 1024-bit RSA modulus," in Advances in Cryptology (Asiacrypt'03), LNCS 2894, pp. 55-74, Springer,New York, 2003.

[13] Lin, M. Hwang, and L. Li, "A new remote user authenticationscheme for multi-server architecture," Future Generation ComputerSystems, vol. 19, pp.13-22, 2003