ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Replay Attack Prevention by Using a Key with Random Number in Kerberos Authentication Protocol

Tanuja Thakur [1], Sachin Dogra[2], Yamini Sood [3]

P.G. Student, Department of Electronics and Communication Engineering, Sri Sai University, Palampur, H.P, India[1]

Assistant Professor, Department of Electronics and Communication Engineering, Sri Sai University, Palampur, H.P, India[2]

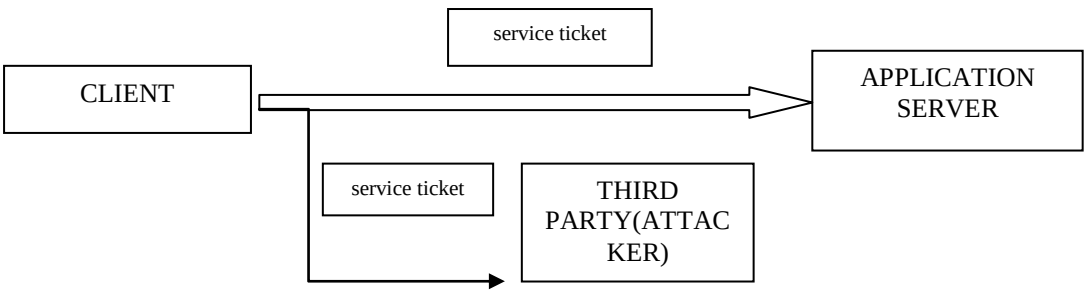
Head of Department, Department of Computer Engineering, Sri Sai University, Palampur, H.P, India[3]

ABSTRACT: Now a day computer networks are growing day by day. With this growth these networks are required to be inter connected with each other which leads to the major usage of internet. Although internet makes accessibility easier for these networks but it decrease data security i.e not acceptable by any user. Hence to increase data security we required strong cryptography in authentication protocol .Kerberos is one of the best window authentication protocols but one of the major drawback of Kerberos is Replay attack. In this attack the intruder replays the same ticket to the application server to use services again and again. Hence we are trying to increase security notations in Kerberos in order to minimize replay attacks. We using a random number generated by TGS. This random number is being used by TGS in a key which is required to encrypt ticket by TGS.

KEYWORDS: Authentication, BAN Logic, Kerberos, Replay attacks , TGS.

I. INTRODUCTION

Authentication Protocol are protocols concerning with security properties e.g. integrity and confidentiality. We have different authentication protocol regarding their usage aspect. Kerberos is a window authentication protocol. It was designed by MIT to provide authentication over an insecure communication network. In Kerberos, authentication is done by a third party i.e both the communicating parties(client and application server) are connected through this party(KDC). Till now kerberos had 5 Versions. First 3 was used internally by MIT where as Kerberos 4 were used outside MIT. But later it was replaced by 5 Version. Kerberos protocol have to be right, but they often are not be because of their vulnerability towards replay attacks. Replay attack is one of the major attack in Kerberos protocol. It is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. It can be easily understood by figures given below. Many of the researchers had worked on mechanisms and modifications of Kerberos in order to make it replay attack resistant.



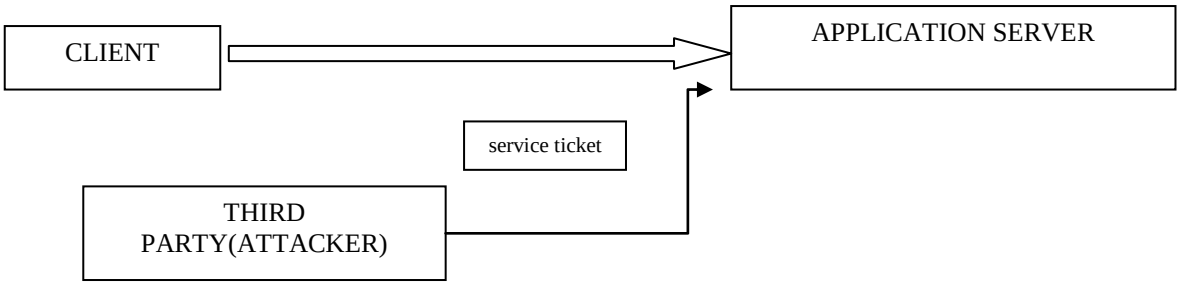
ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Firstly attacker will copy the service ticket when it is given by client to application server in order to get application from the server. Later the same service ticket will be sent by the attacker to get service from application service. Application server will check the service ticket if it is valid then service will be given . Now as attacker is authenticated by the server hence it can use services.



