A Guide to Securing Networks for Wi-Fi (IEEE 802.11 Family)

Department of Homeland Security

Cybersecurity Engineering

Version 1.0 – March 15, 2017

Homeland
Security

Prepared By

United States Department of Homeland Security (DHS)
Cybersecurity Engineering

Revision History

Version	Date	Description	Authors	Section/Page
1.0	3/15/17	First Release	DHS	All

Table of Contents

1. Introduction

This guide summarizes leading practices and technical guidance for securing networks from wireless threats and for securely implementing wireless access to networks. This document is specifically focused on the wireless technologies commonly referred to as "Wi-Fi" as defined in the Institute of Electrical and Electronics Engineers (IEEE) 802.11 family. This guide does not include commercial mobile networks (e.g., 3GPP, LTE). The recommendations in this guide address wireless threats that are universal to all networks and describe security controls that can work together to mitigate these threats.

Wireless capabilities are widely available, even on networks that are not intentionally providing these services. Wi-Fi signals may infiltrate buildings from commercial providers, adjacent buildings and businesses, and other publicly available services. Authorized and unauthorized Wi-Fi services can be used to gain unauthorized access to networks that are otherwise strongly secured. Due to the pervasive nature of Wi-Fi, it is important to consider the risks associated with these technologies and to examine potential impacts to confidentiality, availability, and integrity when conducting risk and threat analyses. On March 31, 2014, the Federal Communications Commission (FCC) increased the availability of the radio frequency (RF) spectrum for high-speed, high-capacity Wi-Fi in the 5 GHz band in support of the ever-increasing demand for Wi-Fi data connectivity.[1]

In response to the growing number of attacks on networks and the risks associated with the pervasive nature of wireless technologies, a number of wireless security guides have been produced by commercial interests, the Federal Government, and the Department of Defense (DoD). Two of the SANS CIS[2] Critical Security Controls for Effective Cyber Defense v6.0—Boundary Defense (Critical Security Control (CSC) 12) and Wireless Access Control (CSC 15)—are specific to wireless risks and threats.

A major recommendation in the guidance above is to deploy a wireless intrusion detection system (WIDS) and wireless intrusion prevention system (WIPS) on every network, **even when wireless access to that network is not offered**, to detect and automatically disconnect devices using unauthorized wireless services.

CSC 12 and CSC 15 recommend monitoring for communication between networks of different trust levels and specifically calling out WIDS as part of the technical approach for monitoring communication. DoD Directive 8100.2, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG), includes the DoD policy for addressing Wi-Fi threats to both wireless local area networks (WLANs) as well

[1] Link to FCC announcement: https://www.fcc.gov/document/fcc-increases-5ghz-spectrum-wi-fi-other-unlicensed-uses

[2] According to the SANS Institute, the "SANS CIS Critical Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks." See Appendix A for link to the SANS CIS webpage.

as wired networks. The directive requires that an active screening capability for wireless devices be implemented on every DoD network. In July 2016, the Office of the Director of National Intelligence issued guidance requiring WIDS capabilities for continuous monitoring.

The significant increase of wireless technology in and around enterprise networks has correspondingly increased the associated risks. These risks include neighboring Wi-Fi networks, hot spots, hotels, mobile hotspot devices such as mobile Wi-Fi (MiFi), and a multitude of mobile devices and smart phones that have Wi-Fi capabilities. The focus on securing enterprise wired networks (through technologies such as firewalls, intrusion prevention systems (IPSs), content filters, and anti-virus and anti-malware detection tools) has made enterprise networks a more difficult target for adversaries. As a result, adversaries are now exploiting less secure end user devices and Wi-Fi networks to penetrate enterprise networks.

In June 2009, Gartner, Inc., a technology research company, performed a study entitled “Next Generation Threats and Vulnerabilities.” This study concluded that **Wi-Fi infrastructure attacks had the highest level of severity and the lowest time to invest for the attacker.** While improvements have been made in Wi-Fi technologies since the time of this report that improve the basic security of Wi-Fi systems, users are still a weak link and must have a significant understanding of the technology in order to safeguard against many types of attacks. The automation of connections for ease of use and insecure default configurations can lead users to inadvertently compromise the security of their device or network.

