AN INTRUSION DETECTION SYSTEM IN REAL TIME FOR WIRELESS 802.11

ABSTRACT

A wireless local area network is subject to attacks due to its means of transmission. The WEP is defined as the security mechanism in wireless network, but it is not sufficiently secure. Intrusion detection systems have been used to mitigate the weaknesses of the WEP. Nowadays, the existing intrusion detection systems of open source code are either static in terms of signature or limited in terms of types of attack detection. In this article we propose a real time intrusion detection system that logs event and it is configurable in terms of signature. The attacks that the system detects include: presence of non authorized element such as users, access points and tools of War Driving, and denial of service.

1 Introduction

Nowadays the number of local wireless networks has been increasing compared to the physical ones. The increase is due to the fact that the wireless network technology together with the cable networks permits an easier set up and mobility to its users.

Cable networks transfer information through links whereby the connection can be physically verified while the wireless networks use air as a means of transmission and the connections do not need wires. In this way an attacker does not need to have wired access, but needs to be in the coverage area in order to connect myself and obtain the information he needs.

It is assumed that together with the number of wireless network, there is an increase of the number of malicious tools which have become more sophisticated representing a serious threat to this kind of environment [1].

The WEP (Wired Equivalent Privacy) is the security protocol by the IEEE pattern 802.11 [2] which intends to provide security to wireless network similar to the physical ones. Its main objective is to protect data transmitted over the wireless link of malicious attackers.

The WEP is a primary protection for a WLAN (Wireless Local Area Network) and many studies have shown weaknesses in the protocol. It can be assumed the WLAN security conditions with the WEP are considered critical [3], what has led to the development of new mechanisms of security such as the WPA (Wi-fi Protected Access) [15] which comes to replace the WEP in opposition to 802.11 b/g. The protocol 802.11i [6], [15] has been expected to overcome the deficiencies of earlier patterns soon.

A WIDS (Wireless Intrusion Detection System) is an extension of the IDS (Intrusion Detection System) for wireless environment. A WIDS is a tool that captures the local wireless communication and generates warnings based on the predetermined signatures of traffic anomalies. The WIDS are usually based on detection and react to attacks through warnings and blockers [8].

From a traditional IDS concept, one can define a wireless IDS as resource which operates in wireless communication, and monitors and analyzes the users actions and systems activities reorganizing attack patterns, identifying abnormal activities, and monitoring the WLANs.

As a WIDS captures all local transmissions, it permits that the administrator has a better information of the network condition and enables him to deal with activities identified in a short interval of time [8].

Some work of open source code which offers solutions for the wireless network security is cited as follows. The wIDS is a tool developed by Mi Keli [10] and detects the suspicious activities with repetitive requests for the association of the determined access point, and the detection of a large volume of requests of authentication in a short interval of time. The wIDS does not depend on that kinds of boards and chipsets, it is only necessary that the interface be functional enough to enter in monitor mode (RFMON - Radio Frequency Monitor) [17] and be ready to work with this program. Another characteristic of the wIDS is the possibility to register the traffic through a file in the pcap format, for further analyses. Some disadvantages of wIDS include: (i) it only detects signatures of attacks included in its code, (ii) it does not
identify the attack completely, warning only the number of requests of associations or authentication made for a destiny.

The Widz is a tool developed by Fatbloke [9] and it is divided into two modules: widzapemon and widz-probemon. The module widz-apemon monitors the active access points in a determined area. If an access point is found, the tool compares it with list of access points authorized which are in a configuration file called widz-apmon.conf. In case the access point found is not in the list, the program sends a warning. The module widz-probemon monitors the general traffic permitting to detect abnormalities such as the quantity of requests of association and detection of MAC address and network identifier (SSID - Service Set Identification) which are not in the list of MACs addresses and SSIDs registered in the Widz. The Widz has the following disadvantages: it does not record the network traffic in a file for future analyzes, it only detects signatures of attacks included in its code, and detects DoS in very long times (10 requests in 10 minutes).

The Snort [5] is a conventional tool to identify possible attacks based on signatures, packets badly formed and suspect traffic of packets. However there are wireless network characteristics that are not addressed by the existing functionalities of this tool. Due to this shortcoming, the project Snort-Wireless [11] was proposed, which is nothing more than a group of complementary codes (patches) to the conventional Snort, which specifically deals with the wireless network characteristics. Nowadays, the Snort-Wireless detects non authorized access points in an environment and scans made by tools like Netstumbler [13]. The Snort-Wireless has a file of signatures where one can add new attacks.

In this article a real time IDS, which logs information for analyses, is proposed. It detects the presence non authorized wireless elements such as users, access points, tools of War Driving and attacks of DoS and it has a flexible base of attack signatures, which permits the addition of new attack signatures during its operation. In order to verify the system, a prototype was developed which implements detection and reconfiguration in real time. The rest of the article is organized as follows. Section 2 illustrates the scenery where the proposed IDS operates and presents the architecture whereby the prototype is built. In section 3 the rules for attack detection are presented. Section 4 describes the tests and section 5 presents the conclusions of the work.

