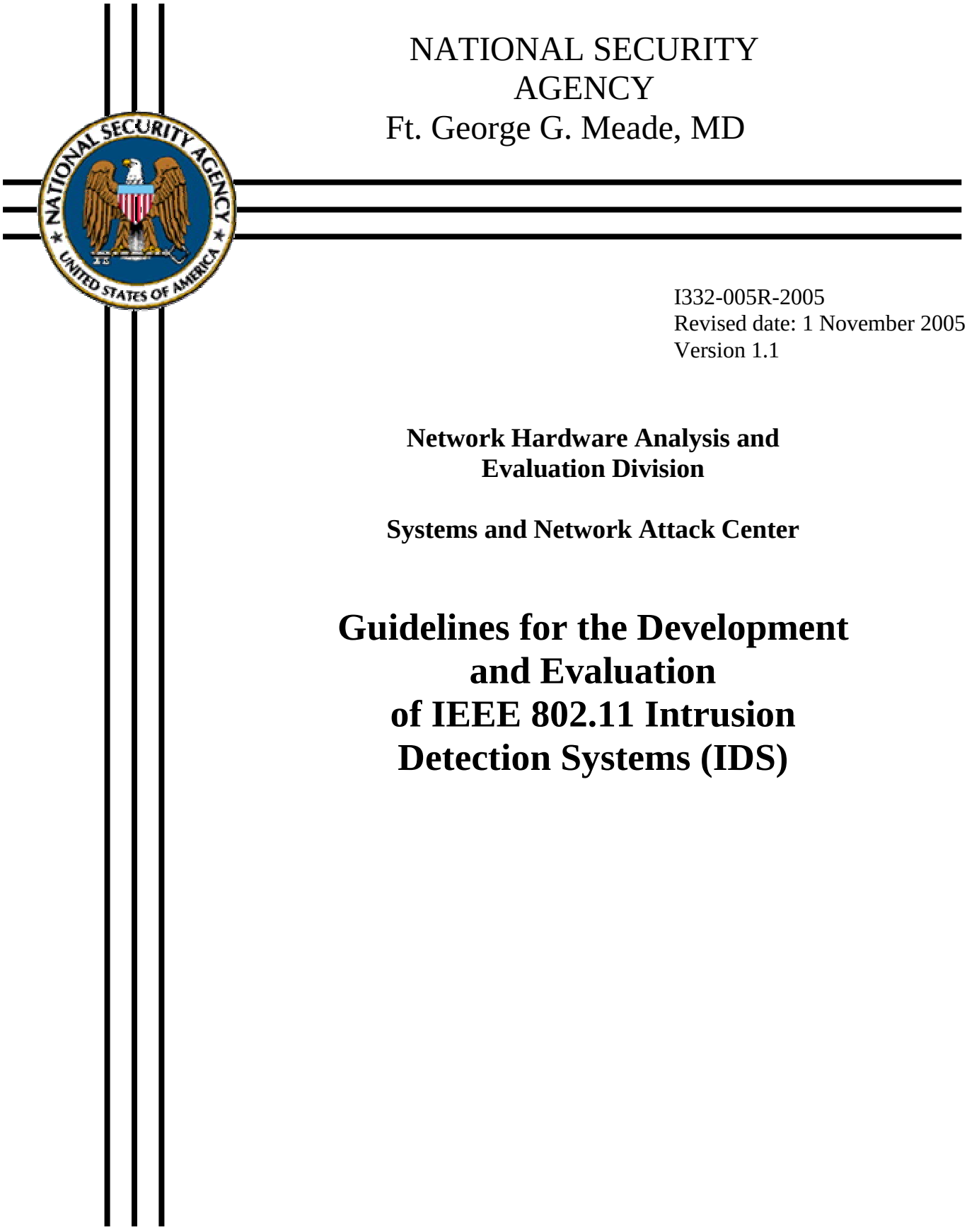

NATIONAL SECURITY
AGENCY
Ft. George G. Meade, MD

I332-005R-2005
Revised date: 1 November 2005
Version 1.1

Network Hardware Analysis and Evaluation Division

Systems and Network Attack Center

Guidelines for the Development and Evaluation of IEEE 802.11 Intrusion Detection Systems (IDS)

FORM A9585F JUL 97
NSN: 7540-FM-001-5611

Table of Contents

Introduction

In today's increasingly wireless world, organizations are quickly realizing the security benefits of constantly monitoring the electromagnetic spectrum within their enterprise. When an organization has an interest in identifying and locating unauthorized wireless hardware and preventing intrusion attempts on their network, the benefits of this monitoring exist regardless of whether or not network owners officially sanction the use of wireless devices. Many government entities have monitored their spaces for the presence of cellular, Bluetooth, infrared, and/or IEEE 802.11 signals for years. The DoD Directive 8100.2 now mandates RF monitoring, intrusion detection, and denial of service prevention in DoD networks. Although not a specific requirement, RF monitoring and intrusion detection could also help federal and military operated health care institutions meet the requirements of the Health Insurance Portability and Accountability Act (HIPAA).

