A KERBEROS-BASED AUTHENTICATION ARCHITECTURE FOR WLANS

Test beds and experiments

Mohamed Ali Kaafar,[1] Lamia Ben Azzouz[2] and Farouk Kamoun[2]
Laboratoire CRISTAL, Ecole Nationale des Sciences de l'Informatique. Université de la Manouba. Manouba, Tunisia. [1] *medali.kaafar@cristal.rnu.tn,*
[2] *{lamia.benzaaouz,farouk.kamoun}@ensi.rnu.tn*

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. In addition to authentication, Kerberos has also the advantage of secure communications via encryption.

Keywords: Wireless authentication, IEEE 802.1X, EAP, Kerberos, test beds.

1. INTRODUCTION

The convenience of IEEE 802.11-based wireless access networks has led to widespread deployment in many sectors. This use is predicated on an implicit assumption of access control, confidentiality and availability. However, this widespread deployment makes 802.11-based networks an attractive target for potential attackers. Indeed, many researches have demonstrated basic flaws in 802.11's encryption mechanisms[1,2] and authentication protocols[3].
Although the IEEE 802.11i framework is proposing solutions to deal with wireless networks security limitations, actually there is not a complete set of standards available that solves all the issues related to Wireless security. We

have then proposed a mobility-aware authentication architecture for 802.11 networks, based on the IEEE 802.11i works and exploiting the Kerberos protocol to overcome security limitations of Wi-Fi networks. In this paper, we propose a Kerberos-like authentication architecture, evaluate and experiment its security. We first begin by presenting concepts related to the IEEE 802.11i architecture such as the EAP-802.1X model and introduces the Kerberos protocol and related approaches in wireless networks. This is followed by a brief description of the proposed architecture (called W-Kerberos) and the authentication process. We then evaluate W-Kerberos on the basis of the IEEE 802.1X-EAP threat model. Next, we describe attacks experimented to test the architecture resistance to wireless vulnerabilities, and conclude with perspectives of this work.

2. THE IEEE 802.1X FRAMEWORK

The IEEE 802.1X standard[4] defines a port-based network access control using the physical characteristics of LAN infrastructures, to perform a data link layer access-control. This standard abstracts three entities [Figure1]:

- 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, authenticating supplicants on behalf of the authenticator.

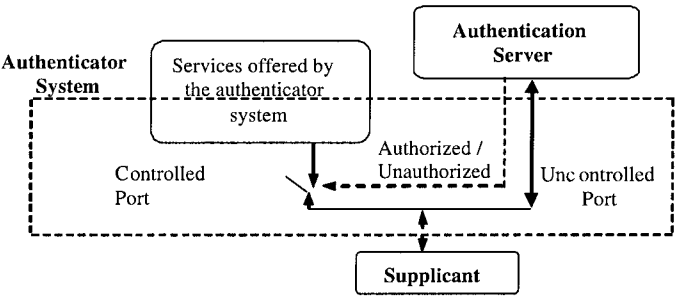

Figure 1. The IEEE 802.1X Set-up.

The IEEE 802.1X framework does not specify any particular authentication mechanism; it uses the Extensible Authentication Protocol (EAP)[5] 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 takes place via the controlled port.

3. THE KERBEROS PROTOCOL

Kerberos was developed as an open software at the Massachusetts Institute of Technology (MIT) as part of its Athena project[6]. 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, 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.

3.1 The Kerberos authentication process

The Kerberos authentication takes place in a set of steps as shown in [Fig.2] and described below:

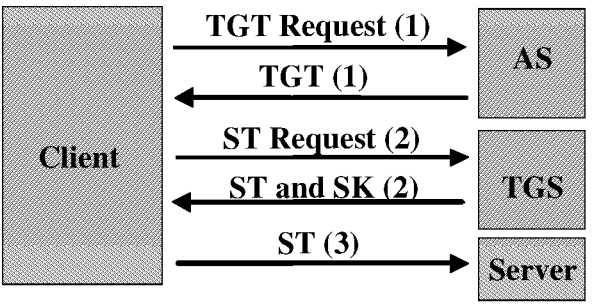

Figure 2. The Kerberos authentication process.