2. Threat Types

By not addressing wireless security, enterprise networks are exposed to the threats listed below. Monitoring for wireless activity and devices enables an enterprise to have better visibility into Wi-Fi use and to identify and mitigate Wi-Fi-related threats. Wi-Fi threats include:

- Hidden or Rogue Access Points (APs) – unauthorized wireless APs attached to the enterprise network may not transmit their service set identifier (SSID) to hide their existence.
- Misconfigured APs – APs with weak or incorrect settings that allow unauthorized devices to connect or expose connection communications to sniffing and replay attacks.
- Banned Devices – devices not allowed on the network by organizational policy (e.g., wireless storage devices).
- Client Mis-association (e.g., department and agency (D/A)) clients connecting to non-D/A networks while at D/A sites) – clients using unsecured and unmonitored networks when secured and monitored network connections are available increases the risk of data loss and system compromise.
- Rogue Clients – unauthorized clients attaching to the network. Rogue clients pose risks of bridging and data loss as well as circumventing established security controls and monitoring efforts.
- Internet Connection Sharing and Bridging Clients – a device that shares its Internet connection or allows connectivity to multiple networks concurrently can be used to

bypass network monitoring and security controls and may result in data loss or provide an unsecured network entry point for an attacker.

- Unauthorized Association – an AP-to-AP association that can violate the security perimeter of the network.
- Ad hoc Connections – a peer-to-peer network connection that can violate the security perimeter of the network.
- Honeypot/Evil Twin APs – an AP setup to impersonate authorized APs intercepting network communications and compromising systems that connect to it.
- Denial of Service (DoS) Attacks – an attack that seeks to overwhelm the system causing it to fail or degrade its usability. These attacks are frequently used in conjunction with other attacks (e.g., honeypot) to encourage a wireless client to associate with compromised wireless APs.

3. Threat Remediation

An active WIDS/WIPS enables enterprise networks to create and enforce wireless security policies. WIDS/WIPS provides the ability to centrally monitor and manage enterprise wireless security with respect to the various threats listed above. Alternatively, during an incident related to these threats, an on-site technician would be required to survey the entire enterprise with a laptop or other wireless network detection device in an attempt to locate and identify a rogue AP. Having a WIDS/WIPS capability in place greatly aids in incident remediation.

Successfully identifying and mitigating rogue APs and wireless devices is a challenging and labor-intensive process, as rogue APs are frequently moved and not always powered on. A WIDS/WIPS capability provides immediate automated alerts to the enterprise security operations center (SOC) and can be configured to automatically prevent any clients from attaching to rogue APs. WIDS/WIPS capabilities are also useful for physically locating rogue APs in order to remove them.

4. Recommended Requirements for Enterprise Wireless Networking

Listed below are sample requirements for consideration when securing an enterprise network from wireless threats. These requirements are derived from the sources listed in Appendix A: Authorities and References and should be tailored to specific considerations and applicable compliance requirements. These requirements are currently tailored to guidance applicable to federal Executive Branch D/As.

- Use existing equipment that can be securely configured and is free from known vulnerabilities where possible.
- Meet Federal Information Processing Standards (FIPS) 140-2 compliance for encryption.
- Be compliant to relevant National Institute of Standards and Technology (NIST) 800-53 controls.

- Use the certificates that reside on personal identification verification (PIV) cards for user authentication to comply with Office of Management and Budget (OMB) Homeland Security Presidential Directive 12 (HSPD-12).
- Support an alternative method of certificate authentication where PIV cannot be used.
- Use Extensible Authentication Protocol-Transport Layer Security (EAP-TLS[3]) certificate based methods or better for to secure the entire authentication transaction and communications.
- Minimally use Advanced Encryption Standard (AES) counter mode cipher block chaining message authentication code[4] protocol (CCMP), a form of AES encryption utilized by Wireless Application Protocol (WAP) 2 enterprise networks. More complex encryption technologies supporting the requirement for an enhanced data cryptographic encapsulation mechanism providing confidentiality and the client's capabilities while conforming to FIPS 140-2 may be used as they are developed and approved.
- Allow for enterprise users to operate seamlessly and allow for login scripts and login activities to function normally. Wireless access clients should be able to transition from AP-to-AP with no service disruption while maintaining the security of the connection.

