A Kerberos-based Authentication Architecture For Wireless LANs.

Mohamed Ali Kâafar[1], Lamia Benazzouz[1], Farouk Kamoun[1], and Davor Males[2].

[1] Ecole Nationale des Sciences de l'Informatique, Université de la Manouba. Tunisia
{Medali.kaafar, Lamia.benazzouz, Farouk.kamoun}@ensi.rnu.tn
[2] Laboratoire d'Informatique de Paris 6 Université Pierre et Marie Curie 8, rue du capitaine Scott 75015 Paris. France
davor.males@lip6.fr

Abstract. This work addresses the issues related to authentication in wireless LAN environments, with emphasis on the IEEE 802.11 standard. It proposes an authentication architecture for Wireless networks. This architecture called Wireless Kerberos (W-Kerberos), is based on the Kerberos authentication server and the IEEE 802.1X-EAP model, in order to satisfy both security and mobility needs. It then, provides a mean of protecting the network, assuring mutual authentication, thwarts cryptographic attack risks via a key refreshment mechanism and manages fast and secure Handovers between access points.

1 Introduction

Over recent years, wireless communication has enjoyed enormous growth, becoming popular in both public and private sectors. Wireless Local Area Network (WLAN) technology is capable of offering instant, high-speed and mobile connectivity. While this technology offers a lot of advantages, it does also introduce issues related to authentication, access control, confidentiality and data integrity. Today, wireless products are being developed that do not address all of the security services related to this technology. Although the IEEE 802.11i framework is proposing a "Robust Security Nework" architecture (RSN) to deal with the security wireless networks limitations, actually there is not a complete set of standards available that solves all the issues related to Wireless security [1].

While the Kerberos approach has been proposed as a standard for enhanced security in IEEE TGe [2], currently there is no valid proposals using a Kerberos-like mechanism to provide authentication in a WLAN environment, preventing from cryptographic attacks and handling fast and secure handovers. In this paper, we propose a mobility aware authentication architecture for the IEEE 802.11 networks, based on the IEEE 802.11i works and exploiting the Kerberos protocol to overcome the RSN limitations and provide a global framework. We first begin by introducing the Kerberos protocol, and concepts related to the RSN architecture such as the EAP-802.1X model. This is followed by a description of the proposed architecture (called W-Kerberos) and the authentication process. Next, we describe the implementation of the system and conclude with perspectives of this work.

2 The Kerberos protocol

The following subsections present the Kerberos protocol and the authentication process in a Kerberos-based system.

2.1 Presentation

Kerberos was developed as an open software at the Massachusetts Institute of Technology (MIT) as part of its Athena project [3]. Since its version 4, Kerberos is under the IETF Common Authentication Technology Working Group responsibility[4].
The Kerberos architecture defines three entities: the client wanting to reach resources of a certain server, the service supplier or server, and the authentication Kerberos server. The latter is based on two distinct logical entities: An AS server (Authentication Server), responsible for the identification of clients, and a TGS server (Ticket Granting Service) which provides clients with access authorizations on the basis of an AS identification. These two entities are regrouped under the name of KDC to mean Key Distribution Center [5].

2.2 The Kerberos authentication process

The Kerberos authentication takes place in a set of steps as shown in Figure 1 and described below:

1. Before the client attempts to use any service of the network, he must be authenticated by a Kerberos Authentication Server AS. This authentication consists in an initial ticket request: Ticket Granting Ticket (TGT). The TGT is used subsequently to get credentials for several services.
2. When the client wants to communicate with a particular server, he sends a request to the TGS asking for credentials for this server. The TGS answers with these credentials encrypted by the user's key. The credentials consist of a temporary session key Sk and a ticket for the service supplier called Service Ticket ST, containing the identity of the client and the session key, all of them encoded with the server's key.
3. The client, wanting to reach a server's ressources, transmits the ticket to this server.
4. The session key, now shared by the client and the server, can be used to encrypt the next communications.

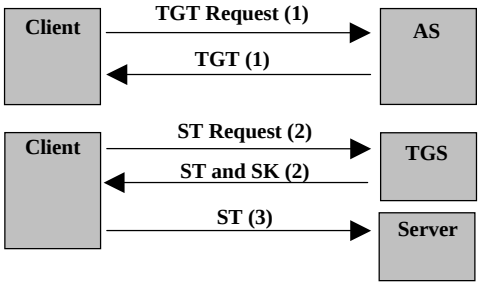

Fig.1. Kerberos service ticket request.