1 Before the client attempts to use any service of the network, a Kerberos Authentication Server AS must authenticate him. This authentication consists in obtaining an initial ticket request: Ticket Granting Ticket (TGT), which will be 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 client identity and the session key, all of them encoded with the server's key.

3 The client, wanting to reach a server's resources, transmits the ticket to this server. The session key, now shared by the client and the server, can be used to encrypt the next communications.

3.2 Kerberos in Wireless environments

The Kerberos use for authentication in WLAN environments has been considered several times. We discuss in the following some of these approaches.

- The "Symbol Technologies" approach is considering the SSID (Service Set Identity) as a service name shared between all the access points, to offer network access, and to make roaming easier. This approach does not offer a perfect forward secrecy. Thus, an attacker compromising an access point, could compromise the entire network.
- The IEEE 802.11e approach[7] is using EAP as an authentication method transporter, and the IAKerb protocol[8] for proxying the client messages to the authentication server. This approach, using a classic Kerberos authentication process, does not offer a transparent authentication and a secure way to deal with handovers; neither does it prevent cryptographic attacks on a generated session key.
- The IP Filter approach[9] is based on the implementation of some IP_tables filters, at the level of the access point. Those filters, constructed on the basis of a Kerberos authentication, are used by the access point to allow or deny the access of client stations to the network. This approach is vulnerable to IP Spoofing attacks, and to IP based DoS attacks[10].

The proposed Kerberos-based solutions do not prevent WLAN networks from cryptographic attacks nor do they handle fast and secure handovers. Thus, in our work, we have been interested by specifying a new Kerberos based architecture for WLAN. In the following subsections, we describe the proposed architecture called Wireless Kerberos: W-Kerberos.

4. 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. W-Kerberos system is composed of 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, and the W-Kerberos server as an authentication and roaming server. A W-Kerberos system is composed of 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, and the W-Kerberos server as an authentication and roaming server.

4.1 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) [Fig.3]. 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].

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. This transmitted Data is encrypted with the client key. To have access to 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 and Handover phases

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[11]. Moreover,

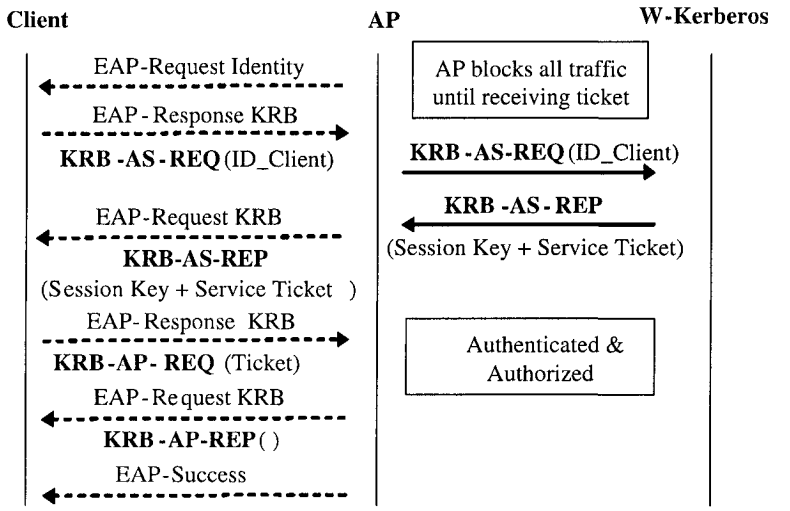

Figure 3. The Kerberos authentication process.

the WKerberos authentication is completely transparent to the client during a Handoff phase, in a way that no new authentication does take place. The client station only activates its context sending a ticket, which will be verified by the new access point[11].

