The 8th International Scientific Conference
"DEFENSE RESOURCES MANAGEMENT
IN THE 21st CENTURY"
Braşov, November 14th 2013

UNDERSTANDING WIRELESS DOS ATTACKS

Florin OGÎGĂU-NEAMȚIU

National Defense University of Romania "Carol I"/ The Regional Department of Defense Resources Management Studies / Brasov / Romania

Abstract :

Technological developments in recent years combined with better price-performance ratio and increasing mobility have led to a major development of wireless network technologies. Often in this process encouraged by the enthusiasm of their findings as well as increased demand from the market for such equipment developers have focused their efforts mainly on creating technologies that will provide better data transfer rates over greater distances and neglected the problem of safeguarding the privacy of data. However, organizations need to control and prevent their network and systems from being exposed to wireless attacks. Because many organizations overlook the potential impact of a Denial of Service (DoS) attack against their wireless networks this paper aims to analyze this kind of attacks and present the massive destructive impact that could range from service degradation to a complete loss of availability of the wireless network within the organization.

Key words: wireless, security, access point, protocol, wep, wpa2, wi-fi, attack, DoS

1.Introduction

The first wireless network was developed in 1971 at the University of Hawaii in a research project called ALOHNET and for the first time radio communication technology interacted with computer network technology.

The first equipment in this area was developed between 1979 and1981 and it was the result of amateur attempts to create wireless data transmission systems. It was only in 1991 that the first workshop discussing the subject was held and in 1997 the 802.11 standards appeared. The great interest shown by the public for this technology increased the spread of this type of equipment and therefore numerous 802.11 standards amendments appeared.

Although initially data security was not a criterion for the first developers to take into account, with the advent of 802.11 standards the WEP (Wired Equivalent Protocol) algorithm was implemented with the intention to provide a level of security comparable to that of a wired network. The standard had serious flaws and in 2004 the 802.11i amendment appeared with the intention to improve security mechanisms. Basically, the amendment introduced enhanced authentication mechanisms, encryption algorithms and key management procedures.

The 802.11i standard also called "Robust Security Network" provides improved authentication mechanisms by using high level protocols like 802.1X, EAP (Extensible Authentication Protocol) and RADIUS (Remote Access Dial In User Service) and a more powerful method of securing data using the protocol AES - CCMP (Advanced encryption Standard - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol).

In 2000 the Wi-Fi Alliance was founded with the goal to create a set of common standards for all producers in order to achieve maximum interoperability. The group worked on the IEEE 802.11i existing schemes and developed WPA (Wi-Fi Protected Access) protocol. As a result, compared to 802.11i standard, WPA did not implement the AES support because many devices that were on the market at that time lacked technological capabilities to cope with increased levels of computational resources required to achieve that encryption algorithm.

With the ratification of the 802.11i amendment in 2004 Wi-Fi Alliance introduced WPA2 protocol, a protocol that is fully compatible with 802.11i standard.

2. Protocols

2.1 WEP

The first wireless security protocol WEP uses for encryption the RC4 algorithm which combines a 40 bits stored key with a 24 bits initialization vector. The station then executes an XOR operation on the result with the actual data required to be transmitted and the resulted encrypted data stream is sent to the client station with the initialization vector. In order to decrypt the data the equipment uses the stored key from its memory and initialization vector attached to the data package.

2.2 WPA

Shortcomings of WEP protocol determined the need to seek an alternative and in 2003 the Wi-Fi organization has standardized WPA protocol. This was a restrictive version of 802.11i but it could be put in practice before the release of the final version.

The measures taken to combat the WEP security breaches are:

a) authentication mechanisms using superior technologies like 802.1X protocol, RADIUS (Remote Authentication Dial In User Service), EAP (Extensible Authentication Protocol). WPA provides mutual authentication, meaning that the client station can be authenticated before being granted access to the WLAN, and WLAN client can authenticate the AP before joining the network;
b) encryption has been improved by using Temporal Key Integrity Protocol (TKIP). It is based on the RC4 encryption algorithm, which is applied over a mixing function that generates a key for each transmission frame (dynamic keys);
c) WPA increases the RC4 initialization vector size to 48 bits and a key size of 128 bits;
d) the use of Michael Integrity Check method to test the integrity of data packets;
e) provides compatibility with 802.11i security standard

