National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

Protection Profile for Wireless Local Area Network (WLAN) Access Systems, Version 1.0, December 1st, 2011

Report Number: CCEVS-VR-PP-0008
Dated: 15 April 2015
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 6940
Fort George G. Meade, MD 20755-6940

ACKNOWLEDGEMENTS

Common Criteria Testing Laboratory

Base and Additional Requirements
Leidos, Inc.
Columbia, Maryland

Additional Requirements
InfoGard Laboratories, Inc.
San Luis Obispo, California

Table of Contents

1 Executive Summary

This report documents the assessment of the National Information Assurance Partnership (NIAP) validation team of the evaluation of the Protection Profile for Wireless Local Area Network (WLAN) Access Systems, Version 1.0 (WLANASPP10). It presents a summary of the WLANASPP10 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the WLANASPP10 was performed concurrent with the first product evaluation against the PP's requirements. In this case the Target of Evaluation (TOE) for this first product was the Aruba Mobility Controllers and Access Points, version 6.3.1.5. The evaluation was performed by the Leidos Inc. Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in October 2014. This evaluation addressed the base requirements of the WLANASPP10, as well as a few of the additional requirements contained in Appendix C.

Another product—the Fortress Mesh Point ES520 and ES580—was evaluated by the InfoGard Laboratories Inc. CCTL and completed in December 2014. This evaluation addressed additional requirements in Appendix C of the WLANASPP10 that had not been evaluated previously. Combined, these two Security Targets include the entirety of the additional SFRs defined in Appendix C of the PP so examination of further Security Targets is unnecessary for the purposes of this VR.

The information in this report is largely derived from the Evaluation Technical Report (ETR), written by the Leidos CCTL. Similarly, for materials covered by the Fortress evaluation that were out of scope of the Aruba Networks evaluation, the ETR produced by InfoGard was referenced. Additional review of the PP to confirm that it meets the claimed APE assurance requirements was performed independently by the VR author as part of the completion of this VR.

The evaluation determined that the WLANASPP10 is both Common Criteria Part 2 Extended and Part 3 Conformant. The PP identified in this Validation Report has been evaluated at a NIAP approved Common Criteria Testing Laboratory using the Common Methodology for IT Security Evaluation (Version 3.1, Rev 4) for conformance to the Common Criteria for IT Security Evaluation (Version 3.1, Rev 4). Because the ST contains only material drawn directly from the WLANASPP10, performance of the majority of the ASE work units serves to satisfy the APE work units as well. Where this is not the case, the lab performed the outlying APE work units as part of this evaluation.

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence provided.

The validation team found that the evaluation showed that the WLANASPP10 meets the requirements of the APE components. These findings were confirmed by the VR author. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

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 evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs). CCTLs evaluate products against Protection Profile containing Assurance Activities, which are interpretations of CEM work units specific to the technology described by the PP.

In order to promote thoroughness and efficiency, the evaluation of the WLANASPP10 was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the Aruba Mobility Controller and Access Point, provided by Aruba Networks, Inc. The evaluation was performed by the Leidos Inc. Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, United States of America, and was completed in October 2014.

The WLANASPP10 contains a set of "base" requirements that all conformant STs must include as well as "additional" requirements that are either conditional or strictly optional, depending on the requirement in question. The vendor may choose to include such requirements in the ST and still claim conformance to this PP. If the vendor's TOE performs capabilities that are governed by any additional requirements, that vendor is expected to claim all of the additional requirements that relate to these capabilities.

Because these optional requirements may not be included in a particular ST, the initial use of the PP will address (in terms of the PP evaluation) the base requirements as well as any additional requirements that are incorporated into that initial ST. Subsequently, TOEs that are evaluated against the WLANASPP10 that incorporate additional requirements that have not been included in any ST prior to that will be used to evaluate those requirements (APE_REQ), and any appropriate updates to this validation report will be made.

The following identifies the PP subject to the evaluation/validation, as well as the supporting information from the base evaluation performed against this PP, as well as subsequent evaluations that address additional optional requirements in the WLANASPP10.

Protection Profile	*Protection Profile for Wireless Local Area Network (WLAN) Access Systems, Version 1.0, December 1, 2011*
ST (Base)	Aruba Mobility Controller and Access Point Series Security Target, Version 1.0, September 29, 2014
Evaluation Technical Report (Base)	Evaluation Technical Report for Aruba Mobility Controller and Access Point Series, Version 1.0, August 6, 2014
ST (Additional)	Fortress Mesh Point ES520, ES820 Security Target, Version 2.0, December 5, 2014
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4
Conformance Result	CC Part 2 extended, CC Part 3 conformant
CCTL (base)	Leidos (formerly SAIC) Inc., Columbia, MD USA
CCTL (additional)	InfoGard, Inc., San Luis Obispo, CA USA

CCEVS Validators (base)	Bradford O'Neill, MITRE Corporation
	Jean Petty, MITRE Corporation
CCEVS Validators (additional)	Patrick Mallett, MITRE Corporation
	Daniel Faigin, Aerospace Corporation

3 WLANAS Description

The WLANASPP10 specifies information security requirements for wireless LAN access systems for use in an enterprise and describes these essential security services provided by this technology that allows it to properly contribute to a secure wireless access solution.

