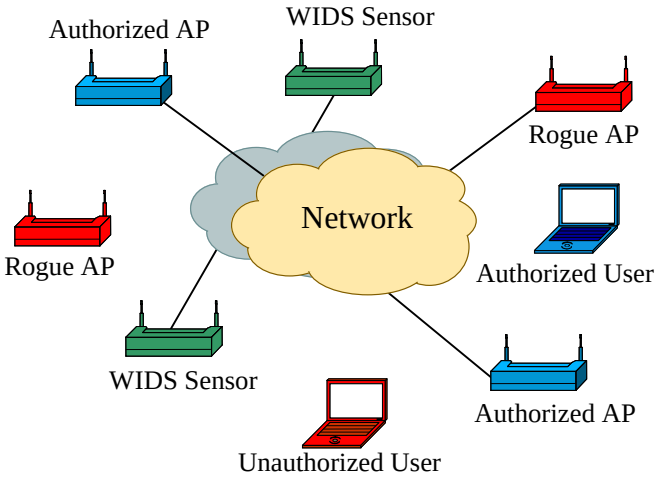
802.11 Wireless LAN Intrusion Detection Systems

In today's increasingly wireless world, organizations are quickly realizing the security benefits of constantly monitoring the wireless spectrum within their enterprise. When an organization has an interest in identifying and locating wireless hardware and preventing intrusion attempts on their networks, the benefits of monitoring exists regardless of whether or not network owners officially authorize the use of wireless devices.

An 802.11 Wireless Intrusion Detection System (WIDS) consists of a group of sensors and a central controller working together to provide 24/7 monitoring of the wireless spectrum. Ideally, information between the sensors and the controller will pass over a separate network dedicated to the WIDS as shown in the figure below, but an acceptable option is to connect the sensors over a virtual LAN established over the data network.



WIDS Deployed in a Wireless Network

Denial of service attacks

The WIDS identifies a denial of service attack by detecting traffic anomalies or deviations from the 802.11 protocols and comparing them to a known set of attack signatures. Upon detecting an attack, the system logs the incident and notifies the system administrator. As new denial of services attacks are discovered, new signatures are added to the WIDS.

Download "Guidelines for the Development and Evaluation of 802.11 Intrusion Detection Systems (IDS) at:

http://www.nsa.gov/snac/

Rogue access points

Rogue access points (APs) can either be connected to the network or exist outside the network. Rogue APs on the network are unauthorized devices connected by an insider who either doesn't understand the risk to the network, understands the risk and with no malicious intent violates policy anyway, or maliciously connects the AP solely for the purpose of gaining remote access to the network for themselves or someone else.

Rogue APs not physically connected to the network are spoofing authorized APs. The rogues attempt to make the authorized clients connect to them with the intent of compromising the client or gaining access to the network. A WIDS knows what access points are in the surrounding air space, and can distinguish between authorized and

Unauthorized APs. Using geolocation techniques, they can report the unauthorized device's physical location in order for the system administrator to find and remove the device from the network.

Deviations from Security Policy

The system administrator can create a wireless security policy and push that policy out to the authorized devices. The WIDS can then monitor the air space and enforce the security policy. For instance, the WIDS can determine if an authorized device is:

- Connected to, or attempting a connection to an unauthorized device.
- Not using the proper encryption or authentication method.
- Not operating within an approved physical location.
- Operating in an ad-hoc or bridging mode.
- Operating on the wrong channel.

Defense in Depth

Conventional wired network IDSs focus on the protocols in the upper five layers of the Open Systems Interconnection (OSI) model while the WIDS monitors Layers 1 and 2. Because a network IDS concentrates its efforts at key wired entry and exit points to the network, it is unaware of any attacks on wireless devices connected to the network. On the other hand, there are many wired network attacks that a WIDS cannot detect, so the two IDS systems actually compliment each other and should be deployed together.

DOD Directive 8100.2

Not only is deploying a WIDS a good idea for protecting any computer network, DoD Directive 8100.2 and its follow-on policy mandates the use of a WIDS on all unclassified DoD wireless local area networks to provide continuous scanning (24 hours/day, 7 days/week) of the RF spectrum for wireless intrusion and denial of service attempts regardless of whether a wireless system is deployed.

Summary

Wireless Intrusion Detection Systems are an essential security component to any network, even for protecting wired networks when the use of wireless hardware is unauthorized. For a complete coverage of WIDS requirements see, "Guidelines for the Development and Evaluation of 802.11 Intrusion Detection Systems (IDS)." This paper is unclassified and available on the Internet at http://www.nsa.gov/snac/.