Analysis of Different Authentication Techniques using Kerberos Protocol

Romendrapal Singh Rathore
M.Tech. Scholar,
Department of Computer Science & Engineering,
Mewar University,Gangrar, Chitorgarh
rjsingh.r@gmail.com

B. L. Pal
Assistant Professor,
Department of Computer Science & Engineering
Mewar University,Gangrar, Chitorgarh
contact2bl@rediffmail.com

***Abstract* — Kerberos is broadly used as a network authentication protocol that is being considered for reliability. lots of works have evaluated its protection, identifying fault and suggesting fasten, so it helps in protocol's development. a number of results present victorious formal -methods based authentication of a important segment of the current version 5, and some still entail security in the computational progression . these results to clasp , encryption in Kerberos should gratify strong cryptographic security concept[5]. We take a close look at various Kerberos's authentication techniques This thesis presents a set of characteristics of various techniques ,their pros and cons . These can be used for those who need to choose an infrastructure , wants to know various methods for authentication and a particular application or knowing the Kerberos widely. The characteristics are used to present an analysis of current infrastructure systems. The criteria exposes the strengths and weaknesses of each system. The characteristics presented here are intended to enhance rather than to confine development in the field.**

Keywords: Hmac, Biometric, Modified kerberos 5 SHA-512, RSA, AES , Blum Blum Shub.

I. INTRODUCTION

Authentication is a fundamental process in securing information resources since it establishes the identity of the system or user wishing to gain access to the resources. Authentication is of major importance to the security of open networks. In open networks, the identities of communicating parties cannot be assumed, but must be authenticated and verified. Traditionally strong forms of authentication are not available in most operating system networking software. Instead, reserved ports or passwords are used, each of which might be easily compromised. Tools to sniff passwords off of the network are in common used by malicious hackers. Thus, applications which send an unencrypted password over the network are extremely vulnerable. Worse yet, client/server applications rely on the client program to be honest about the identity of the user who is using it. Other applications rely on the client to restrict its activities to those, who is allowed to do, with no other enforcement by the server. One of the most basic authentication protocols is a password challenge – a user is asked to demonstrate knowledge of a pre-established password to prove his or her identity. Simple password security is a weak mechanism subject to several types of attacks. To meet the challenge of protecting information and computing systems, researchers and developers have focused attention on authentication protocols. Many authentication protocols have been developed to try to improve on basic password security. [14] describe both the weaknesses of password authentication and more sophisticated and secure protocols such as Kerberos. An authentication protocol allows one or more participants to verify
(i) the identity of the other parties on the basis of at least one of the following: something known (e.g., a shared key), something possessed (e.g., smartcard), or something inherent (e.g., biometrics) and (ii) the active presence of the other during the process. The verification process should not allow the verifier to reuse an authentication exchange with the goal of pretend to be the entity. At the same time, the process must provide the verifier with enough confidence that an attacker is not trying to impersonate a legitimate entity. Different authentication protocols might be categorized based on the following properties: type of cryptography (symmetric vs. asymmetric), reciprocity of authentication (mutual vs. one-way), key exchange, computational and communication efficiency, real-time involvement of a third party (on-line vs. off-line), nature of trust required from a third party, nature of security guarantees, and storage of secrets.[13]

II. THE BASIC OPERATION OF KERBEROS

Kerberos is an authentication protocol to verify a client's identity to allow logging on to a server and to encrypting their communications through secret-key cryptography over an insecure network. It resolves the key distribution problems between client and server with tickets. Clients can log on to a server in two steps. First, they get authenticated at the Authentication server (AS), and get a Ticket- Granting Ticket (TGT). The client presents the TGT to the Ticket-Granting Server (TGS) and gets a real Ticket for a specific server.

