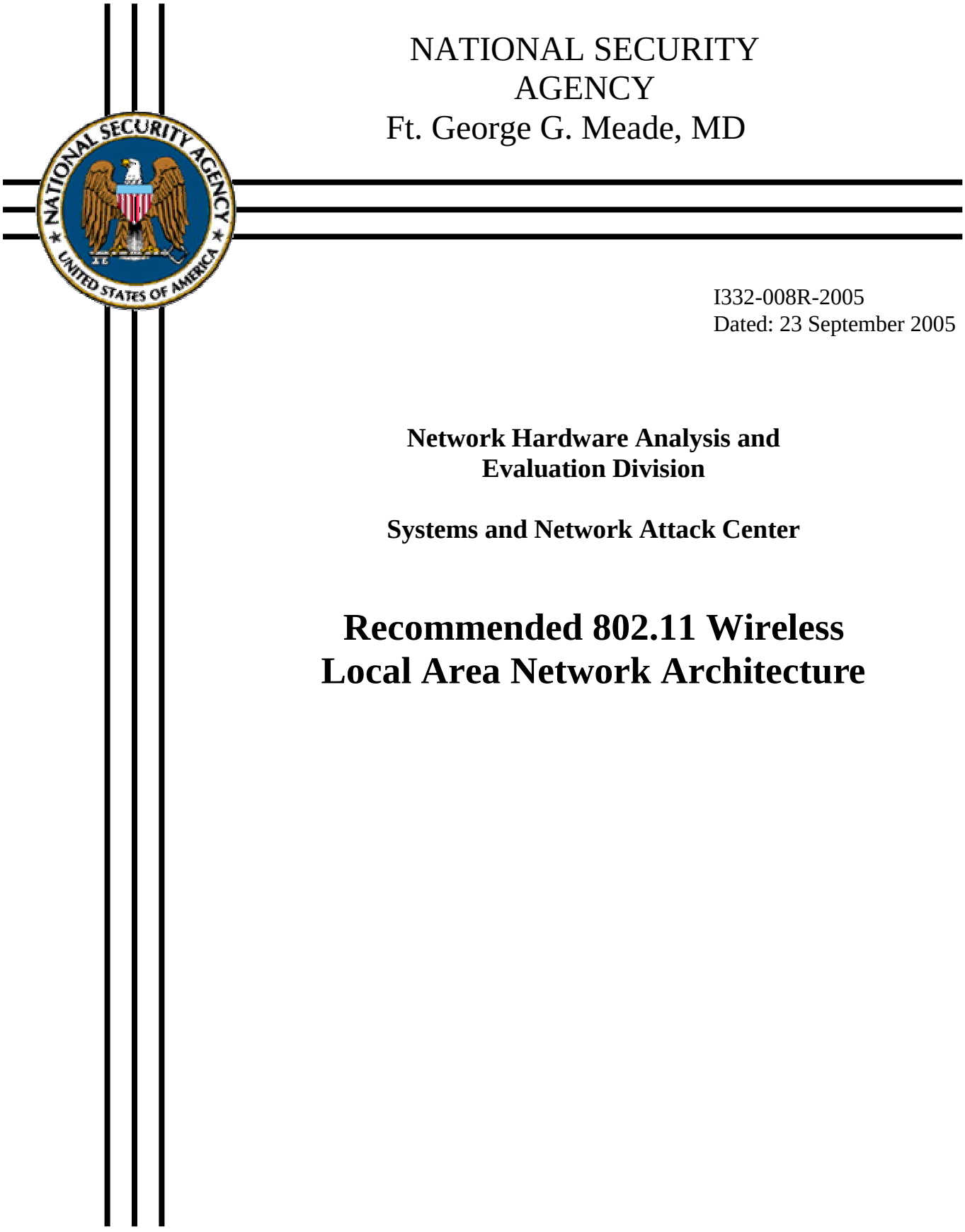

NATIONAL SECURITY
AGENCY
Ft. George G. Meade, MD

I332-008R-2005
Dated: 23 September 2005

**Network Hardware Analysis and
Evaluation Division**

Systems and Network Attack Center

Recommended 802.11 Wireless Local Area Network Architecture

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

Table of Contents

1.0 Introduction

Wireless local area network (WLAN) technology based on the IEEE 802.11 suite of standards is available as built-in options on most new personal computers and as add-on hardware through USB and PCMCIA adapters. The low hardware cost, ease of installation, increased mobility, and network configuration flexibility has led many Government agencies and organizations to implement WLAN solutions for their users to access their enterprise network. With the pervasive use of 802.11 networks throughout the Government and their impending use within the intelligence community, it is imperative for the National Security Agency's (NSA) Information Assurance Directorate (IAD) to make an informed recommendation of a wireless network architecture for Government unclassified networks. Wireless networks with classified data require additional protection solutions that are not addressed here.

In making this recommendation, the evaluation personnel first identified what they thought were the basic requirements of the user, the system administrator (SA), and the owner of the network in order to identify the architecture that would satisfy all three. The user wants the mobility provided through wireless access to the existing wired network so that they can function as if they were at their desk. The SA needs the ability to monitor and manage the wireless network without having to individually reconfigure every access point (AP). The network owner wants the authorized user to securely access the network, but needs to prevent an unauthorized user from extracting, inserting, or changing data in the network or denying the authorized users from obtaining access to the network.

The evaluation personnel also considered the national standards the network owner must meet when implementing WLAN. Both the Department of Defense Directive (DoDD) 8100.2 and the Committee on National Security Systems (CNSS) Policy No. 17 mandate the use of National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2 validated end-to-end encryption for data transmission to and from wireless devices. The Advanced Encryption Standard-Counter-Mode/CBC-MAC Protocol (AES-CCMP) encryption mode used for both IEEE 802.11i and Wi-Fi Protected Access 2 (WPA2) has been approved by the NIST as an acceptable encryption mode. However, other than some vendor proprietary systems, no current IEEE 802.11 device has been certified as FIPS 140-2 validated. Vendors are submitting their WPA2 equipment for approval, but until validated equipment becomes available, another method, such as a FIPS 140-2 validated IPsec tunnel or validated proprietary solutions, must be used to meet the mandates.

