Chapter 1 Introduction

This section identifies the PP-Module as well as the Base PP and provides a Module overview for potential users.

1.1 PP Module Reference

Title: MILS Platform Protection Profile Network Interface Partitioning Module
Sponsor: certMILS Consortium
CC Version: 3.1 (Revision 5)
Assurance Level: see the Base PP.
Version: draft
Keywords: Base-PP, PP-module, Operating System, Separation Kernel, MILS

1.2 Base PP Identification

Base MILS Platform Protection Profile, Version: 1.0

1.3 PP Module Overview

This PP module describes a driver for the partitioning of network interfaces. The function of partitioning of a network interfaces in general is to share a network interface among applications. Sharing can mean that individual applications have exclusive access to some resources of the network interface in the form of a virtual network interface card (VNIC). In a MILS system, access to virtual network interface cards is configured using the partition abstraction.

Partitioning of network cards can optionally be supported via network cards that have virtualization support in hardware. An overview of hardware support for network card virtualization is given in [WIDRB13].

The object of evaluation for this module is a driver that provides the function of partitioning a network card. The use of hardware support is up to the driver implementation: such hardware support for virtualization is not needed when the driver does the abstraction of virtual network interfaces entirely in software. That is, this module can be used both for drivers that use hardware with additional support for virtualization or not.

Chapter 2 Consistency Rationale

This section states the correspondence between the PP-Module and its Base-PP.

2.1 TOE type consistency

The TOE type for which both the Base PP and this PP Module are designed is “a special kind of operating system, namely an SK.”

An SK is a special kind of operating system that allows to effectively separate different containers called “partitions” from each other. Applications themselves are hosted in those partitions. They can also be entire operating systems. The SK is installed and runs on a hardware platform (e.g. embedded systems, desktop class hardware).

The PP module extends the base PP by specifying a software-implemented mechanism to partition a network card. In addition to the System Security Policy (SSP) in the base PP, this module adds a support for the evaluation of a partitioning network driver that is configured by the integrator.

2.2 Security Problem Definition consistency

2.2.1 Assets

The section 3.1 of the Base PP describes the assets to be protected:

- Memory
- CPU time

This PP Module adds the following asset:

- Network device

The new asset is independent and compatible with the assets defined in the Base PP as it does not interfere with the protection of the **Memory** or **CPU time**. It adds protection to network devices.

2.2.2 Threats

The section 3.2 of the Base PP describes the threats contemplated:

- T.DISCLOSURE
- T.MODIFICATION
- T.DEPLETION

This PP Module contemplates the following additional threats:

- T.NET_DISCLOSURE
- T.NET_MODIFICATION

The threat T.NET_DISCLOSURE bring specific compatible scenarios associated to T.DISCLOSURE associated to the confidentiality protection of network traffic.

The threat T.NET_MODIFICATION bring specific compatible scenarios associated to T.MODIFICATION associated to the integrity protection of network traffic.

2.2.3 Organizational Security Policies

Neither the Base PP nor this PP Module define organizational security policies.

2.2.4 Assumptions

This PP Module defines the following additional assumptions:

- A.NET

This additional assumption is compatible with the assumptions defined in section 3.4 of the Base PP. The assumptions included in the Base PP are applicable with no changes.

2.3 Security Objectives consistency

The section 4.1 of the Base PP describes the security objectives to be implemented:

- OT.CONFIDENTIALITY
- OT.INTEGRITY
- OT.AVAILABILITY

This PP Module adds the following security objectives for the TOE:

- OT.NET_CONFIDENTIALITY
- OT.NET_INTEGRITY

These security objectives add security functionality to the TOE regarding the confidentiality and integrity protection of network traffic, which is compatible to the rest of security objectives for the TOE defined in the Base PP.

2.4 Security Functional Requirements consistency

In addition to the set of SFRs included in section 6.1 of the Base PP, this PP Module defines:

- FDP_ACC.2/NET Complete Access Control – Access to Virtual Network Interfaces – This SFR is compatible with the set of SFRs defined in the Base PP as it adds an independent access control policy to network interfaces.
- FDP_ACF.1/NET Security Attribute Based Access Control – Access to Virtual Network Interfaces – This SFR is compatible with the set of SFRs defined in the Base PP as it adds an independent access control policy to network interfaces.
- FMT_MSA.1 Management of Security Attributes – This SFR is compatible with the set of SFRs defined in the Base PP as it adds independent and specific functionality for managing the security attributes of the new access control policy. This SFR must be iterated when used with the Base PP.
- FMT_MSA.3 Static attribute initialisation This SFR is compatible with the set of SFRs defined in the Base PP as it adds independent and specific functionality for initialising the security attributes of the new access control policy. This SFR must be iterated when used with the Base PP.