5. Recommended Requirements for WIDS/WIPS

Even wired networks that do not support wireless access should utilize a WIDS/WIPS solution to monitor and detect rogue APs and unauthorized connections. The following list includes specific recommended requirements for WIDS/WIPS sensor networks and should be tailored based on local considerations and applicable compliance requirements. WIDS/WIPS systems should include the following characteristics:

- Rogue client detection capability. The system will reliably detect the presence of a workstation simultaneously broadcasting IP from a second wireless network interface card (NIC).
- Have a rogue WAP detection capability. WAP detection capability should reliably detect the presence of a WAP communicating inside the physical perimeter of the enterprise.
- Have a rogue detection process capability. Rogue client or WAP detection shall occur regardless of authentication or encryption techniques in use by the offending device (e.g., network address translation (NAT), encrypted, and soft WAPs). Rogue detection should combine over-the-air and over-the wire techniques to reliably expose rogue devices.
- Detect and classify mobile Wi-Fi devices such as iPads, iPods, iPhones, Androids, Nooks, and MiFi devices.
- Detect 802.11a/b/g/n/ac devices connected to the wired or wireless network.

[3] RFC 5216

[4] Cipher block chaining message authentication code is abbreviated as CBC-MAC.

- Be able to detect and block multiple WAPs from a single sensor device over multiple wireless channels.
- Be able to enforce a “no Wi-Fi” policy per subnet and across multiple subnets.
- Block multiple simultaneous instances of the following: DoS attacks, ad hoc connections, client mis-associations, media access control (MAC) address spoofing, honeypot WAPs, rogue WAPs, misconfigured WAPs, and unauthorized associations.
- Detect and report additional attacks while blocking the above listed exploits (detection and reporting capabilities will not be affected during prevention).
- Not affect any external (neighboring) Wi-Fi devices. This includes attempting to connect over the air to provide Layer Two fingerprinting; therefore, the use of existing content addressable memory (CAM) tables is not acceptable to fulfill this requirement.
- Provide minimal communications between sensor and server, and a specific minimum allowable Kbps should be identified. The system shall provide automatic classification of clients and WAPs based upon enterprise policy and governance.
- Provide secure communications between each sensor and server to prevent tampering by an attacker.
- Have at least four different levels of permissions allowing WIPS administrators to delegate specific view and admin privileges to other administrators as determined by the D/A.
- Have automated (event triggered) and scheduled reporting.
- Provide customizable reports.
- Segment reporting and administration based on enterprise requirements.
- Produce live packet capture over the air and display directly on analyst workstations.
- Provide event log capture.
- Import site drawings for site planning and location tracking requirements.
- Manually create simple building layouts with auto-scale capability within the application.
- Be able to place sensors and WAPs electronically on building maps to maintain accurate records of sensor placement and future AP locations.
- Meet all applicable federal standards and Federal Acquisition Regulations (FAR)[5] for Federal Government deployments.

6. Recommended Requirements for Wireless Surveys

Many integrators of wireless solutions can perform a predictive or virtual site survey as part of the proposal or estimating process. This approach utilizes a set of building blueprints or floor plans to determine the optimal placement of sensors and APs within the facility. A predictive site survey takes into account the building dimension and structure but cannot account for potential RF sources because no direct examination of the site is conducted. This approach may be

[5] Federal standards and Federal Acquisition Regulations (FAR)

sufficient for some enterprises and is significantly less expensive than a more thorough RF site survey.

Alternatively, a wireless site survey, also known as a RF site survey, provides a definitive set of information for developing a wireless deployment and security plan. The survey is a defined set of tasks performed in the facility that documents the wireless characteristics of the physical facilities, coverage areas, and interference sources. This information is essential to understanding the optimal number and placement of WAPs and WIDS/WIPS devices to provide desired coverage and functionality in a facility.

Issues that a wireless survey seeks to identify include:

- Multipath Distortion – distortion of RF signals caused by multiple RF reflective paths between the transmitter and receiver.
- RF Coverage Barriers – materials used in construction may not transmit RF signals resulting in unexpected loss of strength and reduced range.
- External and Internal Interference Sources – RF signals used by Wi-Fi are not the only users in that frequency. Identification of interference sources assists in designing a solution that achieves the desired coverage in the most efficient manner.

