Wireless Intrusion Detection System

Snehal Boob
TE (COMP)
C.C.O.E.W
Karvenagar, Pune

Priyanka Jadhav
TE (COMP)
C.C.O.E.W
Karvenagar, Pune

ABSTRACT
The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. The recent denial of service attacks on major Internet sites have shown us, no open computer network is immune from intrusions. The wireless ad-hoc network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. The traditional way of protecting networks with firewalls and encryption software is no longer sufficient and effective.

The IDS engine is the control unit of the intrusion detection system. Its main purpose is to manage the system, i.e., supervise all operations of the intrusion detection system. Its duty depends on the intrusion detection method used.

Wireless has opened a new and exciting world for many of us. Its technology is advancing and changing every day and its popularity is increasing. The biggest concern with wireless, however, has been security.

The traditional wired IDS is a great system, but unfortunately it does little for the wireless world. Implementing WIDS systems is definitely a step in the right direction. If you have wireless and are concerned about attacks and intruders, a WIDS may be a great idea.

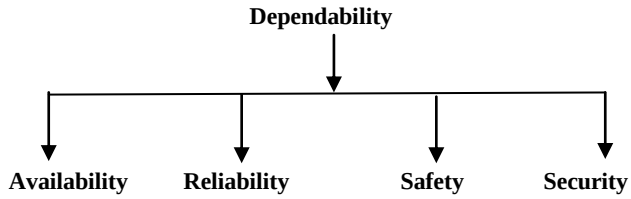
Keywords
Intrusion Detection System, Sensors, Policy Enforcement, Stations & Access Points

1. INTRODUCTION
The networking revolution has finally come of age. The possibilities and opportunities to the changing internet computing are limitless; so too are the risks and chances of malicious intrusions.

It is very important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. We can, however, try to detect these intrusion attempts so that action may be taken to repair the damage later. This field of research is called Intrusion Detection.
Wireless has opened a new and exciting world for many of us. Its technology is advancing and changing every day and its popularity is increasing. The biggest concern with wireless, however, has been security. Along with improved encryption schemes, a new solution to help combat this problem is the Wireless Intrusion Detection System (WIDS). In the security and wireless world this has fast become a major part of securing a network.

1.1 Computer Security and Its Role
One broad definition of a secure computer system is given by Garfinkel and Spafford as ***one that can be depended upon to behave as it is expected to***. It is always a point of benefit to integrate security with dependability and how to obtain a dependable computing system.

Dependability is the trustworthiness of a system and can be seen as the quality of the service a system offers. Integrating security and dependability can be done in various ways. One approach is to treat security as one characteristic of dependability on the same level as availability, reliability and safety as shown in the figure.



A narrower definition of **security** is ***the possibility for a system to protect objects with respect to confidentiality, authentication, integrity and non-repudiation***.

Confidentiality: Transforming data such that only authorized parties can decode it.

Authentication: Proving or disproving someone's or something's claimed identity.

Integrity checking: Ensuring that data cannot be modified without such modification being detectable.

Non – repudiation: Proving that a source of some data did in fact send data that he might later deny sending.

1.2 What is an Intrusion Detection System?
An Intrusion Detection System (IDS) is a software or hardware tool used to detect unauthorized access of a computer system or network. A wireless IDS performs this task exclusively for the wireless network. These systems monitor traffic on your network looking for and logging threats and alerting personnel to respond.

1.3 Why use a Wireless Intrusion Detection System?

The traditional wired IDS system does very little for the wireless world. The problem with wireless is that in addition to attacks that may be performed on a wired network, the medium itself has to be protected. To do this there are many measures which can be taken, however there are even more tools designed to break them. Due to the nature of wireless LANs (WLAN), it can be difficult to control the areas of access. Often the range of a wireless network reaches outside the physical boundaries of an organization. With such a problem with wireless security, developing and implementing WIDS systems is definitely a step in the right direction. If you have wireless and are concerned about attacks and intruders, a WIDS may be a great idea.

A large number of possible attacks can be detected by a WIDS. The following will list major attacks and events that can be detected with the help of a WIDS. Rogue devices, such as an employee plugging in an unauthorized wireless router, incorrect configurations, connectivity problems, jamming, man-in-the-middle attacks, wardrivers, scanning with programs like Netstumbler or Kismet, RF interference, MAC spoofing, DoS attacks, attempts of brute force to get pass 802.1x, strong RFI, or use of traffic injection tools. Different WIDS devices and software have different capabilities in what can be detected. Make sure the WIDS you chose will fit your company's profile.

