IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 10, October 2017

Implementation of WLAN network with strong authentication

HAWA HOCH DIRRANEH[1], HUI ZHOU[1]

College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao, China[1]

Abstract: The Wi-Fi network is increasingly becoming a great technology, and it has excelled itself over the decade. Enabling users to access to the Internet and local networks of corporate or personal without cables'constraints. The current rate achieved through Wi-Fi network make it possible to transfer multimedia streams, but due to the wireless link itself, a strong security constraint also was imposed. The solutions used in wire networks are not adequate and efficient for WLANs. Thus, there is a great interest for me to find and implement the solutions specific to WLAN, even if sometimes they are inspired by an existing solution. The purpose of this article is to choose and deploy the most efficient solution on a test network through studying and analyzing the various authentication solutions on WLANs.

Keywords: Wireless Security, 802.1X, Radius, NPS, Attacks

I. INTRODUCTION

Today the wireless network has made a major success because they can be deployed to handle means of transmissions, without constraining of wires and the outlets. The current promotion for wireless networks mainly focus on the following aspects: the ease and speed of installation, lower cost of the wired system, mobility, and shared broadband services. Although this technology seems to be the most perfect and free, the reality is more difficult, mainly due to the protecting problem of these wireless networks, even if it's a simple attack. The nature of the signal transmission (electromagnetic waves) makes it difficult, even impossible, to completely control of the propagation. So, it is fairly easy to intercept the message and even intrude on such network, and it is necessary to define a mechanism for wireless networks based on strictly security policy such as authentication, integrity checking and encryption.

In this study, we will protect a Wi-Fi network through authentication server in infrastructure mode.

This article first introduces the background of WLAN and related work. The second part of this article presents a comparison of different solutions, including possible solutions.

II. WLAN BACKGROUND AND RELATED WORK

1. MODES OF WIRELESS LOCAL AREA NETWORKS

WLANs operate in two modes: Ad-hoc mode and Infrastructure mode. Ad-hoc mode is also known as point to point and consists of the wireless devices without the need for any central controller or access point (AP). In the infrastructure mode, WLANs infrastructure is expanding a wired network using wireless APs. AP is considered as a bridge between the wired and the wireless network and also acts as a central control unit in a wireless network for all wireless clients. The AP is responsible for managing the transmission and reception of wireless equipment within limited boundaries of the network. A network administrator can use APs from different vendors to increase the size of the network. This paper considers the security in the infrastructure mode.

2. EXISTING WLAN SECURITY SOLUTION

There are different security solutions for the IEEE 802.11 standard like Wired Equivalent Protocol (WEP), WPA, WPA2, and WPA2 using 802.1x servers. We explain the detail of each solution in the following:

WEP is the first security technique used in IEEE 802.11 standards and it provides security level for the WLANs equals to the wired LAN. WEP helps to make the communication secure and provides secret authentication scheme between the AP and the end user. WEP is implemented on initial Wi-Fi networks where the user cannot access the network without the correct key. WEP uses the shared key authentication method in which the user needs two things to access the WLANs, the service set identifier (SSID) and the WEP key generated by the AP.

Attacks on WEP: WEP is considered a weak technique for WLANs security since it uses RC4, a stream cipher that simply performs XOR operation on the data.

DOI10.17148/IJARCCE.2017.61042

2.1. Wi-Fi Protected Access (WPA)/ Temporal Key Integrity Protocol (TKIP)

There is a need to develop a new solution for WLANs security that provides more security than WEP. TKIP is designed on top of WEP to fix all its known weaknesses. To increase the key ability of WEP, TKIP includes four additional algorithms:

1. A cryptographic message integrity check that called Michael Integrity Code (MIC) to protect packets against bit-flipping attacks.
2. An IV sequencing mechanism that includes hashing, as opposed to WEP plain text transmission.
3. A per-packet key mixing function to increase cryptographic strength
4. A re-keying mechanism to provide key generation every 10,000 packets. TKIP encryption algorithm is used to avoid the problem that may exist in WEP technique by generating a separate key for each packet instead of only one key for all packets in WEP.TKIP also solves the drawback that may exist in IVs by increasing the size of IV which will help to solve the problems by using a longer packet counter to avoid the replay protection. By doing all this, TKIP is able to solve the problems available in WEP to some extent.