In addition to centralized management functions and cryptographic services, the WLAN Access System requires the wireless client to perform 802.1X authentication, relying on an authentication server to authenticate the client, before providing network access. The WLAN Access System acts as a pass through device between the wireless client and authentication server. Secure communication tunnels are formed only if authentication is successful. Following successful authentication, the WLAN Access System derives a session key with each wireless client. All subsequent communication between the WLAN Access System and the wireless client is encrypted. The WLAN Access System decrypts traffic that originates from an authenticated wireless client and passes the traffic into the backend network. Likewise, the WLAN Access System encrypts traffic sent from the backend network to the authenticated wireless client. The WLAN Access System supports multiple simultaneous wireless connections and is capable of establishing and terminating multiple cryptographic tunnels to and from those peers.

Conformant TOEs will meet the Expanded Service Set (ESS) requirements in the 802.11 standard using 802.1X authentication; there are no requirements and subsequently no verified claims relating to Independent Basic Service Set (IBSS) operations, or ESS operations using a pre-shared key.

4 Security Problem Description and Objectives

4.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

Table 1: TOE Assumptions

Assumption Name	Assumption Definition
A.NO_GENERAL_PURPOSE	It is assumed that there are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE.
A.NO_TOE_BYPASS	Information cannot flow between the wireless client and the internal wired network without passing through the TOE.

Assumption Name	Assumption Definition
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

4.2 Threats

Table 2: Threats

Threat Name	Threat Definition
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.RESOURCE_EXHAUSTION	A process or user may deny access to TOE services by exhausting critical resources on the TOE.
T.TSF_FAILURE	Security mechanisms of the TOE may fail, leading to a compromise of the TSF.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TOE data and TOE executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to data or TOE resources. A malicious user, process, or external IT entity may misrepresent itself as the TOE to obtain identification and authentication data.
T.UNAUTHORIZED_UPDATE	A malicious party attempts to supply the end user with an update to the product that may compromise the security features of the TOE.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

4.3 Organizational Security Policies

Table 3: Organizational Security Policies

Threat Name	Threat Definition
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 TOE.
P.ACCOUNTABILITY	The authorized users of the TOE shall be held accountable for their actions within the TOE.
P.ADMIN_ACCESS	Administrators shall be able to administer the TOE both locally and remotely through protected communications channels.
P.COMPATIBILITY	The TOE must meet Request for Comments (RFC) requirements for implemented protocols to facilitate inter-operation with other network equipment (e.g., certificate authority, NTP server) using the same protocols.
P.EXTERNAL_SERVERS	The TOE must support standardized (RFCs) protocols for communication with a centralized audit server and a RADIUS authentication server.

4.4 Security Objectives

The following table contains security objectives for the TOE.

Table 4: Security Objectives for the TOE

TOE Security Obj.	TOE Security Objective Definition
O.AUTH_COMM	The TOE will provide a means to ensure users are not communicating with some other entity pretending to be the TOE, and that the TOE is communicating with an authorized IT entity and not some other entity pretending to be an authorized IT entity.
O.CRYPTOGRAPHIC_FUNCTIONS	The TOE shall provide cryptographic functions (i.e., encryption/decryption and digital signature operations) to maintain the confidentiality and allow for detection of modification of TSF data that is transmitted between physically separated portions of the TOE, or stored outside the TOE.
O.DISPLAY_BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.FAIL_SECURE	The TOE shall fail in a secure manner following failure of the power-on self tests.
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.PROTOCOLS	The TOE will ensure that standardized protocols are implemented in the TOE to RFC and/or Industry specifications to ensure interoperability, that also support communication with a centralized audit server and a RADIUS authentication server.
O.REPLAY_DETECTION	The TOE will provide a means to detect and reject the replay of authentication data and other TSF data and security attributes.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.RESOURCE_AVAILABILITY	The TOE shall provide mechanisms that mitigate user attempts to exhaust TOE resources (e.g., persistent storage).
O.ROBUST_TOE_ACCESS	The TOE will provide mechanisms that control an administrator's logical access to the TOE and to control administrative access from a wireless client.
O.SESSION_LOCK	The TOE shall provide mechanisms that mitigate the risk of unattended sessions being hijacked.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and send those data to an external IT entity.
O.TIME_STAMPS	The TOE shall provide reliable time stamps and the capability for the administrator to set the time used for these timestamps.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and provide protections for logged-in administrators.
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its

TOE Security Obj.	TOE Security Objective Definition
	security functionality to ensure it is operating properly.
O.VERIFIABLE_UPDATES	The TOE will provide the capability to help ensure that any updates to the TOE can be verified by the administrator to be unaltered and (optionally) from a trusted source.
O.WIRELESS_CLIENT_ACCESS	The TOE will provide the capability to restrict a wireless client in connecting to the TOE.

