NETWORK AUTHENTICATION ENCRYPTION PROTOCOL BASED ON KERBEROS: A REVIEW

Davinderpreet Kaur[1]
Department of Computer Engineering,
Punjabi University Patiala
E-mail:preetdavinder.91@gmail.com

Brahmaleen Kaur[2]
Department of Computer Engineering,
Punjabi University Patiala
E-mail: brahmleen_sidhu@yahoo.co.in

Abstract - *In this paper, we introduce the Kerberos network authentication protocol developed by MIT(that was developed in the Athena Project at the Massachusetts Institute of Technology). Kerberos deals with clients or users that request for services. A user requests an encrypted "ticket" from an authentication process that can then be used to request a particular service from a server. The user's password does not have to pass through the network. The principle of the system is to provide strong authentication for client server application by using secret key cryptography. Kerberos encryption schemes are proposed revisions that are provably satisfy such notions. In this paper, techniques to encrypt the data over the network communication process are discussed in our related work.*

Keywords**:** *Authentication, Authorization, Access control, computer network security, Kerberos.*

I. INTRODUCTION

The set of protocols and mechanisms are created to deal with the information and network security issues. In the other words we can achieve the information security provided through cryptography. The related aspects of information security such as confidentiality, data integrity, access control, authentication.
Confidentiality used to keep the contents of information from all but those authorized who can have it. In data integrity, the service that address the unauthorized alteration of data ensures that data should not be tampered during transit. The data integrity have ability to detect the data manipulation by unauthorized user. The access control has ability to only authorized user which can be identified their identity to access the services. Authentication is related to identifications. Authentication and accounting schemes is the top of the requirements for security of the computer networks. Protocols (set of rules and procedure or directions to perform the operation step by step method). Protocol play major role to meet the cryptographic goals. The Kerberos protocol technique use to among the communicating parties. Encryption schemes, hash functions, and generation of random numbers are primitives that may utilized to build protocol [4].
First we will describe the [1.1] Project Athena, [1.2] System architecture, Evolution in versions of Kerberos, then Related work, Conclusion and future work in last section.

[1.1] Project Athena**:** Project Athena. Project Athena was established with support from a consortium of computer vendors in May 1983 with a five-year timeline. Athena's focus was to develop strategies and software for integrating computers into MIT's curriculum. In particular, Athena was designed from the start as a networked, client-server system [1] .

[1.2] System Architecture:

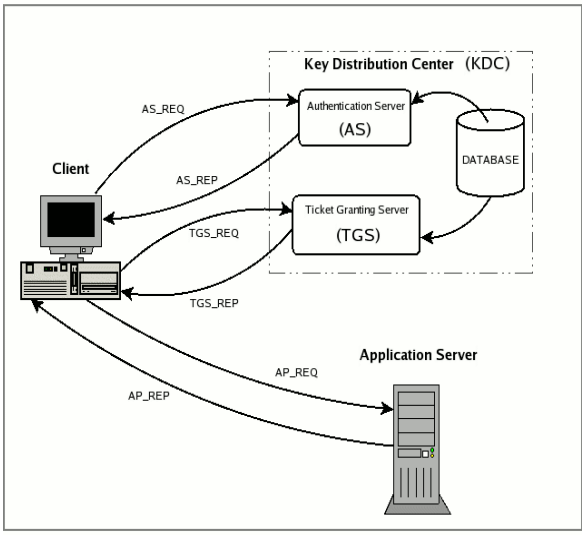

Fig 1.2 Architecture Diagram

When a user logs in, the client transmits the username to the authentication server, along with the identity of the application server the user has to connect to. The authentication server replies to the client. It contains the TGT (encrypted using the TGS secret key) and the session key (encrypted using the secret key of the requesting user). The client now requests for a service ticket. This packet includes the TGT obtained from the previous message and an authenticator generated by the client and encrypted with the session key. The TGS then replies by sending the requested service ticket (encrypted with the secret key of the service) and a service session key generated by TGS and encrypted using the previous session key generated by the AS. The client now requests the application server to access a service. The components are the service ticket obtained from TGS with the previous reply and an authenticator again generated by the client, but this time encrypted using the service session key (generated by TGS) and a timestamp. Now the application server replies by incrementing the timestamp, meaning the client is authenticated and he can access the service he desires.