Before beginning a wireless survey, the following information should be obtained:

- Where in the facility is Wi-Fi access needed?
- Will there be more than one wireless network, such as a work and guest network?
- How many devices and connections will be supported over Wi-Fi?
- What are the data rate needs of these devices over Wi-Fi?
- A facility map or floor plan is essential to overlay the survey results on. This floor plan should be provided to the survey team in a digital file format appropriate to their needs, if possible.

The following list provides specific recommendations for a wireless survey. These recommendations should be tailored based on local considerations and applicable compliance requirements. A survey not intended to serve as a guide for network design and installation, and verification of the wireless communication infrastructure may not require all of the details listed.

The wireless survey should produce the following documents as a product:

- A facilities map(s) showing wireless coverage with the following indicated:
    - Interference sources and strength,
    - Any existing networks’ signal strength and coverage contours,
    - External network sources available in the facility with signal strength coverage contours,
    - Identification of areas where multipath distortion may occur,
    - Recommended WAP placement,

  - Recommended WIDS/WIPS placement, and
  - Indication of signal strength coverage contours using recommended placement.

- A report providing details of findings and recommendations including details of risks, threats, and recommended mitigations. The report should include a RF spectrum analysis that will minimally indicate:
  - RF interference sources,
  - Measurement of signal-to-noise ratio (SNR),
  - RF power peaks, and
  - Wi-Fi channel interference.
- A detailed list of materials needed to accomplish goals and coverages as identified in the survey maps and reports.
- An estimated labor hours report required to install, test, and validate the installation described in the survey maps and reports.

The survey information enables optimization of AP channels, antenna type, AP transmit power levels, and placement for the proposed wireless network installation.

7. Budget Estimation Guide

Configuration and budget estimation guidance is provided below for the technical solutions outlined in these recommendations. The example information is the product of market research conducted by DHS. This guidance should be used for budgetary purposes only and the final costs will be heavily dependent on the physical characteristics of the facilities being considered. **Accurate cost estimation is best determined by working with your Network Infrastructure Support team and requesting competitive proposals from experienced installers of these solutions**.

The following factors should be accounted for to ensure a comprehensive estimate of the total project costs:

- Site Evaluation – a predictive site survey utilizing the site floor plans with documentation on existing network infrastructure can provide an accurate cost estimation for equipment required to cover the facility. While not as precise as an onsite RF survey, this typically provides sufficient accuracy for budget purposes. If your site is over 50,000 square feet (sq. ft.) or has significant potential RF interference sources (e.g., onsite RF transmitters, radar installations, or is older stone, masonry, or steel construction), an RF survey may be indicated. Vendors should be informed of these considerations when requesting estimates.
- Labor – cost should include the initial installation, training for network staff to maintain the solution, and training for the Security Operations team to utilize the solution.

- Physical and Virtual Infrastructure – equipment and service costs to support the solution should include: physical or virtual server costs, network infrastructure costs, network cabling, and power cabling.
- Maintenance and Support – costs include warranty, software support, and licensing costs that are part of the ongoing operations and maintenance of the solution.

Table 1 shows budgetary estimate example details for WIDS/WIPS solutions.

Table 1: Budgetary Estimate Example for WIDS/WIPS Solutions

Item Description	Purpose	Estimated Costs ($)	Unit
Predictive RF Survey	Utilizes facility plans to estimate coverage needs for sensors and APs		sq. ft.
Onsite Support	Utilized for training, system tuning, and configuration services, as well as an onsite RF spectrum survey, if desired		Per day
Sensor	Dual band 802.11AC sensor unit		Per sensor
Cell Sensor Option	Additional radio for detection of US cell phone signals by the 802.11 AC sensor		Per sensor
Management Server Virtual Machine (VM)	A VM image for the management server that can support up to 50 sensors Cloud-based, physical appliances, and other license models are available depending on business needs and goals		Per VM or appliance
Service and Support	Support costs for each component varies depending on response time and level of service desired		Per device or license

8. Bluetooth Security Considerations

Bluetooth technologies (IEEE 802.15) in mobile devices present additional risks for the loss of data and the potential to eavesdrop on conversations. This exposes D/As to a higher risk for loss of confidentiality on D/A-managed devices and networks when Bluetooth is utilized while conducting D/A business. Any device–including laptops, cell phones, and tablets–that has this capability is subject to this risk.

