National Information Assurance Partnership

TM

Common Criteria Evaluation and Validation Scheme Validation Report

U.S. Government
Wireless Local Area Network (WLAN) Client
Protection Profile
For Basic Robustness Environments

Report Number: CCEVS-VR-06-0001

Dated: 17 May 2006

Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6740
Fort George G. Meade, MD 20755-6740

ACKNOWLEDGEMENTS

Validator

Stuart Schaeffer

Aerospace Corporation

El Segundo, California

Common Criteria Testing Laboratory

SAIC

Columbia, Maryland

Table of Contents

1. EXECUTIVE SUMMARY

This report documents the NIAP validator's assessment of the evaluation of the U.S. Government Wireless Local Area Network (WLAN) Client Protection Profile for Basic Robustness Environments. It presents the evaluation results, their justifications, and the conformance results. It acknowledges that the requirements listed in the Protection Profile (PP) are comprehensive and consistent and may be used to develop products whose security targets, which conform to this profile, will satisfy the needs of the sponsoring Government Agency, the National Security Agency (NSA).

The evaluation was performed by the SAIC Common Criteria Testing Laboratory, an accredited Common Criteria Testing Laboratory (CCTL), and was completed in April 2006. The information in this report is largely derived from the PP, provided by NSA, and the Evaluation Technical Report (ETR) written by SAIC. All security functional requirements are derived from Part 2 of the Common Criteria or special explicitly stated requirements using the format of the CC.

Products, that is, Targets of Evaluation (TOE), addressed by this PP are wireless devices that function as network nodes communicating with other nodes of a wired or wireless network in an environment that meets the requirements of the Department of Defense (DoD) Basic Robustness Environments. The target robustness level of "basic" is specified in the Guidance and Policy for the Department of Defense Global Information Grid Information Assurance (GIG) and is discussed in Section 1 of the PP. Products that conform to this PP will provide the minimum security requirements for wireless client devices.

The PP addresses the security requirements for the client, which provides communication between a user of a wireless communication device (hereafter, a wireless user) and a wired or wireless network and its resources. A client device is expected to be a component in a larger system (for example, a wireless card installed in a laptop computer). While this document does not dictate vendor implementations of a client device, it is expected that the wireless card (or other device), any device drivers necessary to operate the TOE as part of the larger system, and any management software that is used to install, configure or operate the WLAN client will be included as part of the TOE in any Security Target (ST) claiming conformance to this PP. The intent is to ensure that vendors/sponsors submit complete products for evaluation rather than restricting the evaluation to specific portions of a product.

This PP requires privacy and integrity of communications over the WLAN, using commercially available cryptographic algorithms. Security administration for the client is also a requirement. The assurance requirements specified in the PP are EAL 2 augmented with Flaw Remediation, TOE CM Coverage, and Misuse – Examination of Guidance.

The TOE is required to provide secure functions for administration, audit, and encryption, but because it is a specialized device for incorporation into a larger system, e.g., a laptop computer, it is not expected to address by itself all of the threats and security policies expected in a Basic Robustness Environment. The hardware platform (e.g., handheld device, notebook computer) in

which the WLAN client is installed and the operating system are components of the environment and are not required to be included as part of the TOE at basic robustness, but the TOE may rely on the IT environment to augment its own security functions. The PP separates threats and policies into those addressed by the TOE and those addressed by the IT Environment, and it identifies security objectives for the environment to be met by assumptions about the environment or by requirements levied on it. Specific environmental requirements are identified in Section 5 of the PP.

Certain characteristics of wireless communication devices and the use of cryptography necessitated some explicit requirements and a small number of refinements to existing CC requirements.

The validator monitored the activities of the evaluation team, provided guidance on technical issues and the evaluation processes, and reviewed successive versions of the Protection Profile, reviewed intermediate evaluation results (i.e., the CEM work units), and reviewed successive versions of the ETR and customer responses. The validator determined that the evaluation showed that the PP satisfies all of the APE security assurance requirements according to the Common Criteria for Information Technology Security Evaluation, Version 2.2 and Part 2 of the Common Methodology for Information Technology Security Evaluation, Version 2.2. Therefore, the validator concludes that the SAIC findings are accurate, the conclusions justified, and the conformance claims correct.

