Secure Partition Manager
Update
Initial Investigation

An Implementation Update

Ken Liu
Mar 18
Backgrounds

- NS RTOS wants to reduce the impact on NS interrupt handling.

- The FF-M updated to 1.1 version supports simpler smaller system.
  - Secure Function Model (SFN).

- SPM needs to be updated to address the two main requirements above.
The NS Interrupt Handling Latency

Time Line & Priority Level

X < 255
NS - IRQ

0
S - Handler

256
SP

Latency

ISR

IRQ Trigger
Existing Execution Timeline and Expected Timeline

Long non-preemptable execution

Reduce the non-preemptable execution

Move tasks into thread mode.
How many privileged thread instance are needed?

If there is ONE NS thread is supported, only ONE is enough:
- Privileged thread has highest software priority (it would get run first if it is there).
- HW priority is still 256 to be preempted by interrupt routine.
How many privileged thread instance are needed?

If there are $N$ NS entities, $N$ is enough:
- Privileged thread has highest software priority (it would get run first if it is there).
- HW priority is still 256 to be preempted by interrupt routine.

Reason:
- Secure firmware execution is typically triggered by NS (NS is the initial user!).

Still want to remove the reset ‘Handler’ execution? Check Secure Function Model.
Secure Functions

service1() { return \texttt{CALL\_WITH\_SP}(\texttt{psa\_call}, \texttt{sp1}); }  
service1() { return \texttt{SVCALL\_WITH\_SP}(\texttt{psa\_call}, \texttt{sp3}); }  
service2() { /* Use caller stack. */ }
Design Goal

1 and 2 can be provided by the implementation individually.
SPM Internal Modules – Call Routine

From Clients

Inter-Process Communication Model Scope

SERVICE MAPPING & MEM/PERMISSION CHECK

Service Mapping & Mem/Permission Check

Thread Management

Handle Mgmt

Primitives (atomic/C.S.)

HAL

IPC Service

Thread Management

Context Mgr

SFN Service Context Management

To SFN Service

To IPC Partition

Arch

API

HAL

SPM Internal Modules

FFM API Interface

Arch

From Clients
SPM Internal Modules – Software Modulization

- SFN Service Context Management
- Handle Mgmt
- Primitives (atomic/C.S.)
- IPC Service Thread Management
- Context Mgr
- HAL
- Thread API

FF-M and Supporting
• There is no secure boundaries under Isolation Level 1, so all plain function call is possible.
• This is for SFN model. IPC model scheduling needs to deal with interrupt cases, which means PendSV can’t be avoided.
• Use SVC to cross isolation boundary.
• Not mandatory to create boundaries inside PRoT domain; but it is a plus if it does.
SPM Internal Modules – Extra Components

- FFM API Interface
- Service Mapping & Mem/Permission Check
- Secure Context
- Handle Mgmt
- Primitives (atomic/C.S.)
- Secure Inter-Process Communication Model Scope
- IPC Service
- Thread Management
- Context Mgr
- Thread API
- HAL
- IRQ
- Exit

Inter-Process Communication Model Scope

Secure Function Model Scope

Non-Secure Client Agent

To IPC Partition
IPC Isolation Levels – Theoretic Timeline

Isolation Level 1 Timeline

- 1 - 255: S - IRQ
- 255: S - PendSV
- 256*: SPM
- 256: SP

Isolation Level 2/3 Timeline

- 0: S - SVC
- 1 - 255: S - IRQ
- 255: S - PendSV
- 256*: SPM
- 256: SP
IPC vs SFN Theoretic Timeline

**IPC Isolation Level 1**

1 - 255

- S - IRQ

255

- S - PendSV

256*

- SPM

256

- SP

**SFN Isolation Level 1**

1 - 255

- S - IRQ

255

- S - PendSV

256*

- SPM

256

- SP