3 W-KERBEROS or Kerberos for the 802.11 networks

The proposed authentication process is based on tickets delivered by a W-Kerberos server. These tickets are going to direct the access points either to allow or not the traffic of a particular client. In the same way, it exploits the notion of dual ports of the IEEE 802.1X framework and the Extensible Authentication Protocol.
We present in the following the IEEE 802.1X framework as a pillar of the IEEE 802.11i architecture, and the EAP protocol as a generic authentication methods transporter. We describe then the proposed Kerberos authentication architecture called Wireless Kerberos: W-Kerberos.

3.1 The IEEE 802.1X framework

The IEEE standard 802.1X [7] defines a port-based network access control using the physical characteristics of LAN (IEEE 802) infrastructures. This can be used to authenticate and authorize network access to certain physical devices. This access control is performed at the data link layer. The IEEE 802.1X standard abstracts three entities (Figure 2).

- The *supplicant*: that wishes to access services, usually the client.
- The *authenticator*: which is the entity that wishes to enforce authentication before allowing access to its services, usually within the device the supplicant connects to.
- The *authentication server*: which the role is to authenticate supplicants on behalf of the authenticator.

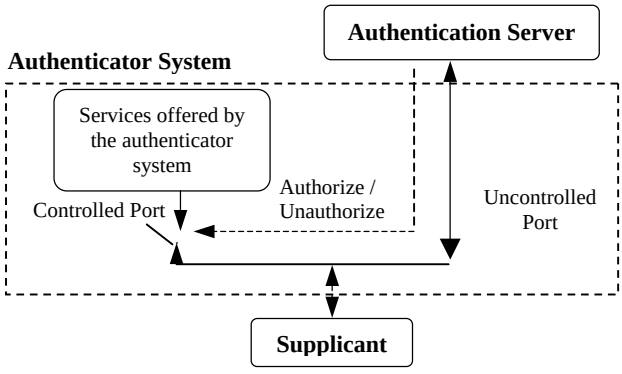

Fig.2. The IEEE 802.1X Setup

The IEEE 802.1X framework does not specify one particular authentication mechanism; it rather uses the Extensible Authentication Protocol (EAP) [8] as its authentication framework. EAP is a protocol that supports exchange of information for multiple authentication mechanisms. The authenticator is responsible for relaying this information between the supplicant and the authentication server.
The authenticator's port-based access control defines two logical ports via a single physical LAN port. These are controlled and uncontrolled ports. The uncontrolled port allows uncontrolled exchange (typically information for the authentication mechanism) between the authenticator and other entities on the LAN, irrespective of the authentication state of the system. Any other exchange between the supplicant and servers takes place via the controlled port.

3.2 The W-Kerberos architecture

The W-Kerberos system is composed of three main entities:

- The *client* trying to have access to the network.
- The *access points* considered as the Kerberos service suppliers, offering the service of access to the network.
- The *W-Kerberos server* allowing identification, tickets transmission, key refreshment and secured Handovers.

In this architecture, the authentication process takes place only once for the user. The principle of "Single Sign-on ", a principle according to which the user identifies himself only one time to the network to reach its different resources is applied. This transparency provides both security and convenience which palliates to certain EAP methods limitations, such as certificate-based methods [9]. Moreover, Mobility, a major asset in the Wireless networks, is handled by the proposed architecture. In fact, the authentication of the Handover phase, during which a client terminal should associate to a new access point, takes place without the exchange of any security context between access points and avoids an initialisation of the authentication process.

4 The authentication process

In the following subsections, we will describe the three main phases of the W-Kerberos authentication process: the initial authentication, the key refreshment or re-authentication and the Handover phase.

4.1 The initial authentication

This phase is typically initiated by the client terminal, which achieved a 802.11 association. In a first step, the client, receiving an EAP Request Identity from the access point, sends an EAP Response message, encapsulating an initial Service Ticket request (KRB-AS-REQ). The key used to encode the KRB messages is shared between the client and the Kerberos server and derived from the password provided by the client[1].

