CONFIDENTIAL CLOUD

Simon Johnson, Senior Principal Architect,

Intel - Security Platform Division

IEEE EDPS – 14th September , 2018

LEGAL DISCLAIMERS AND NOTICES

This presentation contains the general insights and opinions of Intel Corporation ("Intel"). The information in this presentation is provided for information only and is not to be relied upon for any other purpose than educational. Use at your own risk! Intel makes no representations or warranties regarding the accuracy or completeness of the information in this presentation. Intel accepts no duty to update this presentation based on more current information. Intel is not liable for any damages, direct or indirect, consequential or otherwise, that may arise, directly or indirectly, from the use or misuse of the information in this presentation.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Learn more at intel.com, or from the OEM or retailer.

No computer system can be absolutely secure.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

Intel does not represent or warrant that SGX technology is immune to hacking, code-breaking or other efforts to circumvent the SGX technology.

Intel, the Intel Core, and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.

WHY CONFIDENTIAL CLOUD?

Higher value workloads require security guarantees around processing:

- Personal Identifying Information
- Government Confidential Information
- High Value Assets

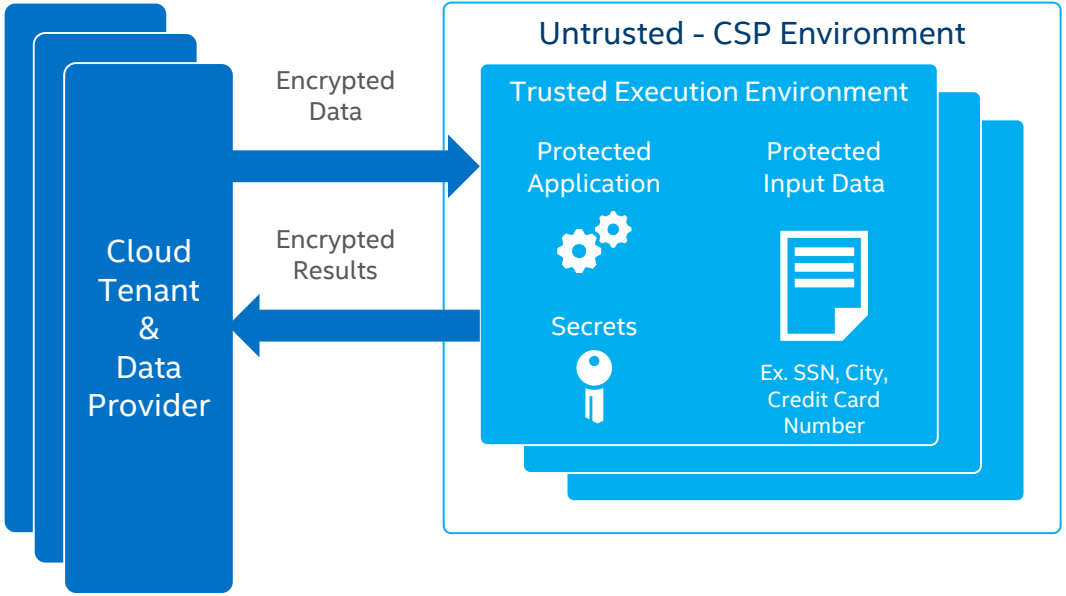
Cloud providers already had many programs for convincing their customers on why they should be trusted.

Snowden revelations tipped the conversation cloud security.

CONFIDENTIAL CLOUD paradigm combats rising paranoia of trusting cloud providers with customer secrets.

WHAT IS CONFIDENTIAL CLOUD?

ENABLES ISLANDS OF PROTECTION TO BE CREATED AT SCALE TO ENABLE TENANT APPLICATIONS TO KEEP CODE AND DATA VISIBILITY FROM THE CSP.