II. RELATED WORK

A brief literature survey regarding attempts made to minimize replay attacks are listed below :

Improvement of Kerberos protocol based on dynamic password and One-time public key

On the basis of the original Kerberos protocol, firstly, the authors have proposed the usage of the Diffie-Hellman algorithm, and put the password in the token, then take the key which has added the dynamic factor as the sharing key between client and authentication server, this improvement can fundamentally solve the password guessing attack. Secondly, the method of the ElGamal algorithm has been presented in this paper. It will generate a new public key in each authentication, and put the new public key as the secret key of the information transmission between client and resource server, this method basically guarantees security of the information transmission. The authors have used the random number, which is associated with the public key, to take the place of the time-stamp to prevent replay attack, it puts the random number and our key together to increase the ability of preventing replay attack. Finally, an analysis of the example of improvement has been carried out. And according to the results of this article the improved Kerberos protocol can ensure the security of the information and password.

Replay attack prevention in Kerberos authentication protocol using triple password

Replay attack and password attacks are serious issues in the Kerberos authentication protocol. Many ideas have been proposed to prevent these attacks but they increase complexity of the total Kerberos environment. In this paper authors present an improved method which prevents replay attacks and password attacks by using Triple password scheme. Three passwords are stored on Authentication Server and Authentication Server sends two passwords to Ticket Granting Server (one for Application Server) by encrypting with the secret key shared between Authentication server and Ticket Granting server. Similarly, Ticket Granting Server sends one password to Application Server by encrypting with the secret key shared between TGS and application server. Meanwhile, Service-Granting-Ticket is transferred to users by encrypting it with the password that TGS just received from AS. It helps to prevent Replay attack.

The use of modal logics in the security protocols analysis

This paper deals just with best known and widely used modal logics. The description of all the logics in detail is beyond the scope of this paper. In general we can say that, the basic constructs for logic verification were outlined with foundation of BAN logic. And, since there are essentially expansions, e.g. SVO logic encompasses BAN itself as well. GNY [5] and AT logic add to and reformulate BAN to better reason about the same class of protocols. Another, VO logic adds rules to reason about key-agreement protocols. The selection of proper modal logic for security protocol verification is the crucial goal in the protocol analysis process. The main contribution of this paper consists in the comparison of various logics, their target area of use and description of specific advantages.

Formal analysis of Kerberos 5

The authors reported on the detailed verification of a substantial portion of the Kerberos 5 protocol specification. Because it targeted a deployed protocol rather than an academic abstraction, this multiyear effort led to the

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

development of new analysis methods in order to manage the inherent complexity. This enabled proving that Kerberos supports the expected authentication and confidentiality properties, and that it is structurally sound; these results rely on a pair of intertwined inductions. The paper also detected a number of innocuous but nonetheless unexpected behaviors, and it clearly described how vulnerable the cross-realm authentication support of Kerberos is to the compromise of remote administrative domains.

III. PROPOSED PROTOCOL

The newly proposed modification to Kerberos protocol, improves the internet service authentication. The existing versions of Kerberos authentication protocol generally focus on the authenticity of the user and the server rather than focusing on the outside attacks on the client-server communication. The attacker present outside the client-server network can try to avail the services of application server by presenting the fake service tickets. The fake service tickets can be generated by using the original service tickets, which the attacker can steal at the time of client-server communication in the network.

Modified Kerberos Protocol

1. $A \rightarrow S$: A, N_a, B
2. $S \rightarrow A$: $\{N_s, B, K_{ab}, (N_s, K_{ab}, key, A)K_{bs}\}K_{as}$
3. Key: $f_{(1)}(RAND \parallel K_{ab})$
4. $A \rightarrow B$: $\{N_s, K_{ab}, key, A\}K_{bs}, \{A, N_a\}K_{ab}$
5. $B \rightarrow A$: $\{N_a, key+1\}K_{ab}$
6. RAND: $f_{(1)}^{-1}(key \parallel K_{ab})$

For the solution of the problem defined we have modified Kerberos. We added a key concatenated with a Random number (RAND) and secret shared key (K_{ab}) using function $f_{(1)}$. As Key will serve as a unique value for client ant service ticket issued to the client. It will uniquely identify a user and will also help in increasing the authenticity of service ticket issued by KDC and also will reduce the replay attack on Kerberos. As if attacker will try to decrypt the key so it's a time consuming to decrypt this key, which will cause a time synchronization problem. In our proposed modification the Kerberos application server requires to decrypt the key using the session key (K_{ab}) and will get a random no (RAND) from it and will requires a database to store these RAND no's and which can be matched against the RAND no. from the replayed ticket and hence increases the authenticity and reduces the replay attack.

