Trusted Firmware – M
log system update

Shawn Shan
October 2020

Agenda

- Background

- SPM Log system

- Secure Partition Log system

- Next steps

arm

Background

Status and requirements

- Log level is required for both SPM and SP to output message in different scenarios.

- SPM only needs simple log format such as hex and string, while SP needs rich formatting.

- Distinctions on log output between SPM and SP are required.

Design principle

- Configurable log levels.

- Separated SPM and SP log APIs.

- Log outputting underlayer is abstracted into HAL API.

arm

SPM Log System

SPM Log level control

- TFM_SPM_LOG_LEVEL_DEBUG
- TFM_SPM_LOG_LEVEL_RELEASE
- TFM_SPM_LOG_LEVEL_SILENCE

TFM_SPM_LOG_LEVEL

arm

SPM Log System

API definition

SPMLOG_DBGMSG(msg);   SPMLOG_DBGMSGVAL(msg, val);

SPMLOG_INFMSG(msg);   SPMLOG_INFMSGVAL(msg, val);

SPMLOG_ERRMSG(msg);   SPMLOG_ERRMSGVAL(msg, val);

int32_t spm_log_msgval(const char *msg, size_t len, uint32_t value)

int32_t tfm_hal_output_spm_log(const char *str, uint32_t len);

arm

SPM Log System

API definition

	TFM_SPM_LOG_LEVEL_DEBUG	TFM_SPM_LOG_LEVEL_RELEASE	TFM_SPM_LOG_LEVEL_SILENCE
SPMLOG_DBGMSGVAL	Enable	Disable	Disable
SPMLOG_INFMSGVAL	Enable	Enable	Disable
SPMLOG_ERRMSGVAL	Enable	Enable	Disable
SPMLOG_DBGMSG	Enable	Disable	Disable
SPMLOG_INFMSG	Enable	Enable	Disable
SPMLOG_ERRMSG	Enable	Enable	Disable

Legend: Enable / Disable

arm

Secure Partition Log System

SP Log level control

- TFM_PARTITION_LOG_LEVEL_DEBUG
- TFM_PARTITION_LOG_LEVEL_RELEASE
- TFM_PARTITION_LOG_LEVEL_SILENCE

TFM_PARTITION_LOG_LEVEL

arm

Secure Partition Log System

API definition

LOG_DBGFMT(…);

LOG_INFFMT(…); ⟶ int tfm_sp_log_printf(const char *fmt, …)

LOG_ERRFMT(…);

int32_t tfm_hal_output_sp_log(const unsigned char *str, uint32_t len);

arm

Secure Partition Log System

API definition

	Enable
	Disable

	TFM_PARTITION_LOG_LEVEL_DEBUG	TFM_PARTITION_LOG_LEVEL_RELEASE	TFM_PARTITION_LOG_LEVEL_SILENCE
LOG_DBGFMT	Enable	Disable	Disable
LOG_INFFMT	Enable	Enable	Disable
LOG_ERRFMT	Enable	Enable	Disable

arm

Next steps

- Stdout function implement (printf) for easier integration.

- SP printf implementation maybe oversize.

- Memory based log device.

arm

arm

Thank You
Danke
Merci
谢谢
ありがとう
Gracias
Kiitos
감사합니다
धन्यवाद
شكرًا
ধন্যবাদ
תודה