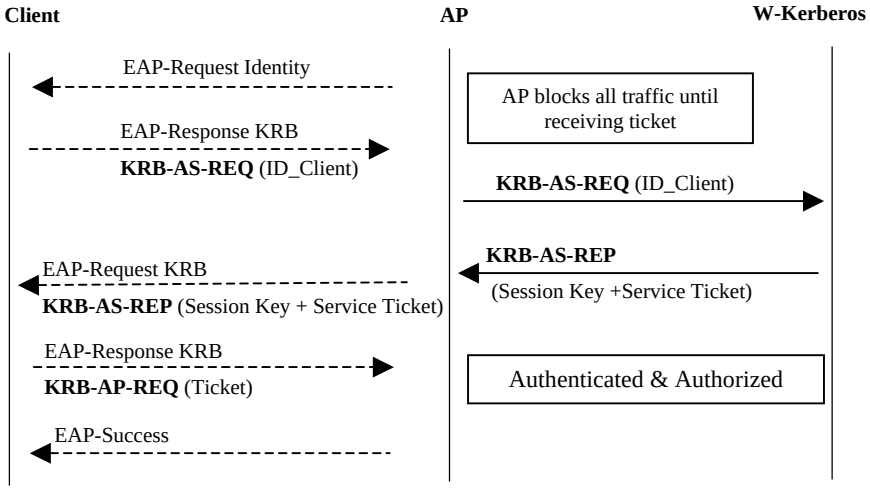

Fig.3. Initial authentication phase.

[1] For more details on key generation see [4].

After receiving the EAP Response, a Kerberos authentication request is sent from the access point to the W-Kerberos authentication server on the non controlled IEEE 802.1X port. The authentication server consults then the basis of principals, fixes the session time (needed for key refreshment), and generates a session key. An answer message KRB-AS-REP containing the session key, the ticket encoded with the AP secret key, and some authentication information is sent to the client via the access point. Data transmitted in this message is encrypted with the client key. To have access to the network resources, the client issues the ticket to the access point as a KRB-AP-REQ message encapsulated in an EAP Response packet. Thus, the client is now authenticated and authorised by the access point.

4.2 The Key refreshment phase

W-Kerberos offers a secure channel for communications via encryption mechanisms where key exchange is dynamic. This avoids the possibility of passive attacks to retrieve encryption keys. Hence, in addition to the ticket validity time, a key refreshment mechanism based on a session time out, sent in the initial authentication ticket, is specified by our architecture (see Figure 4). For this purpose, after having received an initial ticket, the access point calculates two time values:

- The *TTSR* (or Time To Send Re-authentication key): defines the instant when the access point must renew the session key and after which he is waiting for a receipt notification from the client.
- The *TTSN* (or Time To Send Notification) which is the instant when the client is considered as no longer authenticated. The access point will then send a Client Reject message (KRB-Cl-Rej) to the client station and the authentication server.

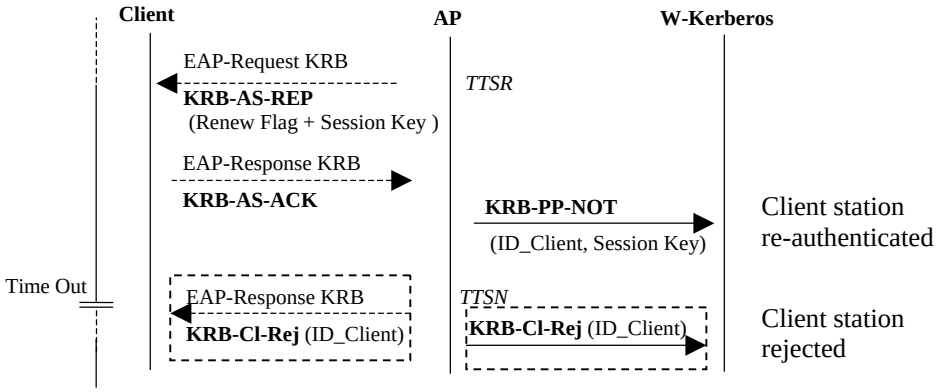

Fig.4. Key refreshment phase.

While receiving the KRB-AS-REP message with the Renew Flag set (indicating that it is a key refreshment), the client station sends a receipt notification (KRB-AS-ACK), using the new session key, to indicate that the key update has been done. The access point has then to mention this to the W-Kerberos server by sending a notification message (KRB-PP-NOT) containing the new session key.

4.3 The Handover phase

This phase is completely transparent to the client in a way that no new authentication does take place. The client terminal will transparently handle all the actions needed to perform a fast, efficient and transparent Handover (Figure 5).