2.0 General Architecture Guidance

Even though the IEEE 802.11 standards only apply to OSI model networking Layers 1 and 2, approved security components must be implemented at many layers in both the network and in the wireless clients. Before integrating a wireless solution into a network, the network owner must define and approve a System Security Policy to drive the wireless architecture and security decisions. Typical approved security components include FIPS 140-2 certified authentication and encryption mechanisms, National Information Assurance Partnership (NIAP) certified firewalls, physical protection of all

equipment including APs and client devices, intrusion detection systems (wired and wireless), anti-virus and anti-spyware software, personal firewalls on the clients, disabling unnecessary applications and services, and user education. Systems must be kept up-to-date with upgrades, patches, and new definition files. Users must understand how to properly use security features as well as why security is important. User training must not be underestimated and should be an ongoing process.

2.1 Recommendations for All WLAN Configurations

The following recommendations apply to all unclassified 802.11 networks. Most of these are settings found within standard products.

Change the default SSID- The SSID is the Service Set Identifier. It is the name that identifies the WLAN, and distinguishes one WLAN from another that may occupy the same physical area. The SSID should be a hard to guess value that provides no identifying information about the organization.

Cloak SSID- The beacon frames contain informational elements that provide identifying information about the wireless network, including SSID, supported rates, direct sequence parameter set, and traffic indication map. The SSID informational element must always be present, but the SSID can be omitted and replaced by a null value. Thus the beacon should not reveal the SSID, and should not provide an attacker any information about the SSID, such as length of the value.

Do not allow broadcast SSID to associate- WLAN clients can send out probe requests to determine the identity of nearby wireless networks. The probe request can be addressed to a specific SSID, or can be addressed to a null SSID. APs can be configured to ignore probe requests with a null SSID, thus requiring the client know this value before being able to connect to the network.

Turn on MAC Address Filtering- Before a client is allowed to connect to the network, the MAC address of the client is verified against a database of allowed values. While MAC filtering is known to be vulnerable to spoofing attacks, this security mechanism provides defense in depth, and makes it one-step harder for an attacker to gain unauthorized access.

