Intel® SGX Trusted Computing Base (TCB) Recovery

Scope

We designed Intel® Software Guard Extensions (Intel® SGX) with the ability to update it in order to address any issues that might arise in the future. Merely providing this update mechanism, however, is not sufficient for a secure service infrastructure: if a client's update is voluntary, then the remote service could be communicating with a client that is out of date and subject to security vulnerabilities. To address this issue, Intel SGX was also given the means to cryptographically prove, via remote attestation, that the client update has taken place. The mechanics of this process have been outlined in the whitepaper titled "Intel® Software Guard Extensions: EPID Attestation and Services"[1].

Until now, Intel has not fully described the effects of performing an Intel SGX Trusted Computing Base (TCB) recovery on the end-user and developer community. This paper is intended to close this gap.

Intel SGX Attestation Review

Attestation is the process of demonstrating that a software executable has been properly instantiated on a platform. Intel SGX Attestation allows a remote party to gain confidence that the intended software is securely running within an enclave on a fully patched, Intel SGX enabled platform. The attestation conveys the following information in an assertion:

- The identities of software being attested.

- The details of unmeasured state (e.g., the mode software is running in).

- Data that the software associates with itself.

Intel SGX uses an asymmetric attestation key, representing the Intel SGX Trusted Computing Base, to sign an assertion with the above information. Any changes to this TCB will result in the need to replace the Intel SGX Asymmetric Attestation key. This process is known as TCB Recovery.

What is the Intel SGX Trusted Computing Base?

The Intel SGX TCB is comprised of the components in the platform that are required to implement the Intel SGX security objectives. Some of these components can be updated through a change in Intel SGX Platform Software, some via CPU firmware (that co-implements the Intel SGX instruction set along with the hardware), while other elements–such as the CPU logic–are immutable.

What are the elements of a TCB recovery?

There are two essential elements to a TCB recovery. The first is the update of the mutable components of the TCB, completed by issuing a CPU firmware update and/or a new version of the attestation software that forms part of the Intel SGX Platform Software (PSW) component. The second is producing a new TCB key set to identify the TCB for a specific platform, which is then used in re-provisioning the platform's Intel SGX attestation key.

Why would it happen?

An Intel SGX TCB recovery can occur if a vulnerability is discovered in either the platform or the implementation of Intel SGX which violates one or more of the Intel SGX security objectives for which it was originally designed. This vulnerability may be corrected through an update to the mutable TCB components.

The primary Intel SGX Security Objectives are:

- Execution Isolation
- Remote Provisioning
- Key Management

Security Objective: Execution Isolation

1. Detect integrity violations of an enclave instance from software attacks by an unprivileged attacker, system software attacker, or system startup/SMM attacker and prevent attacker access to tampered code and data upon detection.

2. For an enclave instance, protect confidentiality of code and data against software attacks by an unprivileged, system software attacker, or system startup/SMM.

3. Provide isolation between all enclave instances such that:

   - An enclave instance cannot read another enclave instances' memory space.

   - Unprivileged software attackers cannot bypass the existing IA-32 access control mechanisms.

   - An enclave continues to abide by the read/write/execute access control policy set by system software.

   - No extra privileges are obtained beyond what system software grants.

4. Prevent replay of an enclave instance by an unprivileged attacker, a system software attacker, or via components at system startup (such as the SMM).

Security Objective: Remote Provisioning

1. Allow an enclave instance to request an assertion of the enclave's identity from the platform that can be remotely verified.

2. Make spoofing an assertion computationally infeasible for unprivileged software, system software, simple hardware, or a skilled hardware attacker.

3. Allow an enclave instance to request locally-verifiable assertions of enclave's identity. Any enclave may verify whether these assertions originated on the same platform.

4. Allow an enclave instance to obtain keys that are bound to the platform and the enclave class identity (or a subset of the enclave class identity). These keys can be used for data sealing and provisioning. Prevent access to other enclave class keys by unprivileged software, system software, simple hardware, a skilled hardware attacker, and other enclaves of different class identities

Security Objective: Key Management

1. Make using a compromised TCB to access the sensitive data of a newer TCB revision computationally infeasible for a software adversary, simple hardware, a skilled hardware attacker.

