National Security Agency/Central Security Service

INFORMATION ASSURANCE DIRECTORATE

IAD Best Practices for Securing Wireless Devices and Networks in National Security Systems

IAG U/OO/814639-15
13 October 2015

IAD Best Practices for Securing Wireless Devices and Networks in NSS

The introduction of wireless communication devices into U.S. Government facilities offers a host of advantages related to mission agility, productivity, and user convenience. At the same time, incorporation of wireless technologies into government systems and networks carries the negative aspect of potentially higher risks to national security systems, as threat actors find ways to exploit these capabilities and the communications carried by them. Failure to plan, inform, incorporate, and execute sound security practices for maintaining the integrity of the wireless components of the information systems they touch risks damage to not only the immediate systems touched by the wireless networks, but also extends to all interconnected information systems that can be reached by an unauthorized intruder to the first system. The ramifications of such security breaches can be profound, potentially resulting in the exfiltration of sensitive national security information, degraded system performance, denial of access, and destruction of data, among other consequences. In short, taking action to manage the wireless risk is fundamental to protecting the connected information systems and, concomitantly, the information contained within them.

IAD has developed a set of best practices for establishing, operating, and using wireless communications devices, either as a component of, or in close proximity to, NSS networks. By implementing the outlined measures, network owners and operators will be better positioned to optimize security, manage risk, and implement vulnerabilities. These best practices have been grouped as they relate to three broad categories:

- Information systems (wireless network infrastructure, operating systems, and physical infrastructure)
- Cellular phones
- Personally-Owned Bluetooth®[1] and other Personal Electronic Devices (PEDs)

The recommendations compiled by IAD are for implementation by all personnel engaged with the establishment, operation, and/or use of wireless devices and wireless networks within U.S. Government national security systems. These recommendations should be viewed as “best practices” (rather than sure-fire solutions), intended as guidance to help manage the risk incurred by the authorization of wireless networks in sensitive facilities. These practices apply to the use of:

- all wireless infrastructure devices that connect to NSS networks,
- cellular phones that have been authorized for use inside secure facilities,
- personally-owned Bluetooth-enabled devices, and
- authorized mobile Wi-Fi devices such as laptop computers, tablets, etc.

IAD will continue to update these recommendations, to keep pace with advances in technologies and to capture knowledge gained by specialists through experience in mitigating the risks associated with the use of wireless systems, networks, and devices in U.S. government facilities.

[1] Bluetooth® is a registered trademark of Bluetooth SIG, Inc.

1 BEST PRACTICES: Information Systems

IAD has compiled the following best practices for securing wireless network infrastructure, operating systems, and physical infrastructure when operating wireless devices in U.S. Government facilities.

1.1 Wireless Network Infrastructure

1 Create, implement and manage a Wireless Security Policy. The fundamental question posed by IAD wireless experts to USG customers relates to the organization's policy, employee awareness of the policy, and enforcement of the policy's mandates. Managers must educate employees on the organization's wireless policy, approved devices, and Operations Security (OPSEC). Employees must always be educated on maintaining positive control of mobile devices.

2 Create and maintain a MAC address whitelist of the site's authorized network. IAD wireless analysts often "discover" rogue access points (APs) and unauthorized end user devices (EUDs) in the facility of interest. Consequently, analysts spend a great deal of time de-conflicting "friend vs. foe" with customer IT teams upon the discovery of various unauthorized network components and mobile devices. Developing and maintaining a MAC address whitelist is a step in resolving this confusion.

3 Securely configure infrastructure devices by changing defaults. IAD wireless analysts debug networks that do not use the most secure management services available. As preventative measures, IAD personnel work closely with customers to educate them on using strong passwords, and also work to encourage the IT teams to disable all unnecessary services, change manufacturer's default service set identifier (SSID) to a non-attributable SSID, and configure APs to not broadcast SSID.

4 Use authentication and WPA2 Enterprise encryption. Wireless Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) have been publicly compromised for years; therefore, IAD strongly recommends using WPA2 enterprise encryption.

5 Implement interface best practices by properly shutting down all unused interfaces. IAD recommends placing unused interfaces in an unused VLAN (i.e., other than VLAN 1) and configuring port security on applicable switch ports to maintain optimal security.