2 Scenery and Architecture

The typical scenery for the operation of WIDS is presented in Figure 1.

![Figure 1: Typical scenery.](image)

The mobile devices are connected through a access point device. They can have access to Internet through the access point, in the infrastructure mode. In addition to the description of the elements which compose the wireless network, it is also presented how the local area network can be attacked. The attacks related to 802.11 discussed in this article include denial of service, the use of Rogue Access Point, War Driving, and unauthorized users.

The architecture of the prototype is presented in Figure 2, and it consists of four modules: capture, analysis, detection and alarm.

![Figure 2: Architecture of the prototype.](image)

The capture module collects and stores the frames for future analyzes, and also sends the data to analysis module. The analysis module uses the protocol 802.11b/g to make the codification and classification of the suspect frames of the data link layer of the wireless environment.
As defined in the pattern IEEE 802.11 [2], there are types of frames which must be analyzed in the WLAN:

1. Management Frame: WLAN uses these frames to establish connections between access point and clients;
2. Control Frame: They are responsible for the access control to the environment;
3. Data Frame: They are used to deliver store.

The detection module monitors the data coming from the analysis module and answers to offensive behaviors related to attacks. This module uses a file of signatures and activates the procedures for intrusion detection. The signatures are kept in a linked list which are loaded during the prototype initiation. The analysis module sends the frames to the detection module, and the detection module compares the already rebuilt and legible frame, with those recorded in the attack signature list and defines what to do with the frame. Figure 3 presents the flow of control of the detection module.

According to Figure 3, each received frame of the analysis module is compared to the contents of each node of the linked list which contains the signatures, in case of signature matching, the detection module sends the frame to alarm module, otherwise it discharges the frame, considering it as the normal network traffic.

The described archive of signatures of attacks described above, is used for identification of possible attacks. The form of writing of the signatures is simple so that new signatures can be recorded. The addition of new signatures in the file, can be carried out in real time, through a function of the system (system call) [16]. It verifies the size and the hash code of the file of signatures. In case that an update in the file occurs, the module executes a procedure that updates the linked list of signatures of attacks in a short interval of time.

The way how the rules are generated for attack signatures is discussed in the following section.

3  Rules for the proposed detection of WIDS

3.1 Detecting unauthorized users

The network mapping is difficult due to the MAC address verification during the scan phase. In the scan phase, the MAC address of the device is verified against a list of MAC addresses stored in the prototype. In case the MAC address of the device is not registered, the prototype sends a warning notifying the administrator. Figure 4 presents the pseudo code for the detection unauthorized users.

![Figure 4: Pseudo code for the detection of unauthorized users.](image)

3.2 Detection of false access points

A Rogue Access Point (Rogue AP) can be seen as strange access point without authorization of a determined network infra-structure. It is usually a small equipment and of short reach installed by badly intentioned users who are not authorized by the security policy of the local network administration. The Rogue AP can open a wide range of opportunities for attacks because it broadcasts the presence of wireless connection [14].

In order to help the network administrator to audit the area, a function is developed in which a prototype captures the frames of beacons [3] transmitted by the access point that serves to announce and divulgate its presence in a determined area. In some instants a beacon frame is captured and the prototype compares the address MAC, the SSID and the channel to their counterparts in a list of access points registered.
In case it does not find it in the list of registered access points, the prototype considers the access point as a Rogue AP and sends a warning notifying the administrator. Figure 5 presents the pseudo code to detect the false access points.

3.3 Detecting scanning tools

The network wireless scanning is popularly known as war driving [1] and it consists of scanning a geographic area searching for information that identifies a wireless network and its characteristics as the SSID, MAC address, WEP cryptography in use and the signal power. Such a procedure is performed in the following way. Before being connected to a WLAN, the client station needs to locate an access point by either listening to the beacon frames or doing a broadcast of probe request frame repeatedly the access point usually replies with a probe response to inform its existence to the client who requested (probe request) to establish the connection.

In this way the tools of scanning as the Netstumbler [13] can explore such a vulnerability, by scanning many access points within reaching area and by transmitting frames of probe request.

An analysis of the traffic of the probe response was made by monitoring the area and it was noticed an abnormal increase in its traffic when the Netstumbler present, because it makes the access point generate these frames provoking this raise.

However entitled users must as well do broadcast of frames of probe request making the access point generate frames of probe response. So the variance analysis of frames probe response is required to determine the main cause in this traffic increase. Through this analysis it was elaborated an average generated by the number of frames of probe response captured at a defined time divided by the quantity of clients per network. Figure 6 presents the pseudo code.

3.4 Detecting the deauthentication DoS

Due to their characteristics, the wireless networks have a greater exposure of attacks of denial of service than the physical ones [1]. In this way a malicious station may seem within reach area of a network and launch an attack to stop the communication.