2.2. WPA / Advanced Encryption Standard

WPA is an enhancement of the WEP algorithm and the authentication of 802.11 networks. Developed by the IEEE to fill the WEP's weaknesses, WPA offers much better security compared to WEP thanks to:

- More random encryption techniques: In WPA, unlike WEP, the random character of the encryption is significantly strengthened, which has the effect of greatly complicate the task of the hacker.

- Ease of use: With WPA, the user will have no problem regarding the representation of the key that must be once in hexadecimal, another in ASCII. Here, use only a simple password.

2.3. WPA2 using 802.1x servers

Many companies recommend using WPA2 using 802.1x security protocol to overcome the dictionary and WPA handshake capture attacks on WPA/WPA2 protocols. This protocol combines the WPA2, which depends on AES encryption, with any strong authentication server. Many of these protocols enhance EAP authentication with stronger protocols such as LEAP (Lightweight EAP), EAPFAST, EAP-TLS (Transport Layer Security) or EAP-PEAP (Protected EAP).

3. ATTACKS ON WLAN SECURITY

This section, we classify all WLAN attacks that target to breach one or more of the six standard security requirements on the two levels the frame level and the RF level. There are many attacks on the frame level. Table.1 summarizes the important wireless attacks at the frame level.

Attack	Description	Security Element
Man in the middle attack (MITM).	If data are unprotected, hackers can intercept data.	Confidentiality Integrity
Dictionary attack	Programs that try large passwords to get the correct one.	Authentication Access control

Table 1: The Frame level Wireless attacks

There are many attacks on the RF level.Table.2 summarizes the important wireless attacks at the RF level.

Attack	Description	Security Element
DoS (Denial of Service)	Congesting a network resource with more requests.	Availability
IP Spoofing.	If the hacker has a rogue access point with enabled DHCP, it can effect on the main DHCP in the network.	Availability

Table 2: The RF level Wireless attacks

DOI10.17148/IJARCCE.2017.61042

III. THE PROPOSED WLAN SECURITY SOLUTION

Authentication is a procedure that consists, for a communication network, of verifying the identity of an entity (people, group, computer), in order to allow the access of the latter to resources (system, networks, applications ...).
In this section, the proposed solution for WLAN security is discussed. It requires working the various authentication solutions of a wireless local area network (WLAN), then make a comparative study of the solutions and choose the solution that suits us.

1. CISCO ACS SOLUTION

Cisco Secure Access Control Server (ACS) is a comprehensive network identification solution that provides the user with a secure experience on Cisco Intelligent Information Networks. It provides the integration and control layer between all users and corporate administrators on the one hand, and network infrastructure resources on the other.
Cisco Secure ACS expands access protection by centrally bringing together authentication, user or administrator access, and policy control, providing greater flexibility and mobility, enhanced security, and increased user productivity. Cisco Secure ACS guarantees the execution of prescribed policies by giving network administrators the ability to control:

- people who can log on to the network;
- The privileges assigned to each user on the network;
- Administrative information that must be recorded for security audit or accounting billing purposes;
- The access of each configuration administrator and the control commands that he can use.

ACS supports most current EAP methods. This software is simple enough to configure. The ACS authentication server unfortunately only runs on Windows and it offers authentication, authorization and the concept of Accounting. It is based on authentication protocols such as TACACS + or RADIUS. In addition, its price is relatively high.

i. The TACACS + protocol

TACACS + is the latest version of the TACACS protocol originally developed by BBN and then taken over by Cisco which will extend it for the first time by XTACACS (extended TACACS) compatible with TACACS, then by TACACS +. TACACS + uses TCP for its transport (unlike TACACS which was based on UDP). It uses port 49 (login). It manages the three AAA functions separately (authentication, authorization, accounting), unlike other authentication protocols.
TACACS + provides an implementation for all three, but one configuration does not require all of them.

ii. The RADIUS protocol

The Remote Authentication Dial in User Service (RADIUS) protocol was created by Livingston and standardized by the Internet Engineering Task Force (IETF) in the form of RFC (Request for Comments). Currently it is RFC 2138 and 2139.All RADIUS clients typically communicate over the local network on a single server, making the administrator's task easier. Management of users and their rights is then easier compared to several servers that should be updated simultaneously on the network.
The RADIUS standard is based on a set of user-related attributes. They are all stored in the RADIUS database of the server. During a connection, an exchange of information takes place between the server and the client (NAS). The RADIUS standard offers a number of attributes that must be implemented. But many specific protocol implementations bring their own set of attributes.