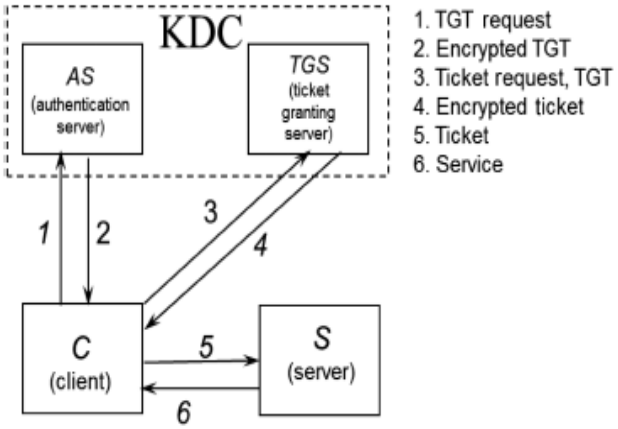

Figure 1. Kerberos Sysytem [12]

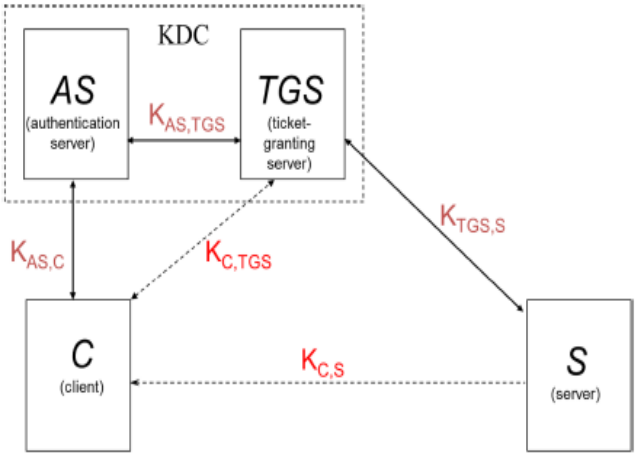

Figure 2. Keys in kerberos [12]

With this ticket, clients can log onto an application server. It is shown in Figure 1. Using the Tickets, Kerberos never sends a password over the network, so the password is protected against eavesdropping or replay attacks. A ticket contains the authentication information of the ticket holder, and is encrypted with the key of the final recipient. so a client holding a ticket has no knowledge of the ticket's content nor can they modify it. As it is encrypted, it can be safely sent across the networks. The types of keys are described in Figure 2. The shared keys, $K_{AS, TGS}$, $K_{AS, C}$, $K_{TGS , S}$ are predefined during the registration process, and $K_{C,TGS}$, $K_{C,S}$ are dynamically generated during authentication.[12]

III. KERBEROS WITH HMAC SYMMETRIC

In this System, All the encryptions could be done using the Hash based message authentication code and also increased the timestamp since transfer such as remote procedure call (RPC) and HTTP rely on the max token size. This algorithm is specified for an random Approved cryptographic hash function, H. With minor modifications, an HMAC implementation can easily replace one hash function, H, with another hash function, H'. Conceptually, the intermediate results of the compression function on the B-byte blocks K0i and K0o can be precomputed once, at the time of generation of the key K, or before its first use. These intermediate results can be stored and then used to initialize H, each time that a message needs to be authenticated using the same key. For each authenticated message using the key K, this method saves the application of the hash function of H on two B-byte blocks i.e. K1i and K1o. This reduction is more significant for authenticating short streams of data. These stored intermediate values shall be treated and protected in the same manner as secret keys[2]

A. Advantages

1. when we use this system , only the authorized persons, who have the decryption algorithm, may recover the original text from the encrypted text. Any other impostor, who wants to perform off-line attack, will not be able to do so because this algorithm protects the message in a much stronger way using variable block cipher with cipher block chaining mode. It is very difficult to decrypt the message even with the algorithm available, Because this algorithm gives an extra layer of protection with a password. The chances of password guessing approach for any intruder are invalidate because this system does not store the password of the client anywhere in the hard disk. So no attempt can be made to find it out.
2. This system can be integrating with the smart card technology and some of the Kerberos systems problems may be overcome. The main concept for improving the security of Kerberos by authenticating the client directly at the beginning and prior to the yielding of the initial ticket, so that one user cannot use the ticket of other and , the use of smart card also have need of user logging into the system not only requied a password, but also to be in ownership of a token. Biometric technology can also be used to enhance security with this system in the smart card. Biometrics information of the cardholder can be placed on the card, so that the smart card can corporate with biometrics scanner to authenticate the user directly at the first stage of processing. Before granting the initial ticket, this authentication could take place, to avoid any intruder to be pretend as the cardholder. This system, can also combines the techniques of cryptography and steganography and may be applied to embed the biometrics information of the cardholder into his photograph in the smart card. this algorithm provides a strong protection to the information against attacks, the biometrics details could not be easily trapped by any intruder [2].