In March 2003, the Systems and Network Attack Center (SNAC) at NSA began a focused effort into the evaluation of 802.11 wireless products and architectures. As a result of this work, the analysts compiled the guideline for the development of a wireless intrusion detection system presented in this document. Analysts wishing to assess the capability of a wireless LAN intrusion detection system (IDS) may use this guideline to evaluate systems against a common metric. It is also the intention of the SNAC to present the requirements in this paper as input toward the generation of a protection profile (http://niap.nist.gov/pp/) thus enabling vendors to create products that meet the standards for use on unclassified or For Official Use Only (FOUO) U.S. Government networks. This document is not all-inclusive and will undergo updates as evaluations continue and technology advances.

Conventional network IDSs focus on the higher layers of the OSI protocol stack. For example, these systems may look for protocol anomalies (deviations from the standards) in an FTP packet or they may seek to identify an instance of a particular worm or virus, such as Code Red or Nimda. They may also identify network port scans or traffic flooding. A wireless IDS (WIDS) does not try to perform these tasks, but instead concentrates it efforts on identifying problems at Layer 1 and Layer 2 in the OSI model, the Physical and Datalink layers, as shown in Figure 1. Although the requirements laid forth in this evaluation guideline do not address the concerns of a conventional network

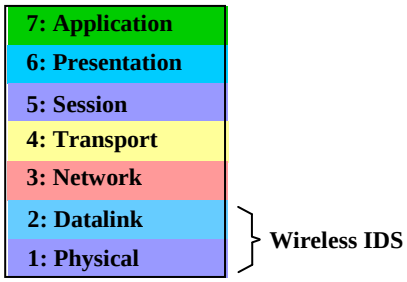

Figure 1: OSI focus of an 802.11 IDS

IDS, for complete protection, a network administrator should also deploy a conventional network IDS on segments connected to the wired network to monitor the higher protocol layers.

The authors base their methodology and presentation order of this evaluation guide on the layered security model illustrated in Figure 2. The first section is the RF Physical Layer. At the heart of any wireless network is the RF communications media over which data passes between the access points (APs) and the clients. Many wireless LAN intrusion detection systems available today focus solely on OSI Layer 2 analysis. However, 802.11 frame analysis by itself is not sufficient to meet the minimum level of information assurance expected of a WIDS so it is also necessary to monitor the RF Physical Layer for signs of intrusion. The second section is Frame Analysis. As already stated, this is the OSI layer that most WIDS already monitor, but SNAC evaluation personnel identified several insufficiencies that still need addressing by WIDS vendors. The third section addresses the monitoring of both authorized and unauthorized client and AP devices themselves to ensure that they are not violating the system security policy. Finally, the General System Requirements section addresses issues such as software assurance, communications between system components, and the handling of data by the system.

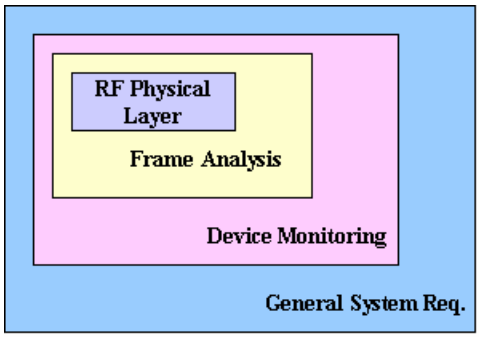

Figure 2: Layered Security Model

This paper leads the reader through each requirement, and, where in the authors' opinion it appears to be necessary, will also include a brief justification or explanation of the requirement. For the purposes of using this paper as an evaluation guide, consider all requirements as having equal weight, but analysts are free to apply unequal weights to their individual evaluations as they see fit. Appendix A contains a concise summary of all of the requirements, in the form of a checklist that analysts may find more useful for evaluation purposes. Appendix B contains a glossary with common IDS and IEEE 802.11 definitions that may not be familiar to the reader.

Terminology

This section defines the terminology used throughout this document.

Term	Meaning
System	"System" refers to the entire IDS architecture, including, but not limited to, the sensors and management computer(s). For the purposes of this paper the terms "IDS", "wireless IDS," and "WLAN IDS" all refer to the "system" as it is defined here.
Administrator	The person(s) who are authorized to make configuration changes to the system.
User	The person(s) who use the system on a daily basis to perform routine tasks. Users do not have as many access permissions as administrators.
Must	This word, or the terms "REQUIRED" or "SHALL," mean that the definition is an absolute requirement.
Should	This word, or the adjective "RECOMMEND," means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
Detect	"Detect" refers to the capability to find and identify an event ("event" is defined below). "Detect" in this document typically refers to finding and identifying an attack. The ability to detect something shall be demonstrable and repeatable.
Event	An event is a distinguishable and meaningful change in the environment observed by the System. An event can be something as simple as detecting a new MAC address or as complex as detecting a denial of service attack.
Log (logging)	Logging means keeping a record of an event that was detected and is typically done to a database or a log file.
Alert	Alerting is the action of notifying someone of an event. Examples of alerting include highlighting something in red, a pop-up alert box or sending an email message. Not all events should generate an alert. Only events deemed important/dangerous by the system designers or system administrators shall cause alerts.
Report	A report is something that is generated either automatically or by a user or an administrator. Reports can be pre-defined or user/administrator configurable. Reports are comprised of events and/or alerts. A possible example is a report of all activity detected for a particular MAC address over a particular time period.

