Low Assurance Protection Profile for a VoIP Infrastructure

Version	1.1
Date	March 14th, 2005
Author(s)	Dirk-Jan Out

Certification ID	BSI-PP-0012
Sponsor	TNO-ITSEF BV
File name	VoIP Low Assurance Protection Profile 1.1 with
No of pages	12

Document information

Date of issue	March 14th, 2005
Author(s)	Dirk-Jan Out
Version number report	1.1
Certification ID	BSI-PP-0012
Scheme	BSI
Sponsor	TNO-ITSEF BV
Sponsor address	Delftechpark 1 2628 XJ Delft The Netherlands
PP Evaluation Lab	SRC
PP Evaluation Lab address	Graurheindorferstrasse 149a D-53117 Bonn Germany
Project leader	Rob Hunter
Target of Evaluation (TOE)	VoIP Infrastructure
TOE reference name	VoIP Infrastructure
CC-EAL number	1
Classification	
Report title	Low Assurance Protection Profile for a VoIP Infrastructure
Report reference name	PP-VoIP Infrastructure-1.1

Document history

Version	Date	Comment
0.1	16-Jul-04	Initial version
0.2	12 Aug 04	Processed comments from Cisco and BSI
0.3	27 Aug 04	Processed further comments from Cisco and BSI
1.0	3-Sep-04	Processed SRC evaluation comments
1.1	14-Mar-05	Processed BSI evaluation comments

1. PP Introduction

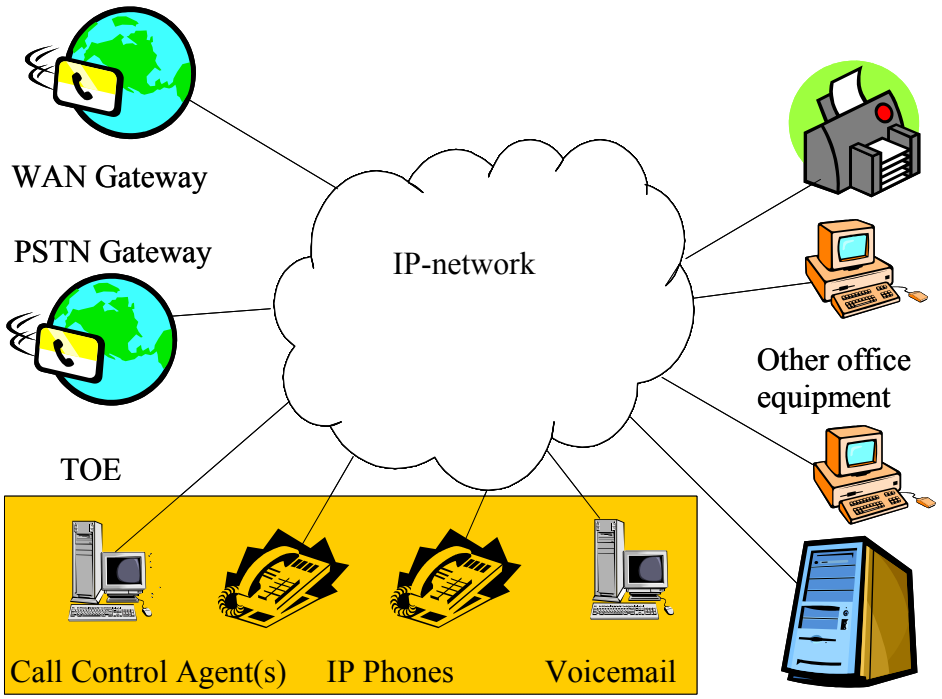
1.1 PP Reference

This is the Low Assurance Protection Profile for a
VoIP Infrastructure,1.1, TNO-ITSEF BV, March 14th, 2005

1.2 TOE overview

The TOE is a VoIP (Voice over IP) infrastructure, as it is used in a typical office environment. The goal of this VoIP infrastructure is to provide telephone and services over an already available IP network thereby obviating the need for a separate telephone infrastructure and allowing the integration between telephony services and other services (e.g. agenda services).
IP telephony enables calls to be made between IP telephone devices and between an IP telephone device and a traditional telephone on a PSTN (Publicly Switched Telephone Network).

A typical[1] IP-network with a typical VoIP infrastructure is depicted below:



[1] Note that this is just a schematic view and not indicative of size: the IP-network may range from one to a few thousand phones, PCs, servers and other pieces of equipment. Additionally, the IP-network may itself consist of multiple connected IP networks or the IP-network may consist of a single telephone connected to a router connected to a WAN.