Disable Open-System and Shared-Key Authentication- The original 802.11 specification details two modes of authentication, both of which should be disabled, as they are not secure. Open-System authentication allows any node to authenticate to the network, with no supporting credentials. Shared-Key authentication initiates a challenge-response exchange between the client and AP, which is vulnerable to off-line key recovery attacks.

Disable "No encryption" and WEP encryption options. By selecting "no encryption," all data frames transmitted on the wireless network will be transmitted in the clear. By selecting WEP encryption, the network is vulnerable to many publicly known attacks against the RC4 algorithm. Both of these options fail to meet the confidentiality requirement of a secure system.

This paper only provides recommendations relating to the wireless portion of the network. Additional perimeter security defenses such as firewalls, filtering routers, etc., traditionally used to protect wired networks should be placed between the wireless network and the wired network. Client devices should be properly configured and locked down. This includes running a personal firewall, anti-virus software, disabling unnecessary applications and services, and keeping the system up to date with the latest patches and software upgrades. Best practices and configuration guides are available to assist in securing the other portions of the network at websites like http://www.nsa.gov, http://iase.disa.mil, and http://csrc.nist.gov.

3.0 WLAN Switched Architecture

The foundation of IAD's recommended architecture for U.S. Government unclassified networks is a WLAN switch-based architecture as illustrated in Figure 1. The basic advantage of a switched architecture is that all the APs connect to a common switch giving the system administrator a centralized point from which to manage and monitor the wireless network and a single entry point to protect from unauthorized wireless access. With centralized management, the SA can view the entire WLAN status, change configuration and/or modify security policy, and push the changes to the network through an authenticated and encrypted link with just a few mouse clicks from a single terminal. Once configured, the central controller monitors the network and enforces the security policy. Other WLAN architectures connect the APs throughout the wired network so that the SA has to manage, monitor, and protect the network from multiple points.

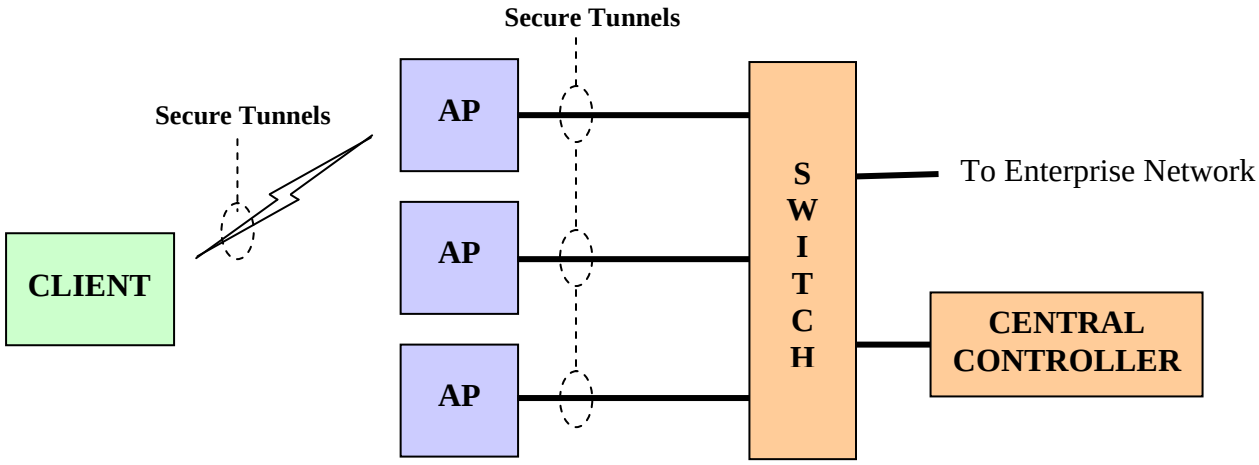

Figure 1. Switched Architecture

A switched architecture is only the basis for the recommended architecture. The following sections will describe and recommend additional factors in the area of authentication and encryption, protecting APs, and wireless intrusion detection systems.

