WHITEPAPER EXCERPT

WI-FI: SECURE ENOUGH FOR FEDERAL GOVERNMENT?

INTRODUCTION

One of the few places that pervasive Wi-Fi is not found these days is in US Federal Government office buildings and military bases. Wi-Fi is secure enough for government use, and is approved by policy. The whitepaper, "Wi-Fi: Secure Enough for Federal Government?", addresses how modern enterprise Wi-Fi networks are secured, describing both generic industry capabilities as well as Aruba-specific innovations that decrease risk for customers. It also highlights different government policies governing Wi-Fi use. The following is an executive overview of the whitepaper.

SUMMARY OF RELEVANT POLICIES

A common misperception is that government policy bans the use of Wi-Fi for security reasons. In reality, a number of policies exist that explicitly permit Wi-Fi, as long as security guidance is followed. Policies and guidelines that are relevant to government use of Wi-Fi include:

- FIPS 140-2
- NIAP/Common Criteria Wireless LAN Access System Extended Package
- DoD 8420.01
- DoD UC-APL
- US Marine Corps "USMC Cybersecurity Directive 005"
- NSA Commercial Solutions for Classified "Campus Wireless LAN Capability Package"
- Committee on National Security Systems CNSSP 17 "Policy on Wireless Systems"
- Committee on National Security Systems CNSSP 15 "Use of Public Standards for Information Sharing"
- Committee on National Security Systems CNSSAM TEMPEST/1-13 "Red/Black Installation Guidance"
- NIST SP800-153
- NIST SP800-53

WI-FI: MORE SECURED THAN WIRED NETWORKS

The security of Wi-Fi is rooted in two interrelated functions: authentication and encryption. The strength of the entire security system rests on doing these two things correctly. All enterprise Wi-Fi vendors who carry the Wi-Fi Alliance "WPA2 Enterprise" certification are capable of basic authentication and encryption sufficient to meet the needs of enterprise users. Some vendors add additional capabilities to meet and exceed the requirements of government users, who typically have more stringent security requirements than the average enterprise user.

Wi-Fi Supports Different Security Levels

Wi-Fi networks and devices are commonplace, giving people broad experience with the technology. Unfortunately, use of Wi-Fi in private homes and in public hotspots often gives a false impression of the level of security that Wi-Fi can provide. Wi-Fi in public hotspots typically uses no security at all - the network is open and anyone can connect. Wi-Fi in private homes is often protected using a pre-shared key. Anyone with access to the key can connect. These are appropriate security levels for a small private network, but this type of security is not appropriate for internal corporate or government networks. For these higher security networks, Wi-Fi must be configured for WPA2-Enterprise. WPA2-Enterprise mandates that all users and devices must *authenticate* themselves using strong credentials (e.g. CAC, PIV, two-factor token) prior to gaining any access to network services. The authentication process is also used to generate one-time dynamic *encryption* keys that protect the privacy and integrity of data as it travels over wireless links. Together, authentication and encryption provide Wi-Fi with far better security than the average wired network.

Defeating Insider Threats

What if an attacker could gain access to the equipment performing the encryption process? For a Wi-Fi network, this is a very real threat, since Wi-Fi access points are deployed in locations that may not have good physical security (e.g. on the ceiling in an office environment.) To defeat this attack, Aruba implements a security architecture that is very different from all other Wi-Fi vendors. In their default configuration, Aruba access points do not perform encryption/decryption and thus do not contain any encryption keys. Instead, access points simply move encrypted Wi-Fi traffic from the wireless domain to the wired domain, pushing them to a centralized network appliance known as a mobility controller - this device will be secured in a datacenter or communications closet. The implication is that an attacker who gains physical control of an Aruba AP - even one who replaces the AP's firmware with custom malicious code - will be unable to break into Wi-Fi sessions that pass through that access point. Non-Aruba APs *must* be physically protected through tamper-evident labels, inspections, PDS (conduit), and locked enclosures - this leads to significantly greater cost.

ACCESS CONTROL FOR MULTI-USE NETWORKS

Many network administrators approach Wi-Fi from the perspective of port-based security, where a given physical port is assigned to a particular security domain or VLAN. In the Wi-Fi world, physical separation does not work. A port-based security approach will have a new Wi-Fi SSID being created for each service or security domain, and physical separation often implies multiple Wi-Fi access points in the same area. Both approaches leads to sub-optimal radio frequency (RF) spectrum utilization, and air-gapped Wi-Fi networks leads to significant expenses for duplicate equipment along with associated installation and cabling costs. It is therefore wise to consider new approaches when deploying multi-service Wi-Fi networks.

All Aruba Mobility Controllers integrate a full stateful firewall, designed to enforce security policies and separation between different types of Wi-Fi users. The firewall delivers *role-based access control* (RBAC) by first putting users into roles, and then enforcing a set of firewall rules per role. Each user gets a separate copy of firewall rules, so traffic separation can be as granular as a single user or device. The mobility controller can act as a traditional L3-4 firewall, enforcing stateful access control lists, and also as a next-generation firewall with Layer 7 application intelligence, recognizing over 1500 enterprise applications through deep packet inspection. The firewall is NIAP-accredited under the Common Criteria Traffic Filtering Firewall Extended Package (TTFW-EP).

To learn more, click here to download the full whitepaper, "Wi-Fi: Secure Enough for Federal Government?"

a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | info@arubanetworks.com

www.arubanetworks.com