Wireless Intrusion Prevention Systems

Jack TIMOFTE
jack.timofte@gmail.com

The wireless networks have changed the way organizations work and offered a new range of possibilities, but at the same time they introduced new security threats. While an attacker needs physical access to a wired network in order to launch an attack, a wireless network allows anyone within its range to passively monitor the traffic or even start an attack. One of the countermeasures can be the use of Wireless Intrusion Prevention Systems.

Keywords*: Network security, IDS, IPS, wireless intrusion detection, wireless intrusion prevention.*

This paper will focus on the WLAN networks security threats and their protection through wireless intrusion prevention systems.

The Wireless Local Area Networks, or WLANs, are defined by the IEEE 802.11 families of standards. An 802.11 WLAN consist of **stations** (laptops, PDAs, mobile phones etc) and **access points** (or APs), which logically connect the stations with a distribution system (DS), typically the organization’s wired infrastructure. A WLAN can run in **ad-hoc** mode, without the use of APs, and involving a direct communication between stations and in **infrastructure** mode, in which case the station connects to a DS via the access point. The identification of stations and APs is made by the use of 48-bit MAC addresses.

The initial security standard introduced for WLANs, called Wired Equivalent Privacy, or shortly WEP, is well-known for its security flaws. Introduced in 1999 as part of the 802.11b, its objective was to secure the wireless communication by using the symmetric encryption protocol RC4. However it took a short time for the WEP weaknesses to be discovered and attack tools to be freely available to the public (like AIRSnort and WEPCrack). For example, AirSnort can determine the encryption key in less then a second, provided that a sufficient number of packets have been gathered – usually in the range of 5 to 10 million. Even if the number appears quite big, on a busy WLAN this volume can be generated in a relatively short time.

To address the issues with WEP, other newer protocols (like Wi-Fi Protected Access) were introduced, which offer a better protection, but still suffer from different security issues.

The adoption of the WLANs in organizations introduced new specific threats for them, and as we will see in this paper some of these issues can be covered by using wireless intrusion prevention systems. The most important threats are presented below.

Rogue access points - represent unauthorized access points and can be internal or external.

The internal rogue AP is connected to the wired network by an unauthorized user (such as a regular employee), outside the control of the IT personnel. It can behave as a gateway for an attacker who can gain access to the network without the need to be physically inside the organization’s perimeter. Therefore the detection and the removal of such rogue access points must be considered a critical aspect. It can be noted that this threat can affect also organizations which do not use WLAN networks in their activity.

The external rogue access point is not connected to the wired organization’s intranet, but emulates a legitimate access point of the network. For example, the attacker can set the rogue access point’s SSID to the same SSID like the legitimate AP, and then increase significantly the signal of the rogue AP. Its purpose is to trick the WLAN clients by connecting to this rogue AP instead of the legitimate AP, since the clients will normally try to connect to the AP with the strongest signal available and to cause the client association to the rogue AP, making it possible to launch other attacks (obtaining user credentials via spoofed web pages etc).

MAC address spoofing. An access point can be configured so that it keeps a list of the legitimate client stations by MAC address. The attacker has the option of compromising such a client, or by spoofing with a legitimate MAC address. The MAC addresses are uniquely assigned at the time of manufacture, but usually this value can be set to arbitrary chosen values using an appropriate software tool.

Denial-of-Service. A denial of service (DoS) attack occurs when a system cannot provide services to authorized clients due to resource exhaustion by unauthorized clients. This can be done by *jamming* (generate random signal on the specified frequencies), *flooding with associations* (the association table maintained by the AP has a maximum value – when this table overflows, the AP cannot accept further client association requests), *forged disassociation* (the attacker sends spoofed disassociation frames with the source MAC address of the AP – in this case the station is still authenticated but has to send a Reassociation request to the AP; to prevent reassociation, the attacker can continue to send disassociation frames for a specific period), *forged deauthentication* (an attack similar to *forged disassociation*, but which uses deauthentication frames).

Monitoring WLAN traffic and breaking the encryption keys. There are open-source tools, like AIRSnort (for WEP), which can be used by anyone to intercept the wireless traffic and computing the encryption keys, provided there are enough data packets.

Given the threats outlined above, it becomes obvious that for any organization using WLANs the monitoring of the air space should be an important measure in assuring a proper network security. Furthermore, considering the potential threat introduced by the internal unauthorized access points, it is highly recommended that any organization monitor its air space.

Wireless Intrusion Prevention Systems (WIPS).

We will use as a starting point the definitions for intrusion detection and intrusion prevention given by NIST [1]: “*Intrusion detection is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Intrusion prevention is the process of performing intrusion detection and attempting to stop detected possible incidents. Intrusion detection and prevention systems (IDPS)1 are primarily focused on identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.* „

There are several types of intrusion detection/prevention systems: *network-based*, *wireless*, *Network Behavior Analysis* and *Host-based*.

