

# Wireless Intrusion Detection Systems

*Jamil Farshchi* 2003-11-05

## Introduction

Threats to wireless local area networks (WLANs) are numerous and potentially devastating. Security issues ranging from misconfigured wireless access points (WAPs) to session hijacking to Denial of Service (DoS) can plague a WLAN. Wireless networks are not only susceptible to TCP/IP-based attacks native to wired networks, they are also subject to a wide array of 802.11-specific threats. To aid in the defense and detection of these potential threats, WLANs should employ a security solution that includes an intrusion detection system (IDS). Even organizations without a WLAN are at risk of wireless threats and should consider an IDS solution. This paper will describe the need for wireless intrusion detection, provide an explanation of wireless intrusion detection systems, and identify the benefits and drawbacks of a wireless intrusion detection solution.

## Threats to wireless local area networks

Wireless local area networks are subject to a variety of threats. The standard 802.11 encryption method, Wired Equivalent Privacy (WEP) is weak. As documented in the paper "Weaknesses in the Key Scheduling Algorithm of RC-4" [1], the WEP key of a wireless transmission can be acquired via brute force attack. So even if WEP encryption is utilized on a WLAN, an attacker can potentially intercept and decrypt sensitive data from wireless communications.

Hackers can also attack a WLAN and gather sensitive data by introducing a rogue WAP into the WLAN coverage area [2]. The rogue WAP can be configured to look like a legitimate WAP and, since many wireless clients simply connect to the WAP with the best signal strength, users can be "tricked" into inadvertently associating with the rogue WAP. Once a user is associated, all communications can be monitored by the hacker through the rogue WAP. In addition to hackers, rogue WAPs can also be introduced by users. Low cost and easy implementation coupled with the flexibility of wireless network communications makes WLANs highly desirable to users. By installing a WAP on an established LAN, a user can create a backdoor into the network, subverting all the hard-wired security solutions and leaving the network open to hackers. It is for this reason that even organizations without a WLAN implementation must strongly consider deploying a wireless IDS solution. It is very possible that users can and will install a rogue WAP, exposing even an exclusively hard-wired organization to the risks of

WLANs.

Networks using 802.11 are also subject to a number of denial of service (DoS) attacks that can render a WLAN inoperable. Wireless communications are inherently vulnerable to signal degradation when encountering physical objects. Trees, buildings, rain, and hills are all variables which can deter wireless communications. In addition to physical obstacles, many common devices such as microwave ovens, cordless phones, and baby monitors can interfere with 802.11 networks. Hackers can also cause malicious DoS attacks by flooding WAPs with association requests and forcing them to reboot. In addition, they can use the aforementioned rogue WAP to send repeated disassociate/deauthenticate requests to deny service to a wireless client.

A variety of other WLAN threats exist and additional vulnerabilities are being identified at an ever-increasing pace. The point is that the threats are real, they can cause extensive damage, and they are becoming more prevalent as the 802.11 technology grows in popularity. Without some sort of detection mechanism, it can be difficult to identify the threats to a WLAN. A lack of threat awareness can lead to a network not adequately secured against the threats facing it. Only when the threats to the network are realized can the WLAN be properly equipped with the necessary security measures.

## **Intrusion detection**

Intrusion detection systems (IDSs) attempt to identify computer system and network intrusions and misuse by gathering and analyzing data. IDSs have traditionally been developed to detect intrusions and misuse for wired systems and networks. More recently, IDSs have been developed for use on wireless networks. These wireless IDSs can monitor and analyze user and system activities, recognize patterns of known attacks, identify abnormal network activity, and detect policy violations for WLANs. Wireless IDSs gather all local wireless transmissions and generate alerts based either on predefined signatures [3] or on anomalies in the traffic [4].

A Wireless IDS is similar to a standard, wired IDS, but has additional deployment requirements as well as some unique features specific to WLAN intrusion and misuse detection.

## **Wireless intrusion detection systems**

Wireless IDSs can be purchased through a vendor or developed in-house. There are currently only a handful of vendors who offer a wireless IDS solution - but the products are effective and

have an extensive feature set. Popular wireless IDS solutions include Airdefense RogueWatch and Airdefense Guard [5], and Internet Security Systems Realsecure Server sensor and wireless scanner products [6]. A homegrown wireless IDS [7] can be developed with the use of the Linux operating system, for example, and some freely available software. Open source solutions include Snort-Wireless [8] and WIDZ [9], among others.

