Security in WLAN using Kerberos

Kirti M.Shinde[*], Prof. R V. Shahabade[**]

[*]Computer Department, Terna Engineering College, Navi Mumbai, India
[**] Computer Department, Terna Engineering College, Navi Mumbai, India

Abstract- The Kerberos Authentication Service, developed at MIT, has been widely adopted by other organizations to identify clients of network services across an insecure network and to protect the privacy and integrity of communication with those services. This paper gives an overview of kerberos in WLAN. It describes the framework used and operation's performed by kerberos in WLAN.

Index Terms- EAP Over LANs (EAPOL), Kerberos realm, proxy server, Personal Digital Assistant.

I. INTRODUCTION

Owning to the growing popularity and use of computers and network-based devices, providing privacy and data integrity have become crucial, in order to protect data, resources and systems from attacks and unauthorised access. For purposes of attack prevention, authentication and access control play a vital role. In recent years, to meet the increasing demands in secure computer communications, various security protocols have been developed. Most of these protocols agreed upon a cryptographic key or achieved authentication specifications. In order to meet increasing demands, various security protocols have been developed. Kerberos is one of these commonly used mechanisms[1] [2] . The Kerberos Authentication Service was developed by the Massachusetts Institute of Technology (MIT) to protect the emerging network services provided by Project Athena. Versions 1 through 3 were used internally [5].

II. LITRATURE REVIEW

The Kerberos Authentication Service, developed at MIT, has been widely adopted by other organizations to identify clients of network services across an insecure network and to protect the privacy and integrity of communication with those services. In this chapter existing security and cryptography techniques of Kerberos are critically analysed [1][2]. In addition, wireless communication networks and their security aspects are also critically analysed. Detailed explanations of kerberos framework and basic operations of kerberos in wireless network are explained.

III. THE FRAMEWORK FOR KERBEROS IN WLAN

The wireless LAN is secured via permitting authorized access to information and services, while preventing unauthorised access to and corrupting the network as shown in Figure 1. Since Kerberos is a trusted 3rd party authentication protocol and application independent, its paradigms and entities are finalized [1][2]. As it can be seen from Figure 3.1, the cryptographic protocol, programs and data containing the credentials of the legitimate entities of a particular wireless LAN environment are installed on each of the entities as well as TGS and KDC. The credentials are the identities of the devices (such as MAC addresses) and they are stored with cryptographic protection.

The cryptographic protocol adopts the challenge-response paradigm. The interactions between the entities are represented using numbers 1-19. These numbers represent the interactions between the legitimate entities of a wireless LAN environment. Numbers 1, 2, 3, 16, 17 represent the interactions between the client and the access point while numbers 4, 15, 18, 19 represent the interactions between the access point and the authentication server. The numbers 5, 6, 7, 8 and 9, 10, 11, 12 represent the interactions between authentication server and KDC, and authentication server and TGS respectively. Also, numbers 13, 14 represent the interactions between KDC and TGS.

The involved steps are explained below:

1. The supplicant (wireless client) sends an Extensible Authentication Protocol over LAN (EAPOL) start message to the authenticator (access point) requesting authentication.

2. The access point (AP) responds with a challenge to the supplicant to supply the supplicant's device identity. The AP also bundles the MAC address of the AP itself along with the challenge on actual network traffic under strong encryption to the supplicant.

3. The supplicant responds to the AP after processing the challenge. The supplicant processes the challenge by decrypting the challenge text and ensuring that the AP's MAC address is found in the supplicant's database of possible APs that the supplicant can use to connect to the server or other nodes in the wireless LAN. The supplicant's response is also under strong encryption.

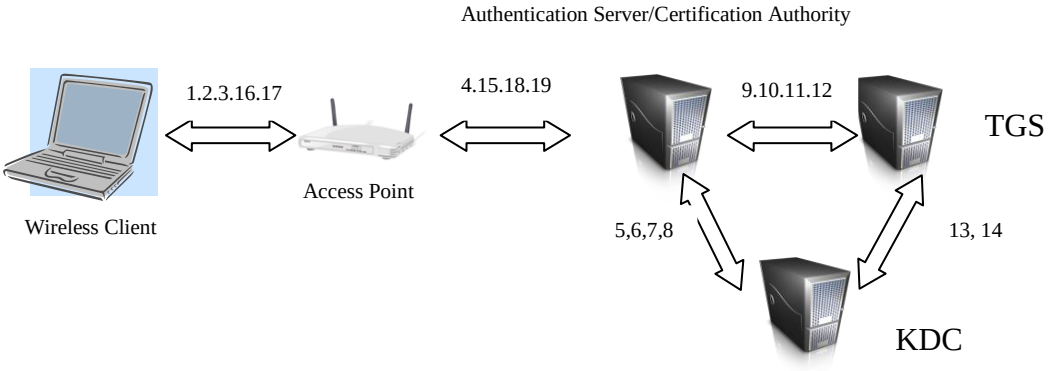

Figure 1: The proposed Framework

4. The AP challenges the authentication server (AS). The challenge text is bundled with the AP's and the supplicant's MAC address still under strong encryption.

