Integrated Security Architecture for WLAN

Marco Carli, Andrea Rossetti and Alessandro Neri
University of Roma TRE – Applied Electronics Department
via della Vasca Navale,84 00146 ROMA ITALY
Ph. +39.06.55177061 – Fax: +39.06.5579078
e-mail: (carli, neri)@uniroma3.it

Abstract—This paper presents a robust, integrated security architecture for Wireless Local Area Network (WLAN). WLANs and wireless applications are growing up in many network environments. They are potentially useful and powerful, but due to their broadcast nature, the security of these systems is still far from the optimum. To achieve security the IEEE protocol 802.11x is being developed, but it suffers of several weaknesses. To overcome these problems, a solution based on the integration of IEEE 802.11x and a server RADIUS is proposed.

Index Terms— Network security, 802.11 protocol, WLAN, WEP.

I. INTRODUCTION

A growing interest in WLANs has been experienced in the recent years.

WLANs represent a possible solution to the ‘last mile’ problem in the wired networks: they provide wireless support for home and business environments where it is too expensive or it is impossible to utilize cables. For example, a WLAN is a possible solution to improve data connectivity in an existing building without the need of cabling every work desk. Besides, using a wireless network, typical physical problems of a wired solution, as loose patch cords, broken connectors, flying cables, etc., are drastically reduced.

The WLAN installation is simple and its topology can be dynamically changed without requiring any structural modification. Due to these reasons, the general idea is to use WLANs for data, voice and multimedia communication. With respect to wired networks, WLANs present poor channel quality, dynamic network behavior, and limited available bandwidth. Besides, a wireless transmission significantly increases the security risk since unauthorized users could intercept the transmissions or can penetrate the WLAN by impersonating legitimate users.

The future growth of this kind of network depends on the development of network protocol for multiple accesses to a wireless medium, with the main constrain of secure information delivering. For these purposes the IEEE protocol 802.11x is being developed [1].

In this paper, starting from the analysis of the weakness of the security architecture based on the current WEP standard, a more robust solution based on the integration of IEEE 802.11x and a RADIUS server is presented.

The remainder of the paper is organized as follows. Section 2 introduces the security analysis of a wireless network using the IEEE 802.1x protocol. Section 3 describes the proposed architecture. Section 4 discusses the experiment results. Conclusions are presented in Section 5.
modify the traffic avoiding that the entities detect this change.

The outcomes of the theoretical vulnerability assessment have been also confirmed by the experiments performed on a WLAN test bed implementing the standard security mechanisms under a wide typology of attacks. The test bed was composed of two access points (11Mbs), one mobile client (laptop) and one host. In order to provide more robust security services in the wireless networks, the IEEE introduced in 2001 the IEEE 802.1x standard. Nevertheless, the 802.1x standard alone does not solve all the problems encountered during the analysis phase. In fact it provides an asymmetric authentication protocol, in the sense that while the mobile host can be authenticated by the network, the mobile host has no meanings to authenticate the Access Point. Thus, the mobile host has to assume that the Access Point is a trusted node. Consequently, the 802.1x is intrinsically prone to two kinds of attacks:

- **Man IN The Middle (MINTM)**, where a third unauthorized entity acts between the Access Point (AP) and the mobile host (client). It deflects the transmission over itself in a transparent way: client and AP can not recognize that the packet flow is modified.
- The second kind of attack, called traffic hijacking, allows to the unauthorized user to disconnect the client and to continue the communication with its identity.

III. THE PROPOSED SOLUTION

In order to extend the security features of the 802.1x standard, we proposed an integrated security architecture complementing the IEEE802.1x, and EAP/TLS security protocols with an external server delivering the authentication, authorization and accounting service (AAA), like a RADIUS server, as outlined in Fig.I.

In the proposed solution we tried to satisfy some major constrains for a secure WLAN communication system. That is:

- **Access control**: to guarantee the access to a private network only to authorized clients; that can be obtained by means of an access key or a digital certificate.
- **Mutual authentication**: both clients and servers must recognize themselves to avoid the introduction of false Access Points.
- **End to end cryptographic coding**: to code the transmitted information point to point.
- **Single user key**: each user must have his key. No duplication should be allowed to avoid the discover of the security keys as in WEP where the keys are static.