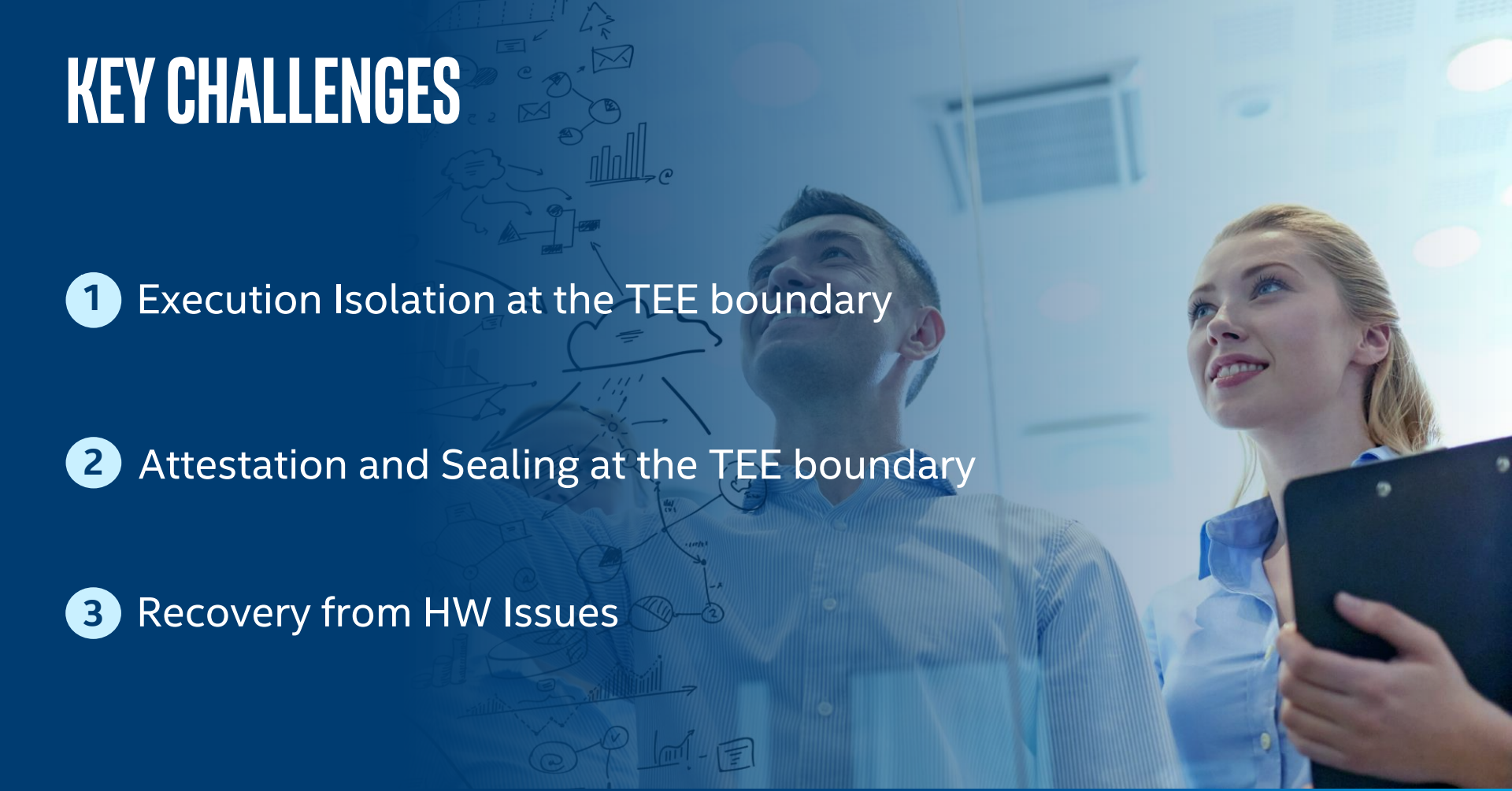


- **Hardens against** attacks from SW that does not belong to the cloud tenant
  - Where possible provide the smallest Trusted Computing Base (TCB)
  - Secrets (data/keys/et al) remain protected even when attacker has full control of platform
- **Provides protections from** physical attacks like memory bus snooping, memory tampering, and “cold boot” attacks against memory contents in RAM
  - Protection for hard-to-protect or unprotected spaces
- Provides **hardware-based attestation** capabilities to measure and verify valid code and data signatures
  - Increases transparency and accountability

WHOSE DOING IT?