IV. KERBEROS WITH BIOMETRIC AUTHENTICATION

This technique focus on encryption and biometrics traits with the registration server, authentication server and the token granting server. This method target on strong cryptography for user's original data with the registration server, noticeably the authentication should be non-reputable so potect from user side attacks and replay attacks .It also take care in the case where the key is compromised. The high performance of this system is achieved by the token granting system . Kerberos is a successful authentication protocol. it is more secure by integrating it with a cryptographic biometric authentication system Whatever a user want to do some thing. The user's actual biometric data accessible and offered to the registration server. The encryption and biometrics traits with the registration server, authentication server and the token granting server contribution in making a power full system. It can protect against approximately all type of possible threats . this system is used to protect a) Biometric template security b) privacy of the user c) faith between client and authenticating server and d) network security related issues [15].RSA technique is used in this system. This system process is combination of three steps 1) Registration 2) Authentication 3) Ticket Granting. In this method focus on the design of a classifier that helps to improve the performance of biometrics and used the randomization scheme for this purpose. [3]

A. Advantages

1. In this system the transaction will be highly secured in the sense that Authentication server creates a ticket which is further encrypted using the Asymmetric key shared by the server and authentication Server. This ticket then sends back to client. Because the ticket is encrypted, it cannot be altered by client or by an opponent..
2. The another advantage of this system is that it is able to achieve classification of a strongly encrypted the work which is extremely secure under a variety of attacks and it can be used in various biometric traits.[3]

V. MODIFIED KERBEROS 5

In this technique Triple-DES in CBC mode as an encryption algorithm, SHA-256 for hashing, and Blum Blum Shub for random number generation are used . In this method, the long-term secret key of the network principle will be independent of the principle's password. means, the KDC will save a profile for every instance in the realm that it manages. The type of the profile data contents may be audio, video, image, or simply text data. The KDC database may have mixed types of profile. The network principle may be a client or a server. Every principle in the network is registered in the KDC database by the principle ID. Then the KDC maps this ID to the proper profile where the profile is named with the principle's ID that belongs to that profile. For generating the principle's secret key, a hashing algorithm is used firstly and then encrypt the output digest. In this system the lifetime of the secret key using the current KDC system time that is appended to the principle's outline every predefined period so if there is a change the input to the hashing function, and as a result, the output of the hashing function and the secret key will also be changed. In this system , the lifetime of the long-term principle's secret key is 1 week, the lifetime of the TGS ticket is 1 day, the lifetime of the application server ticket is 8 hours, and the lifetime of the authenticator is 5 minutes. [4]
This method modified to the KDC database for enhancing the performance of the protocol because the princiiple's long-term secret-key will be independent of the user password. so, this Kerberos version is less vulnerable to password guessing attacks. This system is tested or implemented on a small LAN.[4]

VI. SIGNIFICANT ANALYSIS

A. pros

1. In HMAC based method only the authorized persons, who have the decryption algorithm, can decrypt the encrypted text Any other intruder, who wants to perform off-line attack, will not be able to break the sysem because this algorithm protects the message in a much stronger way using variable block cipher with cipher block chaining mode. In Biometric authentication the authentication is done using the encrypted data set. Hence no identity of the client or the server is revealed to each other .In Modified KERBEROS 5 the long-term secret key of the network principle will be independent of the principle's password. means, the KDC will save a profile for every instance in the realm that it manages.