Step by Step explanation of the ticket exchange process for modified Kerberos is as follows:
In the initial ticket exchange the client obtain the ticket to start communication with the TGS. TGS is a special server which decreases the risk of exposure of the client's secret key K_c. TGS also make the KDC environment transparent to the client (user). As soon as the client received the TGT to communicate with the TGS it deletes its private (secret) key.
We can differentiate the TGS logically from KDC. But TGS take the help of the KDC database and run on the same machine on which the KDC runs.
*Step 1: [Client to KDC (TGS)].*The client starts communicating with TGS by providing the KDC Host, its name (identity or Principal), timestamp (N_a).
$A \rightarrow S$: A, N_a, B

*Step 2: [KDC (TGS) to Client].*The KDC (TGS) replies to the client the session key and timestamp (N_s) encrypted with (K_{as}). It also includes the TGT encrypted with the secret key of TGS ant it contains the Key: $f_{(1)}(RAND \parallel K_{ab})$.
$S \rightarrow A$: $\{N_s, B, K_{ab}, (N_s, K_{ab}, key, A)K_{bs}\}K_{as}$
Now the client has to include the authenticator who can verify the identity of the client to TGS. The authenticator provides the information of the client i.e. the username, timestamp. It is encrypted with the session key of the client and the TGS.
Authenticator = $A = \{C, timestamp\}K_{ab}$
Now as the TGS received the request from the client that what service it needs. The TGS has to verify the identity of the

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

client with the help of the TGT, Authenticator, and the database of the KDC. TGS decrypts the authenticator and the TGT and check whether the client is the genuine user who can use the specified service or not. As the client get authenticated, the TGS generates the service ticket. The ticket contains the username, service name, timestamp, IPlist, session key (K_{ab}), lifetime of the ticket. The client cannot decrypt this ticket because this is encrypted with the secret key which is shared between the KDC environment and the application server.

Step 3: [Client to Application Server]. The client now starts communicating with the application server. The client sends the authenticator and the ticket to the application server. The client and the server now verify each other's identity to themselves.

$$A \rightarrow B: \{N_s, K_{ab}, key, A\}K_{bs}, \{A, N_a\}K_{ab}$$
$$B \rightarrow A: \{N_a, key + 1\}K_{ab}$$

RAND: $f_{(1)}^{-1}(\text{key} \parallel K_{ab})$

The key that is concatenated with RAND (random no) and session key (K_{ab}) application server will maintain the table for random no that is obtained by decrypting the key (RAND: $f_{(1)}^{-1}(\text{key} \parallel K_{ab})$ and can discard the tickets with the same RAND no in it and can reduce the replaying of ticket in Kerberos environment.

Step 4: Now the communication has been started between the client and the application server. To start exchanging messages the client and the server share a common session key (K_{ab}) to encrypt these messages which are sent over the network.

IV. PROOF OF MODIFIED KERBEROS PROTOCOL

In this section, we provide a formal proof to our Proposed Protocol. We have used BAN tool through which we will be proving the validity of our proposed modification in the Kerberos authentication protocol. Our main focus of this proof is on the safe delivery of encrypted message from. In order to achieve this we used BAN to formally verify the safe delivery of our encrypted packet to the server. BAN is a very important tool to evaluate communication protocols. The following table presents the assumptions which have been taken to prove the proposed protocol.

Table : Extracted Assumptions expressed by logic of believe

$S \mid \equiv A \xleftarrow{Kas} S$
$A \mid \equiv A \xleftarrow{Kas} S$
$B \mid \equiv B \xleftarrow{Kbs} S$
$S \mid \equiv B \xleftarrow{Kbs} S$
$S \mid \equiv \#(N_a)$
$A \mid \equiv \#(N_s)$
$B \mid \equiv \#(N_a)$
$A \mid \equiv \#(N_b)$

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

B $\mid\equiv$ #(N_S)
A $\mid\equiv$ S⇒K_{ab}
A $\mid\equiv$ S⇒Key
B $\mid\equiv$ S⇒Key
B $\mid\equiv$ S⇒K_{ab}
Key : $f_{(1)}$(RAND ‖ K_{ab})
RAND : $f_{(1)}^{-1}$(key ‖ K_{ab})

Proof Using BAN Logic:

To have a secure connection, BAN should have three main conditions i.e. message is secure if it contain; time stamp, encrypted key and should have the legitimate RAND (Random no.). The Proof is as follows:

Firstly we will prove that Client i.e. A believes the key K_{ab} and also that A and B shares the key K_{ab} for this we will mainly use the jurisdiction rule of BAN logic.