3.1 Authentication and Encryption

The switched network architecture illustrated in Figure 2 uses two tunnels to provide an adequate level of security to protect U.S. Government unclassified or For Official Use Only data. The first tunnel exists at Layer 2 with its endpoints either between the client and the AP or between the client and the switch. Where this tunnel terminates in the network, at the AP or at the switch, depends on the manufacturer. Some manufacturers have the AP perform the encryption function while other manufacturers will provide functionality at the switch to perform encryption. At this layer, the client equipment is authenticating itself to the network. The recommended protocol for this tunnel is WPA2, but until more products reach the market, WPA can be used for authentication and encryption. Be aware that the upgrade from Wireless Equivalent Privacy (WEP) to WPA is a software/firmware change, but the transition from WPA to WPA2 will require a hardware upgrade. The recommended credentials passed to the RADIUS server in the 802.1x/EAP-TLS authentication exchange are 2048-bit X.509 PKI certificates.

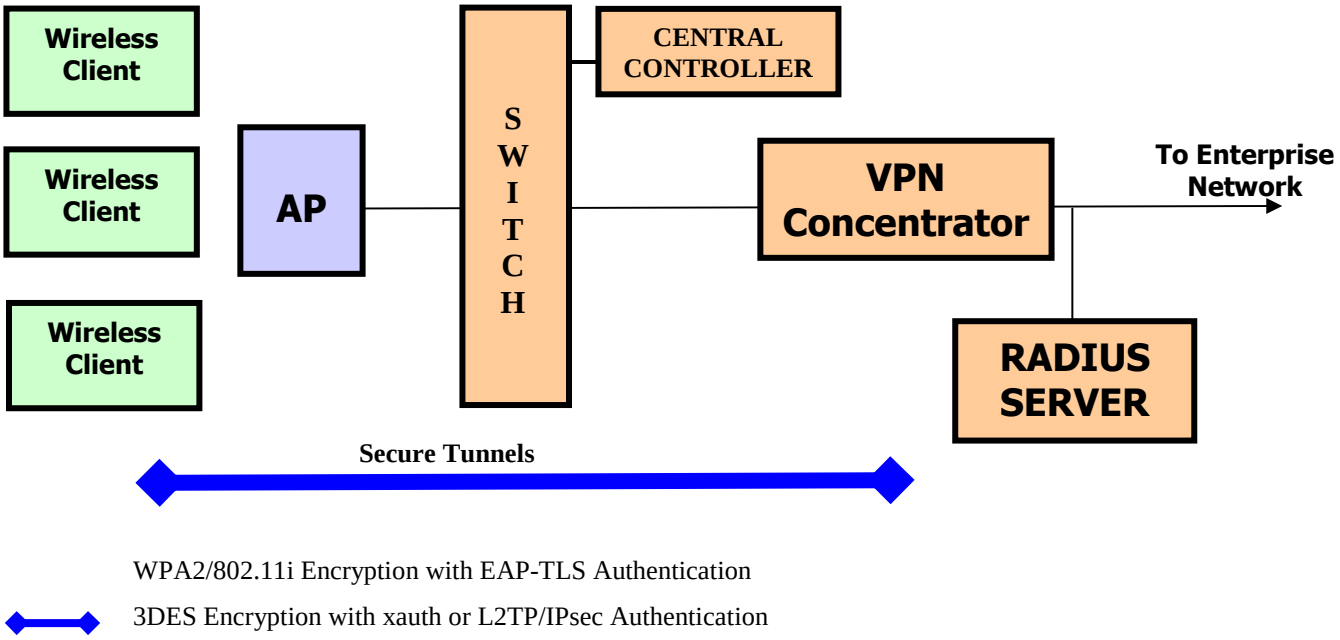

Figure 2. Recommended WLAN Authentication and Encryption Methods

The second tunnel exists at Layer 3 between the client and the concentrator. The user authenticates with either the vendor-supported variation of Internet Protocol security (IPsec) that supports user authentication (*xauth*) or with L2TP/IPsec, which is an Internet Engineering Task Force (IETF) standard. Either one supports user authentication in conjunction with setting up an IPsec tunnel between the client and the concentrator. User authentication can use the same RADIUS server that was used for Layer 2. A variety of user authentication schemes are supported, but the currently recommended scheme is a FIPS 140-2 validated IPsec implementation that supports Group 5 Diffie-Hellman based on 1536 bits and Triple DES encryption. As FIPS 140-2 validated IPsec products

supporting the Advanced Encryption Standard (AES) become available, the Diffie-Hellman exchange should be upgraded to at least 2048-bit, but a NIST-approved elliptic curve with 256 or more bits would be preferred.

