Attestation and Measurement SBI Extensions Proposal

RISC-V Trusted Computing SIG - 2022/07/05

Atul Khare, Ravi Sahita, Samuel Ortiz - Rivos

Relevant Use Cases

- Confidential Computing
  - Remote attestation is a confidential computing keystone
  - Relies on the ability for the platform to provide a signed TCB measurement
  - A trusted, external component verifies the measurement
- Measured boot
  - Each boot component is measured and measurement are stored
  - Each software layer can measure the next one
  - Evidence can be asynchronously verified, locally or remotely
- Trusted boot
  - Each boot component is measured and then verified
  - Each software layer can measure the next one

Requirements

1. Get a TCB attestation evidence
    a. A set of signed measurements for all layers that compose the TCB
    b. Allow for any software layer to request a TCB attestation evidence (a.k.a. Attestation report)
    c. To be sent to the remote or local attestation Verifier
2. Extend the TCB evidence with additional measurements
    a. Allow for any software layer to measure other layers and add them to the TCB
3. Get the platform attestation and measurement capabilities

SBI Extension Proposal

- Attestation and Measurement Extension ID (`0x41545354 “ATST”`)

Function Name	Description
`sbi_attestation_get_evidence`	Get the TCB attestation evidence
`sbi_measurement_extend`	Extend the current measurement
`sbi_attestation_get_capabilities`	Get the platform attestation capabilities

Get Evidence

```
struct sbiret sbi_attestation_get_evidence(unsigned long cert_request_addr,
                                           unsigned long cert_request_size
                                           unsigned long report_data_addr,
                                           unsigned long evidence_format,
                                           unsigned long cert_addr,
                                           unsigned long max_cert_size);
```

Input	Output
X.509 Certificate Signing Request	X.509 Certificate • Signed with attestation keys • Attestation Evidence as X.509 extensions • Additional data as X.509 extension
Additional evidence data (e.g. a nonce)	
Evidence format (DiceTcbInfo or OpenDice)	

Extend Measurement

```
struct sbiret sbi_measurement_extend(unsigned long measurement_addr,
                                     unsigned long measurement_index,
                                     unsigned long hash_algorithm);
```

Input	Output
Data measurement	None
Measurement register index	
Measurement hash algorithm	

Get Capabilities

```
struct sbiret sbi_attestation_get_capabilities(unsigned long caps_addr);
```

Input	Output
None	Attestation capabilities structure ● TCB Security Version Number ● Supported hash algorithms ● Supported evidence formats ● Measurement registers description

Backup

Attestation Capabilities

Field	Description	Type
TCB_SVN	TCB Secure Version Number	Integer
HASH_ALGORITHMS	Supported measurement hash algorithms (SHA-384, SHA-512)	Bitmap
EVIDENCE_FORMATS	Supported X.509 evidence formats (DiceTcbInfo ,OpenDice)	Bitmap
NUM_SMSMT_REGS	Number of static measurement registers	Integer [1-16]
NUM_RMSMT_REGS	Number of runtime measurement registers	Integer [0-16]
MSMT_REGS_INFO	Description of all measurement registers	MSMT_REG array