National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

Protection Profile for Voice over IP (VoIP) Applications, Version 1.3, November 3, 2014

Report Number:	**CCEVS-VR-PP-0023**
Dated:	**March 9, 2016**
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
Acumen Security
Montgomery Village, MD

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 Voice over IP (VoIP) Applications, Version 1.3 (PPVoIP13). It presents a summary of the PPVoIP13 and the evaluation results.

In order to promote thoroughness and efficiency, the evaluation of the PPVoIP13 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 Cisco Jabber 11.0 for Windows. The evaluation was performed by Acumen Security, LLC Common Criteria Testing Laboratory (CCTL) in Montgomery Village, Maryland, in the United States and was completed in November 2015. This evaluation addressed the base requirements of the PPVoIP13, as well as a few of the selection-based requirements contained in Appendix C.

The information in this report is largely derived from the Assurance Activity Report (AAR), written by the Acumen Security.

The evaluation determined that the PPVoIP13 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 PPVoIP13, 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 PPVoIP13 meets the requirements of the APE components. These findings were confirmed by the VR author. The conclusions of the testing laboratory in the assurance activity 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 PPVoIP13 was performed concurrent with the first product evaluation against the PP. In this case the TOE for this first product was the Cisco Jabber 11.0 for Windows, provided by Cisco Systems, Inc. Acumen Security, LLC Common Criteria Testing Laboratory (CCTL) in Montgomery Village, Maryland, in the United States and was completed in November 2015.

The PPVoIP13 contains a set of "base" requirements that all conformant STs must include as well as "additional" requirements that are either conditional or objective, 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 additional 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 PPVoIP13 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 requirements in the PPVoIP13.

Protection Profile	*Protection Profile for Voice over IP, version 1.3, November 3, 2014*
ST (Base)	Cisco Jabber for Windows Security Target, Version 1.0, November 12, 2015
ST (Additional)	N/A
Assurance Activity Report (Base)	Cisco Jabber for Windows VOIP PP Assurance Activity Report Version 1.3 November 11, 2015
Assurance Activity Report (Additional)	N/A
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 and additional)	Acumen Security, LLC, Montgomery Village, MD USA
CCEVS Validators (base)	Sheldon Durrant, MITRE Corporation Ken Elliot, Aerospace Corporation Jerry Myers, Aerospace Corporation
CCEVS Validators (Additional)	Herb Ellis, Aerospace Corporation Kevin Kornegay, Aerospace Corporation

3 PPVoIP Description

This Protection Profile (PP) supports procurements of commercial off-the-shelf (COTS) VoIP Client Applications to provide secure tunnels to authenticated remote endpoints or servers. This PP details the policies, assumptions, threats, security objectives, security functional requirements, and security assurance requirements for the VoIP Application and its supporting environment.

The VoIP Application is intended to provide a secure tunnel to a remote VoIP Application. The tunnel provides confidentiality, integrity, and data authentication for information that travels across the public network. The VoIP Application will interact with a peer VoIP Application using the Security Real-Time Transport Protocol (SRTP) that has been established using the Session Description Protocol (SDP) and the Security Descriptions for Media Streams (SDES) for SDP. All VoIP Applications that comply with this document will support SDES-SRTP. Likewise, compliant TOEs must also protect communications between itself and the SIP Server by using a Transport Layer Security (TLS)-protected signaling channel. To register the TOE within the domain, the TOE is required to be password authenticated by the SIP Server. The TOE is required by this PP to make use of certificates to authenticate both the SIP server end and the TOE itself through the TLS connection

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 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.

Assumption Name	Assumption Definition
A.AVAILABILITY	Network resources shall be available to allow VoIP clients to satisfy mission requirements and to transmit information.
A.OPER_ENV	The operational environment of the TOE appropriately addresses those requirements, threats, and policies not applicable to the TOE itself, but that are necessary to support the correct operation of the TOE.
A.TRUSTED_CONFIG	Personnel configuring the TOE and its operational environment will follow the applicable security configuration guidance.

Table 1: Assumptions

4.2 Threats

Threat Name	Threat Definition
T.TSF_CONFIGURATION	Failure to allow configuration of the TSF may prevent its users from
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. 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
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.USER_DATA_REUSE	Voice data may be inadvertently sent to a destination not intended because it is sent outside the voice call.

Table 2: Threats

4.3 Organizational Security Policies

The VoIP PPv1.3 does not define organizational security policies.