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, and Internet Security Systems Realsecure Server sensor and wireless scanner products. A homegrown wireless IDS can be developed with the use of the Linux operating system, for example, and some freely available software. Open source solutions include Snort-Wireless and WIDZ, among others.

2. WLAN STANDARDS

Most WLANs use the Institute of Electrical and Electronics Engineers (IEEE) 802.11 family of WLAN standards. The most commonly used WLAN radio transmission standards are IEEE 802.11b and IEEE 802.11g, which use the 2.4 gigahertz (GHz) band, and IEEE 802.11a, which uses the 5 GHz band. IEEE 802.11a, b, and g include security features known collectively as Wired Equivalent Privacy (WEP). Unfortunately, WEP has several well-documented security problems. To overcome these, IEEE 802.11i was created; it specifies security components that work in conjunction with IEEE 802.11a, b, and g.

Another set of WLAN standards has been created by a non-profit industry consortium of WLAN equipment and software vendors called the Wi-Fi Alliance. While IEEE was working on finalizing the 802.11i standard, the Alliance created an interim solution called Wi-Fi Protected Access (WPA). Published in October 2002, WPA is essentially a subset of the draft IEEE 802.11i requirements available at that time. WPA provides stronger security for WLAN communications than WEP. In conjunction with the ratification of the IEEE 802.11i amendment, the Wi-Fi Alliance introduced WPA2, its term for interoperable equipment that is capable of supporting IEEE 802.11i requirements. WPA2 offers stronger security controls than either WPA or WEP.

3. COMPONENTS AND ARCHITECTURE

This section describes the major components of typical wireless IDS and illustrates the most common network architectures for these components. It also provides recommendations for the placement of certain components. (Refer Figure 1)

IEEE 802.11 WLANs have two fundamental architectural components:

Station (STA). A *STA* is a wireless endpoint device. Typical examples of STAs are laptop computers, personal digital assistants (PDA), mobile phones, and other consumer electronic devices with IEEE 802.11 capabilities.

Access Point (AP). An *AP* logically connects STAs with a *distribution system* (DS), which is typically an organization's wired infrastructure. The DS is the means by which STAs can communicate with the organization's wired LANs and external networks such as the Internet. Figure1 shows an example of how APs, STAs, and DSs are related.

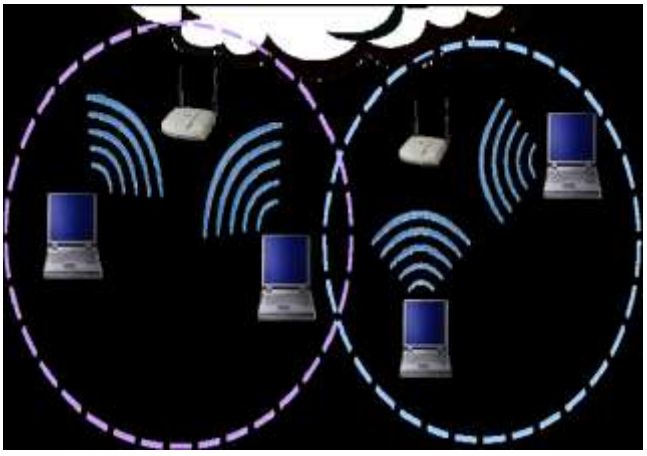


FIGURE1: WIRELESS LAN ARCHITECTURE EXAMPLE

Some WLANs also use wireless switches. A *wireless switch* is a device that acts as an intermediary between APs and the DS.

The IEEE 802.11 standard also defines the following two WLAN architectures:

Ad Hoc Mode: The *ad hoc mode* does not use APs. Ad hoc mode, also known as peer-to-peer mode, involves two or more STAs communicating directly with one another.

Infrastructure Mode: In *infrastructure mode*, an AP connects wireless STAs to a DS, typically a wired network.

3.1 Typical Components

The typical components in a wireless IDS are consoles, database servers (optional), management servers, and sensors.

A wireless IDS work by sampling traffic. There are two frequency bands to monitor (2.4 GHz and 5 GHz), and each band is separated into channels. It is not currently possible for a sensor to monitor all traffic on a band simultaneously; a sensor has to monitor a single channel at a time. When the sensor is ready to monitor a different channel, the sensor must shut its radio off, change the channel, then turn its radio on. The longer a single channel is monitored, the more likely it is that the sensor will miss malicious activity occurring on other channels. To avoid this, sensors typically change channels frequently, which is known as *channel scanning*, so that they can monitor each channel a few times per second. To reduce or eliminate channel scanning, specialized sensors are available that use several radios and high-power antennas, with each radio/antenna pair monitoring a different channel. Because of their higher sensitivities, the high-power antennas also have a larger monitoring range than regular antennas. Some implementations coordinate scanning patterns among sensors with overlapping ranges so that each sensor needs to monitor fewer channels.