The SFR FMT_SMF.1 of the Base PP must include the management functionality associated to the new access control policy defined in this PP Module.

Chapter 3 Conformance claim

This protection profile module claims conformance to

- Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 5. April 2017. CCMB-2017-04-001 [1]
- Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-002 [2]
- Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-003 [3]

as follows

- Part 2 conformant,

The "Common Methodology for Information Technology Security Evaluation, Evaluation Methodology; Version 3.1, Revision 5, April 2017. CCMB-2017-04-004, [4]" has to be taken into account.

This protection profile module is associated with the Base MILS Platform Protection Profile Version 1.0.

3.1 Conformance Rationale

Since a PP module cannot claim conformance to any protection profile, this section is not applicable.

3.2 Conformance Statement

This Protection Profile Module requires strict conformance of any ST or PP claiming conformance to this PP Module.

Note: claiming conformance to this PP Module also requires claiming conformance to the Base MILS Platform Protection Profile.

Chapter 4 Security Problem Definition

This section describes the security aspects of the environment in which the TOE claiming conformance with the PP will be used and the manner in which the TOE is expected to be employed. It provides the statement of the TOE security environment, which identifies and explains all:

- Known and presumed threats countered by either the TOE or by the security environment.
- Organizational security policies with which the TOE must comply.
- Assumptions about the secure usage of the TOE.
-

4.1 Assets

Asset Name	Description	Security Properties to be Preserved
Network device (AS.NET)	Network device, which connects one or several partitions to an external network.	confidentiality, integrity

Table 1: Assets

4.2 Threats

Assets are defined in Table 1 in Section 4.1. The attackers are the defined in the Base PP.

T.NET_DISCLOSURE

An attacker reads network traffic from a VNIC it is not authorized to write to according to the configuration by the integrator.

T.NET_MODIFICATION

An attacker writes network traffic to a VNIC it is not authorized to write to according to the configuration by the integrator.

4.3 Organizational Security Policies

This module defines no organizational security policies.

4.4 Assumptions

The assumptions are the same as in the base PP, plus:

A.NET

The integrator does not use the access control policy to the network card to enable communication between partitions to bypass the SSP.

Chapter 5 Security Objectives

Security objectives are concise, abstract statements of the intended solution to the problem defined by the security problem definition (see previous section). The set of security objectives for a TOE form a high-level solution to the security problem. This high-level solution is divided into two part-wise solutions: the security objectives for the TOE, and the security objectives for the TOE's operational environment.

This section presents the solution to the security problem in terms of objectives for the TOE and its operational environment.

5.1 Security Objectives for the TOE

OT.NET_CONFIDENTIALITY

For each asset, the TOE shall preserve its confidentiality according to Table 1 and the configuration by the integrator.

OT.NET_INTEGRITY

For each asset, the TOE shall preserve its integrity according to Table 1 and the configuration by the integrator.

5.2 Security Objectives for the Operational Environment

The security objectives for the operational environment are the same as for the base PP, plus:

OE.NET

The integrator does not use the access control policy to the network card to enable communication between partitions to bypass the SSP.

5.3 Security Objectives Rationale

	OT.NET_CONFIDENTIALITY	OT.NET_INTEGRITY	OE.NET
T.NET_DISCLOSURE	X		
T. NET_MODIFICATION		X	
A.NET			X

Table 2: Security Objectives Rationale

T.NET_DISCLOSURE

If the security objective OT.NET_CONFIDENTIALITY has been reached, the threat T.NET_DISCLOSURE is completely eliminated.

T.NET_MODIFICATION

If the security objective OT.NET_INTEGRITY has been reached, the threat T.NET_MODIFICATION is completely eliminated.

A.NET

OE.NET directly upholds A.NET.

Chapter 6 Extended Components Definition

This module does not define any extended component.

Chapter 7 Security Requirements

This section defines the Security Functional requirements (SFRs) in relationship with the set of TOE security objectives in the PP-Module and with the security functional requirements of the Base-PP. This PP Module does not introduce specific assurance requirements. The assurance requirements are defined by the Base MILS Platform Protection Profile.

7.1 Security Functional Requirements

7.1.1 FDP_ACC.2/NET Complete Access Control – Access to Virtual Network Interfaces

FDP_ACC.2.1/NET: The TSF shall enforce the [**network device access control policy**] on [**subjects: devices, objects: virtual network interfaces**] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/NET: The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

7.1.2 FDP_ACF.1/NET Security Attribute Based Access Control – Access to Virtual Network Interfaces

FDP_ACF.1.1/NET: The TSF shall enforce the [**network device access control policy**] to objects based on the following: [**subjects: partitions, objects: virtual network interfaces, security attributes: partition ID, attributes defined for the virtual network interface**].

