WHITE PAPER

Intel® Software Guard Extensions (Intel® SGX)

Intel® Software Guard Extensions Trusted Computing Base Recovery

Introduction

Intel engineers designed Intel® Software Guard Extensions (Intel® SGX) so that it can be updated to address future issues. However, this update mechanism alone is insufficient for a secure service infrastructure: If a platform's update is voluntary, then the remote service could be communicating with a platform that is out of date and subject to security vulnerabilities. To address this issue, Intel SGX now has the means to cryptographically prove, via remote attestation, that the platform update has taken place. The mechanics of this process are outlined in the *Intel® SGX: Intel® EPID Provisioning and Attestation Services*[1] white paper.

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. The Attestation Service for Intel SGX (IAS) allows a remote party to gain confidence that the intended software is securely running within an enclave on a fully patched and updated Intel SGX enabled platform. The attestation conveys the following information in an assertion:

- The identities of software being attested
- Details of the unmeasured state (for example, the execution mode of the software)
- Data that the software associates with itself

Intel SGX uses an asymmetric attestation key, representing the Intel SGX TCB, 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 comprises 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, and some via CPU firmware (that co-implements the

[1] Intel® SGX: Intel® EPID Provisioning and Attestation Services

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 that identifies the TCB for a specific platform, which is then used in reprovisioning the platform's Intel SGX attestation key.

Why Would a TCB Recovery Event Occur?

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

- Detect integrity violations of an enclave instance from software attacks by an unprivileged attacker, system software attacker, or system startup/System Management Mode (SMM) attacker, and prevent attacker access to tampered code and data upon detection.
- For an enclave instance, protect confidentiality of code and data against software attacks by an unprivileged attacker, system software attacker, or system startup/SMM.
- 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 the system software grants.
- 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

- Allow an enclave instance to request an assertion of the enclave's identity from the platform that can be remotely verified.
- Make spoofing an assertion computationally infeasible for unprivileged software, system software, simple hardware, or a skilled hardware attacker.
- Allow an enclave instance to request locally verifiable assertions of an enclave's identity. Any enclave may verify whether these assertions originated on the same platform.
- 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

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

Intel SGX Remote Attestation

Detecting When an Intel SGX TCB Recovery Is Required

The 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 responds 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.

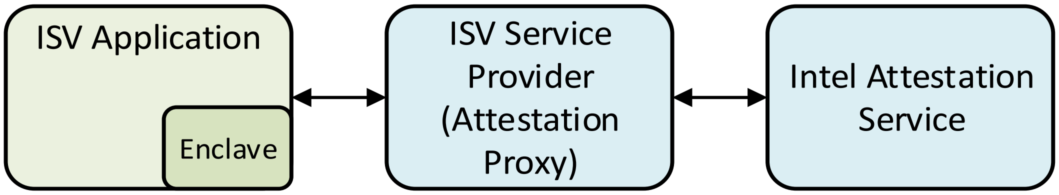
ISV Application
Enclave
ISV Service Provider (Attestation Proxy)
Intel Attestation Service

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 will be OK. In cases where one or more of the platform's TCB elements does not meet the most current TCB level, the isvEnclaveQuoteStatus returned will show GROUP_OUT_OF_DATE, indicating that a TCB recovery for the attesting platform is required. In this case, the HTTP response from IAS also contains two additional headers: Advisory-URL and Advisory-ID. The Advisory-URL header contains the URL to the Intel® Product Security Center and the Advisory-ID header contains a list of one or more related Intel® Product Security Advisory IDs affecting the attested platform. The provided Intel Product Security Advisory IDs correspond to an advisory article (found at the URL provided in the Advisory-URL header) that provides insight into specific Intel SGX related security issues affecting the attested platform.

In some cases, the verification report for the attesting platform may receive an isvEnclaveQuoteStatus of the CONFIGURATION_NEEDED message. This means that the attested platform meets the current TCB level for that platform, but additional BIOS configuration may be required to achieve an improved security posture. As with GROUP_OUT_OF_DATE, a CONFIGURATION_NEEDED response also provides the Advisory-URL and Advisory-ID HTTP header information to better understand which Intel Product Security Advisories are contributing to the response, and what can be done to bring the platform back into compliance. For more information, consult the Attestation Service for Intel® SGX: API Documentation[2].

Bringing the Intel SGX TCB Back Into Compliance

Once the service provider (attestation proxy) has determined that the given platform TCB is out of date, the question becomes how to determine which TCB components need to be updated. When the isvEnclaveQuoteStatus is GROUP_OUT_OF_DATE, or CONFIGURATION_NEEDED, the Attestation Verification Report will 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 software development kit (SDK) API function sgx_report_attestation_status(). This API decodes the platformInfoBlob to discern whether 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: CPU firmware, Intel® Converged Security and Management Engine (Intel® CSME) firmware, or an Intel SGX platform software update. For CONFIGURATION_NEEDED, sgx_report_attestation_status() will likely report that there is no update required since resolution comes in the form of a platform BIOS configuration change.

[2] Attestation Service for Intel® SGX: API Documentation

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 Intel CSME firmware updates, resolution typically takes the form of a BIOS update from the platform original equipment manufacturer (OEM). For PSW updates, 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 to 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 for both `GROUP_OUT_OF_DATE` and `CONFIGURATION_NEEDED` responses. These log entries can then 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 for this application to continue to provide you with a high degree of security. Please contact your device manufacturer's support website for a BIOS update for this system.
- **Intel Manageability Engine Update** (`csmeFwUpdate`). A security upgrade for your computing device is required for this application to continue to provide you with a high degree of security. Please contact your device manufacturer's 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 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 has elapsed (days, weeks, months, and so on). 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 (for example, 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 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 sealing keys:

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

Sealing to the Enclave Identity (`KEYPOLICY_MRENCLAVE`) 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 data 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.

Notices

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. Check with your system manufacturer or retailer or learn more at intel.com.

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

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest forecast, schedule, specifications and roadmaps.

The products and services described may contain defects or errors known as errata which may cause deviations from published specifications. Current characterized errata are available on request.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

WHITE PAPER

Intel® Software Guard Extensions (Intel® SGX)