Review of Network Authentication Based on Kerberos Protocol

Turkan Ahmed Khaleel

Dep. of Computer Engineering

College of Engineering

University of Mosul, Iraq

(received in 14\10\2019, accepted in 26\12\2019)

Abstract: Today, one of the most common things in networks and resource sharing is the need for distributed data systems that include many servers which can be distributed or centralized as well as many customers who are satisfied with the services provided. In this environment, network connections have been supported by multiple devices and terminals to help for all broad sharing medium. Therefore, both user information and server resources need to be protected. Authentication is a crucial solution to achieve the required security and protection of services from denial. Without knowing the identity of the client who are requesting an operation, it is difficult to decide whether to allow the operation or refusal. Using of the classic authentication protocol can be considered as unsuitable idea especially with distributed systems architecture and networks. Attackers can monitor traffic, find out and grab passwords from their rightful owners. For this reason, the need for strong authentication methods has become quite significant to disallow attackers from detecting passwords. Depending Kerberos authentication system is well suited for authenticating users in facing such challenges.

Keywords: Kerberos Protocol, Authentication, Computer Networks, Key Distribution Centre (KDC).

مراجعة مصداقية الشبكة بناءً على بروتوكول كيربيروس

الملخص: اليوم ، أحد أكثر الأمور شيوعًا في الشبكات ومشاركة الموارد هي الحاجة إلى وجود نظم بيانات موزعة تتضمن العديد من الخوادم الموزعة أو المركزية التي تقنع العملاء بخدماتها المقدمة. في هذه البيئة ، يتم دعم اتصالات الشبكة عن طريق أجهزة متعددة ومحطات توفر جميع وسائل المشاركة الواسعة. وبالتالي ، نحن بحاجة إلى حماية معلومات المستخدم وموارد الخادم. المصادقة ضرورية هنا لأمن وحماية الخدمات من الحرمان. دون معرفة هوية العميل الذي يطلب العملية، التي قد يكون من الصعب تحديد ما إذا كان مخول ام لا . يعد استخدام بروتوكول المصادقة الكلاسيكية فكرة غير مناسبة وخاصة عند استخدامها في هندسة النظم والشبكات الموزعة. قد يمكن للمهاجمين مراقبة حركة المرور، ومعرفة كلمات المرور والاستيلاء عليها من أصحابها الشرعيين. لهذا السبب، نحتاج الى أساليب مصادقة قوية لا تسمح للمهاجمين باكتشاف كلمات المرور. نظام مصادقة كيربيروس مناسب تمامًا لتوفير المصادقة للمستخدمين في مثل هذه البيئات.

الكلمات المفتاحية: بروتوكول كيربيروس، بروتوكول المصادقة ، شبكات الكمبيوتر، أمن الشبكات، مركز توزيع المفاتيح.

1. Introduction

Modern distributed systems are providing many services for their users. Following these systems require the ability to accurately determine the user's sending request. In traditional systems, the user identity is verified by checking their password entered during login stage to determine which processes can be executed. Authentication is the term refers to the process of User identity verification. Password-based authentication is not quite sufficient to depend on communications networks. Passwords sent over network can be simply intercepted and subsequently used by hackers and impersonators. Although this issue has been long discovered, the intruders' experience is increased as the range of online communication and participation have increased [1]. In the context of the security of computer networks and distributed systems, authentication is the process of ensuring the identity of the users. It is one of the five most important pillars to assure security and privacy. Other four technology elements are availability, confidentiality, integrity and non-repudiation. The authentication process begins when the user needs to access their information and resources while the system first needs to verify the identity. A traditional method of authentication is the process of logging on to a particular site. For example, users enter their user names and passwords for authentication purposes. The central authority responsible for this process of verifying this login, which must be assigned to each user, authenticates access. However, there is always the possibility of hacking this type of authentication by hackers. The most effective style of authentication, bio metrics, depends on the user's presence and biological composition such as the tissue layer or fingerprint. This technology adds more complex for hackers to interrupt into computer systems [2]. Authentication means identity verification which is the basis for any secure communication. Its importance focuses on not disclosing any information that is required to keep it strictly confidential. Authentication usually requires the provision of credentials to prove the true user identity. It can be done either by a server, which is preferable, a client or a third party. Generally, there are different authentication protocols allowing users to send or receive information according to protocols supported between them. In the field of network security, there are many authentication protocols such as public key authentication, key fragmentation, Kerberos, etc. along with the possible attacks on those methods. This paper demonstrates in detail the Kerberos as an