Intel SGX Remote Attestation

Detecting when an Intel SGX TCB recovery is required

The Intel Attestation Service (IAS) is a verification service for Intel SGX attestation evidence that provides verification of both identity and platform TCB. The application developer, via their own attestation Service Provider (sometimes also called an Attestation Proxy), can submit their client enclave's attestation report to the IAS for verification. The IAS will respond with an Attestation Verification Report: a cryptographically signed report verifying the identity of the enclave and the TCB of the platform the enclave was instantiated on. Figure 1 demonstrates the relationships of all parties involved in the remote attestation process.
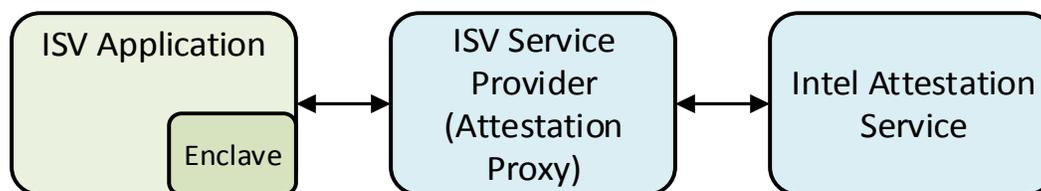
Figure 1. Intel SGX Remote Attestation Process participants

The contents of the verification report returned by the IAS include several fields. The "`isvEnclaveQuoteStatus`" field contains the status of the enclave verification. For platforms whose TCB meets the current expected TCB, the value of this field would be "`OK`". In cases where one or more of the platforms TCB elements does not meet the expected TCB, the "`isvEnclaveQuoteStatus`" returned is "`GROUP_OUT_OF_DATE`" which indicates that a TCB recovery is required. More information on the Intel Attestation Service API can be found https://software.intel.com/sites/default/files/managed/7e/3b/ias-api-spec.pdf.

Bringing the Intel SGX TCB back into compliance

Once the Service Provider (Attestation Proxy) has determined that the given TCB is out of date, the question becomes how to determine which TCB components needs to be updated. When the "`isvEnclaveQuoteStatus`" is "`GROUP_OUT_OF_DATE`", the Attestation Verification Report must also contain a "`platformInfoBlob`" field. This field contains an opaque binary blob that the Service Provider should forward on to the attesting application/platform for processing by the Intel SGX SDK API function `sgx_report_attestation_status()`. This API will decode the "`platformInfoBlob`" to discern if an update is required, and if so, denote the components to be updated to resolve the "`GROUP_OUT_OF_DATE`" status. This may include any or all of the following: a CPU Firmware, a CSME Firmware, or an Intel SGX Platform Software Update.

Based on which components need updating, the developer may signal the end-user or IT administrator to take appropriate steps to resolve the issue. For CPU Firmware or CSME Firmware updates, resolution typically takes the form of a BIOS update from the platform OEM. For PSW updates, Microsoft* Windows* Update will update new PSW packages for Windows 10 (version 1709 or build 10.0.16299) and newer automatically. For legacy Windows OSes and Linux*, the developer must deploy an updated Intel SGX Platform Software package to their users.

End-User TCB Recovery Messaging

Once the Intel SGX enabled application has determined which TCB element(s) need to be updated by using the `sgx_report_attestation_status()` API, it is important to provide clear instructions to the end-user or IT regarding the actions they must take to resolve the issue. In the case of IT-managed or headless systems (servers), the application should generate an appropriate OS event log entry which can be regularly collected, processed, and ultimately resolved by IT operations. For consumer facing applications and platforms, concise messaging for the following conditions applies:

- **Processor Firmware Update** (`ucodeUpdate`) – "A security upgrade for your computing device is required in order for this application to continue to provide you with a high degree of security. Please contact your device manufacturers' support website for a BIOS update for this system."

- **Intel Manageability Engine Update** (`csmeFwUpdate`) - "A security upgrade for your computing device is required in order for this application to continue to provide you with a high degree of security. Please contact your device manufacturers' support website for a BIOS and/or Intel® Manageability Engine update for this system."