And the variables in the diagram above are explained step by step as under:

- *AS_REQ* is the initial user authentication request (i.e. made with kinit) This message is directed to the KDC component known as Authentication Server (AS);
- *AS_REP* is the reply of the Authentication Server to the previous request. Basically it contains the TGT (encrypted using the TGS secret key) and the session key (encrypted using the secret key of the requesting user);
- *TGS_REQ* is the request from the client to the Ticket Granting Server (TGS) for a service ticket. This packet includes the TGT obtained from the previous message and an authenticator generated by the client and encrypted with the session key;
- *TGS_REP* is the reply of the Ticket Granting Server to the previous request. Located inside is the requested service ticket (encrypted with the secret key of the service) and a service session key generated by TGS and encrypted using the previous session key generated by the AS;
- *AP_REQ* is the request that the client sends to an application server to access a service. The components are the service ticket obtained from TGS with the previous reply and an authenticator again generated by the client, but this time encrypted using the service session key (generated by TGS);
- *AP_REP* is the reply that the application server gives to the client to prove it really is the server the client is expecting. This packet is not always requested. The client requests the server for it only when mutual authentication is necessary.

II. EVOLUTION

The modern Kerberos protocol has gone through several major revisions since it was

first conceived as part of Project Athena. During each revision, major improvements have been made in usability, extensibility, and security.

2.1 Early Kerberos (v1, v2, v3)

The early versions of Kerberos (pre-Version 4) were created and used internally at MIT for testing purposes. These implementations contained significant limitations and were only useful to examine new ideas and observe the practical issues that arose during development and testing.

2.2 Kerberos 4

The first version of Kerberos distributed outside of MIT was Kerberos 4. First released to the public on January 24, 1989, Kerberos 4 was adopted by several vendors, who included it in their operating systems. In addition, other, large distributed software projects such as the Andrew File System adopted the concepts behind Kerberos 4 for their own authentication mechanisms.

The basics of what was to become the Kerberos 4 protocol are documented in the Athena Technical Plan. Ultimately, the details of the protocol were documented through the source code in the reference implementation published by MIT.

However, due to export control restrictions on encryption software imposed by the U.S. government, Kerberos 4 could not be exported outside of the United States. Since Kerberos 4 uses DES encryption, organizations outside of the U.S. could not legally download the Kerberos 4 software as-is from MIT. In response, the MIT development team stripped all of the encryption code from Kerberos 4 to create a specialized, exportable version. Errol Young, at Bond University of Australia, took this stripped version of Kerberos 4 and added his own implementation of DES to create "eBones." Since eBones contained encryption software developed outside of the United States, it was unencumbered by the U.S. encryption export controls, and could be legally used anywhere in the world.

Today, several implementations of Kerberos 4 still exist. The original MIT Kerberos 4 implementation is now in a maintenance mode and officially considered "dead." The kth-krb distribution, developed in Sweden, is still actively developed but it is highly recommended that new installations use the superior Kerberos 5 instead.

2.3 Kerberos 5

Kerberos 5 was developed to add features and security enhancements that were not present in Version 4 of the protocol. Kerberos 5 is the latest version of the Kerberos protocol and is documented in RFC 1510.

To correct the deficiencies in the Kerberos 4 protocol, several new features were added. They include:

- A better wire protocol, based on ASN.1
- Credential forwarding and delegation
- Replay cache
- More flexible cross-realm authentication
- Extensible encryption types
- Pre-authentication

In addition to the reference implementation by MIT, many other implementations of Kerberos 5 have been developed, some commercial and some open source. The implementations covered in this book include MIT, Heimdal, Microsoft (Windows 2000 and above), and Apple (Mac OS X and above).

