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 I/O MMU 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 defines the minimum functionality for an I/O MMU driver that a TOE compliant with the Base MILS Platform Protection Profile has to provide. While this module is about a piece of software (the driver), we will first depict how an I/O MMU is used with an SK.

1.3.1 Use of an I/O MMU with an SK

Figure 1 depicts a configuration of an I/O MMU with an SK.

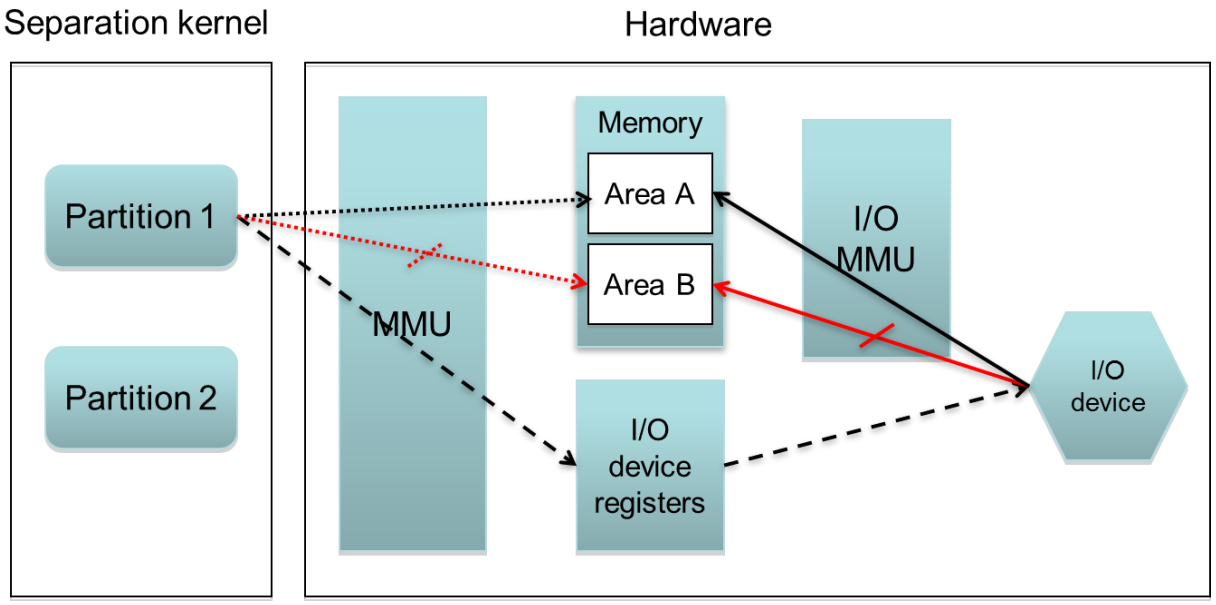

Figure 1: Configuration of an I/O MMU with an SK

In this example,

- the integrator has configured the MMU so that Partition 1 can access Area A (black dotted arrow) but not Area B (red crossed dotted arrow)
- the integrator has configured the MMU so that Partition 1 can access the I/O device (hexagon on the right) via the I/O device registers (dashed arrows)
- the integrator has configured the I/O MMU so that the I/O device can access Area A (black straight arrow) but not Area B (red straight dotted arrow) via DMA operations

If the I/O device had not been blocked access to Area B via the I/O MMU (the last configuration step above) then Partition 1 could have used the I/O device to bypass the MMU.

1.3.2 What this I/O MMU PP Module covers

This PP module assumes that an I/O MMU is provided (see A.HARDWARE_IOMMU). The I/O MMU driver configures the I/O MMU from a privileged CPU mode. The policies enforced by the I/O MMU driver are part of the SSP. During TOE run time, these policies are represented as access controls used by the I/O MMU.

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 PP by specifying a software-implemented mechanism to control an I/O MMU (Input/Output Memory Management Unit), thus adding access control on devices to access memory via DMA. A properly configured I/O MMU can ensure that a partition that has access to a DMA-capable device cannot use the device’s DMA capability to bypass their allocation of memory by the (traditional) MMU (Memory Management Unit).

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 does not add any asset.

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.IO_DISCLOSURE
- T.IO_MODIFICATION

The threat T.IO_DISCLOSURE bring specific compatible scenarios associated to T.DISCLOSURE associated to the confidentiality protection of memory from DMA operations originating from I/O devices.

The threat T.IO_MODIFICATION bring specific compatible scenarios associated to T.MODIFICATION associated to the integrity protection of memory from DMA operations originating from I/O devices.

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.HARDWARE_IOMMU

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.IO_CONFIDENTIALITY
- OT.IO_INTEGRITY

These security objectives add security functionality to the TOE regarding the confidentiality and integrity protection of I/O memory, 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/IOMMU Complete Access Control – Access control by I/O MMU – This SFR is compatible with the set of SFRs defined in the Base PP as it adds an independent access control policy to I/O memory.
- FDP_ACF.1/IOMMU Security Attribute Based Access Control – Access control by I/O MMU – This SFR is compatible with the set of SFRs defined in the Base PP as it adds an independent access control policy to I/O memory.
- 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 CC 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 Module 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
Memory (AS.MEM)	RAM or ROM memory, memory mapped I/O, and port mapped I/O assigned to a partition by the integrator. This asset is the same asset as AS.MEM in the base PP.	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.