In this simulation, the tool Aireplay of kit Aircrack is used [7]. The attack starts by sending an number of frames of deauthentication to the access point. In this way all the stations that are associated to this access point will begin to deauthenticate and restart the scanning process in the access point. The attack can be used to break the WEP key when the clients try to reauthenticate in the access point. An increase in the data traffic occurs, which are captured by tools like the Airsnort [4] to break the WEP key. The following pseudo code presented in Figure 7 in order to deal with this attack.
4 The prototype verification

The prototype was implemented and tested with an access point Enterasys RBTR 2-A which implements the protocol 802.11b and the three desktops, as shown in Figure 8.

The desktop which runs the prototype has three network interfaces. The first PCI interface Dlink DWL-520+ is used to capture the traffic of the local wireless network. The other two interfaces of the Ethernet network which are used to connect the access point to the wired backbone and as well as to the server DHCP, have the operating system Linux Slackware 10 with kernel 2.4.26. The second desktop is a authentic network client, with operating system Windows XP and an interface PCI of wireless network Dlink DWL-G520+, while the third desktop was used to launch attacks to wireless network with operating system Linux Slackware 10 with kernel 2.4.26 and Windows XP operating system, has a PCI interface of Dlink DWL-520+ wireless network.

4.1 Attack signature edition

The file of signatures, used to identify the possible attacks is presented in Figure 9. The writing form is very simple, take for example the first signature "0x50-20-90-Netstumbler" the first field refers to the kind of frame (0x50 - probe response), the second field refers to the time interval in which the quantity of frames occur (20 seconds), and the third field refers to the quantity of frames of this type which have been transmitted (90 frames probe response) and the last field refers to the attack description (Netstumbler).

4.2 Prototype presentation

As described in Figure 10, the prototype shows a list of access points detected and also a list of connected clients.

The BSSID field shows the MAC address of the access point detected, the PWR field shows the level of the signal of the access point or station if the signal is equal to -1, the driver is not supported. The Beacons field shows the number of frames beacon sent by the access point to announce its presence. The Packets field shows the number of data frames captured, the CH field presents the number of the channel in which the access point is operating the MB field presents the speed supported by the access point if the MB field is 11 it indicates 11 Mbps which represents the network 802.11b. The WEP field shows if the algorithm of cryptography is being used. If it presents "N" it means that the network is not using the algorithm and if it presents "Y" it means that the network is using the algorithm.
The ESSID field presents the network identifier which is captured by the probe response frames and the request association. The STATION field shows the MAC address of each station associated to the net. Finally, the WARNING field presents the warnings that are generated in case of attack.

4.3 Detection of scanning tools

In order to simulate the War Driving attack, a desktop with a Netstumbler tool installed was used. First the Netstumbler starts to ask for a connection to the access point. Immediately then the Netstumbler locates an access point and the prototype also detects the presence of the attacker. Figure 11 is the prototype generating a Netstumbler warning.

4.4 Detecting the deauthentication DoS

A desktop running the Aireplay tool is used to represent the DoS attack of deauthentication. The Airplay is triggered by sending messages to the access point by transmitting 500 frames of deauthentication per second. Immediately the prototype detects a very high quantity of frames of deauthentication and rings an alarm. Figure 12 presents the prototype generating a DoS warning of deauthentication.

4.5 Detecting unauthorized users

This function is used to identify MAC addresses which are not authorized in the wireless local network. The prototype contains a list of MAC addresses of all clients who are allowed to use the network. The prototype detects as soon as the unauthorized element reaches the coverage area. Figure 13 presents the prototype generating a detection warning of an unauthorized user with a MAC address (00:0D:88:F0:E7:0C).

4.6 False access point detection (Rogue AP)

An access point of Dlink DWL-2100AP was used to perform the role of Rogue AP. This topology could be simplified, because there are already softwares packages, such as the hostAP [12], which transforms a simple machine with wireless network interface into an access point.
At the association instant, the wireless equipments search for access points with the same SSID and with a better relation noise-signal. Assuming that the Rogue AP is properly positioned, it is chosen for association.

A Rogue AP must send beacon frames informing its SSID and the used channel, or respond to probes of mobile devices. The SSID used is the same of the network being attacked. To obtain the SSID of a network, a scan was performed in the area using a Netsumbler tool.

The channel number is also important to avoid interferences between the Rogue AP and the real access point. Therefore, the Rogue AP was configured to work in a different channel. Figure 14 presents the prototype generating a detection warning of a false access point.

![Figure 14: Prototype generating a warning of false AP.](image)

5 Conclusion

An IDS prototype was developed for wireless networks in order to improve the security of a WLAN. The prototype detects the following attacks: war driving, unauthorized access points (Rogue AP), denial of service, and the presence of unauthorized users. The system permits the attack signature configuration and it has been tested with success. However it may present some performance problem if it has to process a large number of messages. Eventually other data structures as trees can be used with the purpose to improve the performance. Another possible extensions of this work are: (i) test the prototype using the algorithm of security WPA, (ii) extend the prototype to work as a distribution system of IDSs.

References