5. W-KERBEROS EVALUATION

This section evaluates the W-Kerberos architecture on the basis of IEEE 802.11 networks threat model. The following points summarize security services offered by W-Kerberos to thwart different 802.11-specific attacks.

5.1 Confidentiality and Key derivation

Using the Kerberos key distribution to generate a MAC layer key, the W-Kereberos architecture allows the use of different available encryption mechanisms and thwarts different cryptographic attacks via the key refreshment phase.

5.2 Replay attacks and Integrity protection

W-Kerberos deals with replay attacks using EAP sequencing and Kerberos techniques in order to prevent an attacker from capturing a valid authentication message (or an entire authentication conversation) and replay it. Kerberos techniques are based on timestamps (and/or random numbers sequences)[12]. Further, caching authenticators within Kerberos V implementations denies any replays within the allowed time interval of Kerberos (5 minutes by default). Integrity protection provides data origin authentication and protection against unauthorized modification of information for authentication messages. W-Keberos uses an authenticator field to verify the authenticity of WKerb messages[6]. Moreover, the entities have to verify the EAP messages authenticity through an authenticator field added to the EAP messages.

5.3 Dictionary attacks resistance

Kerberos is known to be vulnerable to Dictionary attacks[13]. The W-Kerberos architecture, using a pass phrase to generate a master key could also be vulnerable to such type of attacks. In fact, where password authentication is used, passwords are commonly selected from a small set (as compared to a set of N-bit keys), which raises a concern about dictionary attacks. However, the possibility of using certificates and public key cryptography within a Kerberos environment has been studied[14]. While these techniques are certainly more secure, there is a compromise to consider: Using certificate based authentication means material authentication (in opposition to user one), public key infrastructure set up and less comfort of use for clients.

5.4 Mutual authentication and Protected results indications

This refers first to the ability for clients and access points to ascertain that they are communicating with authentic counterparts and to indicate whether they have successfully done it. Where EAP is tunnelled within another protocol that omits station authentication, there exists a potential vulnerability to man-in-the-middle attack[15,16]. W-Kerberos uses the Kerberos optional mutual authentication mechanisms, where both the access point and the client authenticate themselves. This authentication is mandatory within our proposal, so that rogue access point risks are prevented.

5.5 Denial of Service protection

Avoiding denial of Service (DoS) attacks within a wireless network is of a paramount importance for any security architecture. Performing a DoS attack is generally the first step that an attacker is taken to launch other, more clever attacks. Those attacks have been studied in many works[3,10], and some of them could be prevented by implementing some essential services. The per-packet authenticity used within a W-Kerberos authentication is one way to avoid some of these attacks. This prevent EAP-failure or EAPoL Logoff spoofing attacks[3] (trying to de-authenticate a legitimate client), and typically used to initiate a Man-in-the-Middle attack. Further, avoiding replay attack preserves 802.11 entities, especially access points, from flooding attacks.

6. TESTS AND EXPERIMENTS

In our experiments, we have tested three of the most known 802.11-specific attack implementations[12] (AirSnort, Monkey Jack, Void11) and observed the W-Kerberos behavior and attacks results.

6.1 AirSnort

AirSnort is a wireless LAN tool that recovers WEP encryption keys. It operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. In the W-Kerberos implementation, based on the HostAP driver, dynamic WEP is used as the MAC layer protocol for frames encryption. Our test bed has consisted in multi sessions FTP transfers on five wireless stations running W-Kerberos. The table below presents the obtained results.

This test proves that key refreshment is a mean thwarting some cryptographic attacks, especially WEP crack tools requiring a minimal number of unique key-encrypted captured frames.

6.2 Monkey Jack

Monkey Jack is an implementation of a wireless Man-In-the-Middle attack. It is used within the AirJack toolbox, which is a free 802.11 device driver API, and an 802.11 development environment. AirJack offers many utilities as user space programs, such as wlan-Jack, essid-Jack, monkey-Jack, etc. The principle of the Monkey Jack attack is to take over connections at layer 1 and

Table 1. AirSnort results.