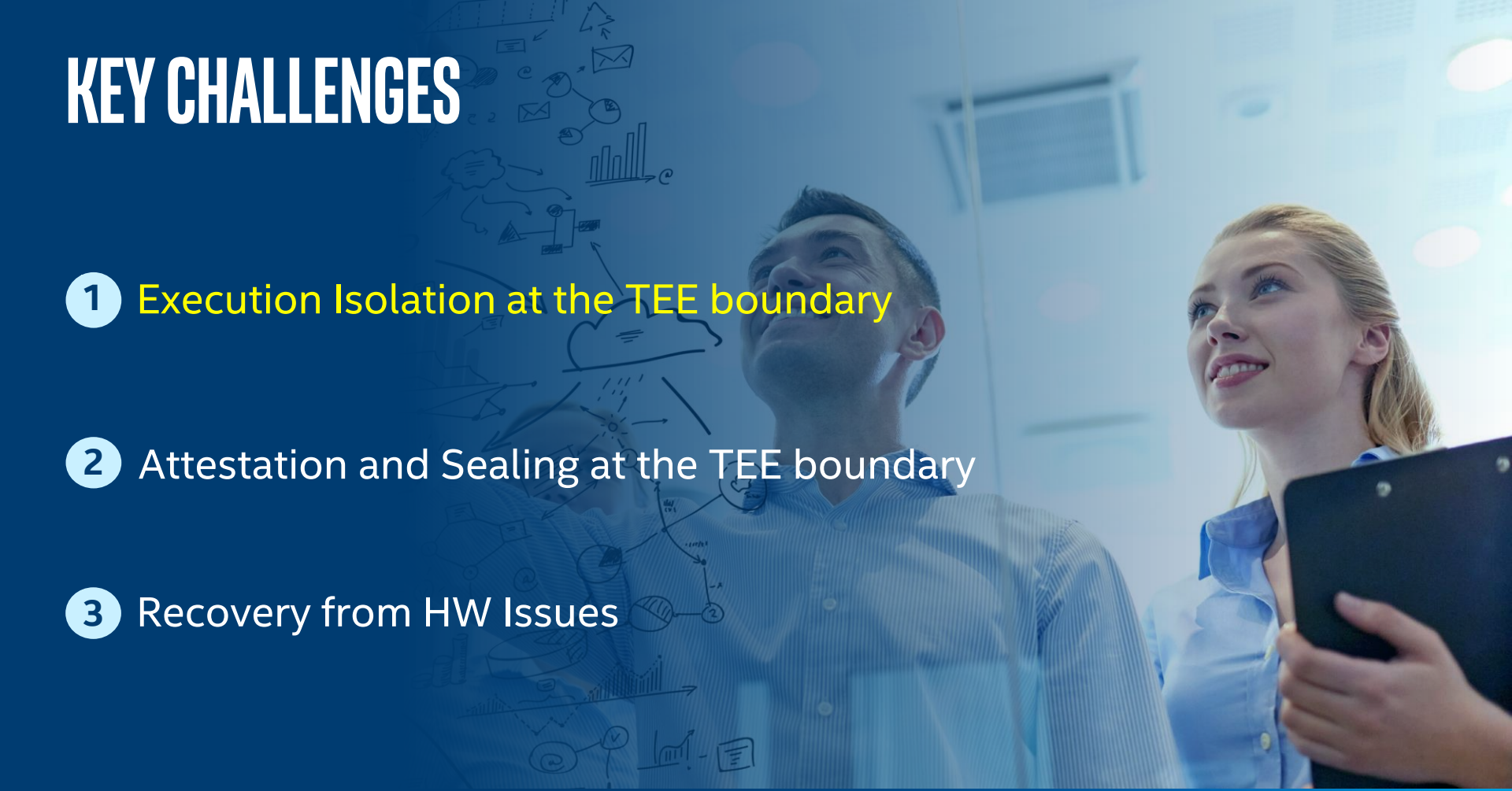
Cloud Players that have already made announcements in this space include:

KEY CHALLENGES



1. Execution Isolation at the TEE boundary
2. Attestation and Sealing at the TEE boundary
3. Recovery from HW Issues

KEY CHALLENGES



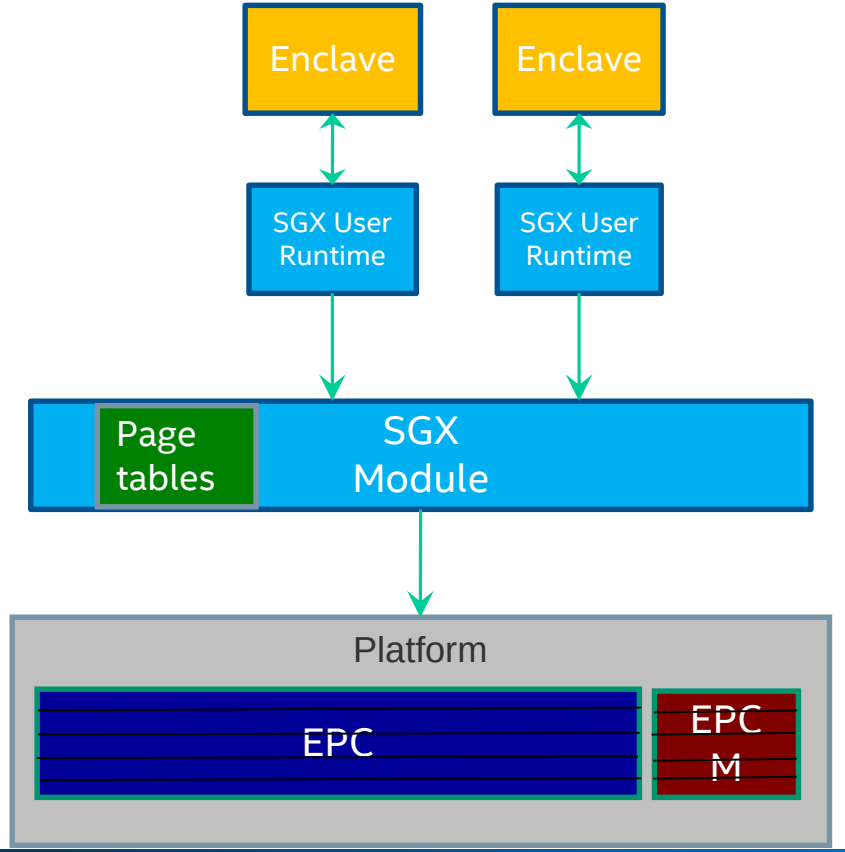
1. Execution Isolation at the TEE boundary
2. Attestation and Sealing at the TEE boundary
3. Recovery from HW Issues