authentication protocol designed to protect the security of users by verifying their identity and protect any distributed system that seeks to achieve important objectives such as integrity, confidentiality, etc. Kerberos is a protocol that provides security for users from stealing their information during sent over the network system from one place to another. Additionally, it provides distributed authentication services that allow the client to act on behalf of a user to verify the identity of the application server. This process occurs without sending its data over the network because it may allow attackers to impersonate the user later [4]. The author in this paper provides a general study and brief overview of the Kerberos authentication model.

The main purpose of using Kerberos is to authenticate among users and services. Despite of the existence researches dealing with the Kerberos protocol, this study was distinguished from others by focusing on the concept of the work of this protocol in addition to present the steps of its representation and its real application with the most important challenges.

The traditional password-based authentication systems are suffering from password inhalation over unreliable networks. For this reason, there was a need to address the limitations of traditional authentication. Kerberos is an authentication system developed at MIT that improves these shortcomings by allowing an auditor (server) to authenticate a parent (client) without having to send his or her password over the network [5].

The Key Distribution Center (KDC) is one of the most important parts of the Kerberos system. In general, the protocol consists of three major parts as shown in Fig.1:

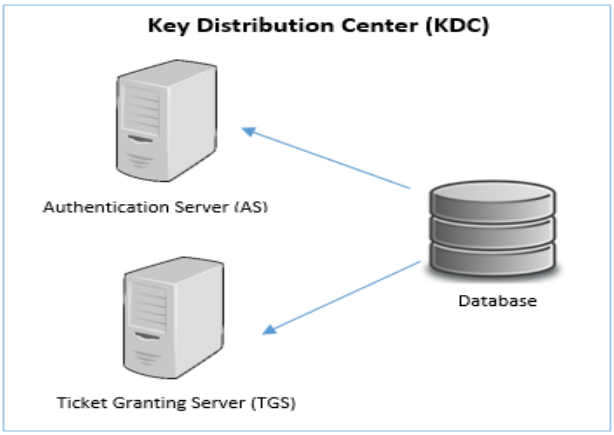

Fig. 1. Kerberos system

- Database to manage all tasks and associated encryption keys.
- Authentication Server (AS), which is responsible for issuing and giving an encrypted ticket (also known as TGT) to users who want to log on to the Kerberos system.
- Ticket Granting Server (TGS), which issues individual service tickets to users.

The ticket is an encrypted data structure that is understandable by the KDC and provides unique encryption keys for each session, it performs two objectives: [6]

- Confirm the identity of the real participants.
- A mission to create a short-lived encryption key that both parties can share for a secure connection.

The Kerberos protocol g enerally consists of two basic phases as shown in Fig.2.

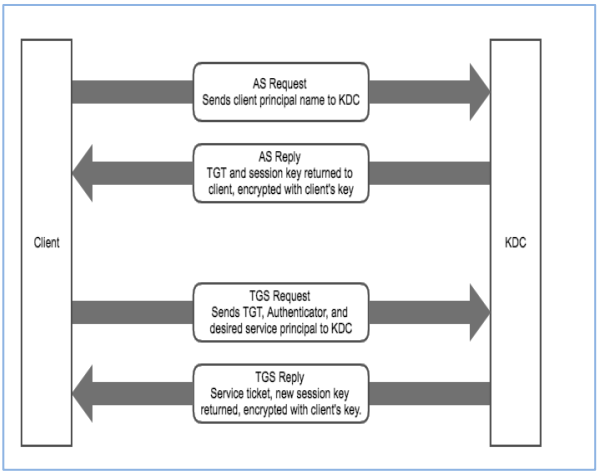

Fig. 2. Kerberos Phases

- The first stage is to verify the identity where the client will send an authentication request (AS_REQ) to the authentication Server (AS), then AS will respond with an encrypted response (AS_REP) which contains the TGT, once the client decrypt the response, they can get the TGT and move on to the second stage.
- The second stage is to access the service through sending a ticketing service request (TGS_REQ), which contains TGT obtained from (AS_REP), to the ticketing service as the TGS will respond with an encrypted response (TGS_REP) that contains a service ticket where the client will need to use it for the access process. In fact, TGT is a special service ticket that required to access TGS which authorizes the customer to access the specified service [5] and [6].