## Architecture

A wireless IDS can be centralized or decentralized. A centralized wireless IDS is usually a combination of individual sensors which collect and forward all 802.11 data to a central management system, where the wireless IDS data is stored and processed. Decentralized wireless intrusion detection usually includes one or more devices that perform both the data gathering and processing/reporting functions of the IDS. The decentralized method is best suited for smaller (1-2 WAP) WLANs due to cost and management issues. The cost of sensors with data processing capability can become prohibitive when many sensors are required. Also, management of multiple processing/reporting sensors can be more time intensive than in a centralized model.

WLANs typically encompass a relatively large physical coverage area. In this situation, many WAPs can be deployed in order to provide adequate signal strength to the given area. An essential aspect of implementing a wireless IDS solution is to deploy sensors wherever a WAP is located. By providing comprehensive coverage of the physical infrastructure with sensors at all WAP locations, the majority of attacks and misuse can be detected. Another benefit of positioning the sensors in close proximity to the WAPs is the enhanced ability to physically pinpoint the geographical location of an attacker.

## Physical response

Physical location detection is a pivotal aspect of a wireless IDS. 802.11 attacks are often carried out in close proximity to the WAP and can be performed in an extremely short timeframe. Therefore, the response to attacks needs to not only be logical, like standard IDSs (i.e. Block the offending IP address), the response also needs to incorporate the physical deployment of individuals to identify the attacker - and the response must be timely. Unlike wired attacks where the hacker is usually great physical distances from the victim network, wireless attackers are often physically located on the local premises. A wireless IDS can aid in detecting the attacker's location by providing at least a general estimate of their physical location. By

correlating the captured 802.11 data with the sensor location as well as the location of the victim WAP, the physical location of the attacker can be more easily identified. An even more ambitious approach to physical location identification would be to also use directional antennae in an effort to triangulate the 802.11 attacker signal source [10]. Once the physical location has been narrowed, a response team equipped with tools like Kismet [11] or AiropEEK [12] can scan the general area identified by the IDS to further narrow the search for the attackers. With this dual-pronged identification approach (using the IDS and scanning tools), the physical response team should be able to identify and intercept the attackers quickly and effectively.

## Policy enforcement

A wireless IDS not only detects attackers, it can also help to enforce policy. WLANs have a number of security-related issues, but many of the security weaknesses are fixable. With a strong wireless policy [13] and proper enforcement, a wireless network can be as secure as the wired equivalent - and a wireless IDS can help with the enforcement of such a policy.

Suppose policy states that all wireless communications must be encrypted. A wireless IDS can continually monitor the 802.11 communications and if a WAP or other 802.11 device is detected communicating without encryption, the IDS will detect and notify on the activity. If the wireless IDS is pre-configured with all the authorized WAPs and an unknown (rogue) WAP is introduced to the area, the IDS will promptly identify it. Features such as rogue WAP detection, and policy enforcement in general, go a long way to increase the security of the WLAN. The additional assistance a wireless IDS provides with respect to policy enforcement can also maximize human resource allocation. This is because the IDS can automate some of the functions that humans would ordinarily be required to manually accomplish, such as monitoring for rogue WAPs.

## Threat detection

A wireless IDS can also aid in the detection of a number of attacks. Not only can a wireless IDS detect rogue WAPs, identify non-encrypted 802.11 traffic, and help isolate an attacker's physical location, as mentioned earlier - a wireless IDS can detect many of the standard (and not-so standard) wireless attacks and probes as well [14].

In an effort to identify potential WAP targets, hackers commonly use scanning software. Hackers or curious individuals will use tools such as Netstumbler or Kismet to map out a given area's WAPs. Used in conjunction with a Global Positioning System (GPS) these scans not only

locate WAPs, but also log their geographical coordinates. These tools have become so popular that there are web sites dedicated to mapping the world's WAP geography. A wireless IDS can detect these and other scans, helping to improve awareness of the threats to the WLAN.

More critical than probe detection, a wireless IDS can also detect some DoS attacks. DoS attacks are relatively common with wireless networks, as many DoSs occur from signal loss due to a frequency conflict or a building that just went up across the street. Sometimes though, as mentioned earlier, hackers can attack the WLAN with the intent of denying it service. A wireless IDS can detect many of the attacks used to DoS WLANs, such as flooding authentication requests or disassociation/deauthentication frames.