Wireless sensors are available in multiple forms:

3.1.1 Dedicated:

A dedicated sensor is a device that performs wireless IDS functions but does not pass network traffic from source to destination. Dedicated sensors are often completely passive, functioning in a radio frequency (RF) monitoring mode to sniff wireless network traffic. Some dedicated sensors perform analysis of the traffic they monitor, while other sensors forward the network traffic to a management server for analysis. The sensor is typically connected to the wired network (e.g., Ethernet cable between the sensor and a switch). Dedicated sensors are usually designed for one of two deployment types:

Fixed—the sensor is deployed to a particular location. Such sensors are typically dependent on the organization's infrastructure (e.g., power, wired network). Fixed sensors are usually appliance-based.

Mobile—the sensor is designed to be used while in motion. For example, a security administrator could use a mobile sensor while walking through an organization's buildings and campus to find rogue APs. Mobile sensors are either appliance-based or software-based (e.g., software installed onto a laptop with a wireless NIC capable of doing RF monitoring).

3.1.2 Bundled with an AP:

Several vendors have added IDS capabilities to APs. A bundled AP typically provides a less rigorous detection capability than a dedicated sensor because the AP needs to divide its time between providing network access and monitoring multiple channels or bands for malicious activity. If the IDS only needs to monitor a single band and channel, a bundled solution might provide reasonable security and network availability. If the IDS has to monitor multiple bands or channels, then the sensor needs to perform channel scanning, which will disrupt the AP functions of the sensor by making it temporarily unavailable on its primary band and channel.

3.1.3 Bundled with a Wireless Switch:

Wireless switches are intended to assist administrators with managing and monitoring wireless devices; some of these switches also offer some wireless IDS capabilities as a secondary function. Wireless switches typically do not offer detection capabilities as strong as bundled APs or dedicated sensors.

Because dedicated sensors can focus on detection and do not need to carry wireless traffic, they typically offer stronger detection capabilities than wireless sensors bundled with APs or wireless switches. However, dedicated sensors are often more expensive to acquire, install, and maintain than bundled sensors because bundled sensors can be installed on existing hardware, whereas dedicated sensors involve additional hardware and software. Organizations should consider both security and cost when selecting wireless IDS sensors.

Some vendors also have host-based wireless IDS sensor software that can be installed on STAs, such as laptops. The sensor software detects attacks within range of the STAs, as well as misconfigurations of the STAs, and reports this information to management servers. The sensor software may also be able to enforce security policies on the STAs, such as limiting access to wireless interfaces.

3.2 Network Architectures

Wireless IDS components are typically connected to each other through a wired network. A separate management network or the organization's standard networks can be used for wireless IDS component communications. Because there should already be a strictly controlled separation between the wireless and wired networks, using either a management network or a standard network should be acceptable for wireless IDS components. Also, some wireless IDS sensors (particularly mobile ones) are used standalone and do not need wired network connectivity. (Refer Figure 2)

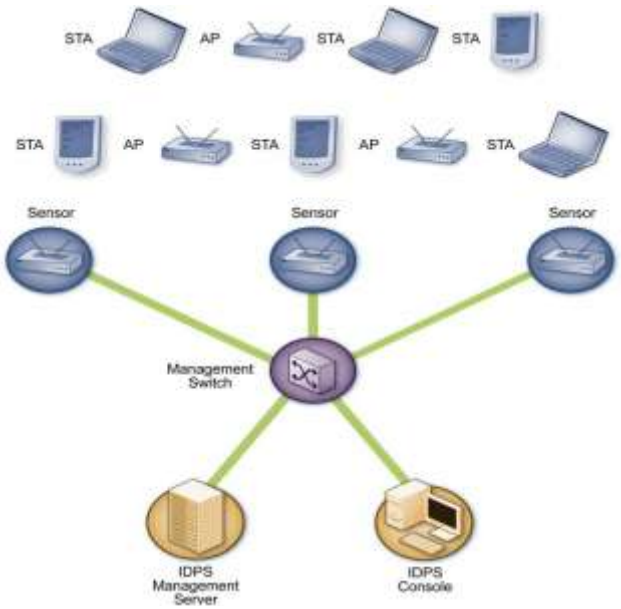


FIGURE 2: WIRELESS IDS ARCHITECTURE

3.3 Sensor Locations

Choosing sensor locations for a wireless IDS deployment is a fundamentally different problem than choosing locations for any other type of IDS sensor. If the organization uses WLANs, wireless sensors should be deployed so that they monitor the RF range of the organization's WLANs (both APs and STAs), which often includes mobile components such as laptops. Many organizations also want to deploy sensors to monitor physical regions of their facilities where there should be no WLAN activity, as well as channels and bands that the organization's WLANs should not use, as a way of detecting rogue APs and ad hoc WLANs.