The following interpretations applied to this evaluation:

National Interpretations:

I-0412: Configuration Items In The Absence Of Configuration Management

International Interpretations:

CCIMB interpretation 65 - Final Interpretation for RI # 65: No component to call out security function management

The information contained in this Validation Report is not an endorsement of the PP by any agency of the U.S. Government and no warranty of the PP is either expressed or implied.

2. IDENTIFICATION

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product and protection profile evaluations. Under this program, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation conduct security evaluations.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products or protection profiles desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

Table 1 provides information needed to completely identify the protection profile, including:

- The Protection Profile (PP): the fully qualified identifier of the PP as evaluated;
- The organizations participating in the evaluation.

Table 1: Evaluation Identifiers

Item	Identifier
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
Protection Profile	*U.S. Government Wireless Local Area Network (WLAN) Client Protection Profile For Basic Robustness Environments*, Version 1.0, March 2006
Evaluation Technical Report	*Evaluation Technical Report For US Government Wireless Local Area Network (WLAN) Client Protection Profile For Basic Robustness Environments, Version 0.3*, September 27, 2005
Sponsor	National Security Agency (NSA)
Developer	National Security Agency (NSA)
Evaluators	SAIC
Validator	The Aerospace Corporation

3. SECURITY POLICY

The following security requirements listed in the PP make up the required security policies:

3.1. Administration Policy

Wireless users, i.e., users of wireless clients, send and receive data via the TOE but do not have direct access to TOE functions and cannot exercise any control over TOE functionality. Only administrators have the access necessary for such control, and they are assumed to be authenticated by the IT environment.

The Administration security policy is defined by

- FMT_MSA, ensuring that only secure values are accepted for security attributes, that default values are restrictive, and that administrators may override the default values;
- Three iterations of FMT_SMF, enabling administrators to turn encryption on and off, select an encryption algorithm, manage encryption keys, and enable and disable auditing.

3.2. Accountability (Audit) Policy

The Audit security policy calls for the capability to log and review the security relevant events listed below. The requirements that define the audit policy, FAU_GEN_EXP, are tailored specifically for wireless clients and hence are explicit.

The PP requires a TOE to generate audit records for four events:

- Dropping a packet that fails to satisfy the Wireless Client Encryption Policy (see below);
- Changing the TOE encryption algorithm, including selecting no encryption;
- Execution of cryptographic self test on start-up or upon request;
- Execution of cryptographic self tests immediately after the generation of a key.

In addition, the audit requirement allows for recording certain other events if doing so “makes sense” in the context of the event that generates the record:

- Errors detected during cryptographic key transfer;
- Destruction of a cryptographic key.

The audit requirement also specifically prohibits the recording of cryptographic keys in audit records.

3.3. Encryption Policy (Data Protection)

The Encryption security policy, i.e., the data protection policy, is defined by a subset of the data protection requirements:

- FDP_IFC, enforcement of the TOE encryption policy;
- FDP_IFF, encryption and flow control of data packets;
- FDP_RIP, ensuring data from a packet does not appear in a subsequent packet or in packet data transferred to the TOE's host computer;
- FCS_CKM.4, destruction of cryptographic keys.

and augmented by explicit requirements:

- FCS_BCM_EXP, implementation and testing of cryptographic modules in conformance with the FIPS 140 cryptographic standard;
- FCS_CKM_EXP, cryptographic key establishment,
- FCS_COP_EXP, random number generation and encryption/decryption operations in conformance with the FIPS 140 cryptographic standard.

3.4. Self Protection Policy

To ensure that the TOE is functioning correctly, FPT_TST is invoked to require that the TOE

- run a hardware self-test at start-up and on demand;
- provide a capability to verify the integrity of all TSF data except audit data;
- provide a cryptographic function to verify the integrity of TSF executable code.