Physical Layer Analysis Requirements

1. Monitor the entire 802.11 bandwidth concurrently.

   Some wireless intrusion detection systems use a single, commercial off-the-shelf 802.11 network interface card (NIC) to monitor the wireless environment. Since most NICs can instantaneously operate only on a single channel, they miss the traffic transmitted on all other channels. To consistently and confidently monitor signals, the system must simultaneously monitor the complete ISM (Industrial, Scientific, and Medical) bands used for 802.11, including 2.4 GHz and 5 GHz. As a result of this requirement, the system must detect all 802.11 frames transmitted on both valid and invalid channels.

2. Accurately detect and log actual frame transmission frequency (channel).

   The system shall correctly determine the center frequency (channel) used for transmission for each frame received, not the frequency (channel) the receiver was on when the frame was captured. The 802.11b/g standard specifies 14 total channels for transmission within the ISM band. The center frequencies for each channel are 5 MHz apart and the channels are 22 MHz wide, resulting in overlap of the signal energy in the frequency domain. Due to this overlap, a receiver can detect a frame transmitted on any frequency (channel) within a five-channel window. If the receiver is tuned to one frequency while an intrusion is occurring at another frequency within the five-channel window, the WIDS must determine and log the actual frequency (channel) on which the intrusion is occurring as opposed to just logging the intrusion as occurring on the channel where the receiver is tuned. This overlapping of signal energy also exists within the 802.11a standard, which specifies 16 channels within the 5 GHz band, of which a subset must overlap. Note that the 802.11a channels authorized for use within the United States do not overlap, but the channels available in other countries do. Figure 3 illustrates the concept of frame overlap.

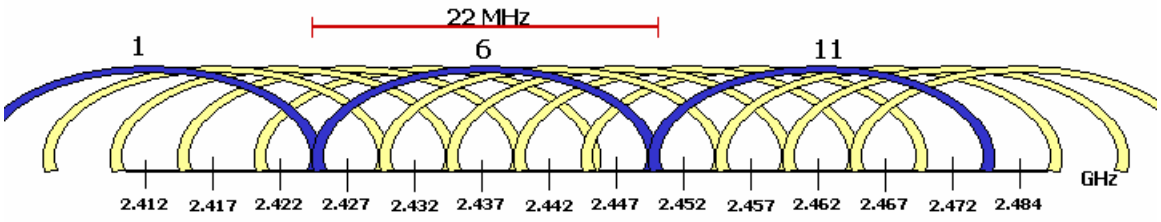

Figure 3: 802.11b frequency channels

3. Physically geolocate all devices, both authorized and unauthorized.

   The WIDS shall provide the ability to pinpoint the location of all 802.11 and non-802.11 wireless hardware operating in the 802.11 bands. Many geolocation techniques exist that could meet this requirement, including, but not limited to, direction finding/triangulation based on angle of arrival and correlation of time of arrival (TOA) or power on arrival (POA) information at multiple receiving posts. The method of geolocation is left to the discretion of the vendor. The system will log the sensor that is closest to the client device or AP.

4. Detect and log signals with a received signal strength above the IEEE 802.11 specified levels.

   The system shall detect and log when it receives an 802.11 frame at a signal level substantially above the IEEE standard. This errant signal may be indicative of an adversary attempting to use non-standard equipment for malicious purposes. This could be from the use of high power transmitters and/or high gain antennas in order to increase the range of the attacker.

5. Detect and log denial of service attacks (DoS) and interference.

   The system must detect interference. The presence of additional signals collocated in the same RF spectrum occupied by 802.11 can severely impact the performance of an 802.11 wireless network. Interference may emanate from seemingly harmless devices, such as microwave ovens, Bluetooth devices, cordless telephones, or even from other 802.11 devices.

   One form of DoS is via RF jamming which is the intentional introduction of interference intended to disrupt an 802.11 wireless network. Another form of DoS is packet injection. Packet injection can take the form of injecting many frames into the network in an effort to saturate/overload the media or injecting frames with specific payloads designed to disrupt the network.

   The system should correlate the presence of new signals with a sudden increase in the frame error rate or a dramatic reduction in throughput, thus indicating a potential denial of service attack.

Frame Analysis Requirements

6. Capture all frames.

   The system shall provide the ability to capture and store at a central location, a single copy of each and every captured 802.11 frame, including Cyclical Redundancy Check (CRC) violations, regardless of the transmission frequency. The system shall provide the ability to store at least a week's worth of data, configure the lifetime of the captured data, and the procedures for automatic backup and remote storage of the captured frames. The format of these captured frames should be compatible with common protocol analyzers, e.g. comma-separated ASCII format.

7. Do not silently discard any frames.

   The system shall not drop any transmitted frames, including those frames with checksum errors or frames that violate the IEEE 802.11 standard. If multiple sensors receive the same frame, the system should note the multiple receipts at the centralized capture location.