2. **2)** HMAC algorithm gives an extra layer of protection with a password so the chances of password guessing approach for any intruder are nullified because this system does not store the password of the client anywhere in the hard disk. Hence no attempt can be made to find it out . In biometric The computations are carried out in the randomized Manner hence no imposter can gain the biometric of the client in plain. Or one user cannot have the ticket of another. the use of smart card requires user logging into the system not only by recalling a password, but also to be in possession of a token.In modified kerberos system the lifetime of the secret key use the current KDC system time that is appended to the principle's side view every predefined period . If there is a change the input to the hashing

function, the output of the hashing function and the secret key will change too.

3. The HMAC algorithm provides a robust protection to the information against attacks. Biometric System provides verifiable defense against replay and client-side attacks . modified Kerberos version is no longer vulnerable to password guessing attacks This method modified to the KDC database for enhancing the performance of the protocol.

B. Cons

1. Some disadvantages have been found with HMAC , like the problem of symmetric key exchanged is quite serious and cannot be solved easily , HMAC cannot be be used if the number of receivers is greater than one because a symmetric key is supposed to be shared only by two parties one sender and one receiver, How does a receiver know that the message was prepared and sent by the sender and not by one of the other receivers ? , there is also a possibility of generation of forged message.

2. Modified kerberos 5 requires to extend implementation in cross-realm operations . Triple DES is highly secure but also has the drawback of requiring 168 bits for the key which can be slightly difficult to have in practical situations .

3. For SHA-256, there is a way to reduce the storage requirement by computing the sixty four constants which are defined to be the first 32 bits of the fractional parts of the cube roots of the first sixty four prime numbers. One way to compute these cube roots is to use Newton-Raphson iterations, which, on 64 bit architectures, quickly converge to provide the first 32 bits of the result.[17]

4. Blum Blum Shub generator has disadvantage that it is computationally intensive. It takes n^2 steps to generate one random bit of the bit-stream. But not a serious draw back if it is used for moderately infrequent purposes, such as generating session keys.[18]

VII. CONCLUSIONS AND PROPOSED WORK

This paper show a comparatively analysis of three authentication techniques using kerberos . In this paper different authentication aspect like hash based, Biometric, TRIPLE des WITH SHA-256 Algorithm are studied.. In this paper the advantages and disadvantages of each techniques has been discussed. this paper focus on enhancing the system performance , reducing the vulnerability and also protect from offline , client side attack with using various techniques.

In future we proposed a system that will combine the characteristics of RSA, SHA- 512 or AES with biometric traits. RSA is primarily used for encrypting a message and RSA can also be used for performing digital signature over a message. SHA-512 algorithm takes a message of length 2128 bits and produces a message digest of size 512 bits . SHA-512 is itself modeled on MD5. It takes 80 steps . the SHA-512 constants are defined to be the first 64 bits of the fractional part of the cube roots of the first eighty primes. Performing simple numerical iterations on 64 bit architecture does not give the required precision as requires in SHA-256 .SHA-512 algorithm delivers a 50% performance improvement over similar implementations of SHA-256. the storage costs for implementing SHA-512 can be reduced by adding a small amount of one-off computation to compute the SHA-512 constants - which will be useful for constrained implementation environment [17] , and with these features it makes the message digest more complex and difficult to break. Montgomery Multiplication has a number of attractive functions in Cryptography and building a Quadratic Residue Cipher, based on BBS that uses Montgomery Multiplication (MM), when BBS and MM put together , they can help us to build a PRNG that is y secure , efficient and fast [18]. AES may be used because it has symmetric and parallel structure – which gives the implementers of the algorithm a lot of flexibility and also stand up well against cryptanalysis attacks ,adapted to modern processors – this algorithm works well with modern processors , It suited to smart cards – the algorithm can work well with smart cards. AES operations involve entire byte and not individual bits of a byte so this provides for more optimized hardware and software implementations of the algorithm .