4. REQUIREMENTS ON THE IT ENVIRONMENT

The TOE is a specialized device for incorporation into a larger system such as a laptop computer. It is presumed that the system in which it is incorporated provides the services typically provided by an operating system. Therefore, a number of security requirements are levied on the IT environment.

4.1. Audit Policy Support

The environment is required to support user accountability via audit records, analysis of potential violations of the TOE security policy, administrator audit review, and protection of the audit trail. This support is provided by:

- FAU_GEN, to associate each auditable event with the identity of the user that caused the event;
- FAU_SAA, to monitor audit events to determine if a potential TOE security policy violation has occurred;
- FAU_SAR, to present audit records in a human-readable format, to restrict viewing of the audit trail to authorized users, and to search, sort, and reorder audit records.
- FAU_SEL, to permit selection of specific events to audit;
- FAU_STG, to protect the audit trail from tampering and alert the administrators if the audit trail exceeds a specified amount of storage.

4.2. User-Subject Binding

FIA_USB is invoked to ensure that user security attributes are correctly associated with subjects (operating system processes) operating on behalf of users and are modifiable.

4.3. Security Management Functions

FMT_MOF is invoked to ensure that only an administrator can control the encryption and decryption of packets and manage auditing.

FMT_MTD is invoked to ensure that only an administrator can set the system time.

FMT_SMR is invoked to ensure that individual users can be associated with the role of Administrator.

4.4. Data Protection

FDP_RIP is invoked to ensure that data from a packet is not available when a resource (e.g., system memory) is allocated to a new packet.

4.5. Non-bypassability

FPT_RVM is invoked to require that the system hosting the TOE ensures that TOE security policy enforcement functions are properly executed before allowing functions within the TOE to proceed.

4.6. Domain Separation

FPT_SEP is invoked to ensure that the TOE and the Environment itself are protected from tampering by untrusted processes and that separation of processes in different security domains is enforced.

4.7. Reliable Time Stamps

FPT_STM is invoked to ensure that the date and time information used by the TOE are reliable.

5. ASSUMPTIONS

Because the TOE is a wireless network interface device incorporated into a larger system, it is expected that the TOE will rely on the larger system for access control (user authentication and authorization, protection against unauthorized access, and monitoring of unattended sessions) and protected storage of and access to the audit trail. Therefore, the following five threats identified in the Basic Robustness Environment are not addressed by the TOE but are assumed to be addressed by the environment.

Table 1. Basic Robustness Threats not Applicable to the TOE

T.AUDIT_COMPROMISE (Identical to T.ACCIDENTAL_AUDIT_COMPROMISE in the Consistency Guide)	A user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.
T.MASQUERADE	A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.
T.UNATTENDED_ SESSION	A user may gain unauthorized access to an unattended session.

T.UNAUTHORIZED_ ACCESS	A user may gain access to user data for which they are not authorized according to the TOE security policy.
T.UNIDENTIFIED_ ACTIONS	The administrator may not have the ability to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.

5.1. Usage Assumptions

The TOE is expected to be installed in an IT environment (e.g., PC hardware and O/S) that can address threats and policies outside the capabilities of the TOE and meets the IT environmental requirements necessary to support the correct operation of the TOE.

Administrators are non-hostile, appropriately trained and follow all administrator guidance.

Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment.

5.2. Environmental Assumptions

The IT environment is assumed to be capable of providing functionality to counter the threats listed in Table 1. Specifically, it is assumed to provide identification and authentication of users, control of user access to data, separation of an Administrator role from roles assumable by non-administrator users, protection of audit data in storage, and the ability to monitor and act on session inactivity.