8. Filter captured frames.

   The system must provide the ability to setup and configure filters to determine which captured frames get stored on the system. This feature is necessary for organizations with privacy and legal concerns, but it could also serve as a means for reducing the log size.

9. Correlation between captured frames and the sensor of origin.

   The system shall identify and log what sensor(s) captured a frame. This requirement applies to frames of all types and subtypes.

10. Detect and log protocol anomalies.

    The system must detect and log all violations of a particular wireless LAN standard, including, but not limited to, IEEE 802.11a/b/g, 802.1x, and 802.11i. For example, the 802.11 standard delineates many frame fields as having typical, unused, or reserved values. The system must log when non-zero values appear in these reserved fields or when fields have atypical values. Proprietary extensions to frames, such as additional information elements in beacons, must also be logged. The protocol anomaly detection engine shall also have the ability to detect and log undersized and oversized frames.

    The system shall provide the ability to tailor protocol anomaly signatures to fit individual needs. This entails the ability to create new attack signatures or to modifying existing signatures.

11. Detect and log attack signatures.

    The system shall perform stateful frame inspection to detect and log attacks spanning multiple frames.

    The system shall support user-defined intrusion events. No IDS vendor can predict all attacks the system will need to detect, so the system must have the ability to modify and exclude existing signatures, as well as have the ability to create custom signatures added by the system administrator. For the purpose of constructing these custom signatures, the system shall give the administrator complete control over every field in an 802.11 frame and provide the ability to combine filters using logical operators like AND, OR, and NOT. This capability will allow the administrator to keep current with evolving network threats without having to wait for signature updates from the vendor.

12. Analyze statistics.

    The system shall detect and log deviations from the established network traffic baseline. It must compute this baseline automatically, but the system administrator shall have the ability to override particular levels if desired. If the network's activity deviates from a known profile, the system shall use statistical analysis, also known as profile based or anomaly detection, to generate an alarm.

    The system must monitor specific network traits including, but not limited to, bandwidth usage, number of users/wireless clients, time of usage, user/wireless client location, and type of traffic.

    One use for the statistical analysis will be to log an event when a client is seen utilizing the network outside of its regular usage pattern. Even if the usage is benign, the system should note the event because multiple events of this type may indicate a serious problem. In addition, the system shall detect other anomalies, including, but not limited to, active probing, de-authentication and disassociation flooding, and RTS/CTS/NAV abuse.

Device Monitoring

13. Track connection status of all clients.

The system shall track the connection status of each client (authorized or unauthorized) in real time, including, but not limited to, whether the client is offline, associated, or authentication pending. It must also detect and log illegal state transitions, such as, a client device transmitting data frames to a network device before being associated and authenticated. In order for this accumulated profiling information to be useful in determining usage patterns for each device and revealing deviations from normal patterns, the system must accumulate and analyze this profiling information over time. The system shall provide the system administrator with the ability to set this time length.

14. Detect and log unauthorized 802.11 transmitters.

    The system shall detect and log any unauthorized 802.11 transmitters operating in the area detectable by the sensors. Given the ubiquity of wireless equipment, it is reasonable to assume that three distinct threats to network security in the WLAN environment exist. First is the unwitting insider. It is increasingly likely that any laptop bought on the open market will have wireless capabilities. Moreover, it is quite likely the purchaser may not be aware of that fact. Such a person may accidentally activate this wireless device repeatedly over the course of an extended time period if undetected. Second is the witting insider, who may or may not have malicious intent. An example of a witting insider without malicious intent would be someone accustomed to using wireless on their home network deciding to ignore their organization's wireless policy because they enjoy the convenience of using wireless. Lastly, an example witting insider with malicious intent would be an insider with unauthorized hardware intending to use that hardware to attack or bypass the network's security measures.

15. Detect and log unauthorized clients attempting to connect to the network.

    The system must detect and log any unauthorized clients attempting to connect to the wireless network. It must distinguish between the mere existence of unauthorized hardware and an attempt by someone to use that hardware to connect to the wireless network. It is clear that the latter case presents a much greater danger to the enterprise network. There exist many documented instances of authorized personnel attaching unauthorized communications interfaces to their information appliances for the purposes of "making things easier." Logging events of both types makes the threat level more clear.

16. Detect and log authorized devices communicating with unauthorized devices.

The system must detect and log any authorized clients associating to an unauthorized access point or communicating in ad-hoc mode with an unauthorized client.

17. Detect and log OSI Layer 2 (L2) temporal anomalies.

    Temporal anomalies include, but are not limited to, activities such as MAC address spoofing and masquerading. The system shall detect and log an event where an attacker spoofs the MAC address of an authorized client, as determined by an analysis of the current MAC header sequence numbers of the received frames.

    The system shall detect and log an event where two sensors in physically separate (non-overlapping) locations receive frames with the same MAC address at the same time.

    The system shall detect and log an event where a user's MAC address appears in multiple physically distant locations in too short a time span. For example, if a MAC address shows up in New York at 12:00GMT and then again at 12:05GMT in Los Angeles, the MAC address appearing in these two physically distant locations in such a short time frame must trigger an alarm. The system shall provide the ability for the administrator to set the allowable time frame. This requirement shall apply to both clients and access points.