➢ **Comparison between TACACS + and RADIUS**

	TACACS +	**RADIUS**
Protocols	TCP: port 49	UDP: 1812 and 1813 Or UDP: 1645 and 1646
Encryption	Encryption of the entire package	Password encryption
Authentication and Authorization	Authorization and authentication are independent	Authorization related to authentication
Profile issue	Profile issued fields by fields at the request of the NAS	Global profile sent to NAS when authentication is complete
Challenge / Response	bidirectional	unidirectional
Primary use	Peripheral administration	Access to the network

Table 3: Comparison table between TACACS + and RADIUS

2. NETWORK POLICY SERVER (NPS) SOLUTION

NPS, or Network Policy server, is one of the roles available on Windows server (2008 and 2012). It is the replacement of IAS (Internet Authentication Service) available on Windows 2003 Server. Like a RADIUS server, NPS manages authentication and authorization according to the various connection modes (local, VPN ...)
It allows among other:

- Access to local resources via a remote connection (VPN ...);
- Authentication via Active Directory;
- Rights management via GPO.

But that does not stop there. These possibilities are the same as for IAS.

3. "FreeRadius" FREE SOLUTION

FreeRadius is a free Radius server for authentication. The radius protocol allows to connect via a UDP packet exchange, generally on port 1812. Radius also integrates an accounting module, allowing for example invoicing. Radius allows authentication via various means such as clear authentication, by MAC address, via MySQL / PgSQL database, MSCHAPv1 protocol and MSCHAPv2 or LDAP directory.
Radius also supports 802.1X with EAP tunnel authentication (PEAP / TLS / TTLS). FreeRadius relies on a system of modules that are activated / deactivated during authorization and authentication phases. The service can manage different virtual servers in order to manage several types of conflicting authentications, internal tunnels or proxy radius requests (in the case of chaining different radius servers).
The authorization phase defines the modules that will intervene to allow the user to use the connection. The authentication phase will rely on different modules to authenticate the user, via his password or his MAC address.

4. COMPARATIVE TABLE

This table presents the different characteristics of the possible solutions.

	Cisco ACS Solution	**Network Policy Server (NPS) solution**	**"FreeRadius" Free Solution**
Security	supports EAP and 802.1x methods - uses the RADIUS protocol or TACACS + - manages AAA; - enhanced security.	- supports EAP methods; - manages AAA; - uses the RADIUS protocol, 802.1X; - Authentication via AD; - Rights management via GPO.	-supports multiple protocols (RADIUS, EAP ...) - manages AAA - Effective solution for securing networks
Advantages	-It is a software that is easy to configure - Provides automatic management of the configuration in fact it saves the last modifications made to the system -measure the use of BP on inter-site links in real time	- Optimal security - Enhanced encryption - Transparency - User Authentication - Excellent performance - NPS is useful in complex network environments with users who access the network remotely and in different ways.	-RADIUS free, powerful and modular server - It is a powerful configuration system - the password is no longer transmitted over the network - It ensures the reliability
Disadvantages	- ACS only works under Windows	- NPS only works under Windows	- the RADIUS server must have the user's password in clear to authenticate the user
Cost	- Its price is relatively high.	- Low cost of network equipment.	-prix network equipment

Table 4: Comparative table of the different solutions.

DOI10.17148/IJARCCE.2017.61042

Choice of solution:
We chose the Network Policy Server (NPS) solution, which was the most convincing. It is a solution that is functional in a Windows server system and better matches our needs to set up our test network. A low-cost solution for management, offers a fairly secure connection capacity based on authentication and authorization protocols such as RADIUS, EAP and 802.1x. It is an easy to deploy solution and is easily modifiable, flexible and adequate.

IV. STRUCTURE AND NPS TECHNOLOGY

1. STRUCTURE OF NPS

NPS adopts RT-IPC and real-time synchronization provided by Real-Time Mach kernel for avoiding unbounded priority inversions. In network systems, fast responses are very important, NPS adopts the static prioritized worker model for reducing the worst case duration of priority inversion. NPS has two sets of workers: one is for processing requests from applications and the other is for processing packets from the network. Outgoing packets are processed by output worker threads, and the thread inherits the priority of an application. Incoming packets are processed by input workers. The priorities input workers are assigned according to the priorities in headers of packets. Also, there is one manager thread which receives Ethernet packets from a network. Since Ethernet packets do not support the notion of priorities, the thread is executed at the highest priority in the system.

2. MODEL OF THE PROPOSED SYSTEM

The following illustration shows NPS as a RADIUS server for a variety of access clients.