Key refreshment time(min)	***Key size*** *(bits)*	***Average throughput***	***Average captures*** *(frame/sec)*	***Observations and results***
0: Static key	128	2.8 Mbits/s	186	Key has been retrieved in 9095 seconds (about 2 hours 31min) capturing 1 681 138 ciphered frames.
0: static key.	64	3.6 Mbits/s	192	Key has been retrieved in 5390 seconds (about 1 hour 30 min) capturing 1 032 887 ciphered frames.
60	64	3.9 Mbits/s	194	Key has not been retrieved by AirSnort, collecting more than 5 200 000 ciphered frames.

2, and to insert attack machine between victim and access point. It consists of three main phases:

- *Phase 1:* De-authentication attack, sending de-authentication frames to the victim using the access point's MAC address as the source.
- *Phase 2*: Client capture, victim scans channels to search for a new access point, and then associates with fake access point on the attacker's machine. Fake access point is on a different channel than the real one, and is generally duplicating its ESSID.
- *Phase 3*: Connection to the access point, attacker's machine associates with the real access point and is now inserted between the two entities. It tries to pass frames through.

We have tested this attack on two different architectures. The first was based on EAP-MD5 as a non-mutual authentication method, and the second on a W-Kerberos scheme. Monkey Jack versus EAP-MD5 was a total success. The attacker has successfully de-authenticated the client station in about 2 seconds. The victim, then associates with the fake access point and the attacker passes through authentication frames. The attack lasts 5 seconds.

For the W-Kerberos architecture, the first phase of this attack was the same as the first test. The attack machine, via de-authentication frames (those frames being not authenticated), has been able to capture the victim station (phase 1 and 2). However, when trying to relay authentication frames, the access point must have knowledge of the access point secret key, to decrypt the session key

in the service ticket. Moreover, any address modification is detected when verifying the authenticator field of the authentication messages, so the fake access point was unable to authenticate itself when asked to answer the authentication request of the client station. Thus, in our test the attack process failed and terminated with some errors on the attacker's machine interfaces.

6.3 Void11

Void11 is an open source implementation of some basic 802.11b DoS attacks. It mainly consists of:

- The *Deauth* tool (Network DoS): flooding wireless networks with de-authentication frames and spoofed ESSID, so that authenticated stations will drop their network connections.
- The *Auth* tool (Access point DoS): flooding access points with de-authentication frames and random stations addresses, so that access points will deny any service.

The W-Kerberos has been compared to material authentication test beds. The results for the "Deauth" tool are the following:

Table 2. Void11 Deauth tool results.

Clients	***Auth. Method***	***Auth. AP***	***Auth. Server***	***Test Time***	***Results***
Client1 MAC1	EAP-TLS	Cisco Aironet AP 350 Series	FreeRadius	12 sec	Deauthenticated
Client2 MAC2	EAP W-Kerb	HostAP W-Kerb	WKerberos Server	25 min	Associated, Authenticated

These results prove the resistance of the W-Kerberos to attacks based on forgery of spoofed EAP messages, and particularly de-authentication messages. The Man In the Middle attacks, being typically based, on such denial of service, are very reduced with an authenticator field in the EAP messages.

The second scenario has consisted in testing the hostAP soft access point, implementing the W-Kerberos authentication, and verifying its capacity of resistance to de-authentication frames flooding from random stations addresses. The results are the presented in [Table 3].

Table 3. Void11 Auth tool results.

AP	***Auth. Server***	***Observations & results***
Cisco AP 350	FreeRadius	The access point stops broadcasting beacons during 15 minutes. Authenticated clients are disassociated.
Cisco AP 1100	FreeRadius	Clients are disassociated, but re-associate periodically. The access point continues to broadcast beacons.
HostAP WKerb	W-Kerberos	Authenticated clients continue to be associated and authenticated, but the access point rejects any new authentication. Key refreshment messages are received at time.