5. The AS sends an EAP Over LANs (EAPOL) start message to the KDC requesting authentication.

6. The KDC responds with a challenge to the AS to supply the AS's device identity. The KDC point also bundles the MAC address of the AS itself along with the challenge on actual network traffic under strong encryption to the AS.

7. The AS challenges the KDC. The challenge text is bundled with the AS's, AP's and the supplicant's MAC addresses still under strong encryption.

8. The KDC responds to the application server's challenge after processing the content of the challenge text. The process involves the decryption of challenge text and a confirmation or proof of knowledge of the existence of both AS and the address of the server. The KDC sends this response under encryption to the AS.

9. The AS sends an EAPOL start message to the TGS requesting authentication.

10. The TGS responds with a challenge to the AS to supply the AS's device identity. The TGS points also bundles the MAC address of the AS itself along with the challenge on actual network traffic under strong encryption to the AS.

11. The AS challenges the TGS. The challenge text is bundled with the AS's, AP's and the supplicant's MAC addresses still under strong encryption.

12. The TGS responds to the AS's challenge after processing the content of the challenge text. The process involves the decryption of challenge text and a confirmation or proof of knowledge of the existence of both AS and the address of the server. The TGS sends this response under encryption to the AS.

13. The KDC server challenges the TGS. The challenge text is bundled with the KDC's, AP's and the supplicant's MAC addresses still under strong encryption.

14. The TGS responds to the KDC's challenge after processing the content of the challenge text. The process involves the decryption of challenge text and a confirmation or proof of knowledge of the existence of both KDC and the address of the KDC. The TGS sends this response.

15. The AS responds to the AP's challenge after processing the content of the challenge text. The processing involves the decryption of the challenge text and a confirmation or proof of knowledge of the existence of both the AP and the supplicant within the secured database of the server. The response includes the MAC address of the server. The AS sends this response under encryption to the AP.

16. The AP challenges the supplicant to run the program to authenticate the end user.

17. If the user responds correctly to the authentication request, the supplicant responds accordingly to the AP.

18. The AP sends the users sign-on response from the supplicant to the AS for the necessary processing.

19. The AS responds to the AP with either the ACCEPT packet or the REJECT packet, depending on the outcome of the processing, to the AP. This makes the AP to transition to the authorized state to allow traffic to and from the supplicant with the ACCEPT message or unauthorised state with the REJECT message.

The proposed model presented above is addition of a new variant on highly confidential, popular authentication protocol, Kerberos for wireless LANs.

IV. BASIC OPRATION OF KERBEROS IN WIRELESS COMMUNICATION NETWORK

In wireless networks, although Kerberos relies on the provisions of IEEE 802.1 x standards, owing to the fact that, its operation is system and application independent, security features for authentication are independent as well. Kerberos protocol assumes that initial transactions take place on an open network where clients and servers may not be physically secure and packets travelling on the network can be monitored and even possibly be modified.

Due to the critical function of the KDC, multiple KDCs are normally utilized, where each KDC stores a database of users, servers, and secret keys. However, since the KDC stores secret keys for every user and server on the network; they must be kept completely secure. If an attacker were to obtain administrative access to the KDC, the attacker would have access to the complete resources of Kerberos realm[4].

Kerberos tickets are cached on the client systems. If an attacker gains administrative access to a Kerberos client system, he can impersonate the authenticated users of that system. In other words, the authentication service authenticates the client

and replies to the client with a ticket to the TGS. The TGS receives the ticket from the client and checks its validity and replies to the client with a new ticket for the server the client wishes to use. In order to prevent ticket hijacking, Kerberos KDC must be able to verify that the user who is presenting the ticket is the same user to whom the ticket was issued. This is shown in Figure 2.