SGX HIGH-LEVEL HARDWARE/SOFTWARE PICTURE

Application Environment

Privileged Environment

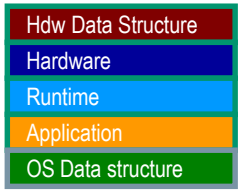
New Exposed Hardware



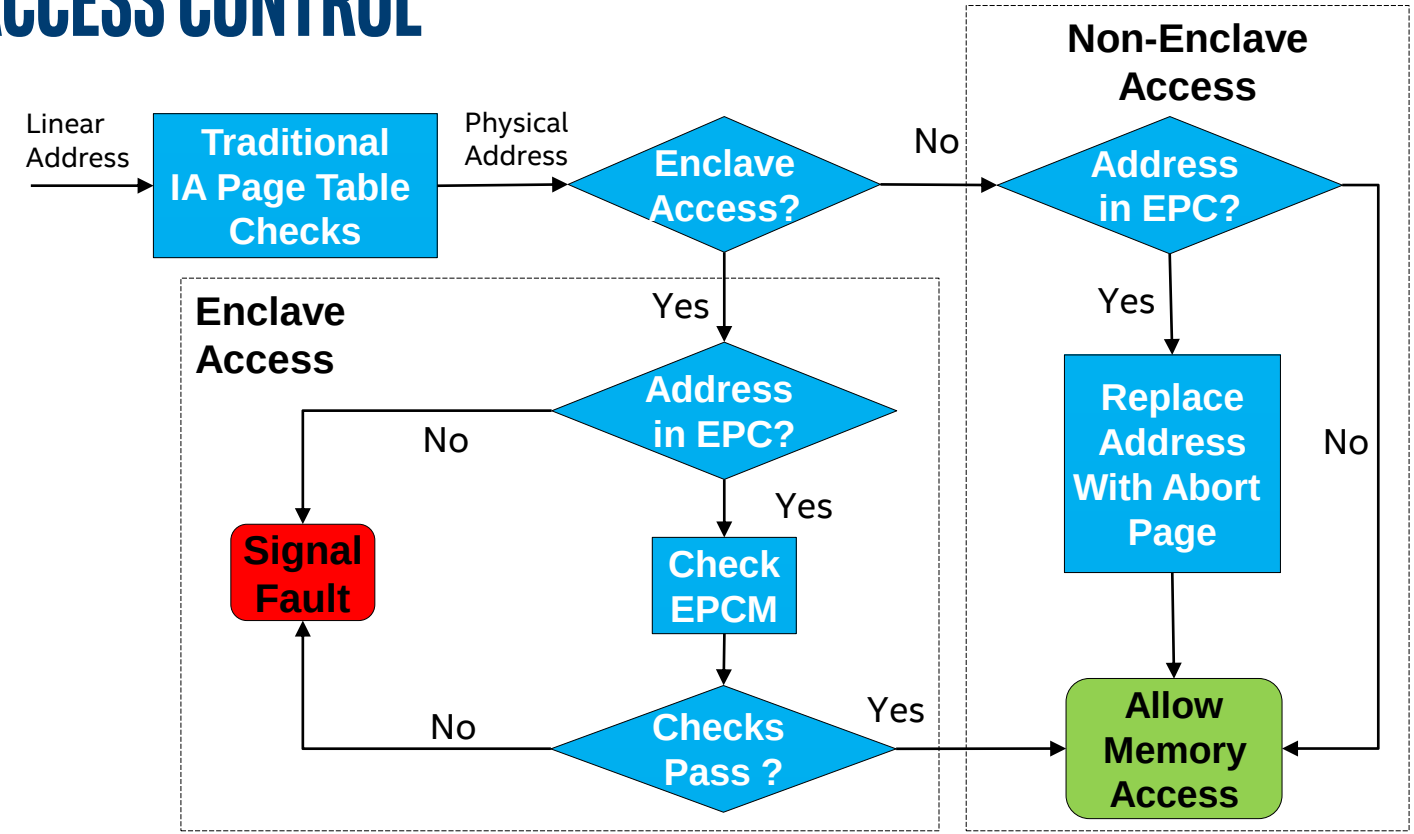
New Application Level Instructions
EEXIT
EGETKEY
EREPORT
EENTER
ERESUME