2.3 WPA2

Launched in 2004 the protocol is 100% compatible with the 802.11i standard and comes with some improvements over the WPA security mechanisms:

a) the use of the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) protocol, based on the Advanced Encryption Standard (AES) for encryption and message authentication. Although the TKIP standard was kept for compatibility with older systems the RC4 encryption vulnerabilities have been eliminated;
b) the implementation of WRAP (Wireless Robust Authenticated Protocol) which is based on the Offset Codebook (OCB) of the AES. Unfortunately, as several parties requested intellectual rights for this protocol, IEEE recommended the use of WRAP protocol only as an alternate component;
c) WPA 2 implements secure roaming support. Thus, two mechanisms are introduced for quick and secure client relocation between two APs:

- storing the credentials of the recent used wireless connections allows the client to quickly reconnect to an AP to which he has previously been connected without the need for re-authentication;
- the pre-authentication support allows customers to connect to a new AP while maintaining the connection with the older AP.

3. Wireless DoS attacks

The idea of a wireless network introduces multiple opportunities for attack and penetration that are either much more difficult or completely impossible to execute with a standard, wired network. During the past few years, wireless LAN security threats have increased rapidly which has affected users, vendors as well as manufacturers. The level of attacks has become more and more complex as more and more sophisticated and highly automated applications were made available. One of the most destructive attacks of a network and especially of a wireless network is a DoS (Denial of Service) attack.

In a DoS attack an attacker tries to stop the provision of services of a protocol/application or a particular machine within the network. Although the reasons for this kind of attacks are varied and do not necessarily lead into compromising data they obstruct access to networking resources of the organization and cause considerable damage. In a wireless environment such attacks generally target the access points because, given their role of nodes of interconnection, their operational status affects a lot of other users. An analysis of this type of attack revealed that in the first 3 months of 2013 the number of DoS attacks increased by approximately 27% compared to the same period of the last year. [3] In the next lines we are going to introduce the main DoS attack modes, present their mode of operation and provide some protection measures.

3.1. DoS by de-association / de-authentication

The 802.11i standard defines the conditions which must be satisfied by the client in order to be allowed to associate to the network. As depicted in Figure 1, before a station is granted the right to transmit it has to pass the authentication and then the association process. Consequently, when a station or AP wants to interrupt communication they will send a de-authentication request. Unfortunately, those messages are not secured so it is very easy to spoof the mac addresses of the station or AP and forge the de-authentication requests.

In a DoS by a deautentication attack one will try to take advantage of this behavior and send false data packets to the client or AP in order to make him believe that the other party wants to interrupt the connection (to de-authenticate). Because the client is involved in a communication it will immediately start the reconnection procedure. However, if the attacker will repeatedly send deautentication packets the client station will enter a connection-disconnection cycle and interrupt the transfer of useful data. This kind of attack offers great flexibility to the attacker and he can choose which station to attack or by capturing the AP's MAC address and using the broadcast MAC address he can target all stations connected to the network.

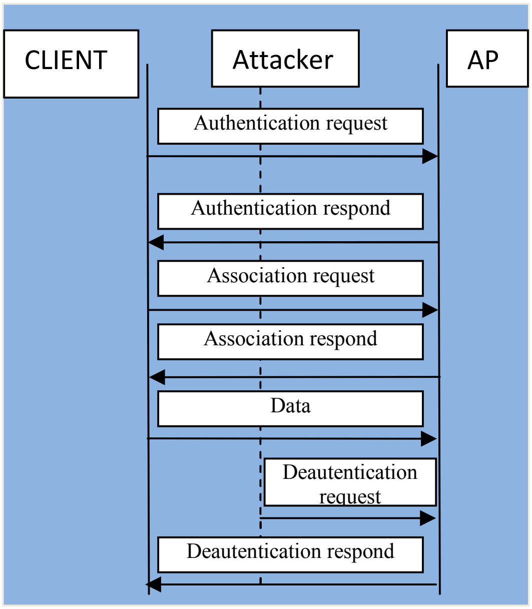
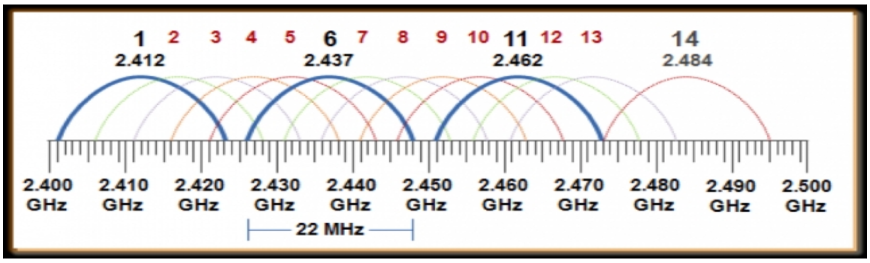