The following table contains objectives for the Operational Environment.

Table 5: Security Objectives for the Operational Environment

TOE Security Obj.	TOE Security Objective Definition
OE.NO_GENERAL_PURPOSE	There are no general-purpose computing capabilities (e.g., compilers or user applications) available to the TOE, other than those services necessary for the operation, administration and support of the TOE.
OE.NO_TOE_BYPASS	Information cannot flow between external and internal networks located in different enclaves without passing through the TOE.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the IT environment.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

5 Requirements

As indicated above, requirements in the WLANASPP10 are comprised of the "base" requirements and additional requirements that are conditionally optional. The following are table contains the "base" requirements that were validated as part of the Boeing evaluation activity referenced above.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
	FAU_GEN.2: User Audit Association
	FAU_SEL.1: Selective Audit
	FAU_STG.1: Protected Audit Trail Storage (Local Storage)
	FAU_STG_EXT.1: External Audit Trail Storage
	FAU_STG_EXT.3: Action in Case of Loss of Audit Server Connectivity
FCS: Cryptographic Support	FCS_CKM.1(1): Cryptographic Key Generation (Symmetric Keys for WPA2 Connections)
	FCS_CKM.1(2): Cryptographic Key Generation (Asymmetric Keys)
	FCS_CKM.2(1): Cryptographic Key Distribution (PMK)
	FCS_CKM.2(2): Cryptographic Key Distribution (GTK)
	FCS_CKM_EXT.4: Cryptographic Key Zeroization
	FCS_COP.1(1): Cryptographic Operation (Data Encryption/Decryption)
	FCS_COP.1(2): Cryptographic Operation (Cryptographic Signature)
	FCS_COP.1(3): Cryptographic Operation (Cryptographic Hashing)

Requirement Class	Requirement Component
	FCS_COP.1(4): Cryptographic Operation (Keyed-Hash Message Authentication)
	FCS_COP.1(5): Cryptographic Operation (WPA2 Data Encryption/Decryption)
	FCS_IPSEC_EXT.1: Internet Protocol Security (IPsec) Communications
	FCS_RBG_EXT.1: Cryptographic Operation: Random Bit Generation
FDP: User Data Protection	FDP_RIP.2: Full Residual Information Protection
FIA: Identification and Authentication	FIA_AFL.1: Authentication Failure Handling
	FIA_PMG_EXT.1: Password Management
	FIA_UIA_EXT.1: User Identification and Authentication
	FIA_UAU_EXT.5: Password Based Authentication Mechanism
	FIA_UAU.6: Re-authenticating
	FIA_UAU.7: Protected Authentication Feedback
	FIA_8021X_EXT.1: 802.1X Port Access Entity (Authenticator) Authentication
	FIA_PSK_EXT.1: Pre-Shared Key Composition
	FIA_X509_EXT.1: X509 Certificates
FMT: Security Management	FMT_MOF.1: Management of Security Functions Behavior
	FMT_MTD.1(1): Management of TSF Data (General TSF Data)
	FMT_MTD.1(2): Management of TSF Data (Reading of Authentication Data)
	FMT_MTD.1(3): Management of TSF Data (Reading of Authentication Data)
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Management Roles
FPT: Protection of the TSF	FPT_FLS.1: Fail Secure
	FPT_RPL.1: Replay Detection
	FPT_STM.1: Reliable Time Stamp
	FPT_TST_EXT.1: TSF Testing
	FPT_TUD_EXT.1: Trusted Update
FRU: Resource Utilization	FRU_RSA.1: Maximum Quotas
FTA: TOE Access	FTA_SSL_EXT.1: TSF-initiated Session Locking
	FTA_SSL.3: TSF-initiated Termination
	FTA_SSL.4: User-initiated Termination
	FTA_TAB.1 Default TOE Access Banners
	FTA_TSE.1: TOE Session Establishment
FTP: Trusted Path/Channels	FTP_ITC.1: Inter-TSF Trusted Channel
	FTP_TRP.1: Trusted Path

The following table contains the optional requirements contained in Appendix C, and an indication of what evaluation those requirements were verified in (from the list in the *Identification* section above). Requirements that do not have an associated evaluation indicator have not yet been evaluated. These requirements are included in an ST if associated selections are made by the ST authors in requirements that are levied on the TOE by the ST.