New Kernel Level Instructions

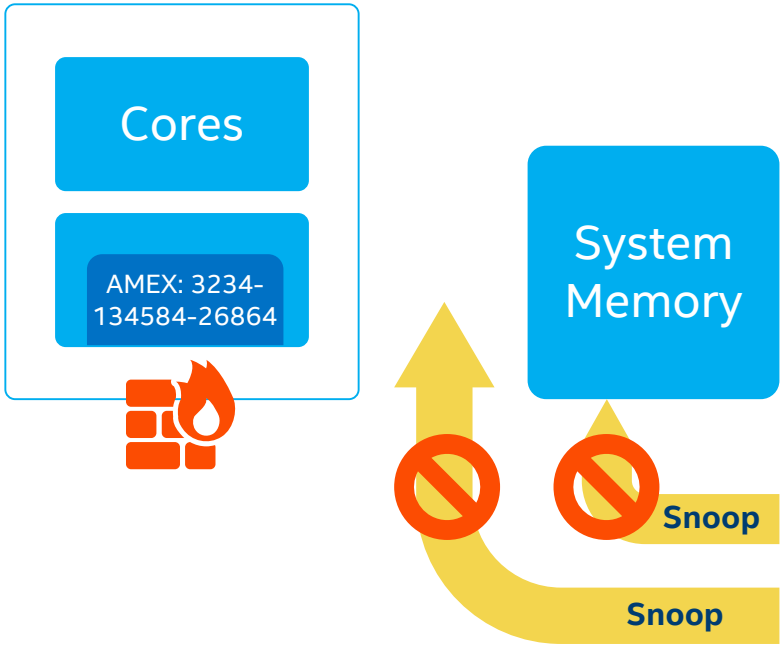
ECREATE	ETRACK
EADD	EWB
EEXTEND	ELD
EINIT	EPA
EBLOCK	EREMOVE



SGX ACCESS CONTROL



SGX: MEMORY PROTECTION OUTSIDE CPU

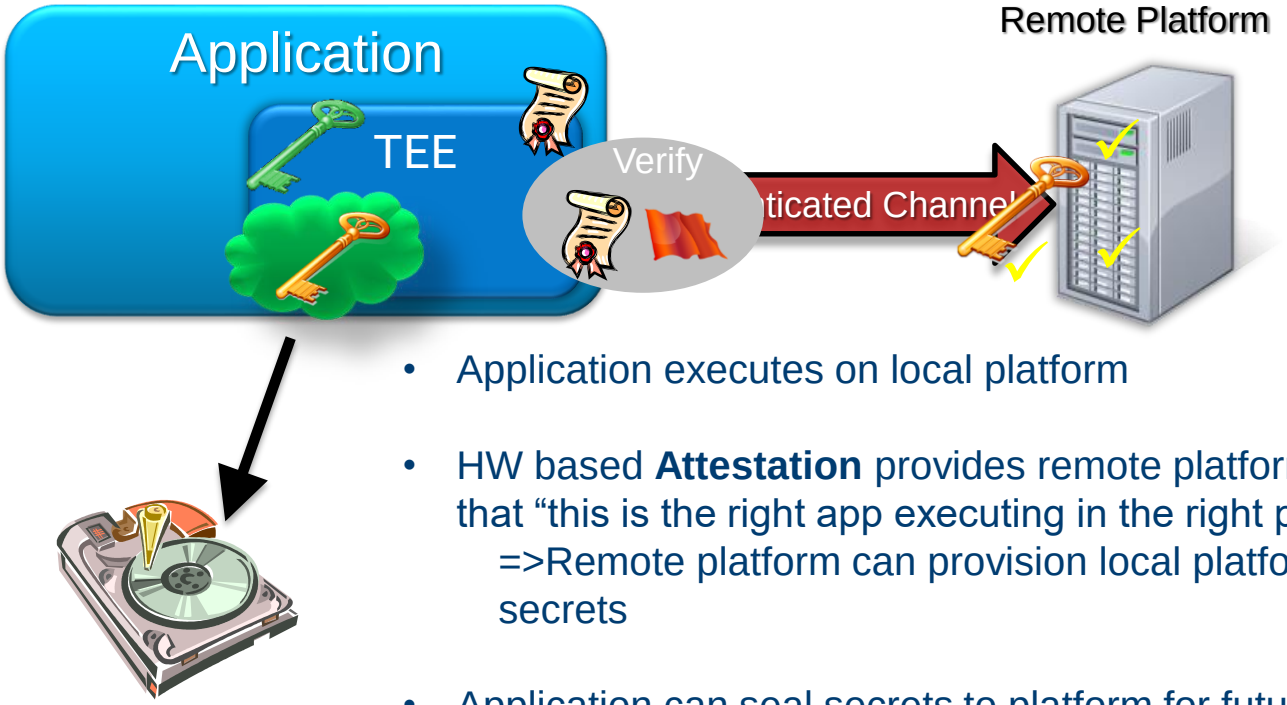


1. Security perimeter is the CPU package boundary
2. Data and code unencrypted inside CPU package
3. Data and code outside CPU package is encrypted and integrity checked
4. External memory reads and bus snoops see only encrypted data

KEY CHALLENGES

1. Execution Isolation at the Application boundary
2. Attestation and Sealing at the Application boundary
3. Recovery from HW Issues