A typical wireless intrusion prevention system consist of:

- *wireless sensors* – used to monitor and analyze activity;
- *management server* – receives information from the sensors and perform analysis;
- *database server* – used to store event information generated by sensors and management servers;
- *console* – represents the interface for the users and administrators.

In a wireless intrusion prevention system, a normal sensor cannot monitor all the traffic on a band (which consists of more channels) simultaneously and can monitor only a single channel at a time; to cover multiple channels, it uses a technique called channel scanning, which involves monitoring each channel a few times per second. To reduce or avoid this limitation, there are specialized sensors that use several radio modules and can monitor several channels at the same time.

The intrusion prevention systems can detect incidents using mainly three methodologies: signature-based, anomaly-based and stateful protocol analysis. Most systems use multiple detection methodologies, either separately or integrated, for a more accurate detection.

Signature-based detection involves comparing signatures against observed events in order to identify possible incidents; this method is very effective in the detection of known threats but does not provide good results in detecting previously unknown threats.

Anomaly-based detection involves creating 'normal' activity patterns and comparing the observed events against these patterns. The intrusion detection/prevention system has an initial training phase, in which the system learns the normal behavior and creates profiles, which are used as a base for comparison. A static profile is determined in the training phase and remains unchanged, whereas a dynamic profile is constantly adjusted as additional events are observed.

Stateful protocol analysis is the process of comparing predetermined profiles of generally accepted definitions of benign protocol activity for each protocol state against observed events to identify deviations.

The main types of events which can be detected by wireless intrusion prevention systems are:

- *unauthorized WLANs and WLAN devices* (rogue APs, unauthorized stations, unauthorized WLANs);
- *poorly secured WLAN devices* (misconfigurations, use of weak WLAN protocols and implementations);
- *unusual usage patterns* (using anomaly-based detection);
- *the use of wireless network scanners* – obviously only active scanners can be detected;
- *Denial of Service (DoS) attacks* (flooding, jamming);
- *Impersonation* and *man-in-the-middle attacks*.

The prevention capabilities refer to *wireless actions* (such as terminating the connections between a rogue or misconfigured station and an authorized AP by sendinq deassociation messages to the endpoints) and *wired actions* (such as blocking a switch port on which a particular station or AP is connected).

Another feature contained in most wireless intrusion prevention systems is *tracking the location* of the threat – by using triangulation (estimation of the approximate distance from multiple sensors by the strengths of the threat's signal received by each sensor and calculation of the physical location based on this information)

Given the importance of the wireless security, many companies have developed wireless intrusion detection/prevention systems. One of the well-known WIPS is AirDefense (www.airdefense.net), which uses context-aware detection, correlation and multi-dimensional detection engines, and it claims to have a very low rate of false positives. The system can detect ad-hoc stations, rogue access points, as well as open or misconfigured access points, masquerade attacks (like MAC spoofing), man-in-the-middle attacks, denial-of-service attacks. The system can be configured to play an active role and respond automatically to wireless threats by stopping the corresponding device before it is able to cause damage to the network. For the rogue internal APs, the AirDefense system can identify the switch port to which the AP is connected and turn it off, thus preventing the rogue device from accessing the network. In addition, the system can help system administrators to troubleshoot wireless network performance, has location tracking capabilities and can generate standard or customized reports.

There are also open source tools, such as Snort-Wireless or Kismet, which have mainly intrusion detection capabilities.

Limitations

Although a Wireless IPS can do a lot of things, it has its limitations. For example, it cannot detect a passive sniffer – and usually an attacker can first collect data traffic before launching an attack. This period of passive sniffing is quite dangerous, but there is nothing to do in this direction. The only countermeasure is to use the proper protection through encryption.

Another notable problem refers to the deployment of sensors. As opposed to a wired IDS/IPS system, where the location of the sensors follows the logical structure of the network, the wireless sensors have to be placed based on physical location.

In addition, there are the common IDS/IPS limitations, like the issues of false positives.

Conclusion

As we saw, the WLANs brought not only advantages, but also some specific security threats. For organizations using WLANs, it is obvious that they need protection against wireless threats. However a real-time wireless intrusion detection tool for the detection/removal of rogue access points is a must for almost any organization. There are many WIPS products available, at different price tags, and even open-source. The development of new wireless standards and security protocols is expected to enhance the WLANs' security, but we estimate that wireless intrusion prevention systems will continue to play a key role in assuring the organization's security.

References

1. Karen Scarfone, Peter Mell, *NIST 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS)*, Feb 2007
2. Ken Hutchiunson, *Wireless Intrusion Detection Systems*, SANS Institute, October 2004
3. Bruce Potter, *Wireless Intrusion Detection*, Network Security Volume 2004, Issue 4
4. Fluhrer, Mantin and Shamir, *Weaknesses in the Key Scheduling Algorithm of RC-4*, 2001
5. IEEE 802.11 Standards Website, http://**ieee**802.org/11/
6. AirDefense Website, http://www.airdefense.net
7. AirSnort Website, http://snort-wireless.com
8. Kismet Website, http://www.kismetwireless.net