As a result, the first stage represents the authentication process while the second stage is the licensing process.

2. Working of Kerberos Protocol

An authentication server (AS) with a database of secret keys (similar to passwords) for all clients (Kc) and servers (Ks) to authenticate the client's identity on behalf of the auditor [5]. The

core of the protocol consists of the following four steps as shown in Fig. 3.

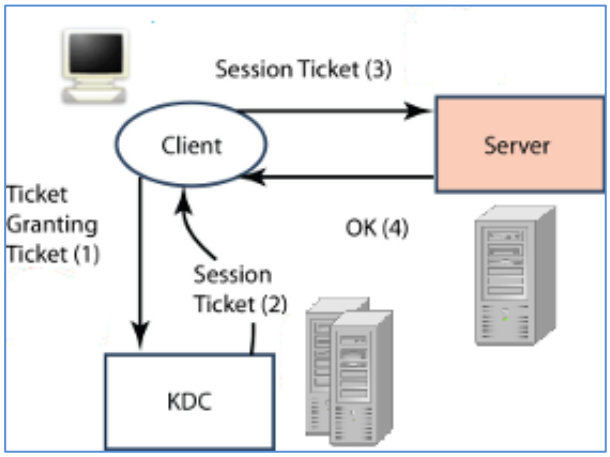

Fig. 3. Working of Kerberos

To initiate a session with server, the client sends an authentication request (1) to the AS including of the server ID and a random number such as the current time. Upon receipt of this request, AS will create a ticket and notarized (2). The card which been encrypted using the secret server key (Ks) contains the session key (Kcs) that will be used to encrypt transactions with the server. The binder consists of Kcs, key expiration time and nonce (used by the client to match the request with the response). Authentication will be encrypted using Kc if the customer is genuine [7] and it will help them to decrypt the session key from the authenticator. Fake client who does not know the Kc will not be able to decrypt Kcs from responding. After obtaining the session key, the client sends the application request (3) to the server encrypted using Kcs with the ticket [7].

The server who owns the secret key Ks can decrypt the session key Kcs from the ticket, and uses Kcs to validate the client request and is also responsible for terminating the session (4). Both client and server can use Kcs to provide many connections and sessions. AS is an important and effective destination as it is responsible for granting tickets (TGS) to all servers in its domain. In this scheme, customers must be licensed once only by the AS for a ticket granting they used to obtain tickets for each of the servers of TGS. Kerberos uses the DES encryption algorithm to generate keys and public key encryption with one-time passwords to provide better security. The protocol is not immune to phishing via password guessing attacks and Trojan horses that get user passwords. Therefore, Kerberos is not a panacea for the security matter although it solves most security issues [7] and [8].

Currently, there are two versions of Kerberos to be used: Version 4 and Version 5. The rest of the previous versions of Kerberos 1, 2 and 3 are not actually used widely because they were established in the development and trial phase. Kerberos version 4 has not been used for long time due to its many vulnerabilities compared with version 5. The slight abbreviation between these two versions are briefly defined in different aspects [8]. Version 5 has longer ticket lifetime with renewal ability. It can accept any symmetric key algorithm, depends different protocol to describe data types and has a load over version 4.

Authentication Dialogue of Kerberos encrypts passwords across the network, eliminates the threat against users and prevents the intruder from inhaling the network. Rather than authenticating each user individually and each service provided by the network separately, as with simple password authentication, Kerberos differs in this attribute if it uses strong symmetric and reliable encryption by the third party (the main distribution center or KDC) and to provide authentication to a group of users. A set of services offered by the network or computers operated by KDC [9].

When the user requests an authentication of the KDC, it sends set of credentials (tickets) with the session number back to the user's device, maintains contact with the user and provides services until the session is ended. The Kerberos protocol remains responsible for protecting the authenticity of communication with the user and on the same ticket rather than requiring them to authenticate a new password [9].