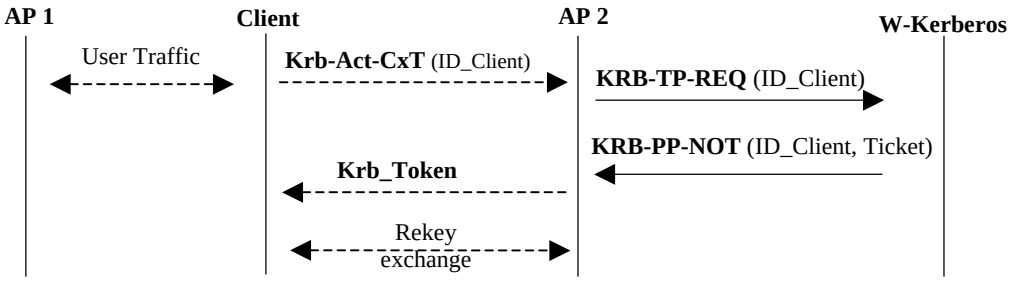

Fig.5. Handover phase.

As soon as the client terminal performs the IEEE 802.11 reassociation, it has to send a context activation message Krb-Act-CxT to the new access point, in order to move to the authenticated status. The access point contacts the W-Kerberos authentication server by sending a ticket request (KRB-TP-REQ). The server validates if this client is already authenticated, generates a ticket inserting the session key in progress, and sends back a notification to the access point (KRB-PP-NOT).
Once its context activation is acquitted (by the means of a Krb_Token message), the client can then, have its traffic going on once again. The access point maintains now a context of this client, associating the physical address of the terminal to the session key. A Rekeying exchange is initiated by the access point for each HandOver. The time out values for this exhange are extracted from the ticket sent by the W-Kerberos server.

5 Implementation

This section describes the W-Kerberos architecture implementation. This architecture is mainly composed of the client (W-Kerberos Client), the W-Kerberos authenticator (the access point) and the authentication server (W-Kerb). In the following, we will present each architecture component.

5.1 W-Kerberos Client

The W-Kerberos client is composed of two modules : WClient and WXsupplicant.

WClient. This module handles the different Kerberos messages from and to the W-Kerberos server. This entity is in charge of the Kerberos messages encryption, the authenticity check, tickets transmission. The GSS-API library [10] has been used for this client's implementation.

WXsupplicant. WXsupplicant is an extension of the client side open source implementation of the IEEE 802.1X standard called XSupplicant [11]. Some useful Kerberos authentication functions have been added to the Xsupplicant source and a new authentication type has been implemented.

5.2 W-Kerberos authenticator

A physically secured computer bridges the Wireless network (IEEE 802.11) to the wired network (Ethernet IEEE 802.3). The W-Kerberos authenticator was implemented using HostAP [12], which is a Linux driver for wireless LAN cards supporting the Host AP mode, i.e. it takes care of IEEE 802.11 management frames and acts as an access point. Over HostAP, a layer was implemented to take in charge the Kerberos service at the access point level. Our authenticator will then act as a "Kerberized[2]"server offering the service of network access. It is composed of three main components (Figure 6).

HostAP-802.1X. This entity is responsible for the IEEE 802.1X client authorizations. Besides the MAC addresses control carried out to either allow or not the traffic, it will also check the EAP packets authenticity[3].

EAP / W-Kerberos. The 802.1X implementation, present within the HostAP module, supports a RADIUS authentication server. We have then, implemented an EAP kerberos method that manages on the one hand, the EAP packets from the client terminal, and on the other hand, Kerberos packets sent to the W-Kerberos authentication server.

AP Server. It represents the Kerberos service of access to the network. It is under this server's name that we must record the access point close to the W-Kerberos server. This layer is in charge of tickets validity verification, message authenticity check, context activation in Handover phase, etc.

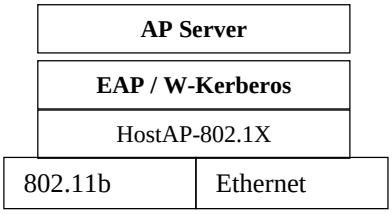

Fig.6. The W-Kerberos authenticator.

[2] The term Kerberized is used for applications that include Kerberos authentication as a feature.
[3] For this purpose, we have added an authenticator attribute at the level of EAP packets [6].

