

**Wireless Intrusion Detection Systems (WIDS):
Protecting the Wireless Perimeter**



Prepared for
The IT Security Community and our Customers

Prepared by

Lunarline, Inc.
1875 I ST, NW, Suite 500
Washington, DC 20006
www.lunarline.com

16 October 2006

By Matt Metheny, PMP, CISSP, CAP, CISA

Abstract

This paper discusses the wireless intrusion detection (WIDS) technology as a benefit for the protection of wireless networks against attacks through detection and prevention. The wide use of wireless local area networks (WLANs) has required the increased of WIDS technology to focuses on protecting the wired and wireless infrastructure from internal and external threats. This report will give a brief introduction to WIDS, describe the current threats associated with WLANs , provide a list of the potential benefits offered by the implementation of wireless intrusion detection and prevention, and illustrated how WIDS plays an assurance role in the enforcement of the organization's wireless policy.

Table of Contents

Abstract.....	2
Introduction.....	4
Introduction to Wireless IDS (WIDS) Technology	4
Current Threats Associated with WLANs	5
Potential Benefits Offered by WIDS	5
WIDS Role in Corporate Wireless Policy Compliance	6
Conclusion	7
References.....	8

Introduction

Emerging wireless intrusion detection (WIDS) technology provides significant security benefits for protecting wireless networks through the detection and prevention of attacks and a method for policy enforcement that significantly strengthens information assurance in the adoption of wireless networks. Wireless technology is becoming more and more a central part of the IT infrastructure for everyday communication and connectivity of industry standardized applications such as laptops, cell phones, PDAs, and control sensors. The maturity of wireless technology will continue to grow and lowers costs, resulting in an accelerated end-user acceptance as a sensible alternative.

As wireless technology becomes more feasible for a broader range of applications, businesses are adopting wireless local area network (WLAN) infrastructures because they are more flexible and less expensive to support and maintain than traditional wired networks. This realization is primarily found in businesses that market wireless network access as an option for Internet connectivity. Businesses such as cafes, airports, and hotels deliver Internet access in locations where wired networks would logistically be impossible to establish, and would accommodate the number of potential “for-fee” Internet users seeking access.

Introduction to Wireless IDS (WIDS) Technology

Before we discuss some of the major threats to wireless networks, we should briefly describe WIDS technology. Most people do not understand the differences between wireless and wired intrusion detection technology. The key difference is the fundamental basics of the transmission media that is being monitored – wireless communication transmits data over radio frequencies (RF). Wireless technology uses various frequency ranges and modulation techniques to allow an expanded bandwidth capacity for increased user connectivity. Wireless intrusion detection is more complex than the standard wired equivalent most notably because it must have the capability to monitor multiple frequencies ranges and individual frequencies within a particular range (also known as channels) to detect intruders or rogue wireless access points (WAPs).

Depending on the specific needs of the WIDS, at minimum the scanning can be limited to a specific set of frequencies. However, if the scanning is limited, the level of detection may also be limited. As an example, limiting the range of coverage for the WIDS would be like putting only one security system alarm sensor on a house with multiple entry points (doors, windows, etc.). You may be able to monitor one entry, but the other entries will still be open to intruders.

Unlike a wired network IDS, where the main function of the IDS is to monitor a network segment, or an entire network to watch for patterns or signatures associated with an attack. A wireless network IDS has a much more expansive set of entry points and techniques for obtaining access and must support extended functionality. The WIDS needs to understand not only the data level patterns or signatures associated with attacks,

but also the RF signatures (or fingerprints) of a particular network, and provide a mechanism to alert when certain types of patterns are considered malicious activity.

Current Threats Associated with WLANs

An understanding of the key mechanisms used to attack WLANs are important as part of identifying the information assurance needs of the organization prior to the adoption of wireless networks. In this section we will discuss many of the commonly executed attacks.

War Driving and Denial-of-Service (DoS) Attacks

War driving is a popular hack on wireless networks. War driving specifically involves a scanning technique that identifies and publishes the locations (sometimes through the use of Global Positioning technology) of wireless networks. In many instances, war driving involves driving around to log wireless network activity. “War-driving programs stop short of actually establishing the connection, but instead just use the probe requests/response aspect of the 802.11 protocol to its advantage” (<http://www.informit.com/guides/printerfriendly.asp?g=security&seqNum=183&rl=1>, para. 12). This deliberate technique to identifying wireless networks that accept connections from unauthorized individuals could provide an attacker the opportunity to perform advanced denial-of-service (DoS) attacks that would limit the availability of the wireless access.

Spoofing (WAP and MAC)

The security failures of the wireless network and the various nodes connected, allow attackers ease of opportunity because physical access is not required. Many organizations do not enable security features on WAPs such as disabling the broadcasting of ¹SSID, or including a ²MAC level access control list (ACL) to prevent unauthorized access to the wireless network itself. “The MAC ACL grants or denies access to a computer using a list of permissions designated by MAC address” (Karygiannis & Ownes, 2002, p 42). This invites attackers into the network because the access controls, and basic security mechanisms within the WAP are decreased leaving the it open to automated attacks and encryption exploitations.