Bluetooth technologies are designed to create a personal area network (PAN) that supports the connection of devices such as audio, keyboard, mice, or data storage devices to a system. All versions of the Bluetooth specification include unsecured modes of connection, and these are typically the easiest connections to establish. Bluetooth signals have been exploited at distances of several hundred feet, and this should be taken into consideration when evaluating the risks and establishing policies around its usage.

Mitigation methods for Bluetooth risks should include the development of a Bluetooth usage policy, enforcement of configuration management for D/A-managed devices based on this policy, and user awareness training that informs users of the risks associated with using Bluetooth. More detailed information on threats and mitigations for Bluetooth technologies can be found in NIST SP 800-121 rev 1.

Appendix A: Authorities and References

Listed below are the technical authorities, references, standards, and publications used in the creation of this guide.

Authorities and References	Description
CIO Council Mobile Security (Baseline, Framework, and Reference Architecture)	CIO Council's government mobile and wireless security baseline of standard security requirements https://cio.gov/wp-content/uploads/downloads/2013/05/Federal-Mobile-Security-Baseline.pdf
DHS 4300A	DHS Sensitive System Policy https://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_4300a_policy_v8.pdf
CSC 12 Boundary Defense	The CIS Critical Security Controls for Effective Cyber Defense https://www.cisecurity.org/critical-controls/
CSC 15 Wireless Access Control	The CIS Critical Security Controls for Effective Cyber Defense https://www.cisecurity.org/critical-controls/
DoD Directive 8100.02	Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG) http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf
DoD Instruction 8420.01	Commercial Wireless Local Area Network Devices, Systems, and Technologies http://www.dtic.mil/whs/directives/corres/pdf/842001p.pdf
NIST SP 800-160	NIST SP 800-160 Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems (While not specifically related to this topic, this publication provides guidance on security engineering applicable to all systems.) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf

Authorities and References	Description
FIPS 140-2	Security Requirements for Cryptographic Modules http://csrc.nist.gov/groups/STM/cmvp/standards.html
GAO 11-43	GAO Report to Congressional Committees: Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk http://www.gao.gov/new.items/d1143.pdf
Gartner, Inc.	Next Generation Threats and Vulnerabilities, June 2009
HSPD-12	Policies for a Common Identification Standard for Federal Employees and Contractors https://www.dhs.gov/homeland-security-presidential-directive-12
NIST 800-153	Guidelines for Securing Wireless Local Networks (WLANs) http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-153.pdf
NIST 800-53 rev 4	Security and Privacy Controls for Federal Information Systems and Organizations http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
NIST SP 800-121 rev 1	Guide to Bluetooth Security http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-121r1.pdf
SANS CIS Critical Security Controls	The SANS CIS Critical Security Controls are a recommended set of actions for cyber defense that provide specific and actionable ways to stop today's most pervasive and dangerous attacks. http://www.sans.org/critical-security-controls/

Appendix B: Acronyms and Abbreviations

Acronym	Definition
AES	Advanced Encryption Standard
AP	access point
CAM	content addressable memory
CBC-MAC	cipher block chaining message authentication code
CCMP	Counter mode CBC-MAC protocol
CIO	Chief Information Officer
CSC	Critical Security Control
D/A	department and agency
DHS	Department of Homeland Security
DoD	Department of Defense
DoS	denial of service
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
FAR	Federal Acquisition Regulations
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
GAO	Government Accounting Office
GIG	Global Information Grid
HSPD	Homeland Security Presidential Directive
IEEE	Institute of Electrical and Electronics Engineers
IPS	intrusion prevention system
MAC	media access control
MiFi	mobile Wi-Fi
NIC	network interface card
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PAN	personal area network

Acronym	Definition
PIV	personal identification verification
RF	radio frequency
SOC	security operations center
SNR	signal-to-noise ratio
SP	Special Publication
SSID	service set identifier
VM	virtual machine
WAP	wireless access point
WIDS	wireless intrusion detection system
WIPS	wireless intrusion prevention system
WLAN	wireless local area network

U.S. DEPARTMENT OF HOMELAND SECURITY

Homeland
Security