This picture shows the following elements:

- An *IP-network*: a network connecting all the other IP elements
- A *number of IP telephone devices:* This refers to any device that supports placing calls in an IP network. IP Telephone devices are included as well as applications installed on user systems with speakers and microphones. IP Telephone devices may offer so-called IP-phone services such as user directory lookups and Internet access for stock quotes;
- A *Call Control Agent*: a central entity that provides call control and configuration management for IP telephony devices. This device provides the core functionality to provide call setup, and route calls throughout the network to other voice devices including voice gateways and voice-mail systems
- *Voicemail system*: provides IP-based voice-mail storage and services such as user directory lookup and call forwarding.
- *PSTN gateway:* A gateway between the IP-network and a PSTN providing access to legacy voice systems
- *WAN gateway*: A gateway between the IP-network and a IP-based WAN.
- *Other office IT equipment* (printers, servers, computers etc.) that are connected to the IP-network.

The TOE consists of the Call Control Agent, the Voice Mail system and the IP Telephone devices[2]. All other depicted elements are not part of the TOE.

The TOE offers the following functionality:

- Making telephone calls from/to other telephones in the TOE
- Making telephone calls from/to other telephones not in the TOE
- Able to restrict calls to certain numbers and to change these restrictions
- Logging connection information of phone calls
- Storage and secure retrieval of voice mail

The TOE requires a connection to an IP-based network[3] to function. It does not require further non-TOE hardware/firmware/software.

[2] Other configurations are allowed (e.g having the Voice Mail system integrated with the Call Control Agent).

[3] See footnote 1 for an explanation of the term IP-Network in this PP.

2. Conformance claims

2.1 Conformance claim

This Protection Profile:

- claims conformance to CC version 2.4 release 256 and v2.4Draft Interpretation[4] #1-#17
- is CC Part 2 conformant and CC Part 3 conformant.
- does not claim conformance to any other PP.
- is EAL 1 conformant

2.2 Conformance claim rationale

PP-related conformance claim rationale
This PP does not claim conformance to another PP, so there is no rationale related to this.

Package-related conformance claim rationale
This PP is EAL1 conformant. The EAL1 package contains no uncompleted operations. As no SARs were added to EAL1, the SARs in this PP are consistent with EAL1.

2.3 Conformance statement

Security targets or other PPs wishing to claim conformance to this PP can do so as *strict-PP-conformance*. Demonstrable-PP-conformance is not allowed for this PP.

[4] V2.4 Draft Interpretation #n are interpretations that are made during the v2.4 Trial Period. They address problems with CC v2.4 as they occur.

3. Definition of terms

3.1 Definition of subjects, information and operations

This section is added to define the terms that are used in the Security Objectives of the Operational Environment and SFRs.

3.2 Subjects

S.USER	A human that uses S.IN_PHONE
S.ADMIN	A human that administers the TOE
S.PHONE	S.IN_PHONE or S.OUT_PHONE
S.IN_PHONE	A VoIP telephone that is part of the TOE Attribute: telephone_number
S.OUT_PHONE	A phone (VoIP or otherwise) that is not part of the TOE Attribute: telephone_number

3.3 Operations

The operations that are performed by the TOE are:

R.CONNECT	S.PHONE connecting to another S.PHONE
R.GET_VMAIL	S.USER retrieving voicemail from the TOE
R.DEL_VMAIL	S.USER deleting voicemail from the TOE

3.4 Objects

D.ALLOWLIST	TSF data: a relation representing the allowed connections between devices

4. Security Objectives for the Operational Environment

The operational environment of the TOE shall conform to the following objectives:

OE.PHONE_LOCATION	The operational environment of the VoIP phones shall be a general office-type environment: physical access is restricted to office personnel, visitors and the like.
OE.AGENT_LOCATION	The operational environment of the Call Control Agent and the Voice Mail System shall be a general server room environment: physical access will be restricted to authorised administrative personnel.
OE.NETWORK	The Operational Environment shall contain an IP-network[5].
OE.NW_FEATURES	If required[6], the IP-Network shall ensure that: • VoIP traffic will not be able to monopolise the IP-Network to the point that other network traffic is hindered; • Other network traffic will not be able to monopolise the IP-Network to the point that VoIP traffic is hindered; • VoIP traffic will not be able to connect to some (or all) office equipment

[5] See footnote 1 for an explanation of the term IP-Network in this PP.

[6] This objective is of an optional nature. It has been included to:

1) assist ST authors in formulating their security objectives for the operational environment
2) ensure that it is clear that if this functionality is required, it should be provided by the network and not by the TOE.