5.3. Clarification of Scope

Products that comply with this PP are considered to be suitable for use in Basic Robustness environments. This PP addresses seven of the threats in the *Consistency Manual for the Development of U.S. Government Protection Profiles for use in Medium Robustness Environments, Release 3.0*:

Table 2: Threats Countered by the TOE

T.ACCIDENTAL_ADMIN_ ERROR	An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
T.CRYPTO_COMPROMISE	A user or process may cause key data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified or

	deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.
T.POOR_DESIGN	Unintentional errors in requirements specification or design of the TOE may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_IMPLEMENTATION	Unintentional errors in implementation of the TOE design may occur, leading to flaws that may be exploited by a casually mischievous user or program.
T.POOR_TEST	Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities.
T.RESIDUAL_DATA	A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.
T.TSF_COMPROMISE	A user or process may cause, through an unsophisticated attack, TSF data, or executable code to be inappropriately accessed (viewed, modified, or deleted).

The PP addresses two of the three security policies in the Basic Robustness Environment:

Table 3: Organizational Security Policies Addressed by the TOE

P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.CRYPTOGRAPHY	Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services).

Because the TOE is an internal component of a larger system, it is incapable of directly displaying information to a user. It relies on the larger system to do this, and therefore the PP does not address one security policy of the Basic Robustness Environment:

Table 4: Basic Robustness Policy Not Addressed By the TOE

P.ACCESS_BANNER	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

Finally, the TOE supports one security function policy, not an organizational security policy, but a named set of rules described in the security functional requirement of the PP and enforced by the TOE:

Table 5. Security Function Policy

P.WIRELESS CLIENT ENCRYPTION SFP	The users/access system administrators shall specify that the TOE encrypt/decrypt user data as it transits to/from wireless network.

6. ARCHITECTURAL INFORMATION

A WLAN is a network in which network nodes communicate by broadcasting wireless (radiated) signals rather than a physical wired connection. A wireless client is a device that transmits and receives signals to and from another network node via a wireless access system. A typical implementation is a PC card inserted into a laptop computer communicating with a wired network through a wireless router. A client might also be circuitry embedded in a handheld device such as a Blackberry. It not intended to provide any direct network services to users, relying on the IT environment for packet creation and management

Systems (i.e., network nodes) containing wireless clients are generally easily carried about and used in public spaces, and even in restricted operational environments their signals might be detected by unauthorized equipment. In order to maintain confidentially of transmissions, encryption is essential. For much government use, trusted strong encryption is needed, and clients that conform to this PP require the use of FIPS certified encryption software.

7. DOCUMENTATION

No external supporting documentation was used in the evaluation.

8. RESULTS OF THE EVALUATION

The U.S. Government Wireless Local Area Network (WLAN) Client Protection Profile For Basic Robustness Environments has satisfied the evaluation requirements of the APE section of the CEM. The PP was assessed against the protection profile requirements as stated in the Common Criteria for Information Technology Security Evaluation Version 2.2.

9. VALIDATOR COMMENTS

None.

10. GLOSSARY

CC	Common Criteria
CM	Configuration Management
COTS	Commercial Off-The-Shelf
DoD	Department of Defense
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
GIG	Global Information Grid
ISSE	Information System Security Engineers
IT	Information Technology
OSP	Organization Security Policy
PKI	Public Key Infrastructure
PP	Protection Profile
PUB	Publication
RF	Radio Frequency
SF	Security Function
SFP	Security Function Policy

11. BIBLIOGRAPHY

[1] Consistency Instruction Manual For development of US Government Protection Profiles For use in Basic Robustness Environments, Release 3.0, 1 February 2005

[2] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and General Model, Version 2.4, March 2004, CCIMB-2004-03-001

[3] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, January 2004, CCIMB-2004-01-002

[4] Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2, March 2004, CCIMB-2004-03-003

[5] Common Evaluation Methodology, Part 1: Introduction and General Model, Version 0.6, 97/01/11, CEM-97/017

[6] Common Evaluation Methodology ASE/APE Trial Use Version, Version 2.4, March 2004, Revision 256, CCIMB-2004-03-004

[7] Common Criteria Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation, Version 1.1, February 2002, CEM-2001/0015R

[8] FIPS PUB 140-2:Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, May 25, 2001.

[9] Global Information Grid (GIG) Policy 6-8510, Information Assurance Guidance,16 June 2000