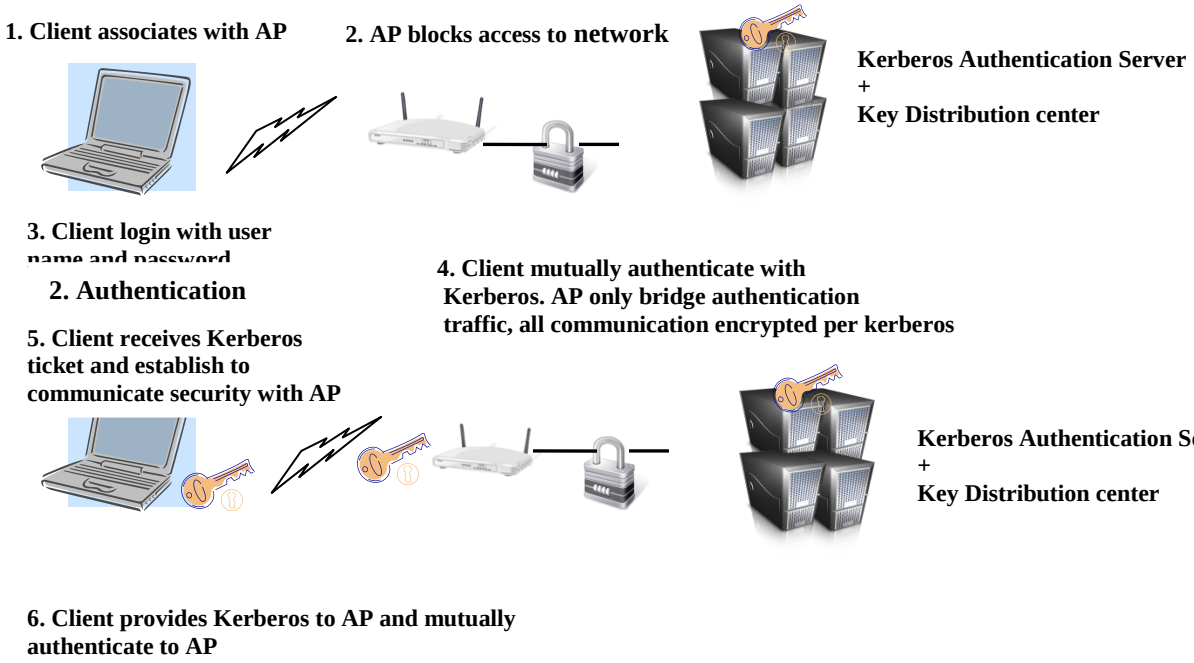

Figure 2: Kerberos in action in a wireless network

The performance evaluation of Kerberos security protocol have two different achievements, public key assistance and the addition of a proxy server.

Firstly, they used public-key infrastructures Public Key Cryptography for Initial Authentication in Kerberos (PKINIT), Public Key Cryptography for Cross-Realm Authentication in Kerberos (PKCROSS) and Public Key Utilizing Tickets for Application Servers (PKTAPP). In PKINIT, messages are added to change user secret key authentication to public key authentication. It manages secret keys for large number of clients. Nevertheless, it does not address key management of large number of realms. Additionally, as mentioned above, Kerberos uses key distribution and all tickets in its realm are issued by KDC. Since all authentications pass through the KDC, this causes performance bottleneck. At this point, PKTAPP is used for trying to eliminate bottleneck and reduce communication traffic by implementing authentication exchange directly between client and application server.

Secondly, in the same study they have proposed the use of proxy servers, Initial Authentication and Pass through Authentication using Kerberos V5 and GSS-API (IAKERB) and Charon for mobile communication systems. Former one is used as a proxy server, when a client could not establish a direct connection with KDC. Latter one adapts standard Kerberos authentication to a mobile Personal Digital Assistant (PDA) platform. Charon uses Kerberos to establish a trust relationship between a user and a proxy. However, as a result, it is possible to say that, although some additional public-key infrastructures are added to various stages of Kerberos, in terms of server and network capacity, they are fully suitable for simpler networks and could not work with more than one application server. In addition to these, a proxy is used to increase encryption process for both client and server; however, it produces delays during the transactions of authentication messages between client and server. Additionally, since wireless network speed increases, the proxy became insuffient and affects the response time.

Kerberos assisted authentication in mobile ad-hoc networks has been created by utilizing traditional features of Kerberos. Their logic appears to lack evidence that the notorious flaws of traditional Kerberos have been addressed in their solution. These flaws include replay attacks and distributed session keys. However, their solution seems to address issues of password guessing attacks.

V. CONCLUSION

In this paper Basic terms and techniques used in this research are defined. Kerberos authentication protocol and its basic operation in wireless communication networks are studied. The existing authentication methods developed for Kerberos in wireless communication networks are critically analysed . The

design of authentication protocols, generally, tends towards the adoption of public key infrastructure methods. This trend is a result of the observed weaknesses and limitations of the shared key schemes. In the context of shared key schemes, compromise of the shared key within any host or principal inadvertently compromises the entire system. KDCs bottleneck problem is solved through PKTAPP. Speed is increases. But password guessing attack is possibility still Kerberos is one of the most preferred authentication mechanisms.

REFERENCES

[1] Smitha Sundareswaran,Chi Tsong Su ,"Kerberos: An Authentication Service for ComputerNetworks".

[2] Bhaskar PalBhaskar Pal, "An Introduction to Kerberos", Dept. of Computer Sc. & Engg., Indian Institute of Technology KharagpurIndian Kharagpur.

[3] Derek Konigsberg, Kerberos,"The Network Authentication Protocol."

[4] John T. Kohl Digital Equipment Corporation, B. Clifford Neuman Information Sciences Institute University of Southern California, Theodore Y. Ts'o Massachusetts Institute of Technology,"The Evolution of the Kerberos Authentication Service".

[5] Jennifer G. Steiner,Project Athena Massachusetts Institute of Technology Clifford Neuman, Jeffrey I. Schiller, Kerberos: An Authentication Service for Open Network Systems", Cambridge, MA 02139 steiner @ATHENA. MIT.EDU, Department of Computer Science, FR-35 University of Washington Seattle, WA 98195 bcn@CS. WASHINGTON.EDU.

AUTHORS

First Author – Kirti Shinde, ME (App), Terna engineering college, Nerul, navi Mumbai, shindekirti9@gmail.com.
Second Author – Prof R.V. Shahabade, ME ,Computer Department, Terna Engineering College, Navi Mumbai, rvs2009@rediffmail.com