5. Security Requirements

5.1 Extended components definition

As this PP does not contain extended security requirements, there are no extended components.

5.2 SFRs

Application Note: This PP only models telephony and voice mail. If a given VoIP solution allows other services than these two, it is the intention that this is modelled through the addition of other operations and ACC/ACF/MSA/MTD requirements.

The SFRs are grouped for easy understanding:

- Restricting access to certain telephone numbers
- Storing and retrieving voicemail
- Managing telephones
- Identifying users
- Logging and auditing
- Self-protection

5.2.1 Restricting access to certain telephone numbers

Informal Explanation (informative)

- *For each VoIP phone there is a list of "forbidden numbers" (e.g. 1-900 numbers, international numbers)which they cannot call. This list may be empty.*
- *A VoIP phone cannot call numbers on this list*
- *Only the admin may change this list*

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **Connect_Policy**[7] on **[[S.PHONE, D.ALLOW_LIST, R.CONNECT].**

FDP_ACF.1 Security attribute based access control[8]

FDP_ACF.1.1 The TSF shall enforce the **ConnectPolicy** to objects based on the following: **[S.PHONE/telephone_number, D.ALLOW_LIST]**

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

S.IN_PHONE may R.CONNECT to S.PHONE if: [S.IN_PHONE/telephone_number, S.PHONE/telephone_number] is in D.ALLOW_LIST;

Application Note: The word ALLOW_LIST does not mean that only "white-list" approaches are allowed. Both implementations based on "Deny all except what is listed" and "Allow all except what is specifically listed" are acceptable.

FMT_MTD.1 Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to **modify** the **D.ALLOW_LIST** to **S.ADMIN**.

[7] The SFP Connect_Policy is defined by FDP_ACC.1, FDP_ACF.1 and FMT_MSA.1 and supported by all other SFRs.

[8] The third and fourth element were completed with "None" and subsequently refined away.

5.2.2 Voice mail

Informal Explanation (informative)

- *Users have to authenticate themselves to be able to retrieve and/or delete their voicemail*
- *Unless explicitly specified otherwise, they can do other actions without authenticating themselves*

FIA_UAU.1 Timing of authentication

FIA_UAU.1.1 The TSF shall allow **all actions except R.GET_VMAIL, R.DEL_VMAIL, [assignment: other actions]** on behalf of **S.USER** to be performed before **S.USER** is authenticated.

FIA_UAU.1.2 The TSF shall require **S.USER** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of **S.USER**.

5.2.3 Managing telephones

Informal Explanation (informative)

- *Only the administrator can change the telephone number of a VoIP telephone*
- *The SFR is limited to S.IN_PHONE: the TOE can change only telephone numbers of telephones that are part of the TOE.*

FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **ConnectPolicy** to restrict the ability to **modify** the security attributes **S.IN_PHONE/ telephone_number** to **S.ADMIN.**

FIA_UAU.2 User authentication before any action

FIA_UAU.12.12 The TSF shall require **S.ADMIN** to be successfully authenticated before allowing any other **actions related to the other SFRs** on behalf of **S.ADMIN**.

5.2.4 Identifying users

FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles

- **S.USER**
- **S.ADMIN**

FMT_SMR.1.2 The TSF shall be able to associate users with roles

FIA_UID.2 User identification before any action

FIA_UID.2.1 The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.

Application Note: A possible method for identification may be the part of the TOE with which users interact. S.USER will interact with S.PHONE while S.ADMIN will interact with the Call Control Agent.

5.2.5 Logging and auditing

FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;

b) All auditable events for the **not specified** level of audit; and

c) **[Registration of a new S.IN_PHONE,**
[assignment: details of calls made by S.IN_PHONE],
modification of the configuration of S.IN_PHONE,
failed authentication events,
[assignment: other specifically defined auditable events]].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: *other audit relevant information*]

Application Note: This PP does not prescribe what is actually done with the generated audit data. The ST author should add FAU_SAR, FAU_SAA and/or FAU_ARP requirements where necessary to describe his specific solution.

5.2.6 Self-protection

Informal Explanation (informative)

- *It is not possible to logically modify the TOE such that it no longer meets the other requirements*

FPT_SEP.1 TSF domain separation

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.3 SARs

The SARs for this PP are the package EAL 1 with one refinement in AGD_USR.1.3:

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment. **This shall include any and all means in which S.IN_PHONE can be used to eavesdrop on S.USER by e.g.:**

- **The microphone being on**
- **A call being turned into a conference call**