Kerberos authentication as shown in Fig. 4, identifies each user and gives them a unique non-replicable identity by the KDC. When the user registers by password on a network with Kerberos authentication to their workstation, the request is sent to their manager on the KDC as part of an application for a ticket granting tickets (or TGT) from the authentication server [9].

The user’s request will be sent in two ways, either by a special login program that is transparent and reliable or can be sent manually by the user. The KDC has been checking the user request in the master database. If the asset been

found, the KDC creates the TGT, encrypts it to protect by using the user key and sends the encrypted TGT to that user [9].

Although Kerberos is strong and been widely used but it still has some points of contention. The protocol assumes secure password storage in the AS file, this action

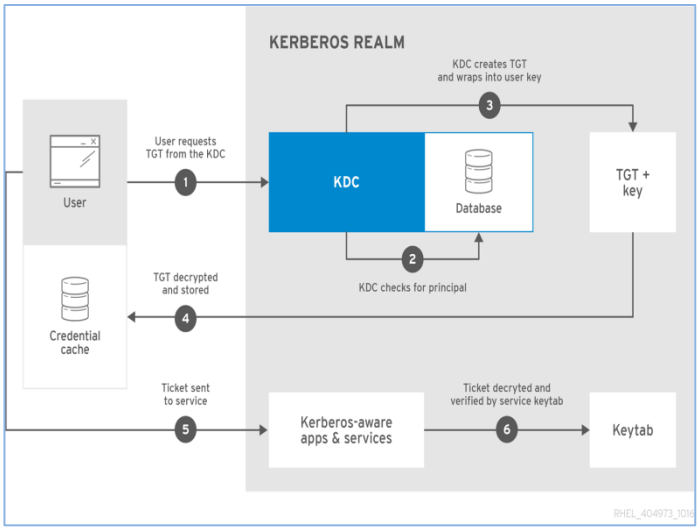

Fig. 4. Kerberos Authentication

putting them at the risk of providing all services. Furthermore, it is dangerous to store session keys in addition to the tickets in the system. It may cause a problem in the system that deals with multiple users at the same time and the errors that may occur to give the wrong permission which will enable the display of user session keys [10].

The Kerberos protocol could face repatriation attacks because it relies on time stamps for authentication. Therefore, it is necessary to provide accurate synchronization of the time of devices in distributed systems. This provides a server that may not mark the correct time from knowing the time by reading the user card [10].

One of the challenges that may face the credibility and security of user logon assigned to Kerberos are Trojan programs that capture user logon and revoke Kerberos-based system security. Knowing the user's secret key may help unhindered access to all

services. One of the best solutions to this vulnerability is to use the response and challenge method, where the server creates a special encryption device that works with Kc and responds to the user's request. User pass code will be given for a one-time. Separating the protocol from the encryption algorithm is a powerful authentication technology that protects the system from many types of attacks [11] and [12].

The Cryptographic algorithms used with the Kerberos protocol are the underlying layer that will rely on primarily. With the development of technologies and devices such as the appearance of desktops at GHz speeds, it was noticed that the security provided by 56-bit DES algorithms is insufficient. Conversely, using other algorithms such as AES 128 provides better size and security and this can enhance the security of Kerberos systems [12]. Considering for Kerberos independent from the basic encryption algorithm will have better results and thus provide stronger authentication and security for this protocol, although it has some challenges but its advantages are much higher [12].

One of the key challenges for Kerberos which are not protocol-related is that any application wants to use the Kerberos protocol must be updated in the code to establish a secure connection. This aspect could therefore lead to higher costs and longer time. It can be unreliable for all applications by companies and organizations due to its cost [13].

The Kerberos protocol relies on the use of time stamps to establish a secure connection depending on server synchronization and without delay. For example, the times required for servers may take a few minutes, often to synchronize their hours. But it is possible to mislead the user about the correct time, since old authentication can be restarted without a problem. Additionally, a solution to this problem can be implemented by adding user response as an alternative to time-based authentication [13].

The Kerberos protocol relies heavily on high dependency of the KDC server. If this server crashes, the network and the authentication system will collapse completely. This is undesirable especially for distributed systems because they are very expensive. Therefore, the system needs to put in place higher security measures with respect to the primary or secondary servers. Prevents anyone from accessing the Kerberos server, if they penetrate this system, they will be able to penetrate all network services [12].

