Verifiable Launch

Verifiable launch ensures that an enclave's execution environment is configured correctly and its initial state is as expected. This process involves:

Root of Trust

Establishing a trusted starting point (RTM) for the measurement process

Measurement

Creating a cryptographic fingerprint of the enclave's initial state

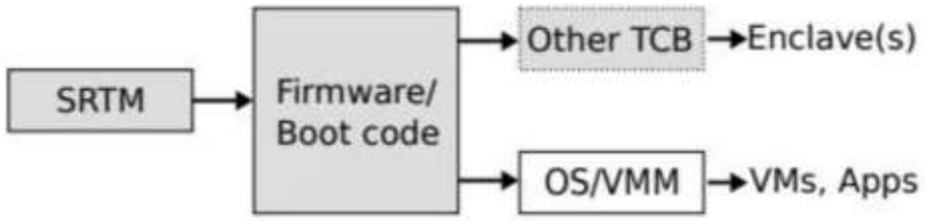
Attestation

Providing proof of the enclave's state to a verifier

This process establishes trust in the enclave before any sensitive operations are performed.

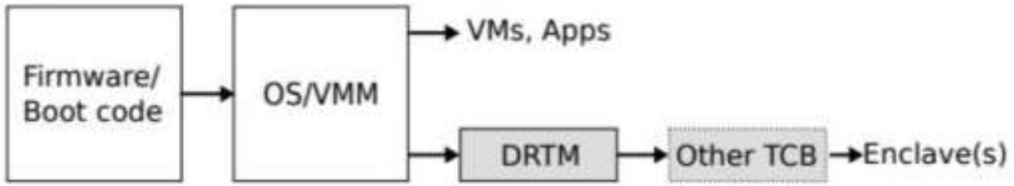
Root of Trust for Measurement (RTM)

Static RTM (SRTM)



Unbroken chain of trust from system reset to enclave execution

Dynamic RTM (DRTM)



Establishes a new RTM without trusting previously executed code

Most TEEs use SRTM. Only a few systems from Intel and AMD leverage DRTM, likely because the main motivation—excluding boot code from the TCB—only applies to platforms with legacy boot code.

Measurement Process

The measurement process creates a cryptographic fingerprint of the enclave's initial state:

Initial Measurement

Starting at the RTM, each component in the chain of trust measures the next component before transferring control

Integrity Checking

Components are not only measured but also integrity-checked (e.g., signature verification) before execution

Secure Storage

Measurements are stored securely in protected registers or memory regions to prevent tampering

TEEs use similar measurement techniques, typically involving cryptographic hashes over the initial memory of the enclave.