18. Detect and log presence of ad-hoc networks.

    The system shall detect and log any event indicating the presence of an ad-hoc (peer-to-peer) network. Examples of ad-hoc events are: a single device transmitting beacons advertising the presence of an ad-hoc network, two or more devices transmitting data frames in ad-hoc mode, or the termination of an ad-hoc network.

19. Detect and log presence of 802.11 bridges.

    The system will detect and log the presence of an 802.11 bridge, a single device transmitting beacons looking for a bridge, and/or two or more devices transmitting bridge data frames.

20. Detect and log deviation from the security policy.

    Channel policy: In order to reduce interference between APs in the network and APs in other nearby networks, the Administrator will often select the channels over which the system will operate. The system must have the ability to detect and log the transmission of network traffic over unauthorized channels.

SSID cloaking: In some APs, the Administrator can choose to "cloak" the AP's set service ID (SSID) so that the AP does not transmit the SSID in the beacon frame. The informational element containing the SSID will still appear in the frame, but it will contain a null value in place of the SSID string. The system must have the ability to detect and log if a particular access point is violating the SSID cloaking policy.

Authentication policy: The Administrator can configure the authentication policy for open-system authentication, shared key authentication, 802.1x port-based authentication, or any combination of these methods. The system must have the ability to detect and log if a particular client is not adhering to the authentication policy.

Encryption policy: The Administrator can configure the network to operate with or without encryption. The system must have the ability to detect and log if a particular client is not adhering to the encryption policy.

Allowing broadcast SSID to associate: An adversary attempting to locate APs with cloaked SSIDs can configure their client to send out network probe requests using a null or broadcast SSID in the probe. Upon receiving a broadcast probe request from a client, the AP will send a probe response containing the SSID and allow the client to associate. The Administrator can and should configure the AP not to respond to or associate with clients sending probe requests that contain a broadcast SSID. The system must have the ability to detect and log if an access point is violating the null SSID association policy.

General Security Requirements

21. Use secure[1] remote system administration.

Secure remote administration is one of the most important features in a wireless intrusion detection system, since any compromise could render the entire system useless. For example, an unauthorized party that gains remote access to the administrator's console might disable or modify specific sensor rules or could modify the allowed MAC addresses database. The system administrator must use basic principles of Information Assurance when managing the system. The system must provide the ability to use Confidentiality, Integrity, and Availability (CIA) methods to ensure that all components of the system are in a known configuration and to provide the administrator with timely alerts

[1] A secure service provides Confidentiality, Integrity, and Availability (CIA).

The system shall provide all of the following:

At least one secure remote communications path enabled for event monitoring, such as but not limited to HTTPS, SSH, or SFTP.[2]

At least one secure remote communications path for system software updates (sensor rule sets, firmware, etc.), such as, but not limited to, HTTPS, SSH, or SFTP.[2]

The ability to automatically or manually disable all non-secure communications paths for system updates or event monitoring including, but not limited to, HTTP, SNMPv1, FTP, and Telnet over both wire line and wireless transports. The preferred method is to completely remove these capabilities from the system.

The ability to properly encrypt and authenticate all alerts pushed to a remote system administrator over media such as SMS text messages or e-mail.

22. WIDS system health monitor.

    The system shall monitor and indicate the health of the WIDS and all of its individual components. The system shall generate, send, and log an alert whenever individual sensors and other WIDS components fail to communicate.

23. Secure links between WIDS components.

    The system must employ appropriate methods to ensure that the connections between all WIDS components are secure. At a minimum, this must include the use of FIPS certified encryption and two-way authentication. It should also include a strictly regulated constant traffic volume flow to ensure that someone monitoring flow patterns between the system components cannot garner any useful information about the system operation.

24. Support for up to the full data rate of the physical channel.

    In case an adversary tries to hide evidence of an attack in a flood of packets, the WIDS must capture and parse all 802.11a/b/g traffic up to the maximum bit rate. The system must process every frame transmitted. In the event every frame is a malicious frame, the system must not miss any alerts.

[2] The algorithms mentioned in this paper are representative of standard algorithms seen in commercial practice and not representative as sole necessary minimums for government systems.

25. Wireless sensors shall operate in a receive mode only.

The system's sensors shall not transmit RF energy at any time. All WIDS monitoring components must be passive, wirelessly non-addressable elements on the network to ensure that they do not introduce any unintended access or new vulnerabilities into either the wired or wireless networks. If the system uses standard 802.11 hardware, the vendor shall take the necessary steps to physically disable the transmit capability. Software driver modifications are not sufficient to meet this requirement. The system will detect, log, and generate an alarm if any frames originate from a wireless sensor interface just as if it was any other unauthorized wireless device.

26. Ability to create display filters for WIDS events.

The system must provide the ability to filter alerts via the system GUI. The system must provide the ability to create custom filters based on a single or a combination of fields in the alert.

27. Event correlation over time.

The system must correlate events over an administrator adjustable time period, from any one sensor and across multiple sensors. This must allow the system to detect attacks and scans occurring over long periods of time and/or distributed throughout a network.