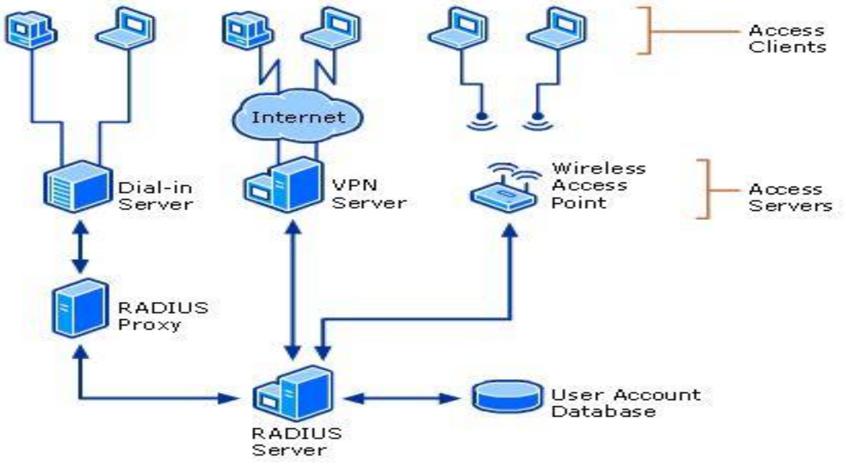

Fig. 1 Components of an NPS Infrastructure

Fig. 1 shows the Components of an NPS Infrastructure. A user sends a request to the NAS to allow a remote connection the NAS routes the request to the RADIUS server. The RADIUS server consults the identification database and returns one of the following three responses:

ACCEPT - Successful identification
REJECT - Identification rejected
CHALLENGE - Radius needs additional information and therefore sends a kind of small "challenge" to solve to confirm authentication.
Note: CHANGE PASSWORD is a possible fourth answer but it does not include standard Radius returns.

3. LIMITATION TO THE PROBLEM

When you provide employees in your organization and their computers with network connectivity through network access servers, such as virtual private network (VPN) servers, wireless access points, and access servers from a remote location, you can use NPS to create, centrally manage, and enforce network access policies that determine whether users and computers can or cannot access the network.

DOI10.17148/IJARCCE.2017.61042

V. CONCLUSION

Wireless LAN security is an important and compound issue. Although WLANs are providing flexibility and low cost, it is exposed to the danger of hacking if the security doesn't be achieved. The WEP protocol does not achieve the standard security requirements. This paper proposes a security solution that works into two levels, authentication and authorization according to the various connection modes (local, VPN ...). The proposed solution incorporates AES encryption, in conjunction with 802.1x, RADIUS proxy to forward connection requests to a remote NPS, provides a required frame security level for WLANs. However to guarantee network access control for users, we have implemented an authentication-based security policy based on a RADIUS server that checks the identification database to find out what type of authentication is required identification scenario requested by the user. We ended up securing our test network against all intrusions.

ACKNOWLEDGMENT

I would like to thank to the almighty for giving me the knowledge and courage to complete the research work on WLAN network with strong authentication. Moreover, I express my gratitude to my respected supervisor **DR. Zhao**, for following me to do research work deliberately. Finally, I wish to express my gratitude to my family and my friends, for providing endless support in every aspect possible, to ease my path on this journey.

References

[1] Server RADIUS, http://www.freeradius.org.
[2] Client 802.1X libre, http://www.open1x.org.
[3] Cisco Systems, Security Policy for Cisco Wireless LAN Controllers.USA, 2013.
[4] IEEE 802.1x. [Online].Available: https://en.wikipedia.org/wiki/IEEE_802.1x.
[5] J. Urpi "FreeRADIUS for small and mediumsized companies": AMK Logistic Systems, 2012.
[6] Siemens company, "WLAN security today: WLAN is more secure than wired network", July2008.
[7] RFC2284 EAP, http://www.ietf.org/rfc/rfc2284.txt.
[8] RFC2716EAP-TLS, http://www.ietf.org/rfc/rfc2716.txt.
[9] Internet Draft on EAP-PEAP, http://www.globecom.net/ietf/draft/draft-josefsson-pppext-eap-tls-eap-02.html.
[10] Internet Draft on EAP-TTLS, http://www.ietf.org/internet-drafts/draft-ietf-pppext-eap-ttls-03.txt.
[11] Server RADIUS, http://www.freeradius.org.
[12] Client 802.1X libre, http://www.open1x.org.