Attestation

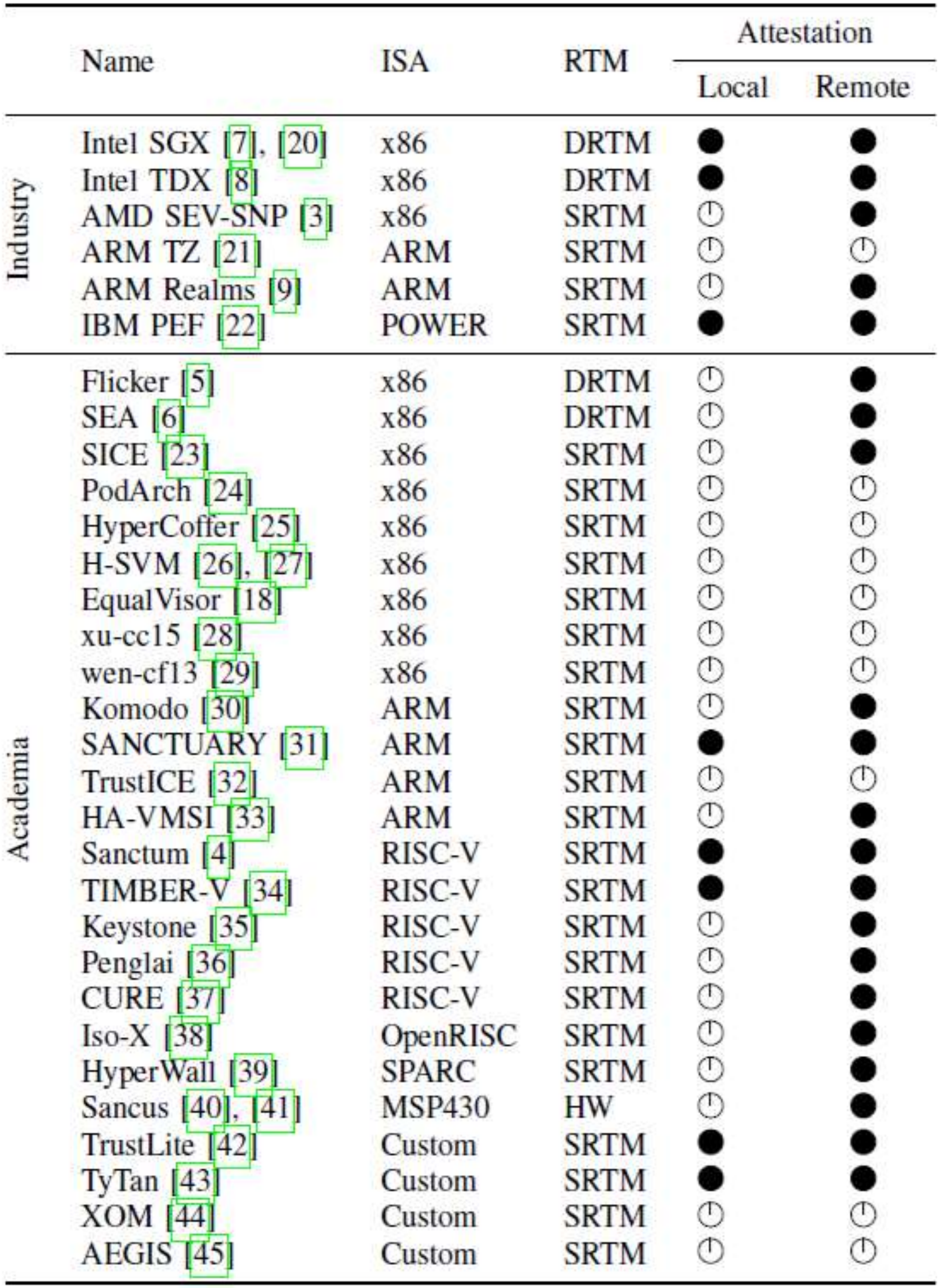
Local Attestation

- For verifiers co-located on the same platform
- Typically uses symmetric cryptography
- More efficient than remote attestation
- Limited to intra-platform verification

Remote Attestation

- For verifiers not on the same platform
- Uses asymmetric cryptography
- Often involves certificate chain verification
- Supported by most TEE solutions

Attestation allows a verifier to check that the enclave has been launched correctly and its initial state matches expected reference values.



	Name	ISA	RTM	Attestation	
				Local	Remote
Industry	Intel SGX [7], [20]	x86	DRTM	●	●
	Intel TDX [8]	x86	DRTM	●	●
	AMD SEV-SNP [3]	x86	SRTM	○	●
	ARM TZ [21]	ARM	SRTM	○	○
	ARM Realms [9]	ARM	SRTM	○	●
	IBM PEF [22]	POWER	SRTM	●	●
Academia	Flicker [5]	x86	DRTM	○	●
	SEA [6]	x86	DRTM	○	●
	SICE [23]	x86	SRTM	○	●
	PodArch [24]	x86	SRTM	○	○
	HyperCoffer [25]	x86	SRTM	○	○
	H-SVM [26], [27]	x86	SRTM	○	○
	EqualVisor [18]	x86	SRTM	○	○
	xu-cc15 [28]	x86	SRTM	○	○
	wen-cf13 [29]	x86	SRTM	○	○
	Komodo [30]	ARM	SRTM	○	●
	SANCTUARY [31]	ARM	SRTM	●	●
	TrustICE [32]	ARM	SRTM	○	○
	HA-VMSI [33]	ARM	SRTM	○	●
	Sanctum [4]	RISC-V	SRTM	●	●
	TIMBER-V [34]	RISC-V	SRTM	●	●
	Keystone [35]	RISC-V	SRTM	○	●
	Penglai [36]	RISC-V	SRTM	○	●
	CURE [37]	RISC-V	SRTM	○	●
	Iso-X [38]	OpenRISC	SRTM	○	●
	HyperWall [39]	SPARC	SRTM	○	●
	Sancus [40], [41]	MSP430	HW	○	●
	TrustLite [42]	Custom	SRTM	●	●
	TyTan [43]	Custom	SRTM	●	●
	XOM [44]	Custom	SRTM	○	○
	AEGIS [45]	Custom	SRTM	○	○

Attestation Report Contents

Basic Information

- Enclave measurements
- TCB measurements
- Nonce for freshness

Extended Information

- Runtime attributes (e.g., SMT enabled/disabled)
- Software version numbers
- Migration policies
- TCB version information

Custom Data

- Public key certificates
- Channel establishment data
- Application-specific information

Modern TEEs include more comprehensive information in attestation reports compared to early designs that only included measurements and nonces.

Secret Provisioning

Provisioning secrets into enclaves is often the final step during launch. Two main approaches exist:

Pre-Attestation Provisioning

Some TEEs allow enclaves to be provisioned with secret data prior to attestation:

- Secret data included in initial enclave state
- Reflected in the measurement
- Encrypted before delivery to the platform
- Examples: IBM PEF, AMD SEV-SNP, PodArch

Post-Attestation Provisioning

Other TEEs require attestation before any secret data can be provisioned:

- Enclave appends custom data to attestation report
- Data authenticated during attestation
- Used to establish secure communication channel
- Based on key exchange protocols