REFERENCE

[1] Alan H. Harbitter, Daniel A. Menascé . *Performance of Public-Key-Enabled Kerberos Authentication in Large Networks*

[2] R. Kogila. *An Enhanced Authentication Scheme Using Kerberos with Hash-Based Message Authentication Code.* IJCSMC, Vol. 2, Issue. 7, July 2013, pg.350 – 355

[3] Shashidhar M S, Suresha D . *Implementation of Secure Biometric Authentication Using Kerberos Protocol* International Journal of Advanced Research in Computer Science and Software Engineering Volume 3, Issue 3, March 2013.

[4] Eman El-Emam, Magdy Koutb , Hamdy Kelash , and Osama Farag Allah *An Authentication Protocol Based on Kerberos International Journal of Network Security, Vol.12, No.3, PP.159{170, May 2011*

[5] Alexandra Boldyreva ,Virendra Kumar. *Extended Abstract: Provable-Security Analysis of Authenticated Encryption in Kerberos.* Georgia Institute of Technology, School of Computer Science, 266 Ferst Drive Atlanta, GA 30332-0765 USA.

[6] John T. Kohl , B. Clifford Neuman . *The Evolution of the Kerberos Authentication Service.* Information Sciences Institute University of Southern California.

[7] Aruna Kumari , Shakti Mishra , D.S. Kushwaha. *A New Collaborative Trust Enhanced Security Model Distributed System.* 2010 International Journal of Computer Applications (0975 - 8887) Volume 1 – No. 26.

[8] Manoj Kumar , Nikhil Agrawal**.** *Analysis of Different Security Issues and Attacks in Distributed System A-Review*. International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 4, April 2013**.**

[9] Marvin A. Sirbu , John Chung-I Chuang. *Distributed Authentication in Kerberos Using Public Key Cryptography*. Carnegie Mellon University, Pittsburgh, Pennsylvania 15213.

[10] Thomas Y.C. Woo Wireless Networking Research Department Bell Laboratories Lucent Technologies**,** Simon S. Lam Department of Computer Sciences The University of Texas at Austin Austin, Texas 78712-1188**.** *Authentication for Distributed Systems.*

[11] Phillip L. Hellewell, Timothy W. van der Horst, and Kent E. Seamons Internet Security Research Lab Brigham Young University Provo, UT, USA. *Extensible Pre-Authentication in Kerberos.*

[12] Jung Eun Kim, Yoohwan Kim. *A Secure Credit Card Transaction Method Based on Kerberos*Journal of Computing Science and Engineering Vol. 5, No. 1, March 2011. pp. 51-70.

[13] Olga Kornievskaia . *Symmetric and Asymmetric Authentication:A Study of Symmetric and Complementary Properties and Their E_ect on Interoperability and Scalability in Distributed Systems.*

[14] Kaufman, C., R.Perlman, and M Speciner, *Network Security, PrivateCommunication in a Public World. 1995*, Englewood Cliffs, New Jersey; PTR Prentice Hall.

[15] R. Rivest, A. Shamir, and L. Adelman, *" A method for obtaining digital signatures and public key cryptosystems"*, Commun ACM, Vol 21, no 2 , pp. 120-126, 1978.

[16] B. Clifford Neuman and Theodore Ts'o.*" Kerberos: An Authentication Service for Computer Netwotks"*, IEEE Communications Magazine, Volume 32, Number 9, pages 33-38, September 1994..

[17] Shay Gueron 1, 2, Simon Johnson 3, Jesse Walker4 1 Department of Mathematics, University of Haifa, Israel 2 Mobility Group, Intel Corporation, Israel Development Center, Haifa, Israel 3 Intel Architecture Group, Intel Corporation, USA 4 Security Research Lab, Intel Labs, Intel Corporation, USA *" SHA-512/256".*

[18] M.G.Parker, A.H.Kemp, and S.J.Shepherd, *"Fast blum-blum-shub sequence generation using montgomery multiplication*," vol. 147, 2000, pp. 252–254.

[19] Atul Kahate "*Cryptography and Network Security*" Second Edition . Tata McGraw Hill Education Private Limited, New Delhi.