3.2 Physical Protection of Access Points

Unless there is a concern that someone might modify or damage the AP, the need to physically protect the AP depends on between which points the encryption/decryption of the wireless data occurs.

- If the encryption only occurs between the client and the AP, the AP must be physically protected because the AP's wired interface provides an open link into the network.
- Even if there is Layer 3 encryption between the client and the concentrator, if the Layer 2 encryption occurs between client and the AP, it is better to physically protect the APs to prevent someone from performing Layer 2 denial-of-service attacks from the AP interface.
- If the Layer 2 encryption occurs between the client and a cryptographic module at the switch with Layer 3 encryption between the client and the concentrator as in Figure 2, the AP does not need to be physically protected.

3.3 Wireless Intrusion Detection Systems

The use of a Wireless Intrusion Detection System (WIDS) is highly recommended for any network, including those that do not allow wireless. In January 2005, NSA published, "Guidelines for the Development and Evaluation of IEEE 802.11 Intrusion Detection Systems (IDS)." This paper basically describes the ideal WIDS for use on unclassified or Unclassified For Official Use Only (FOUO) U.S. Government networks. The paper can be used as either an evaluation criteria or as an aid in selecting a WIDS. Currently, no WIDS meets the criteria described in this paper. However, it will be used as input for a Protection Profile that vendors can build to and meet NIAP requirements. Until a WIDS can be built which meets these guidelines, either select a switched architecture system that includes wireless IDS functionality or deploy a separate wireless IDS. At a minimum, the selected wireless IDS should:

- Operate in receive mode only;
- Detect unauthorized hardware, such as APs, connected to the network;
- Correlate captured frames to sensor of origin;
- Perform direction finding to locate unauthorized hardware;
- Detect Media Access Controller (MAC) spoofing;
- Detect deviation from BSS policy;
- Track connection status of all clients;
- Detect ad-hoc communications between clients;
- Detect disassociation and de-authentication denial of service attacks;
- Detect unauthorized clients attempting to connect;

- Detect authorized clients attempting to connect to unauthorized hardware;
- Have secure remote configuration of sensors over the wired network.;
- Monitor health of WIDS and provide an alarm if a sensor fails;
- Have a secure link for passing information between system components.

4.0 Conclusion

As more WLAN switched-architecture based systems come to market and current vendors make upgrades to implement the latest technology advances, the recommendations outlined in this paper will become easier to meet. Many vendors have, or are, submitting their systems or system components to the appropriate organizations in order to obtain FIPS 140-2 validation. Once the vendors acquire these validations, it should be possible to purchase a non-proprietary WPA2-based, WLAN switched-architecture system out of the box that can be used for unclassified or unclassified FOUO U.S. Government networks.

ACRONYMS

AES	Advanced Encryption Standard
AES-CCMP	Advanced Encryption Standard-Counter-Mode/CBC-MAC Protocol
AP	Access Point
BSS	Basic Service Set
CBC-MAC	Cipher Bock Chaining-Message Authentication Code
CNSS	Committee on National Security Systems
DES	Data Encryption Standard
DoDD	Department of Defense Directive
EAP-TLS	Extensible Authentication Protocol-Transport Layer Security
FIPS	Federal Information Processing Standard
FOUO	For Official Use Only
IA	Information Assurance
IAD	Information Security Directorate
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IPsec	Internet Protocol Security
L2TP/IPsec	Layer Two Tunneling Protocol/Internet Protocol Security
NIAP	National Information Assurance Partnership
MAC	Media Access Controller
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OSI	Open System Interconnection
PCMCIA	Personal Computer Memory Card International Association
PKI	Public Key Infrastructure
RADIUS	Remote Authentication Dial-In User Service
SA	System Administrator
SSID	Service Set ID
USB	Universal Serial Bus
VPN	Virtual Private Network
WEP	Wireless Equivalent Privacy
WIDS	Wireless Intrusion Detection System
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2