Technology Profile Fact Sheet

Title: Wireless Intrusion Detection System

Aliases: WIDS

Technical Challenge: Wireless local area networks (WLAN's) have proliferated around the globe and are used in industry, in government, and at home. The benefits of mobility that are provided by wireless local area networks are well known. However, there is also some risk involved. There are many security threats that are unique to the wireless networking environment since it uses an open, uncontrolled transmission medium. A wireless intrusion detection system can help to mitigate the risks involved with wireless networking and provide a more secure operating environment for a WLAN. For these reasons, in June of 2006, the Department of Defense (DoD) issued a supplement to DoD Directive 8100.2, which describes the policy for usage of commercial wireless devices, services, and technologies in the DoD Global Information Grid (GIG). The supplement sets forth the requirement that all DoD WLAN's must be protected by a wireless intrusion detection system at all times. The problem is that even the best wireless intrusion detection systems currently available are not good enough to protect wireless networks transmitting sensitive or classified information. The WIDS that NSA has developed addresses some of the shortcomings of other wireless intrusion detection systems.

Description: The supplement to DoD Directive 8100.2 also states that wireless intrusion detection systems should be validated under the National Information Assurance Partnership (NIAP) Common Criteria as meeting applicable U.S. Government protection profiles for basic or medium robustness environments. The WIDS that NSA has developed was designed to meet many of the requirements specified in the draft version of the medium robustness protection profile for a wireless intrusion detection system, which is currently undergoing the ratification process. The WIDS has the ability to detect and alert on: rogue access points and clients, rogue devices actively communicating with valid devices, ad-hoc networks, bridged networks, deviations from the network security policy, devices running the program Netstumbler, packet flooding denial-of-service attacks, MAC spoofing, and frames having 802.11 protocol violations. The system can also determine the channel that a packet was transmitted on, versus the channel that it was received on. In addition, the system allows a user to create custom capture filters and attack signatures.

Demonstration Capability: There is a prototype to demonstrate the technology.

Potential Commercial Application(s): The Wireless Intrusion Detection System can be used to provide defense-in-depth protection for any wireless local area network.

Patent Status: A patent application has been filed with the USPTO.

Reference Number: 1514