6 Upgrade critical operating systems, hardware and software. IAD strongly recommends:

- installing the latest stable versions of the operating system or software (i.e. Cisco®[2] routers, Cisco switches, McAfee®[3] Sidewinder firewalls)
- implementing routing authentication across all routers, and

[2] Cisco® is a registered trademark of Cisco Systems, Inc.
[3] McAfee® is a registered trademark of McAfee, Inc.

- upgrading hardware for outdated routers and switches.

The latest hardware and software upgrades include security patches to protect systems from known vulnerabilities and exploits that could compromise network security.

7 If possible, physically separate the internal network infrastructure. IAD analysts have proved that separation of the internal network infrastructure from the DMZ, preferably in a secure room, maintains the best security and minimizes RF attacks.

8 Manage what's being transmitted. IAD recommends disabling Wi-Fi capability in the BIOS of laptops and in any other devices not approved for Wi-Fi capability, and reconfiguring end user devices (EUDs) to transmit only on 5 GHz Wi-Fi channels. Configure the access points (APs) to not forward Spanning Tree Protocol Packets into the wireless domain. Configure APs to operate only in 5 GHz band to lessen congestion, improve security (due to enhanced attenuation in the walls, preventing packets from escaping out of the building), and make the network visible to fewer devices. Lower the power output of the APs to a level that just provides coverage to the desired area(s).

9 Change the Pre-Shared Key. IAD recommends updating often and periodically for maximum protection.

10 Perform regular vulnerability assessments. IAD wireless analysts perform "spot checks" on dozens of networks each year. They hope that the Best Practice advice outlined here is adopted by a larger customer set to manage risk to wireless network infrastructure and strengthen network defense.

1.2 Operating Systems

1 Implement regular maintenance cycles for domain servers.
2 Implement application whitelisting for all desktop systems.
3 Remove unnecessary/unauthorized software.
4 Implement technical controls to restrict USB usage to authorized devices (or brands).
5 Disable USB/mass storage on all systems that do not require it for normal operations.
6 Upgrade legacy operating systems.
7 Upgrade legacy databases.
8 If not necessary, disable IPv6 on all systems.
9 Renew/maintain software maintenance subscriptions in order to apply the latest software updates.

1.3 Physical Infrastructure

1 Install a wireless intrusion detection system (WIDS) to monitor wireless traffic.

2 Move all phone lockers outside of entry points or outside the building.
3 Install “perimeter entry” detectors for cell band and Wi-Fi devices.
4 Install cell band & Wi-Fi detectors in strategic “interior” locations to catch any intentional device entry or authorized devices are inadvertently left in “wireless on” mode.
5 Install detectors to verify mobile devices in lockers are turned off.
6 Apply TEMPEST film to the windows. The IAD TEMPEST team may be able to provide additional or better TEMPEST solutions.

2 BEST PRACTICES: Cellular Phones

1 Uninstall older open-faced cell phone lockers and install lockers that have RFI shielding inside each locker.
2 Require all phone locker doors to be closed except when inserting or extracting EUDs.
3 Require all cell phones in lockers to be turned off.

3 BEST PRACTICES: Personally-Owned Bluetooth and other Personal Electronic Devices (PEDs)

1 Review “Equipment Acceptance” procedure/policy regarding presence of Bluetooth capabilities.
2 Risk mitigation programs should be implemented, and contain at a minimum the following items:
   a. Formal device approval process
   b. Mitigation(s) required prior to use
   c. Annual refresher training
   d. Registration process
   e. Document describing permitted use
   f. Electronic detection equipment to detect authorized/unauthorized devices

ACRONYMS

AP	Access Point
BIOS	Basic Input/Output System
EUD	End User Device
NSS	National Security Systems
OPSEC	Operation Security
PED	Personal Electronic Devices
SSID	Service Set Identifier
VLAN	Virtual Local Area Network
WEP	Wireless Equivalent Privacy
WIDS	Wireless Intrusion Detection System
WPA	Wi-Fi Protected Access

DISCLAIMER OF ENDORSEMENT

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

CONTACT INFORMATION

Industry Inquiries
410-854-6091
email: bao@nsa.gov

Client Requirements And General Information Assurance Inquiries
IAD Client Contact Center
410-854-4200
email: IAD_CCC@nsa.gov