4.4 Security Objectives

The following table contains security objectives for the TOE.

TOE Security Obj.	TOE Security Objective Definition
O.PROTCOMMS	The TOE will provide protected communication channels with authorized IT entities (SIP Server and other VoIP applications).
O.TSF_SELF_TEST	The TOE will provide the capability to test some subset of its 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.

Table 3: Security Objectives for the TOE

The following table contains objectives for the Operational Environment.

TOE Security Obj.	TOE Security Objective Definition
OE.AUTHORIZED_USER	The user of the TOE is non-hostile and follows all user guidance.
OE.OPER_ENV	The operational environment will provide a SIP infrastructure to establish a VoIP connection; a PKI to provide certificates; and an execution domain to support correct operation of the TOE.
OE.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

Table 4: Security Objectives for the Operational Environment

5 Requirements

As indicated above, requirements in the PPVoIP13 are comprised of the "base" requirements and additional requirements that are selection based. The following are table contains the "base" requirements that were validated as part of the Cisco evaluation activity referenced above.

Requirement Class	Requirement Component
Security Functional Requirements for VoIP Applications (TOE)	
FCS: Cryptographic Support	FCS_CKM_EXT.2(1): Cryptographic Key Storage
	FCS_SRTP_EXT.1: Secure Real-Time Transport Protocol (SRTP)
FDP: User Data Protection	FDP_VOP_EXT.1: Voice Over IP Data Protection
FIA: Identification and Authentication	FIA_SIPC_EXT.1: Session Initiation Protocol (SIP) Client
FMT: Security Management	FMT_SMF.1: Specification of Management Functions

FPT: Protection of the TSF	FPT_TUD_EXT.1: Extended: Trusted Update
FTP: Trusted path/channels	FTP_ITC.1(1): Inter-TSF Trusted Channel (SDES-SRTP)
Security Functional Requirements for VoIP Client Application or Client Platforms	
FCS: Cryptographic Support	FCS_CKM.1(1): Cryptographic Key Generation (Asymmetric Keys)
	FCS_CKM.1(2): Cryptographic Key Generation
	FCS_CKM_EXT.4: Cryptographic key material destruction (Key Material)
	FCS_COP.1(1): Cryptographic Operation (Data Encryption/Decryption)
	FCS_COP.1(2): Cryptographic Operation (for cryptographic signature)
	FCS_COP.1(3): Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4): Cryptographic Operation (For keyed-hash Message Authentication)
	FCS_RBG_EXT.1: Extended: Cryptographic operation (Random Bit Generation)
	FCS_TLS_EXT.1: Transport Level Security
FIA: Identification and Authentication	FIA_X509_EXT.1: Extended: X509 Certificate Validation
	FIA_X509_EXT.2: Extended: X509 Certificate Use and Management
FMT: Security management	FMT_SMF.1: Specification of Management Functions
FPT: Protection of the TSF	FPT_TST_EXT.1: Extended: TSF Self-Test
	FPT_TUD_EXT.1: Extended: Trusted Update
FTP: Trusted Path/Channels	FTP_ITC.1(2): Inter-TSF Trusted Channel (TLS/SIP)

Table 5: Base Requirements

The following table contains the additional selection-based 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
FIA: Identification and Authentication	FIA_X509_EXT.2(1) Extended: X509 Authentication	

Table 6: Selection-Based Requirements

The following table contains the objective requirements that specify security functionality that is desirable that are contained in Annex D. It is expected that these requirements will transition from objective requirements to baseline requirements in future versions of this PP.

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit Data Generation
	FAU_SEL.1: Selective Audit
FTP: Trusted Path/Channel	FTP_ALT_EXT.1: Extended: Trusted Channel Alert

Table 7: Objective Requirements

6 Assurance Requirements

The following are the assurance requirements contained in the PPVoIP13:

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

Table 8: Assurance Requirements

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

Table 9: Evaluation Results

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 PPVoIP13 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 Organizations. *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 Organizations. *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 Organizations. *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 Organizations. *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] *Cisco Jabber for Windows Security Target*, Version 1.0, November 12, 2015

[7] Acumen Security LLC, *Validation Report for the Cisco Jabber for Windows* Version 1.0 November 13, 2015

[8] Acumen Security LLC, *Cisco Jabber for Windows VOIP PP Assurance Activity Report* Version 1.3 November 11, 2015

[9] Protection Profile for Voice over IP, version 1.3, November 3, 2014