Beyond these requirements, it is necessary to guarantee a complete support to the user mobility. In order to access to Local Network, it is necessary to deal with an access door. It is usually represented by the network interface in wired networks or by the Access Point (AP) in the wireless networks. The proposed solution is based on the IEEE 802.1x standard, that defines an authentication mechanism based on a dual door access concept, i.e., two logical doors: the access door and the service door are mapped on the same physical door. Since the user is outside the network, until not authenticated, the mobile host uses the access door to gain access to the authentication and identification services. None of the other services is available to him since the controlled service door is usually closed. When authenticated, the service door opens for the full services delivery.

![Fig. 1: centralized security architecture](image)

Fundamental features of the proposed solution are:

- The use of a centralized security architecture, based on a RADIUS server, and consisting of three distinct units: the client, the authentication and access system and the centralized authentication system.
- The possibility to use more than one authentication mechanism (so that the flexibility of the whole system is increased).
- Use of the `dual` door as foreseen by the 802.1x standard.

The higher security layer adopts the TLS protocol for digital certification. The point to point EAP-TLS communication protocol handle the authentication phase among the users and can provide the keys used by the user to encrypt the messages between the client and the AP, solving in this way a problem of the WEP protocol.

In a local wireless framework, the AC should handle the access and the opening of a secure session between the wireless client and the network itself by using the third entity: the authentication server dialoging using the EAP TLS protocol. As depicted in Figure 3, the connection procedure is a composed by steps process.

In the first phase, the client requests the WLAN access and identifies itself to the AP by starting an EAP/TLS handshake for the mutual authentication. It is based on the exchange of digital certificates and agreement on those parameters to be used to protect the subsequent information flows. During this phase it is also possible to define a dynamical session key for...
the encryption of the final authentication phase and the distribution of the dynamic WEP key.

The previous problems are solved using this protocol, which allows also to dynamically generate and distribute the WEP keys. It allows also to periodically executing the authentication process to prevent particular kind of attacks: in fact, if the time necessary to violate the generic key is equal to ‘x’ time units, it is enough to renegotiate the key every \( y < x \) time units to avoid this vulnerability.

To access to a WLAN, a user must authenticate itself by interacting with the RADIUS server. In this moment the controlled door is in the Open status. Only when this procedure is completed the terminal can get the access to the network.

During the ‘attempt of connection’ interval the door is in Locked status; if the authentication phase is successful, the door status changes to connection allowed.

IV. EXPERIMENTAL RESULTS

The solution proposed has been successful tested. From our results it is evident that to realize a secure wireless network without changing the IEEE 802.11 standard it will be necessary to introduce an external unit (as the Radium Server) together with auxiliary protocols as 802.1x e EAP/TLS. By having a third entity as security system presents advantages in the flexibility. It can be adapted to future security mechanism and protocols and it can be expanded in modular way.

The two kinds of attacks, previously considered, have been tested.

1. **MITM (Man In The Middle).**

The proposed solution EAP/TLS is able to reduce and avoid this attack, thanks to the mutual authentication and by creating an encrypted session to exchange the security parameters. The hacker is still able to detect and to intercept the encrypted traffic by using a sniffer, but he will not able to interact, as the real client, with the AP and to connect to the wireless client as a real AP. This is obtained thanks to the digital certificate shared between the entities during the handshaking process. Both client and server can authenticate each other by using a temporary key used only during this phase.

2. **Hijacking**

This attack is based on the sniffing of the EAP-Success message, sent by the AP to the client and used for ending the mutual authentication procedure. After this step message it starts a ‘secure’ session. Before sending the information packet, a security key must be created.
During this time interval, the hijacking attack can be performed. By using EAP/TLS the hacker does not know the secret key of WEP coding. That is the hacker’s packet is not considered by the AP since it does not know the coding scheme utilized. Hijacking attacks can be avoided by using session keys obtained with algorithms, as Diffie Hellman, that do not require the transmission of such keys. The malicious user is not able to intercept or to compute them. These keys protect also the authentication phase and the subsequent transmission of the WEP coding key.
V. CONCLUSIONS

In this paper the security aspects of a wireless LAN have been analyzed. The weakness of the existing architecture have been evidenced by realizing a test network. To overcome these problems, an integrated solution has been designed and realized. Experimental results show the effectiveness of the proposed solution. It is based on an authentication server RADIUS, together with the IEEE 802.1x protocol and the EAP/TLS protocol. The main advantage of having a third entity in a security system is the flexibility (it can be adapted to several future security mechanism) and it can be adapted to a growing number of users.

REFERENCES

[8] Nikita Borisov; Ian Goldberg; David Wagner - “Intercepting Mobile Communications: The Insecurity of 802.11”,
http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf, California at Berkeley ; September 2001
RFC 2284 - March 1998