Common Criteria Evaluation and Validation Scheme

National Information Assurance Partnership (NIAP)

Title: Wireless Intrusion Detection/Prevention Systems Essential Security Requirements

Maintained by: NIAP

Unique Identifier:

Version: 1.0

Status: Final

Date of issue: 28 March 2016

Approved by: NIAP

Supersedes:

Status

The NSA has been requested to develop an Essential Security Requirements (ESR) document that specifies the essential requirements for Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS). This is the initial draft for an Extended Package (EP) to the Network Devices collaborative Protection Profile (cPP).

Background and Purpose

This document describes the high-level set of security requirements that a WIDS/WIPS will satisfy when evaluated against the EP written for such technology.

There are well-known attacks targeting IEEE 802.11 networks (referred to as WLAN for the remainder of this document) such as rogue access points, Denial of Service Attacks (DoS), and Man-in-the-Middle Attacks. A WIDS/WIPS should be used as part of a layered security approach in order to detect and mitigate some of the attacks that are unique to WLAN. A WIDS/WIPS helps protect the network by analyzing and collecting IEEE 802.11 traffic to detect WLAN intrusions. A WIDS/WIPS typically consists of multiple sensors that passively scan their surrounding RF environment on the WLAN radio frequency spectrum for IEEE 802.11 traffic and a centralized mechanism such as a Server or Controller that processes the data collected by the sensors and detects, alerts, and logs intrusion attempts.

Traditional wired IDS/IPS and WIDS/WIPS serve similar functions but they focus on different segments of the network. A wired IDS/IPS detects intrusions on the wired network, while a WIDS/WIPS detects intrusions on the wireless network. A wired IDS/IPS is not able to detect WLAN-based attacks. Wired IDS/IPS requirements are not covered in this EP. They are addressed in the collaborative Protection Profile for Network Devices/collaborative Protection Profile for Stateful Traffic Filter Firewalls Extended Package for Intrusion Prevention Systems (IPS).

Use Cases

A WIDS/WIPS should be used as part of any network deployment both in spaces where a WLAN is deployed and in spaces where policies do not permit the use of wireless networks. In the first case, a WIDS/WIPS detects attacks against the WLAN and its end user devices, as well as unauthorized WLAN devices or unauthorized connections. In the second case a WIDS/WIPS detects the use of wireless network/devices where wireless networks are not permitted.

Resources to be protected

A WIDS is used to detect attacks that compromise the confidentiality and integrity of user and system data traversing through the WLAN network or accessible through the WLAN network as well as the availability of the WLAN network to legitimate users. There is the potential of the wired network being compromised through vulnerabilities in the wireless network. Therefore, protecting the wireless network also plays a part in protecting the overall network. Below are the security objectives that will be addressed by the WIDS/WIPS:

Unauthorized Disclosure of Information

Sensitive information on a protected WLAN might be disclosed resulting from disclosure/transmitted information in violation of policy, such as sending unencrypted sensitive data. The WIDS/WIPS will be capable of collecting and analyzing WLAN data to detect unauthorized disclosure of information.

Unauthorized Access

An attacker may attempt to gain inappropriate access to one or more networks, endpoints, or services, such as by getting an end user device to connect to an unauthorized AP by impersonating an authorized AP. If malicious external devices are able to communicate with devices on the protected WLAN, then those devices may be susceptible to the unauthorized disclosure of information.

Disruption or Denial of Services (DoS)

Attacks against the WLAN infrastructure might lead to denial of services within a protected WLAN. A wireless DoS may occur in two ways: at the physical layer through RF Jamming, or at the data link layer through packet injection.

Attacker access

The fact that WLAN communications happen over the air extends the attack vectors outside of the physically protected spaces. WIDS/WIPS address a range of WLAN security threats through detection of and reaction to potentially malicious traffic on monitored WLANs. The malicious traffic may pose a threat to one or more endpoints on the monitored networks, or to the network infrastructure.

Target of Evaluation

A WIDS typically consists of multiple sensors that passively scan their surrounding RF environment on the WLAN radio frequency spectrum for IEEE 802.11 traffic and a centralized mechanism such as a Server or Controller that processes the data collected by the sensors. The WIDS/WIPS could use an Embedded (be part of the WLAN infrastructure) or Overlay (independent from WLAN) architecture depending on vendor implementation. The following are to be part of the evaluation:

- Monitoring, detection and reporting capabilities offered by the WIDS/WIPS.
- Use of secure communication paths between WIDS/WIPS components
- Use of secure communication paths for WIDS/WIPS management and event monitoring.
- Use of secure communication paths with external components (e.g., database and log server)

Essential Security Requirements

The following are high level descriptions of the capabilities expected from the WIDS/WIPS. The categories below include selection based requirements and some optional requirements. Detailed requirements will be provided in the draft EP.

Monitoring Capabilities

- 2.4, 4.9/5.0 GHz frequency bands
- All IEEE 802.11 (a, b g, n, ac) channels, including those outside regulatory domain
- Transmit power levels
- Bandwidth usage
- Number of end user devices connected to the network
- Client connection status
- Times of usage
- Channel usage

Detection Capabilities

- Unauthorized IEEE 802.11 Devices
- Unauthorized AP connected to the wired network infrastructure
- Peer-to-Peer Connections
- Bridges (to include but not limited to devices that bridge two network interfaces, Soft APs, and point to point wireless bridges)
- SSID Misuse
- Misconfigured devices
- Use of unauthorized authentication methods
- Use of unauthorized encryption methods
- Device Impersonation (SSID and/or MAC address)
- Denial of Service (through packet injection or RF based flooding)
- Protocol Violations
- Active Network Probing
- Illegal State Transitions

- WIDS/WIPS Components Failures

Detection Techniques

- Signature based detection
- Customizable Attack Signatures
- Protocol anomaly analysis
- Anomaly based detection

Management and Reporting

- Customizable alerts
- Descriptive alerts
- Logs and reports in industry standard formats
- Traffic capture file in industry standard formats
- Ability to send logs to an external log server

Secure Communication Paths

- Use of secure communication paths for inner WIDS/WIPS communications (between WIDS/WIPS components).
- Use of secure communication paths for WIDS/WIPS management and event monitoring.
- Use of secure communication paths with external components such as database and log server.
- Ability to disable non-secure communication paths.

Device Location Tracking

- Ability to physically locate WLAN devices.

Network Forensics

- Packet capture of raw frame that triggered an intrusion alert.
- Ability to store and securely export packet captures to external server.
- Ability to specify the types of alerts that should trigger a packet capture, duration of capture, and how long to keep captures.

Prevention Mechanisms

- Ability to enable wireless containment/isolation of a human-confirmed rogue device.
- Ability to enable wireside containment of a confirmed rogue device connected to wired infrastructure.

Optional Extensions

The following are high level descriptions of the capabilities that are optional and not required from the WIDS/WIPS.

Detection of non 802.11 devices

- Unauthorized devices/activity on Cellular Spectrum
- Unauthorized devices/activity on the 60 GHz band
- Unauthorized devices/activity on the sub GHz band

RF Spectrum Analysis

- Ability to configure dedicated sensor for full-time spectrum analysis

Outside the TOE's Scope

The following list contains items that are explicitly out-of-scope for any evaluation against the product PP.

- Cellular network traffic analysis
- Bluetooth traffic analysis
- Wired IDS/IPS (covered in IPS EP)