The hostAP access point survived to this attack, and authenticated clients are not rejected. Further, their refreshment keys arrive at time, so there is no risk concerning any cryptographic attack. These results demonstrate the resistance of the W-Kerberos architecture based on the HostAP module to DoS attacks.

7. CONCLUSIONS AND FURTHER WORKS

In this paper, we have presented a Kerberos-based authentication architecture for Wi-Fi networks. Furthermore, we have evaluated this architecture on the basis of the IEEE 802.11 threat model. Experimentations have shown that key refreshment is a mean thwarting some cryptographic attacks, and that mutual authentication and protecting the authentication results guarantees a prevention against Man In the Middle attacks. Finally, W-Kerberos has been robust enough to resist to Denial of Service attacks.

The specified architecture provides then 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. Moreover, this architecture is highly

customizable, allowing the use of different encryption mechanisms and maintaining thus ability to plug-in different cryptographic algorithms.

The Ticket concept existing in the W-Kerberos protocol is well adapted to mobility needs within an IEEE 802.11 environment. Future works will expand this work considering the exploitation of proactive key distribution to specify a fast and secure handover, performance evaluation in different scenarios and especially handover overhead, and public key cryptography extension.

NOTES

1. For more details on key generation, see[6]

REFERENCES

1. Scott Fluhrer et al., "Weaknesses in the Key Scheduling Algorithm of RC4". In proceedings of the eighth Annual Workshop on Selected Areas in Cryptography, Toronto, August 2001.
2. Nikita Borisov et al., "Intercepting Mobile Communications: The Insecurity of 802.11". In Seventh Annual International Conference on Mobile Computing And Networking, Rome, Italy, July 2001.
3. M. Mishra, W.Arbaugh, "An initial Security Analysis of the IEEE 802.1X Standard". Technical report, University of Maryland. February 2002.
4. IEEE 8021X, "Port-based Network Access Control. IEEE Std 802.1x". IEEE Standard, June 2001.
5. L.Blunk, J. Vollbrecht, "PPP Extensible Authentication Protocol (EAP)". RFC 2284, March 1998.
6. J. Kohl, C. Neuman, "The Kerberos Network Authentication Service (V5)". RFC 1510, September 1993.
7. IEEE, "TGe Security Baseline Draft" Draft IEEE 802.11e, March 2001.
8. J. Trostle et al., "Initial and Pass Through Authentication Using Kerberos V5 and the GSSAPI (IAKERB)". Internet draft, October 2002.
9. A. Lakhiani, "A transparent authentication protocol for Wireless Networks", Master thesis, University of OHIO, March 2003.
10. D.B. Faria, D.R. Cheriton. "DoS and Authentication in Wireless Public Access Networks". In Proceedings of the First ACM Workshop on Wireless Security , Atlanta, September 2002.
11. M.A. Kaafar et al., "A Kerberos-based authentication architecture for Wireless Lans". In proceedings of the Third IFIP-TC6 International Conference on Networking (Networking 2004), Athens, Greece, May 2004.
12. C. Neuman et al. "The Kerberos Network Authentication Service (V5)", Internet Draft draftietf-krb-wg-kerberos-clarifications-05.txt, June 2003.
13. T. Wu, "A Real-World Analysis of Kerberos Password Security". In proceedings of the sixth Annual Symposium on Network and Distributed System Security, San Diego, February 1999.

14. B.Tung, et al., "Public Key Cryptography for initial authentication in Kerberos". Internet Draft draft-ietf-cat-kerberos-pk-init-18.txt, March 2001.
15. N.Asokan et al., "Man-in-the-middle in tunneled authentication protocols". Technical Report 2002/163, IACR ePrint archive, October 2002.
16. J. Puthenkulam et al., "The compound authentication binding problem". Internet draft draft-puthenkulam- eap-binding-01.txt, October 2002.