Unfortunately, while the rules surrounding encryption export out of the United States have been relaxed on open source software as of January 2000, the MIT distribution is still

available to U.S. residents only. Because of the overly cautious actions of the MIT lawyers, a group in Sweden is developing and distributing the Heimdal Kerberos 5 distribution, which is unencumbered by any export control laws [2].

III. RELATED WORK

It presents a successful formal method based verification of a significant portion of the current Kerberos version 5 and some even imply security in the computational setting**.** Encryption in Kerberos should satisfy strong cryptographic security notation. Kerberos encryption scheme nor their proposed revisions are known to provably satisfy such notations[3].

The principle's secret key will be independent of the user password to overcome the weak password chosen by the network principle that are susceptible to password guessing attack. The secret key controlled using the system clock. Triple –Des is used for encryption, SHA-256 for hashing for random number generation[4].

This is focused on developing authentication protocol for wireless network irrespective of the technologies or the administrative domain. A secure protocol was proposed which adopts strong features of Kerberos based on tickets for rigorous mutual authentication and session key establishment along with issuance of token so that the mobile station can have access to not only the roaming partner of home network but also to the roaming partner of previous visited networks. The performance evaluation and comparative analysis of the proposed protocol is carried out with the already implemented standard protocols and most remarkable research works till date to confirm the solidity of the results presented.[5]

Authentication, Authorization and Accounting (AAA) infrastructures has been preferred for that operation. Thus, the lack of a correct integration between these infrastructures and Kerberos limits the service access only to service provider's subscribers. To avoid this limitation, we design an architecture which integrates a Kerberos pre-authentication mechanism, based on the use of the Extensible Authentication Protocol (EAP), and advanced authorization, based on the standards SAML and XACML, to link the end user authentication and authorization performed through an AAA infrastructure with the delivery of Kerberos tickets in the service provider's domain.

The interfaces, protocols, operation and extensions are detailed which are required for our solution. Moreover, important aspects are discussed such as the implications on existing standards. [6]

Network operators and educational and research communities are extending the access to their Internet application services to external end users by deploying, with other domains, the so-called identity federations. In these federations, end users use the identity and authentication credentials registered in their home organizations for accessing resources managed by a remote service provider. Current identity federation solutions focus mainly on assisting network access and web services .The AAA infrastructure and the bootstrapping of the security association the solution uses the so-called Protocol for Carrying Authentication for Network Access (PANA).[7]

CONCLUSION

Kerberos is being widely used for authentication and key distribution in application services within a single domain. However, Kerberos cross-realm infrastructures are not widely deployed in federated networks. Instead, domains are usually interconnected by means of an AAA infrastructure for service access control. Unfortunately, this enormously difficulties that end users subscribed in one domain can access by using Kerberos the services provided by other domain in the federation.

REFERENCES

[1]G. W. Treese ‘‘Berkeley Unix on 1000 Workstations: Athena Changes to 4.3BSD,’’ in *Usenix Conference Proceedings* (Winter, 1988).

[2]S. P. Dyer ‘‘Hesiod,’’ in *Usenix Conference Proceedings* (Winter, 1988).

[3] Alexandra Boldyreva et al. “Provable security analysis of authenticated encryption in Kerberos” (2007) IEEE symposium on security and privacy proceedings.

[4] Eman El –Emam et al. “An authentication protocol based on Kerberos 5” (2010),International journal of network security,vol.12, No.3.

[5] Anish Prasad Shrestha et al. “Kerberos based authentication for inter-domain roaming in wireless heterogeneous network”, (2010),Elsevier.

[6] Rafael Marín-López et.al “Providing EAP-based Kerberos pre-authentication and advanced authorization for network federations” Dept. Information and Communications Engineering (DIIC), University of Murcia, (2011) Elsevier.

[7] Alejandro Pérez-Méndez et.al, “Out-of-band federated authentication for Kerberos based on PANA”, Dept. Information and Communications Engineering (DIIC), University of Murcia, (2013) Elsevier.