28. Ability to import traffic captures from external sources.

The system should provide the ability to import traffic collected from sources other than the system sensors and replay this traffic through the system detection engines. External sources may include, but are not limited to, tcpdump, Ethereal, or commercial capture products. For example, a technician may go to a remote site and collect traffic using capture software loaded on a laptop or tablet PC. Upon returning to the office, the technician could then upload the data file to the system server and replay the traffic to determine if problems or attacks existed in the remote environment.

29. Provable sensor firmware/software integrity.

The system must provide cryptographically sound methods (e.g. MD5 or SHA-1 digital signatures[2]) to verify the sensor firmware and software has not been tampered. The firmware/software integrity verification will apply when installing new firmware/software (i.e., matching the hash values with values given by the vendor) as well as for periodic checks of all

sensors. The management computer(s) should provide an automated method for verifying the integrity of all sensors.

30. Provable management computer(s) software integrity.

    The system shall provide cryptographically sound methods (e.g. MD5 or SHA-1 digital signatures[2]) to verify nobody has tampered with the software on the computer(s) used to manage the system. The most common example of this requirement is using a file integrity monitor (e.g. Tripwire™) to monitor changes on a computer system.

31. Filtering alarms and events.

    To minimize false alarms, the system must provide the ability to selectively activate and deactivate the displaying of individual/unique alarms and events. For example, if a sensor is known to be malfunctioning, the system shall provide the ability for an administrator to turn off the events and alarms pertaining to that individual sensor.

32. Support for standardized logging and report formats.

    The system shall support the ability to export event logs and reports into industry standard formats. Standard logging formats include comma separated values (CSV) and common log format (CLF). An example of a CLF log is the log files generated by the Apache web server. An example of a standard report format would be in Extensible Markup Language (XML).

Conclusion

The authors intend that the requirements listed in this document to serve as a guideline for the development and evaluation of WLAN intrusion detection systems. Analysts tasked to examine the functionality and competence of WIDS can use this paper as a checklist in their evaluation. Analysts should focus on each of the four categories presented: RF physical layer, frames, devices, and overall system characteristics. With this guideline, evaluators can evaluate and compare WIDS available for sale today against a common set of criteria.

This guideline will also serve as input into the creation of a WIDS protection profile. A system built to meet all the Protection Profile requirements would constitute an ideal 802.11 WIDS to monitor unclassified and For Official Use Only (FOUO) Government networks only.

Appendix A: Summary of Requirements

Physical Layer Analysis	Comments	Score
1. System must monitor the entire 802.11 bandwidth concurrently		
The entire 2.4 GHz ISM band is monitored		
The entire 5.8 GHz ISM band is monitored		
Detect frames transmitted on both valid and invalid channels		
2. Accurate detection and logging of actual frame transmission frequency		
The system detects and logs the frequency the frame was transmitted on, not the frequency the receiver was on when the frame was captured		
3. Ability to physically locate all 802.11 devices		
The system detects and logs the sensor closest to the device		
The system is able to geolocate the device		
4. Detection of a signal with a received signal strength above the IEEE 802.11 specified levels		
The system detects and logs a signal with a higher than IEEE standard signal strength, possibly due to the use of a high gain antenna		
5. Denial of service/Interference detection		
The system detects active RF interference in the frequency range allowed by 802.11a/b/g		
The system detects DoS attacks including RF jamming, packet injection, and publicly available DoS tools		
The system correlates changes in frame error rate and throughput due to active RF interference		

Frame Analysis	Comments	Score
6. Capture all frames		
The system captures all frames, even those with CRC or other 802.11 protocol violations		
The system stores all frames that have been captured		
The system has the ability to configure captured data lifetime, the procedures for automatic backup, and remote storage of captured frames		
7. Do not silently discard any frames		
The system processes all frames through the detection engines, even those frames with CRC errors or 802.11 protocol violations		
When multiple sensors receive the same frame, the multiple receipts are noted at the centralized capture location		
8. Filter captured frames		
Administrators can setup and configure filters to determine which frames are stored on the system		
9. Correlation between captured frames and the sensor of origin		

Captured frames are tagged with the sensor(s) of origin		
10. Detect and log protocol anomalies		
The system detects and logs violations in the 802.11a/b/g standards		
The system detects and logs atypical field values, proprietary extensions, and undersized and oversized frames		
The system detects and logs violations in the 802.11i standard		
The system detects and logs violations in the 802.1X standard		
The system provides the ability to tailor (create or modify) protocol anomaly signatures to meet individual needs		
11. Detect and log attack signatures		
The system performs stateful frame inspection and detects and logs attacks spanning multiple frames		
The system detects ASLEAP		
The system detects Netstumbler		
The system detects Wellenreiter when in active mode		
The system detects a DISASSOC DoS attack		
The system detects a DEAUTH DoS attack		
The system supports user defined signatures		
The administrator can create custom filters with complete control over every field in an 802.11 frame		
The administrator can create custom filters by combining other filters with logic operators such as AND, OR, NOT		
The administrator can modify and exclude existing signatures		
12. Analyze statistics		
The system calculates normal traffic patterns		
The system allows the administrator to manually edit the traffic baseline		
The system detects deviations from normal network traffic baselines		
The system monitors bandwidth usage, number of users, time of usage, user location, and traffic by type		