$$\frac{A\mid\equiv\ A\overset{K_{as}}{\longleftrightarrow}S, A\lhd\{N_s, K_{ab}, B, \{N_s, K_{ab}\ key\ , A\}K_{as}}{\mathrm{A}\mid\equiv \mathrm{S}\sim\{N_S, K_{ab}, B, \{N_S, K_{ab}, key, A\}K_{bs}\}K_{as}} \quad (1)$$

$$\frac{A\mid\equiv \#(N_S)}{\mathrm{A}\mid\equiv \#\{N_S, K_{ab}, B, \{N_S, K_{ab}, key, A\}K_{bs}\}K_{as}} \quad (2)$$

$$\frac{(1),(2)}{\mathrm{A}\mid\equiv \mathrm{S}\mid\equiv \{N_S, K_{ab}, B, \{N_S, K_{ab}, key, A\}K_{bs}\}K_{as}} \quad (3)$$

$$\frac{(3), A\mid\equiv S\Rightarrow A\overset{K_{ab}}{\longleftrightarrow}B}{\mathrm{A}\mid\equiv A\overset{K_{ab}}{\longleftrightarrow}B}\ (\text{Using jurisdiction rule}) \quad (4)$$

Now as B is required to believe the session key to access the key, it first needs to believe the Ticket. Proof for this is:

$$\frac{B\mid\equiv \#(N_S)}{\mathrm{B}\mid\equiv \#\{N_S, key, K_{ab}, A\}K_{bs}} \quad (5)$$

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

$$\frac{B| \equiv \ B \overset{K_{bs}}{\longleftrightarrow} S, A \lhd \{N_s, key, K_{ab}, A\}K_{bs}}{\text{B}| \equiv \text{S}\sim\{N_S, key, K_{ab}, A, \}K_{bs}} \quad \text{(6)}$$

$$\frac{(5), (6)}{\text{B}|\equiv \text{S} \mid \equiv \{N_S, key, K_{ab}, A, \}K_{bs}} \quad \text{(7)}$$

Therefore B believes A.

$$\frac{A| \equiv A \overset{K_{ab}}{\longleftrightarrow} B, A \lhd < key > K_{ab}}{\text{A}| \equiv \text{B} \sim \text{key}} \quad \text{(8)}$$

As in equation (8) K_{ab} is shared secrete key and Key is concatenated using K_{ab} so A believes in key we have generated and can use it to find the RAND no and verify the ticket received and hence reduces the replay attack and increases the Authentication.
As shown for more authentication, we can add the key that is concatenate nation with RAND (random no) and session key K_{ab} as it will reduce the replay attack as Application server can maintain the random no table by decrypting the key and can discard the tickets with the same RAND no in it.

V. CONCLUSION

In this paper we have proposed a modification to Kerberos, which provides a protection against replay attack. Security is necessary in all aspects of fields. Kerberos provides third party authentication but many replay attacks occurred on Kerberos. The approach used in this thesis attempts to prevent replay attack by using random number generation and checking. When a ticket has been generated by the KDC-Authentication server, it introduce a random number in the ticket. This random number will only be decrypted by the application server. The application server store the random number for each user and later check this random number for equality with the new user's random number. If the random number will be same, then the user requesting the service will be an attacker. The application server detects a replay of previous ticket and simply reject the request made by the attacker.

REFERENCES

[1] John T. Kohl, B. Clifford Neuman, and Theodore Y. T'so, "The Evolution of the Kerberos Authentication System. In Distributed Open Systems", IEEE Computer Society Press, pp. 78-94, 1994.
[2] Tom Yu, Sam Hartman, and Ken Raeburn. "The Perils of Unauthenticated Encryption: Kerberos Version 4". In Proceedings of the Network and Distributed System Security Symposium. The Internet Society, February 2004.
[3] B. Clifford Neuman and Theodore Ts'o. "Kerberos: An Authentication Service for Computer Networks", IEEE Communications, vol. 32, no. 9, pp. 33-38, September 1994.
[4] Abdelmajid, N.T., Hossain M.A., Shepherd, S., Mahmoud, K, "Improved Kerberos Security Protocol Evaluation using Modified BAN Logic", IEEE Computer and Information Technology (CIT), 2010.
[5] Bellovin S. M., M. Merritt, "Limitations of the Kerberos Authentication System" Computer Communication Review, vol. 20, pp. 119-132, 1991.
[6] Clark John and Jeremy Jacob, "A survey of authentication protocol literature", 1997.
[7] Neuman C., T. Yu, S. Hartman, K. Raeburn, "The Kerberos Network Authentication System" (RFC4120) July 2005.
[8] http://web.mit.edu/kerberos/papers.html. 12th Nov., 2014, 3:00 PM.
[9] http://kerberos.org/software/tutorial.html. 20th Nov., 2014, 11:00 AM.
[10] Abadi, M., Tuttle, N. "A Semantic for a Logic of Authentication", In: Proceedings of the ACM Symposium on Principles of Distributed Computing, pp. 201-216, 2001.
[11] Burrows, M., Abadi, M. and Needham, R. "A Logic of Authentication". ACM Trans. Computer Systems, vol. 8, pp. 18-36,February 1990.
[12] http://en.wikipedia.org/wiki/Authentication_protocols. 12th Sep., 2014, 10:00 AM.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