Application note: The attacker is an untrusted subject in a partition that uses I/O functionality in an attempt to either read data from memory areas not assigned to the partition or to write to memory areas not assigned to the partition.

T.IO_DISCLOSURE

An attacker in partition that uses I/O functionality attempts to read data from a memory area not assigned to the partition.

T.IO_MODIFICATION

An attacker in partition that uses I/O functionality attempts to write data to a memory area not assigned to the partition.

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.HARDWARE_IOMMU:

The hardware shall have an I/O MMU, which is capable of restricting DMA accesses of drivers to certain memory regions. The I/O MMU shall only be configurable from a privileged CPU mode, thus, it can only be configurable through the TOE to configure the policies specifying these access restrictions. These policies are part of the SSP. During TOE run time, these policies are represented as access controls used by the I/O MMU.

Chapter 5 Security Objectives

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.IO_CONFIDENTIALITY

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

OT.IO_INTEGRITY

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

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.HARDWARE_IOMMU

The hardware shall have an I/O MMU, which is capable of restricting DMA accesses of drivers to certain memory regions. The I/O MMU shall only be configurable from a privileged CPU mode, thus, it can only be configurable through the TOE to configure the policies specifying these access restrictions. These policies are part of the SSP. During TOE run time, these policies are represented as access controls used by the I/O MMU.

5.3 Security Objectives Rationale

	OT. IO_CONFIIDENTIALITY	OT. IO_INTEGRITY	OE.HARDWARE_IOMMU
T.IO_DISCLOSURE	X		
T. IO_MODIFICATION		X	
A.HARDWARE_IOMMU			X

Table 2: Security Objectives Rationale

T.IO_DISCLOSURE

If the security objective OT.IO_CONFIDENTIALITY has been reached, the threat T.IO_DISCLOSURE is completely eliminated.

T.IO_MODIFICATION

If the security objective OT.IO_INTEGRITY has been reached, the threat T.IO_MODIFICATION is completely eliminated.

A.HARDWARE_IOMMU

A.HARDWARE_IOMMU is directly upheld by OE.HARDWARE_IOMMU.

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/IOMMU Complete Access Control – Access control by I/O MMU

FDP_ACC.2.1/IOMMU: The TSF shall enforce the [**I/O MMU access control policy**] on [**subjects: devices, objects: memory**] and all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2/IOMMU: 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/IOMMU Security Attribute Based Access Control – Access control by I/O MMU

FDP_ACF.1.1/IOMMU: The TSF shall enforce the [**I/O MMU access control policy**] to objects based on the following: [**subjects: devices, objects: memory areas, security attributes: device ID, attributes defined for the memory area**].

FDP_ACF.1.2/IOMMU: The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [assignment: list of rules for accessing memory by the I/O MMU].

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

FDP_ACF.1.4/IOMMU: 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 [**I/O MMU 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 [**I/O MMU 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 I/O MMU**] to specify alternative initial values to override the default values when *a device is assigned to a partition*.

Application note: in some systems the I/O MMU 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 I/O MMU 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.IO_CONFIDENTIALITY	OT.IO_INTEGRITY
FDP_ACC.2/IOMMU	X	X
FDP_ACF.1/IOMMU	X	X
FMT_MSA.1	X	X
FMT_MSA.3	X	X

Table 3: SFR Rationale

OT.IO_CONFIDENTIALITY

The SFRs FDP_ACC.2/IOMMU and FDP_ACF.1/IOMMU ensure that non-privileged executables can only access memory (AS.MEM) according to the SSP. FMT_MSA.1 and FMT_MSA.3 contribute to the objective fulfilment by managing the security attributes of the I/O MMU access control policy.

OT.IO_INTEGRITY

The SFRs FDP_ACC.2/IOMMU and FDP_ACF.1/IOMMU ensure that non-privileged executables can only access memory (AS.MEM) according to the SSP. FMT_MSA.1 and FMT_MSA.3 contribute to the objective fulfilment by managing the security attributes of the I/O MMU 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/IOMMU	FDP_ACF.1	yes (FDP_ACF.1/IOMMU)
FDP_ACF.1/IOMMU	FDP_ACC.1	yes (FDP_ACC.2/IOMMU)
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 resources.

FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1]	yes (FDP_ACC.2/IOMMU)
	FMT_SMR.1	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.
	FMT_SMF.1	Base PP

Table 4: SFR Functional Requirements Dependencies Analysis

Chapter 8 Application Notes

A meaningful instantiation for the list of rules for accessing memory by the I/O MMU could also be that it is fully configurable: e.g. “The operation of accessing memory is allowed by the I/O MMU if and only if it is allowed when configured by the integrator.”

Chapter 9 List of Abbreviations

Abbreviation	Translation
DMA	Direct Memory Access
I/O	Input/Output
I/O MMU	Input/Output Memory Management Unit
MILS	Multiple Independent Levels of Safety / Security
MMU	Memory Management Unit
PP	Protection Profile
SK	Separation Kernel
SSP	System Security Policy
TOE	Target of Evaluation

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