Device Monitoring	**Comments**	**Score**
13. Track connection status of all clients		
The system indicates whether a client is authorized or unauthorized		
The system indicates whether a client is offline, associated, has authentication pending, and/or is authenticated		
The system detects and logs illegal state transitions		
The system accumulates and analyzes profiling information over time		
The system provides the ability to set time length.		
14. Detect and log unauthorized 802.11 transmitters		
The system detects and logs unauthorized client MAC addresses		
The system detects and logs unauthorized AP MAC addresses		

15. Detect and log unauthorized clients attempting to connect to the network		
The system detects and logs an unauthorized client actively attempting to connect to a valid network		
16. Detect and log authorized devices communicating with unauthorized devices		
The system detects and logs an authorized device actively communicating with an unauthorized device		
17. Detect and log OSI Layer 2 (L2) temporal anomalies in both clients or APs		
The system detects MAC spoofing and masquerading		
An event is logged if two sensors in physically separate (non-overlapping) locations receive frames with the same MAC address at the same time		
An event is logged if a user/MAC address appears in physically distant locations in too short a time		
18. Detect and log presence of ad-hoc networks		
The system detects a single device broadcasting beacons for an ad-hoc network		
The system detects two or more devices actively participating in an ad-hoc network		
The system detects when an ad-hoc network is terminated		
19. Detect and log presence of Wi-Fi bridging		
The system detects a single device broadcasting beacons for a Wi-Fi bridge		
The system detects two or more devices actively participating in a bridged network		
20. Detect and log deviation from the security policy		
The system detects a device operating on the wrong channel		
The system detects a violation in the broadcast SSID policy of a network		
The system detects a violation in the authentication policy of a network		
The system detects a violation in the encryption policy of a network		
The system detects a violation in the allowing NULL SSID association policy of a network		

General Requirements	**Comments**	**Score**
21. Secure remote system administration		
At least one secure remote communications path is enabled for event monitoring - i.e. HTTPS, SSH, SFTP, SNMPv3		
At least one secure remote communications path is enabled for system updates (sensors rulesets, firmware, etc) - i.e. HTTPS, SSH, SFTP, SNMPv3		
All un-secure remote communications paths are disabled, including, but not limited to, HTTP, SNMPv1, FTP, Telnet (system shall provide the ability to automatically or manually disable these or they are completely removed)		
All alerts pushed to a system administrator, such as pager or SMS messages and emails, are properly encrypted and authenticated.		

22. IDS health monitor.		
The system maintains indication as to the health of the system		
The system generates, sends, and logs alerts when IDS components fail to communicate		
23. Secure links between IDS components		
All traffic between IDS components uses FIPS certified encryption		
All traffic between IDS components uses two-way authentication		
All traffic between IDS components maintains a constant traffic flow so traffic rate analysis is not profitable		
24. Support for up to the full data rate of the physical channel		
The system captures and parses all 802.11a/b/g traffic up to the maximum bit rate, and is able to process every frame received. In the event every frame is a malicious frame, no alerts are missed		
25. Wireless sensor shall be in receive only mode		
No wireless frames are transmitted when the sensor boots		
No wireless frames are transmitted during normal operation of the sensor		
The system detects, logs, and generates an alarm if a wireless sensor transmits		
26. Ability to create display filters for IDS events		
Administrator can create custom filters based on a single or a combination of fields in any alert		
The system provides the ability to filter alerts via the GUI		
27. Event correlation over time		
Events from a single and multiple sensors are correlated over time		
The administrator set the time period length for correlation		
28. Ability to import traffic captures from external sources		
The system is able to import commercial capture software, tcpdump, or Ethereal files and replay them through the IDS detection engines		
29. Provable sensor firmware/software integrity		
Cryptographically sound methods (e.g. MD5 or SHA-1) digital signatures are used to prove that the firmware and software that exists on the sensors has not been tampered with		
30. Provable management computer(s) software integrity		
Cryptographically sound methods (e.g. MD5 or SHA-1) digital signatures are used to prove that the software in use on the management computer(s) has not been tampered with		
31. Filtering alarms and events		
System user can selectively activate and deactivate the displaying of individual/unique alarms and events		
32. Support for standardized logging and report formats		
System supports the ability to export event logs and reports into industry standardized formats		

Appendix B: Glossary and Definitions

Many of the definitions that appear in this section were taken from www.dictionary.com and www.searchnetworking.com.

802.1X
Port based network access control.

802.11
IEEE protocol that defines a standard for wireless local area networking.

802.11a
IEEE extension to the 802.11 protocol that defines wireless local area networking in the 5.8 GHz band, using OFDM.

802.11b
IEEE extension to the 802.11 protocol that defines wireless local area networking in the 2.4 GHz band, using HS-DSSS (High speed DSSS).