3.3.1 Physical Security: Sensors are often deployed into open locations (e.g., hallway ceilings, conference rooms) because their range is much greater there than in closed locations (e.g., wiring closets). Sensors are sometimes deployed outdoors as well. Generally, sensors in open interior locations and external locations are more susceptible to physical threats than other sensors. If the physical threats are significant, organizations might need to select sensors with anti-tamper features or deploy sensors where they are less likely to be physically accessed (e.g., within view of a security camera).

3.2.2 Sensors Location

The actual range of a sensor varies based on the surrounding facilities (e.g., walls, doors). Some wireless IDS vendors offer modeling software that can analyze building floor plans and the attenuation characteristics of walls, doors, and other facility components to determine effective locations for sensors. Sensor range can also vary based on the location of people within the facility and other changing characteristics, so sensors should be deployed so that their ranges have some overlap (e.g., at least 20%).

4. MANAGEMENT

Most wireless IDS products offer similar management capabilities. This section discusses major aspects of management—implementation, operation, and maintenance—and provides recommendations for performing them effectively and efficiently.

4.1 Implementation

Once a wireless IDS product has been selected, the administrators need to design architecture, perform IDS component testing, secure the IDS components, and then deploy them. Implementing a wireless IDS can necessitate brief wireless network outages if existing APs or wireless switches need to be upgraded or have IDS software installed. Generally, the deployment of sensors causes no network outages.

4.2 Operation and Maintenance

Wireless IDS consoles offer similar management, monitoring, analysis, and reporting capabilities. One significant difference is that wireless IDPS consoles can display the physical location of threats. A minor difference is that because wireless IDS sensors detect a relatively small variety of events, compared to other types of IDSs, they tend to have signature updates less frequently.

5. 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 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.

6. THREATS AGAINST WLANS

Wireless attacks typically require the attacker or a device placed by the attacker to be within close physical proximity to the wireless network. However, many WLANs are configured so that they do not require any authentication or require only weak forms of authentication; this makes it much easier for local attackers to perform several types of attacks, such as a man-in-the-middle attack.

Most WLAN threats involve an attacker with access to the radio link between a STA and an AP (or between two STAs, in ad hoc mode). Many attacks rely on an attacker's ability to intercept network communications or inject additional messages into them.

Hackers can also attack a WLAN and gather sensitive data by introducing a rogue WAP into the WLAN coverage area. 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.

7. SUMMARY

Wireless has and is opening many new possibilities for expanding networks. Its potential is amazing.

A wireless IDS monitors wireless network traffic and analyzes its wireless networking protocols to identify suspicious activity. The typical components in a wireless IDS: consoles, database servers (optional), management servers, and sensors.
Wireless sensors are available in multiple forms.
Wireless IDS components are typically connected to each other through a wired network. Because there should already be a strictly controlled separation between the wireless and wired networks, using either a management network or a standard

network should be acceptable for wireless IDS components. Choosing sensor locations for a wireless IDS deployment is a fundamentally different problem than choosing locations for any other type of IDS sensor.
Compared to other forms of IDS, wireless IDS is generally more accurate; this is largely due to its limited scope.

8. CONCLUSION

As with most new technologies, wireless has several vulnerabilities. It is important to note that absolute security is an abstract concept – it does not exist anywhere. All networks are vulnerable to insider or outsider attacks, and eavesdropping. No one wants to risk having the data exposed to the casual observer or open malicious mischief.

Wireless IDS solutions are available from both the open-source and commercial markets and both have their own advantages.
Wireless intrusion detection systems are an important addition to the security of wireless local area networks. 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.

9. REFERENCES

[1] Wireless Intrusion Detection Systems Including Incident Response & Wireless Policy, by Jeff Dixon. http://www.infosecwriters.com/text_resources/pdf/Wireless_IDS_JDixon.pdf

[2] An Overview of the Wireless Intrusion Detection System,byOliverPoblete. http://www.sans.org/reading_room/whitepapers/wireless/overview-wireless-intrusion-detection-system_1599

[3] Guide to Intrusion Detection and Prevention Systems (IDPS), NIST special publication 800-94, by Karen Scarfone PeterMell http://www.sans.org/reading_room/whitepapers/wireless/overview-wireless-intrusion-detection-system_1599

[4] Wireless Intrusion Detection Systems, Security Articles**,** by Jamil Farshchi