- **Intel SGX Platform Software Update** (`pswUpdate`) - "A security upgrade for your computing device is required in order for this application to continue to provide you with a high degree of security. Please visit this application's support website for an Intel SGX Platform SW update."

Attestation Policies

To ensure that Intel SGX enabled solutions are always operating with the latest platform TCB and minimizing risk, it is strongly advised that the Attestation Service Provider (Attestation Proxy) define and enforce an attestation policy. An attestation policy could define such things as first-time attestation policy, frequency of required attestation policy, and an optional grace period policy.

First-Time Attestation Policy

The first-time attestation policy must require the Intel SGX enabled client application to successfully complete a full attestation flow before allowing any sensitive data to be provisioned to the enclave by the Service Provider. Should the attestation flow fail with "`GROUP_OUT_OF_DATE`" status, the potentially vulnerable platform should update its TCB before any sensitive data are provisioned to it, therefore reducing the risk of exposure.

Frequency Policy

The frequency policy must require an Intel SGX enabled client application to successfully complete an attestation flow after a given length of time had elapsed (days, weeks, months, etc.). This period is arbitrary, and should be based on the organization's risk tolerance for the compromise of sensitive data due to a vulnerability on an out of date platform. For organizations with low risk tolerance (e.g., Banking), the attestation frequency policy might be once per day or once per week. Organizations with higher risk tolerance may define a frequency policy of once every 180 days. A typical frequency policy is once every 30 days.

Frequency policy implementation is a time-to-live policy for any sensitive data provisioned to an Intel SGX client application after at least one successful attestation has been completed. In short, the sensitive data is valid only for a specific period of time before expiration, and re-attestation is required to provision a new set of data.

Grace Period Policy

For certain use cases, it might be appropriate to provide a grace period to allow the Intel SGX enabled application to continue use the provisioned sensitive data while notifying the

platform owner that updates are required due to a "`GROUP_OUT_OF_DATE`" response. Such a grace period policy would allow the Service Provider (Attestation Proxy) to trust a "`GROUP_OUT_OF_DATE`" response received by the IAS for a short period of time so as to allow an end-user or IT organization sufficient time to resolve the out-of-date TCB components.

Enclave Sealed Data Migration during a TCB Recovery

Intel SGX Sealing Key Policies

When requesting a sealing key (`EGETKEY`), the enclave selects a policy for which it may access that sealing key. These policies are useful for controlling the accessibility of sensitive data to future versions of the enclave.

Intel SGX supports two policies for Seal Keys:

- Sealing to the Enclave Identity (`KEYPOLICY_MRENCLAVE`)
- Sealing to the Signer Identity (`KEYPOLICY_MRSIGNER`)

Sealing to the Enclave Identity produces a key that is available to any instance of this exact enclave.

> *Warning: This policy will not allow future software to access the sensitive data sealed by this enclave.*

Sealing to the Signer Identity produces a key that is available to other enclaves signed by the same Signing Authority. *This policy can be used to allow newer (updated/upgraded) enclaves to access data stored by previous versions.*

Sealed Data Migration support using sgx_seal_data() API

The Intel SGX SDK provides the `sgx_seal_data()` API function to support sealing of enclave data that can be migrated from an older enclave instance to a newer enclave instance. The `sgx_seal_data()` API function also supports the case where the CPU Security Version Number (CPUSVN) may have been updated (via CPU Firmware update) which may occur as a result of a TCB recovery. CPUSVN is one of the key derivation inputs to seal keys generated by the `EGETKEY` instruction.

> *Warning: It is strongly advised that you do not use keys obtained from `sgx_get_key()` to encrypt/seal data directly unless you store the full key request as metadata with the sealed data. Failure to store the key request can lead to sealed data that cannot be recovered after a TCB recovery. The `sgx_seal_data()` API function described above manages all of the metadata for correct enclave data sealing functionality.*

References

1. EPID Attestation and Services – https://software.intel.com/sites/default/files/managed/ac/40/2016%20WW10%20sgx%20provisioning%20and%20attesatation%20final.pdf

2. Intel Software Guard Extensions Developer Reference Guides
   https://software.intel.com/en-us/sgx-sdk/documentation