In addition to the aforementioned attacks and probes, a wireless IDS can spot many of the other 802.11 threats as well. MAC address spoofing, one of the more common attacks, can be used by an attacker to masquerade as a WAP or wireless client. MAC address spoofing is also used in several tools including HostAP and WLAN-jack. A wireless IDS can detect the presence of MAC address spoofing in a number of ways, including sequence number analysis [15]. A wireless IDS also has the ability to recognize ad-hoc networks, a common configuration which potentially allows hackers to exploit a wireless device. In contrast, a wireless IDS can detect unique and non-standard threats through the utilization of user developed rules. This flexibility, common with standard IDSs, allows a wireless IDS to be scaleable and to address many distinctive detection requirements.

These features can add a strong layer of security to a WLAN. In addition to threat detection, merely letting people know that an IDS is in operation can add an element of deterrence and therefore, enhance security.

## Wireless IDS drawbacks

The benefits to a wireless IDS are numerous, but there are several drawbacks to consider before deploying such a system. Wireless intrusion detection is a rather new technology. Caution should be taken before applying any new technology to an operational network. Because the technology is new, there may be bugs, or worse vulnerabilities which could potentially *weaken* the WLAN security. Wireless IDS technology is developing at a rapid pace though, and this caveat may not be a deterrent in the future. A potential turn-off to a wireless IDS solution may be cost.

The expense of the vendor solutions may be prohibitive. In such a case, a homegrown solution

can be developed, but this approach may prove costly as well due to the extensive human capital that may be required to develop such a solution. Also, the cost of the wireless IDS solution (vendor-based or homegrown) will grow in conjunction with the size of the WLAN to be monitored, due to the requirement for a greater number of sensors. Therefore, the larger the WLAN, the more expensive the wireless IDS deployment will be.

A wireless IDS is only as effective as the individuals who analyze and respond to the data gathered by the system. A wireless IDS, like a standard IDS, can require vast human resources to analyze and respond to threat detection. In fact, it can be argued that a wireless IDS will require more human resources than a standard IDS because with a wireless IDS, individuals will be required to both attend to the logical (alert data) and physical aspects (finding and catching the hackers) of an attack. While the technology is still relatively new, the costs may be prohibitive, and the human capital outlay may be higher than that of a standard IDS, a wireless IDS can still prove to be a beneficial component of a security solution.

## **Conclusion**

Wireless intrusion detection systems are an important addition to the security of wireless local area networks. While there are drawbacks to implementing a wireless IDS, the benefits will most likely prove to outweigh the downsides. With the capability to detect probes, DoSs, and variety of 802.11 attacks, in addition to assistance with policy enforcement, the benefits of a wireless IDS can be substantial. Of course, just as with a wired network, an IDS is only one part of a greater security solution. WLANs require a number of other security measures to be employed before an adequate level of security can be reached, but the addition of a wireless IDS can greatly improve the security posture of the entire network. With the immense rate of wireless adoption, the ever-increasing number of threats to WLANs, and the growing complexity of attacks, a system to identify and report on threat information can greatly enhance the security of a wireless network.

## References

- [1] Fluhrer, Mantin and Shamir. [Weaknesses in the Key Scheduling Algorithm of RC-4 \[postscript\]](#) (2001)
- [2] Airdefense Inc. [Wireless LAN Security: Enterprise Rouge Detection](#) [Online]
- [3] Mark Gerken. [Rule-Based Intrusion Detection](#) [Online] (1997)
- [4] Jamil Farshchi. [Statistical-Based Intrusion Detection](#) [Online] (2003)
- [5] [Airdefense](#)
- [6] [Internet Security Systems Wireless Products](#) [PDF file]
- [7] Yu-Xi Lim, Tim Schmoyer, John Levine, Henry L. Owen. [Wireless Intrusion Detection and Response. Proceedings of the 2003 IEEE Workshop on Information Assurance](#) [PDF file]
- [8] [Snort-Wireless](#)
- [9] [WIDZ Wireless Intrusion Detection System](#) [PDF file]
- [10] Lackey, Roths, Goddard. [Wireless Intrusion Detection](#) [PDF file] (2003)
- [11] [Kismet 802.11 Wireless Sniffer](#)
- [12] [Airopeek by Wildpackets](#)
- [13] Jamil Farshchi. [Wireless Network Policy Development](#) [Online] (2003)
- [14] LURHQ Threat Intelligence Group. [Intrusion Detection: In-Depth Analysis](#) [Online]
- [15] Joshua Wright. [Detecting Wireless LAN MAC Address Spoofing](#)

## Author Credit

View [all articles](#) by Jamil Farshchi on SecurityFocus.

[Privacy Statement](#)

Copyright 2006, SecurityFocus