5.3 The Wireless Kerberos server (W-Kerb)

The authentication server must be physically secured. This server's physical violation could compromise the entire system. On the other hand, W-Kerberos being basically based on the Kerberos architecture, it was necessary to define a W-Kerberos messages management module within the Kerberos server. This module is called W-Kerb. Its main task is to deal with the W-Kerberos messages that are sent by hosts and access points.

Conclusions and further works

In this paper, we have proposed a kerberos-based Wireless authentication architecture that conforms to the IEEE 802.11i standard and is mobility aware. Mobility has been the major virtue of Wireless computing and as Wireless networks are deployed, users will expect secure mobility support even when presented with effective access control. The ticket concept existing in the Kerberos protocol is well adapted to such needs.
Although the Kerberos protocol is known to be vulnerable to dictionnary attacks, several works could address this vulnerabily [14], [15]. On the other hand, the W-Kerberos architecture provides transparent authentication of users and access points, as well as a secure channel for communications via encryption mechanisms where key exchange is dynamic and changes periodically via a key refreshment mechanism and a secure Handover phase. The specified architecture provides also, an effective means of protecting the network from unauthorized users and rogue access points, making then the possibility to steal valuable information ruled out, due to the fact that Kerberos provides mutual authentication, i.e., clients and access points ascertain that they are communicating with authentic counterparts. Finally, this architecture is highly customizable, allowing the use of different available encryption mechanism and maintaining thus ability to plug-in different cryptographic algorithms.
The main goal of this work has consisted in analysing and defining the security level within the IEEE 802.11 networks, with a security architecture proposal trying to satisfy both security and mobility needs. Future activities will expand this work, considering: public-key based techniques in the Kerberos model, the implementation of further components of the architecture focusing on the Handover phase, and performances evaluation in different scenarios to assess best values for various parameters (session time, ticket validity time) in term of security and overhead.

References

1. M. Casole, "WLAN security–Status, Problems and Perspective", in Proceedings of European Wireless 2002, Florence Italy, February 2002. Available from: http://www.ing.unipi.it/ew2002/proceedings/sec002.pdf
2. IEEE. 802.11 "TGe Security Baseline Draft", March 2001
3. The MIT Kerberos distribution. Available from: http://www.mit.edu/ afsnet.mit.edu/project/krb5 /.f/kerberosindex.html
4. J. Kohl, C. Neuman, "The Kerberos Network Authentication Service (V5)", September 1993. Available from: http://www.ietf.org/rfc/rfc1510.txt
5. N. Fischbach, "Kerberos en environnement ISP", January 2003. Available from: http://www.securite.org/ presentations/Krb5/ OSSIR2001-krb5_1.13.ppt
6. M. Mishra, W.Arbaugh, "An initial Security Analysis of the IEEE 802.1X Standard", February 2002. Available from: http://www.cs.umd.edu/~waa/ 1x.pdf
7. IEEE. Standards for local and metropolitan area networks: Standard for port based network access control. IEEE Draft P802.1X/D11, March 2001
8. Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)", March 1998. Available from: http://www.faqs.org/rfcs/rfc2284.html
9. F. Moioli, "Security in Public Access Wireless LAN Networks", M.Sc. Thesis, Royal Institute of Technology, Stockholm, June 2000. Available from: http://downloads.securityfocus.com/library/fabio-thesis.pdf
10. J. Linn, "Generic Security Service Application Program Interface", September 1993. Available from: http://www.ietf.org/rfc/rfc1508.txt
11. The open1x project, Web site: http://www.open1x.org
12. A linux wireless card driver, software access point. Available from: http://www.hostap.epitest.fi/
13. A. Chickinsky, Litton/TASC, "Wireless LAN Security Threats", IEEE 802.11-01/258, May 2001. Available from: http://grouper.ieee.org/groups/802/11/ Documents/DocumentHolder/1-258.zip
14. T. Wu, "The Secure Remote Password Protocol", In proceedings of the fifth Annual Symposium on Network and Distributed System Security, San Diego, March 1998. Available from: http://www.isoc.org/isoc/conferences/ndss/98/ wu_sl.pdf
15. B.Tung, et al., "Public Key Cryptography for initial authentication in Kerberos", Interbet Draft, 2001. Available from: http://www.ietf.org/internet-drafts/draft-ietf-cat-kerberos-pk-init-18.txt