FDP_ACF.1.2/NET: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: set of rules that the TSF uses to decide if a partition is allowed to access a virtual network interface].

FDP_ACF.1.3/NET: The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [**none**].

FDP_ACF.1.4/NET: The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].

7.1.3 FMT_MSA.1 Management of Security Attributes

FMT_MSA.1.1 The TSF shall enforce the [**network device access control policy**] to restrict the ability to [selection: change_default, query, modify, delete, [assignment: other operations]] the security attributes [assignment: list of security attributes] to [assignment: the authorised entity].

7.1.4 FMT_MSA.3 Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [**network device access control policy**] to provide [selection: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**programs executing with the processor privileges required to program the VNIC**] to specify alternative initial values to override the default values when *a VNIC is assigned to a partition*.

Application note: in some systems access to the VNIC may be configured statically upon system initialization and the TSF will not change this configuration. This still satisfies FMT_MSA.3.2. In the case where the VNIC is configured dynamically, an additional SFR should be added defining the conditions that need to be satisfied for such a dynamic reconfiguration.

7.2 Security Requirements Rationale

	OT.NET_CONFIDENTIALITY	OT.NET_INTEGRITY
FDP_ACC.2/NET	X	X
FDP_ACF.1/NET	X	X
FMT_MSA.1	X	X
FMT_MSA.3	X	X

Table 3: SFR Rationale

OT.NET_CONFIDENTIALITY

The SFRs FDP_ACC.2/NET and FDP_ACF.1/NET ensure that non-privileged executables can only access the network (AS.NET) according to the configuration by the integrator. FMT_MSA.1 and FMT_MSA.3 contribute to the objective fulfilment by managing the security attributes of the network device access control policy.

OT.NET_INTEGRITY

The SFRs FDP_ACC.2/NET and FDP_ACF.1/NET ensure that non-privileged executables can only access the network (AS.NET) according to the configuration by the integrator. FMT_MSA.1 and FMT_MSA.3 contribute to the objective fulfilment by managing the security attributes of the network device access control policy.

7.3 Security Functional Requirements Dependencies Analysis

The following dependencies are defined for the SFRs used in this PP Module:

SFR	**Dependencies**	**Satisfied?**
FDP_ACC.2/NET	FDP_ACF.1	yes (FDP_ACF.1/NET)
FDP_ACF.1/NET	FDP_ACC.1	yes (FDP_ACC.2/NET)
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	yes N – The TOE does not implement roles. The entities accessing the resources are trusted partitions that do not play different roles in the access to such

SFR	Dependencies	Satisfied?
		resources.
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	yes (FDP_ACC.2/NET) N – The TOE does not implement roles. The entities accessing the resources are trusted partitions that do not play different roles in the access to such resources. Base PP

Table 4: SFR Functional Requirements Dependencies Analysis

Chapter 8 Application Notes

Hardware support for network card virtualization is not required for the driver in this module. However, such hardware support can optionally be used where available.

A possible instantiation for FDP_ACF.1.2/NET could be “The operation of accessing virtual network interfaces is allowed by partitioning network driver if and only if it is allowed by the integrator in the configuration.”

In some cases, an ST could like to make statements on network bandwidth, using network quotas or priority-based Ethernet [Qbv]. Network quotas are not in scope of this module. Nonetheless, an ST author could additionally state such properties it in the ST if desired.

Chapter 9 List of Abbreviations

Abbreviation	Translation
MILS	Multiple Independent Levels of Safety / Security
PP	Protection Profile
SSP	System Security Policy
SK	Separation Kernel
TOE	Target of Evaluation
TSF	TOE Security Functionality
VNIC	Virtual Network Interface Card

Chapter 10 Bibliography

[1] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 5. April 2017. CCMB-2017-04-001

[2] Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-002

[3] Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-003

[4] Common Criteria for Information Technology Security Evaluation. Evaluation Methodology. Version 3.1, Revision 5. April 2017. CCMB-2017-04-004

[Qbv] “IEEE 802.1: 802.1Qbv - Enhancements for Scheduled Traffic.” Accessed March 1, 2018. http://www.ieee802.org/1/pages/802.1bv.html.

[WIDRB13] Wang, Anjing, Mohan Iyer, Rudra Dutta, George N. Rouskas, and Ilia Baldine. “Network Virtualization: Technologies, Perspectives, and Frontiers.” Journal of Lightwave Technology 31, no. 4 (February 2013): 523–37. https://doi.org/10.1109/JLT.2012.2213796.