802.11g
IEEE extension to the 802.11 protocol that defines wireless local area networking in the 2.4 GHz band, using OFDM.

802.11
IEEE extension to the 802.11 protocol that defines security enhancements.

Ad-hoc Network
A network consisting of two or more clients when no AP is present. This is also known as a peer-to-peer network.

AP
Access Point.

Association
The act of requesting access to the network. In 802.11 networks, association takes place after authentication has successfully completed.

Authentication
The act of verifying one's credentials to the network. The original 802.11 standard defines two forms of authentication: open-system and shared-key.

Bluetooth
A standard for short-range radio links in the 2.4 GHz spectrum between mobile computers, mobile phones, digital cameras, and other portable devices.

Bridge
A telecommunications device that filters traffic between two networks.

Channel
The wireless path used to convey an RF signal from the sender to the receiver. In wireless communications, channels are designated by an RF frequency.

CIA
Confidentiality, Integrity and Availability.

Client
A station such as a laptop, desktop, or PDA that contains a wireless network interface card and communicates on a wireless network. Clients may communicate with APs using 802.11 infrastructure mode or they may communicate directly with other clients using 802.11 ad-hoc mode.

CRC
Cyclical Redundancy Check

CTS
Clear to Send

DoS
Denial of Service. Type of attack designed to make a resource unavailable to authorized users.

DSSS
Direct Sequence Spread Spectrum.

EAP
Extensible Authentication Protocol. Used with 802.1X authentication. Users must first present credentials to an AAA server, such as a RADIUS server, before access to the wireless network is granted.

Ethereal
A publicly available network data sniffer/analyzer. Includes support for many protocols.

Federal Information Processing Standards (FIPS)
Standards developed to address Federal requirements for interoperability of different systems, for the portability of data and software, and computer security.

Frame
A Layer 2 structure. Packets created by higher layer protocols are divided into frames before transmission. 802.11 frames contain a MAC header, payload, and CRC checksum.

FTP
File Transfer Protocol. A communications protocol governing the transfer of files from one computer to another over a network. FTP provides no confidentiality or assurance.

Geo-location
The process of pinpointing the position of a person or object on the surface of the earth.

GHz
Gigahertz. Billions of cycles per seconds. Typically used in frequency measurements.

GUI
Graphical User Interface. Allows a user to point and click instead of having to remember many keyboard commands.

HTTP
Hypertext Transfer Protocol. A protocol used to request and transmit files, especially web pages and web page content, over the Internet or other computer network.

HTTPS
Hypertext Transfer Protocol, Secure. A variant of HTTP using SSL to securely request and transmit files such as web pages and web page content.
IDS
Intrusion Detection System.

IEEE
Institute of Electrical and Electronics Engineers.

IP
Internet Protocol. Part of the TCP/IP protocol suite.

Infrastructure network
A network consisting of one or more APs and clients that communicate directly with the APs. In this type of network clients cannot communicate with one another directly. All traffic goes through the AP.

ISM
Industrial, Scientific, Medical.

Jamming (active)
Transmitting a signal specifically for the purpose of interfering with the operation of pre-existing signal. The result of active jamming is a denial of service to the original transmitter.

LAN
Local area network.

MAC
Media access control. "MAC address" refers to the unique six-byte identifier given to every network adapter manufactured.

MHz
Megahertz. Millions of cycles per second. Typically used in frequency measurements.

NAV
Network Allocation Vector.

NIC
Network Interface Card.

OFDM
Orthogonal Frequency Division Multiplexing.

OSI
Open Systems Interconnection. Refers to the logical structure for a communications network, as created by the International Organization for Standardization (ISO).

PC
Personal Computer.

POA
Power On Arrival. How much power the receiver measures when a frame arrives.

RF
Radio Frequency.

RFC
Request for Comments. One of a series of Internet informational documents and standards widely followed by commercial software and freeware in the Internet and Unix communities.

RTS
Request to Send.

SFTP
Secure File Transfer Protocol. Method of transferring data using encryption. Unlike FTP, SFTP provides for confidentiality and assurance.

SMS
Short Message Service. Small text messages typically sent to a cell phone.

SNMPv3
Simple Network Management Protocol (version 3). The Internet standard protocol defined in RFC 1157, developed to manage nodes on an IP network.

SSH
Secure Shell. A Unix shell program for logging into and executing commands on a remote computer. SSH provides secure encrypted communications between two untrusted hosts over an insecure network.

SSID
Set Service ID. The common name for an 802.11 wireless network. In some cases, knowledge of the SSID is required before network access can be gained.

SSL
A protocol designed to provide encrypted communications on the Internet/ SSL is layered beneath applications such as HTTP, SMTP, Telnet, and FTP and is layered above the connection protocol TCP/IP.

Telnet
Terminal emulator client program allowing a user to login and connect to a remote server.

TOA
Time Of Arrival. When the frame arrives at a receiver.

WiFi
Wireless Fidelity. The name originally referred only to 802.11b products, but now encompasses 802.11a/b/g. All products that bear the Wi-Fi logo are compatible and have passed a series of interoperability tests.

WLAN
Wireless Local Area Network. Refers to 802.11 networks.