CRITICAL FEATURES: ATTESTATION AND SEALING



- Application executes on local platform
- HW based **Attestation** provides remote platform assurance that “this is the right app executing in the right platform “
  =>Remote platform can provision local platform with secrets
- Application can seal secrets to platform for future use

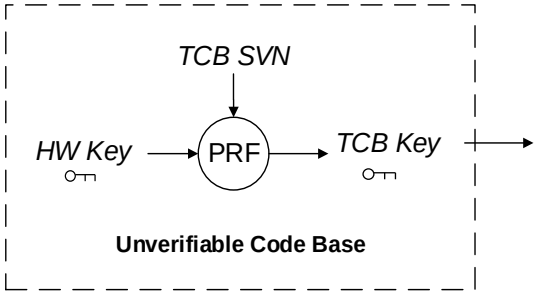
KEY CHALLENGES

1. Execution Isolation at the Application boundary
2. Attestation and Sealing to the Application boundary
3. TCB Recovery

TCB RECOVERY

TCB recovery is the process of being able to cryptographically demonstrate that the TCB has been updated to fix a potential security issue

- First we issue all the HW component with a "Security Version Number"
- This is used to derive a "TCB specific" key from the HW key in the part.
- When a new update is issued all keys are derived from the new TCB specific key.

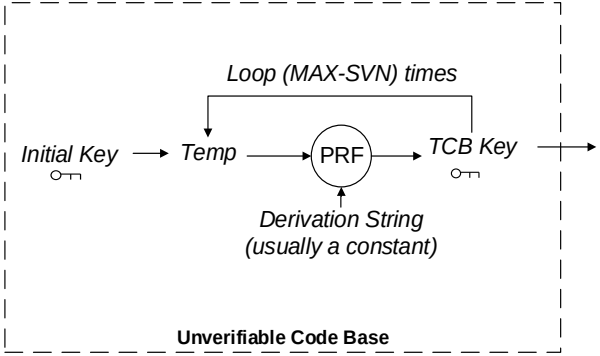


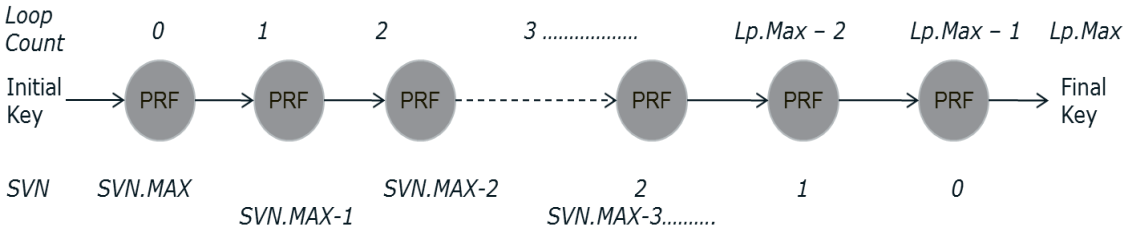
- Note: this mechanism cannot be modified as part of a TCB update itself.

DATA MIGRATION

But what about all the data sealed to an previous TCB key?

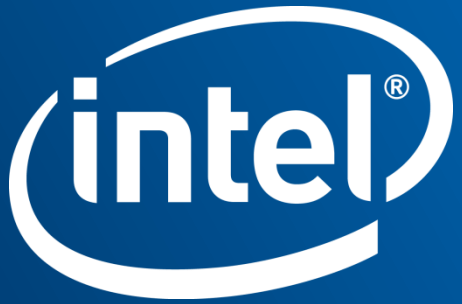
- A backwards loop is used to provide forward secrecy, but allows “previous” TCB specific keys to be retrieved
- This allows the CPU to “go back” to previous keys by performing additional PRF’s





TO DO...

1. Language integration and tools
2. Moving beyond LibraryOS models
3. Integrating Attestation into Applications
4. Tools to help developers write safer TEE code
5. Test suites for classic Side-Channel protections (e.g. Caches & TLBs)


intel

SOFTWARE.INTEL.COM/SGX

The site has the latest info on:

- SDK & Developer Resources
- White Papers
- Support Forum