[13] N. Agray, W. van der Hoek, and E. P. de Vink. "On ban logics for industrial security protocols. In B. Dunin-Keplicz and E. Nawarecki, editors, From Theory to Practice in Multi-Agent Systems, Second International Workshop of Central and Eastern Europe on Multi-Agent Systems (CEEMAS2001) , volume 2296 of Lecture Notes in Computer Science , pages 29–36. Springer, 2001.
[14] Yun-yun Du, Hong-yun Ning, Ping Yang, Yan-xia Cui, "Improvement of Kerberos protocol based on dynamic password and One-time public key", in 10th International Conference on Natural Computation (ICNC), IEEE,pp. 1020 – 1025, 2014.
[15] Jianhua Huang, Xi He. "Improvement of Kerberos Agreement Based onDynamic Password System". Computer Security, (2): pp.66-69, 2009.
[16] Tianxu Huang, Haiyan Wang. "Analysis and an Improved Scheme ofKerberos System". Computer Applications, 23(3): pp.13-15, 2003
[17] Ian Downard. "Public-key Cryptography Extensions into Kerberos". EEEPOTENTIALS, (1), 2001.
[18] Xuelian Cai. "Improve Kerberos Protocol Based Challenge / ResponseTechnology".Computer & Digital Engineering, 41(9): pp.1489-1497, 2013.
[19] Chundong Wang, Chaoran Feng. "Security Analysis and Improvement for Kerberos Based on Dynamic Password and Diffile-Hellman Algorithm", International Conference on Emerging Intelligent Data andWeb Technologies, pp. 257-260, September 2013.
[20] Weidong Tang, Weimin Li. "Improving Kerberos protocol with ElGamalalgorithm".Computer Engineering and Design, 28(2): pp. 343-34, 2007.
[21] Feng Chen, Zhengquan Xu, Yanyan Xu. "Improving Kerberos.ComputerApplications", 27(12): pp.116-120, 2007.
[22] Y. Kirsal, and O. Gemikonakli, "Further Improvements to the KerberosTimed Authentication Protocol," International Conference onTelecommunications and Networking, University Bridgeport,Bridgeport, May 2007.
[23] Bellovin S M, Merritt M. "Limitations of the Kerberosauthentication system". Proceedings of the Winter 1991 UsenixConference. 1991.
[24] Riqing Chong. "Improvement and Application of Kerberos Protocol Based On ECC and USBKEY". Shanghai: shanghai normal university,2010: pp.1-46.
[25] El-Emam, Eman, Magdy Koutb, Hamdy Kelash, and Osama Farag Allah. "An optimized Kerberos authentication protocol." InInternational Conference on Computer Engineering & Systems (ICCES), pp. 508-513. IEEE, 2009.
[26] Dua, Gagan, Nitin Gautam, Dharmendar Sharma, and Ankit Arora. "Replay attack prevention in Kerberos authentication protocol using triple password." arXiv preprint arXiv:1304.3550 (2013).
[27] William Stallings, "Cryptography and network security principles andpractices," 4th ed., Pearson Prentice Hall, pp. 415, 2006.
[28] D. Hu, and Z. Du, "An Improved Kerberos Protocol Based on Fast RSAAlgorithm," IEEE International Conference on Information Theory andInformation Security (ICITIS), pp.274-278, December 2010.
[29] OPavel and TRoman. "The Use of Modal Logics in the Security Protocols Analysis". In: Proceedings of the 12th ConferenceSTUDENT EEICT 2006,pp. 395-399, ISBN 80-214-3163-6, 2006.
[30] F Butler, I Cervesato, A DJaggard, AScedrov, & C Walstad."Formal analysis of Kerberos 5". Theoretical Computer Science, vol. 367, no. 1, pp. 57-87, 2006.