Another problem may happen due to the using of a weak password by the user, so that an attacker who guesses the

password can impersonate the client [13]. Because of the message is encrypted with the client key derived from the client password, therefore, anyone can try to guess this key and impersonates the legitimate client. In this case, the Kerberos system is not effective against guessing attacks [13].

To sum up, Kerberos must be integrated with different encryption techniques with paying attention to password selection and generate message encryption keys. The Kerberos V5 authentication protocol is very powerful and capable of addressing all types of plagiarism attacks [12].

3. Discussion and Conclusion

In this review, Kerberos Authenticator has many advantages that make it highly effective to be recommended. It is primarily a stable authentication protocol among other security models. One of the strength features of this system is that only encrypted messages are sent over the network which add difficulties to decrypt the message. The strength of the user password depends on the client and according to the authentication server, the messages are encrypted, where the encryption strength depends on the encryption algorithm itself. Kerberos can be made to become stronger when the server been separated from the encryption server.

Encryption is the first layer of Kerberos when encrypting the key or decoding Kc. The Kerberos system can also explicitly allow authentication that answers the challenge question to decrypt the permit card. The Kerberos Authentication Protocol (KDC and services) can be developed to add the use of intelligence machine modeling techniques which by their nature can mimic the pattern of user behavior, study their effectiveness and may enhance this identification of legitimate user with diagnose intruders whose activity differs from the authenticated user.

References

[1] Zhang L., (2012) .The Research of Log-Based Network Monitoring System, In: Gary Lee(Ed.): Advances in Intelligent Systems. Advances in Intelligent and Soft Computing, Vol. 138. Springer, Berlin, Heidelberg, 315-320.

[2] Dua, G.; Gautama, N. ; Sharma, D. and Arora, A., (2013). Replay Attack

Prevention in Kerberos Authentication Protocol Using Triple Password, International Journal of Computer Networks & Communications, Vol. 5 (2), 59-70.

[3] Koganti, V. S.; Galla L. K.; Nuthalapati N.; and Kakarlapudi A. V., (2017). Authentication protocols using encryption techniques, IEEE, International Conference on Control, Instrumentation, Communication and Computational Technologies.

[4] Ozha, T., (2013) Kerberos: An Authentication Protocol, Int. J. Computer Technology & Applications, Vol. 4(2), 354-357.

[5] Garman J., (2010). Kerberos: The Definitive Guide, Publisher: O'Reilly Media. 272.

[6] Kohl J., Neuman B.C., Ts'o T.Y., (1994). The evolution of the kerberos authentication system. Distributed open systems, IEEE Computer Society, Los Alamitos, CA, 78–94.

[7] Schmeh K., (2001). Cryptography and Public Key Infrastructure on the Internet, John Wiley & Sons, 197-198.

[8] Andrew B. A., (2013) Kerberos: A Review of the Modification in Versions 4-To-5 Transition, African Journal of Computing & ICTs, Vol. 6(3), 127-134.

[9] Muehlfeld M., Hanzelka F., Maňásková L., Petrová A. Š., Čapek T., Ballard E. D., (2019). System-Level Authentication Guide, Chapter 11. Using Kerberos, Red Hat, Inc., 101-115.

[10] Butlera F., Cervesato I., Jaggard A. D., Scedrov A., Walstad C., (2006). Formal analysis of Kerberos 5, Theoretical Computer Science Vol. 367(1–2), 57-87.

[11] Butler F., Cervesato I., Jaggard A.D., Scedrov A., (2002). A formal analysis of some properties of Kerberos 5 using MSR, in: Fifteenth Computer Security Foundations Workshop CSFW-15, IEEE Computer Society Press, Cape Breton, NS, Canada, 175–190.

[12] Cervesato I., Jaggard A., Scedrov C. Walstad, (2005)Specifying Kerberos 5 cross-realm authentication, in: Proc. WITS'05, ACM Digital Library, 12–26.

[13] Bellovin S. M. and Merritt M. (1990). Limitations of the kerberos authenication system, Computer Communication Review, Vol. 20(5), 119-132.

[14] Shrestha A. P., Choi D. Y., Kwon G. R., Han S. J., (2010). Kerberos based authentication for inter-domain roaming in wireless heterogeneous network, Computers & Mathematics with Applications, Vol. 60(2), 245-255.