Figure 1 - 802.11i Authentication and association process

3.2 Jamming AP

Another method which can be used to achieve a DoS attack on a wireless network is by jamming frequencies that are used for communication. Currently 802.11 refer to the use of 2.4 GHz, 3.6 GHz, 4.9GHz and 5 GHz spectrum for wireless networking [11]. Each spectrum is divided into several partially overlapping channels. For example, the range of 2.4 GHz is divided into 14 channels of which 11 are used in the United States and 13 in Europe.



Pict. 2 - The 2.4GHz channels

With the help of adequate hardware and software equipment an attacker can identify the frequency used for communication and by using a high-power noise emission he can block the signal from the AP and consequently the stations are unable to connect or pass traffic.

3.3 Queensland DoS

The previous attack required specialized equipment to create a high power radio signal, equipment that costs a lot and is not always available. The Queensland method eliminates this drawback. This type of attack speculates the behavior of CSMA / CA (Carrier Sense Multiple Access / Collision Avoidance) protocol used is wireless networking to initiate data transmission. The protocol specifies that before sending a signal the station has to listen if some communication occurs on the selected channel. The station will initiate transmission only if the channel is free. By putting a NIC into continuous transmit mode no other communication can be initiated.

3.4 Association DoS attack

An association DoS attack consists of two phases. The first phase of this attack is to capture the MAC address for one or more stations. Then, using these addresses, the attacker floods the target AP with association packages causing equipment to create a huge number of entries in the association table. During this process the equipment's memory fills up and customer services are limited or stopped.

4. How to protect

An effective protection against DoS attacks is very hard to obtain because even if 802.11i has increased security measures it does not provide protection against this kind of attack. It is very important for an administrator to quickly identify such an attack and take appropriate measures. The most useful tool is a wireless intrusion prevention system (WIPS). It can help organizations establish a performance baseline for the network, detecting the DoS signatures, identify emerging attacks (a DOS de-authentication attack usually is followed by a "Evil twin" attack), identify emerging access points within network, provide detailed logs of the activities within the network, and even detect the source of the attack.

Because the DoS attack uses the unprotected association / disassociation / authentication / de-authentication packets IEEE developed the 802.11 w amendment in order to increase the security of management frames. So using equipment supporting this amendment could improve wireless security.

To defend against physical attacks strategic placement of access points is crucial. The equipment layout has to be made based on good area coverage, minimization of the signal spread outside of the desired space and interference avoidance. Because the frequencies are unlicensed and everybody can use them a lot of interferences can appear from other wireless equipment (wireless cameras, bluetooth devices, cordless phones, etc) or even other access points.

5. Conclusion

Recent years have witnessed a trend towards wireless technology. The latter provides organizations with advantages which are very attractive to them: quick provision of service, cost cuts, high mobility, etc. However, it has also created big vulnerabilities which can be exploited by attackers and create huge losses - DoS attacks being one of the most destructive of them.

Because the media used for signal propagation is the air it is very hard to create physical boundaries of the internal network. Combined with the automatic network discovery and association services provided by the modern operating systems a very good environment for an attacker to exploit the vulnerabilities of this kind of systems is created.

References:

[1] Ken Masica, “Securing WLANs using 802.11i”, Lawrence Livermore National Laboratory, 2007;

[2]” http://www.wi-fi.org/files/wp_9_WPA-WPA2%20Implementation_2-27-05.pdf”, last retrieved 07.09.2013;

[3]” http://www.pcworld.com/article/2035407/ddos-attacks-have-increased-în-number-and-size-this-year-report-says.html” last retrieved 07.09.2013;

[4]” http://en.wikipedia.org/wiki/List_of_WLAN_channels”, last retrieved 02.10.2013;

[5]” http://en.wikipedia.org/wiki/Beacon_frame”, last retrieved 15.10.2013;

[6]http://en.wikipedia.org/wiki/Denial-of-service_attack, last retrieved 11.10.2013.