Potential Benefits Offered by WIDS

The benefits of deploying wireless IDS technology vary depending on the requirements of the organization. If the assurance of the wireless network has very limited security requirements, then wireless IDSs would probably not be a suitable

¹ “The SSID is an identifier that is sometimes referred to as the “network name” and is often a simple ASCII character string” (Karygiannis & Ownes, 2002, p 42).

² A MAC address is a hardware address that uniquely identifies each computer (or attached device) on a network” (Karygiannis & Ownes, 2002, p 42).

solution. However, as with any system operations, the benefits must be understood through a thorough risk analysis which will weigh the cost associated with security measures, and the overall ³residual risks that are realized after implementation of wireless IDS technology.

In this section we will discuss wireless IDS technology, and describe how they can provide significant security benefits for protecting wireless networks against attacks. The major benefits of wireless IDS technology that would enhance the defensive posture can be categorized in two different groups:

- Real-time Network Monitoring and Radio Frequency (RF) Management
- Intrusion Detection and Response

Real-time Network Monitoring and Radio Frequency (RF) Management

In any wireless network deployment the monitoring and management of the network and the RF spectrum within the environment is part of a threat recognition and awareness capability. The WIDS provides the capability of analyzing and monitoring the RF spectrum, and the generation of alarms upon detection of unauthorized wireless devices that violate the organizations security policies (Karygiannis & Ownes, 2002, p. 47). This capability of identifying suspicious network activity such as increased bandwidth usage, network reconnaissance, RF interferences, and unknown ⁴rogue wireless access points (WAP) or ad-hoc networks are a critical part of a responsive wireless security network. The responsiveness to an attack on a wireless network cannot be predicted, and requires an active monitoring presence and a real-time view of the wireless frequency spectrum to analyze harmful RF activity

Intrusion Detection and Response

The detection and response to an attack on the wireless network is another key requirement delivered by the deployment of WIDS to prevent the attack on a wireless network infrastructure. The analysis and management of air traffic over the wireless RF network increases the effectiveness for an active and responsive security presence that is important for countering intruders that may take advantage of the anomalies that exist because of security limitations in the current standards or the failure to implement wireless security features during deployment of the wireless network.

WIDS Role in Corporate Wireless Policy Compliance

With any new protective measure, a policy needs to be adopted to regulate and control the use of wireless technology, and provide guidance to the community of the application of a wireless-enabled device (e.g., access points, laptops, PDAs) within the

³ Risks remaining after specific security measures have been implemented.

⁴ "A rogue AP is a Wi-Fi Access Point that is set up by an attacker for the purpose of sniffing wireless network traffic in an effort to gain unauthorized access to your network" (<http://www.winplanet.com/article/3187-.htm>, para. 1).

organizations IT infrastructure. The WIDS helps enforce this policy by enabling it to search through packets for non-compliance such as traffic encryption and rogue WAPs.

The WIDS is an important defense in-depth mechanism that can help ensure the security of the corporate IT infrastructure, and prevent the unauthorized deployment of rogue WAPs that could be misconfigured, or create an undefended entry point for intruders. As discussed in the Security Focus article written by Jamil Farschi (2006), the essential components of a security policy include:

- **Logging and Accounting** – aids in the activity tracking, accountability of use, and misuse detection.
- **Wireless Access Point (WAP) Security** – ensure physical location of WAP, and access privileges for both connection and administration.
- **Client-based Security** – security measures employed on wireless clients including the software requirements (firewall and anti-virus), configuration settings (ad-hoc communication) and encryption.
- **Wireless Scanning** – scanning frequency of wireless network and tool identification
- **Education and Awareness** – user community security awareness and training to maintain awareness and knowledge of the organization network security policies and procedures, including basic security training of security “best practices”.

After the policy has been developed and disseminated, there needs to be continuous monitoring and strict enforcement to ensure the security of the organization is not hindered because of policy violators. The WIDS provides the capability to ensure technical and operational components in the policy are enforced by checking for suspicious activity, unauthorized deployment or configuration of a WAP, and encryption to meet data protection requirements. The enforcement activities are critical to make certain any information stored, processed, or transmitted over the organization’s network are protected and prevents unauthorized access to privacy information (confidentiality), decreases the reliability of the information (integrity), or limits avenues for attackers to exploit system access (availability).

Conclusion

As wireless networks become more common in today’s IT infrastructure, wireless intrusion detection is slowly becoming a critical component for both active and passive security monitoring. WIDS not only provides a security monitoring function, but also ensures protection against threats outside the organization’s network perimeter, and internally with the enforcement of the organizations wireless policy. WIDS implementation delivers the multi-tiered defense in-depth strategy that is required for an organization to deliver the highest level of information assurance and increased overall security that spans across the organizational boundaries.

References

- Farshchi, J. (2005). SecurityFocus. *Wireless Intrusion Detection Systems*. Retrieved September 11, 2006 from <http://www.securityfocus.com/infocus/1742>
- Karygiannis, T. & Ownes, L. (2002). *Wireless Network Security*. Retrieved September 7, 2006 from csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
- Pacchiano, R. (n.d.). *Software Reviews. Rogue Access Points: The Silent Killer*. Retrieved September 16, 2006 from <http://www.winplanet.com/article/3187-.htm>.
- Peikari, C. & Fogie, S. (2002). *informIT. War-Driving Exposed*. Retrieved September 22, 2006 from <http://www.informit.com/guides/printerfriendly.asp?g=security&seqNum=183&rl=1>