Requirement Class	Requirement Component	Verified By
FAU: Security Audit	FAU_SAR.1: Audit Review	Aruba Mobility Controller and

Requirement Class	Requirement Component	Verified By
		Access Point Series, October 2014
	FAU_SAR.2: Restricted Audit Review	Aruba Mobility Controller and Access Point Series, October 2014
	FAU_STG_EXT.4: Prevention of Audit Data Loss	Fortress Mesh Point ES520, ES820, December 2014
FCS: Cryptographic Support	FCS_HTTPS_EXT.1: HTTPS	Aruba Mobility Controller and Access Point Series, October 2014
	FCS_SSH_EXT.1: Secure Shell	Aruba Mobility Controller and Access Point Series, October 2014
	FCS_TLS_EXT.1: Transport Layer Security (TLS)	Aruba Mobility Controller and Access Point Series, October 2014
FPT: Protection of the TSF	FPT_ITT.1: Basic Internal TSF Data Transfer Protection	Aruba Mobility Controller and Access Point Series, October 2014

6 Assurance Requirements

The following are the assurance requirements contained in the WLANASPP10:

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic Functional Specification
AGD: Guidance documents	AGD_OPE.1: Operational User Guidance
	AGD_PRE.1: Preparative Procedures
ALC: Life-cycle support	ALC_CMC.1: Labeling of the TOE
	ALC_CMS.1: TOE CM Coverage
ATE: Tests	ATE_IND.1: Independent Testing - Sample
AVA: Vulnerability Assessment	AVA_VAN.1: Vulnerability Survey

7 Results of the evaluation

The CCTL produced an ETR that contained the following results. Note that for APE elements and work units that are identical to APE elements and work units, the lab performed the APE work units concurrent to the ASE work units.

APE Requirement	Evaluation Verdict
APE_CCL.1	Pass
APE_ECD.1	Pass
APE_INT.1	Pass
APE_OBJ.2	Pass
APE_REQ.1	Pass

8 Glossary

The following definitions are used throughout this document:

- **Common Criteria Testing Laboratory (CCTL)**. An IT security evaluation facility accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) and approved by the CCEVS Validation Body to conduct Common Criteria-based evaluations.
- **Conformance**. The ability to demonstrate in an unambiguous way that a given implementation is correct with respect to the formal model.
- **Evaluation**. The assessment of an IT product against the Common Criteria using the Common Criteria Evaluation Methodology as interpreted by the supplemental guidance in the WLANASPP Assurance Activities to determine whether or not the claims made are justified.
- **Evaluation Evidence**. Any tangible resource (information) required from the sponsor or developer by the evaluator to perform one or more evaluation activities.
- **Feature.** Part of a product that is either included with the product or can be ordered separately.
- **Target of Evaluation (TOE)**. A group of IT products configured as an IT system, or an IT product, and associated documentation that is the subject of a security evaluation under the CC.
- **Validation**. The process carried out by the CCEVS Validation Body leading to the issue of a Common Criteria certificate.
- **Validation Body**. A governmental organization responsible for carrying out validation and for overseeing the day-to-day operation of the NIAP Common Criteria Evaluation and Validation Scheme.

9 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and General Model*, Version 3.1, Revision 2, dated: September 2007.

[2] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 2: Security Functional Requirements*, Version 3.1, Revision 2, dated: September 2007.

[3] Common Criteria Project Sponsoring Organisations. *Common Criteria for Information Technology Security Evaluation: Part 3: Security Assurance Requirements*, Version 3.1, Revision 2, dated: September 2007.

[4] Common Criteria Project Sponsoring Organisations. *Common Evaluation Methodology for Information Technology Security* – Part 2: Evaluation Methodology, Version 3.1, Revision 2, dated: September 2007.

[5] Common Criteria, Evaluation and Validation Scheme for Information Technology Security, *Guidance to Validators of IT Security Evaluations*, Scheme Publication #3, Version 1.0, January 2002.

[6] Leidos, Inc. *Aruba Mobility Controller and Access Point Series Security Target*, Version 1.0. September 29, 2014.

[7] InfoGard Laboratories, Inc. *Fortress Mesh Point ES520, ES820 Security Target*, Version 2.0. December 5, 2014.

[8] InfoGard Laboratories, Inc. *Evaluation Technical Report for Aruba Mobility Controller and Access Point Series,* Version 1.0, August 6, 2014.

[9] Protection Profile for Wireless Local Area Network (WLAN) Access Systems, Version 1.0, December 1, 2011.