230420.Slide.SGX

Created: 2023-05-01 22:17:30

Questions

- Slideshow - Intro to Intel SGX
  - Below slideshow is “Intro to Intel SGX” `(Slides.SGX.0420.md)`
- My Questions
  - Why is Intel SGX not suited for password managers? `(Slides.SGX.0420.md)`
  - What does “size of TCB” mean? `(Slides.SGX.0420.md)`
  - What is “accountable decryption”? `(Slides.SGX.0420.md)`
  - What is endorsement key? `(Slides.SGX.0420.md)`
- Privacy CA
  - What is “Privacy CA”? `(Slides.SGX.0420.md)`
  - How does the Solution 1 “Privacy CA for provisioning ak” work? Please list the steps. `(Slides.SGX.0420.md)`
- Launch Enclave
  - What is “Launch Enclave”? `(Slides.SGX.0420.md)`
  - Is Launch Enclave a software? `(Slides.SGX.0420.md)`
  - Does Launch Enclave run in OS? `(Slides.SGX.0420.md)`
  - Does the binary of Launch Enclave reside in BIOS or ME? `[title]` `(Slides.SGX.0420.md)`
  - Is Launch Enclave provided by another vendor (No Intel)? `(Slides.SGX.0420.md)`

Q & A

Slideshow - Intro to Intel SGX

Question: Below slideshow is “Intro to Intel SGX” `(Slides.SGX.0420.md)`

Answer: … …

My Questions

Question: Why is Intel SGX not suited for password managers? `(Slides.SGX.0420.md)`

Answer:

Intel SGX is not well-suited for password managers primarily because of its limitations in handling input/output (I/O) operations. Password managers usually require user interaction for entering master passwords, copying generated passwords, and auto-filling login forms. These actions involve I/O operations that are outside the scope of the enclave’s protected environment.

In addition, Intel SGX is vulnerable to certain side-channel attacks, which can potentially leak sensitive information, such as passwords or encryption keys, by analyzing the access patterns of the CPU cache or other hardware resources. While Intel SGX provides strong isolation and protection against software-based attacks, it cannot completely secure applications that require sensitive I/O operations, such as password managers or banking apps.

However, this does not mean that Intel SGX is entirely useless for such applications. It can still be used to enhance specific aspects of these applications, like securing the storage and processing of sensitive data within the enclave. But, due to the I/O limitations and side-channel vulnerabilities, it is not a comprehensive solution for securing password managers or similar applications.

Question: What does “size of TCB” mean? `(Slides.SGX.0420.md)`

Answer:

“Size of TCB” refers to the size of the Trusted Computing Base. The Trusted Computing Base is a term used in computer security to describe the set of all hardware, firmware, and software components that are critical to a system’s security. The TCB is responsible for enforcing the security policies of a system, and its integrity is crucial to maintain the overall security of the system.

The size of the TCB is an important consideration because it generally correlates with the potential attack surface and the complexity of the system. A smaller TCB typically indicates a more focused and manageable set of components, which can be more easily analyzed, verified, and secured. On the other hand, a larger TCB can introduce more potential vulnerabilities and make it more difficult to ensure the security of the system.

In the context of hardware security mechanisms, like Intel SGX, a smaller TCB may provide stronger protection against attacks, as there are fewer components that could be exploited. Reducing the size of the TCB is one of the primary goals in designing secure systems, as it helps to minimize the attack surface and the potential for security vulnerabilities.

Question: What is “accountable decryption”? `(Slides.SGX.0420.md)`

Answer:

Accountable decryption is a concept in cryptography that aims to ensure that the decryption of encrypted data can be traced back to a specific party or entity. This concept is often employed in systems where multiple parties have access to the decryption keys, and it’s important to know who decrypted the data for various reasons, such as security, auditing, or legal compliance.

In an accountable decryption scheme, the decryption process generates a unique proof or decryption tag that can be used to identify the party responsible for the decryption. This proof or tag is often linked to the decryption key or the party’s identity in a way that cannot be forged or tampered with. This allows for the attribution of decryption actions to specific parties, enabling better control and monitoring of access to sensitive information.

Accountable decryption can be implemented through various cryptographic techniques, including threshold cryptography, digital signatures, and zero-knowledge proofs. The choice of technique depends on the specific requirements and the overall system design.

Question: What is endorsement key? `(Slides.SGX.0420.md)`

Answer:

An endorsement key (EK) is a unique, private cryptographic key that is embedded within a security device or module, such as a Trusted Platform Module (TPM) or a hardware security module (HSM). This key is generated during the manufacturing process and is paired with a corresponding public key. The private portion of the endorsement key is never exposed outside of the secure environment and is used to prove the authenticity and integrity of the device.

The public portion of the endorsement key is typically used along with a certificate issued by the manufacturer, which serves as a proof of the device’s authenticity. This certificate is called the endorsement certificate and is used to establish trust in the device’s identity during secure communications or attestation processes.

In summary, the endorsement key is a fundamental component of hardware-based security solutions, as it helps to establish trust and verify the authenticity of a device or module in secure communications and attestation scenarios.

Privacy CA

Question: What is “Privacy CA”? `(Slides.SGX.0420.md)`

Answer:

A Privacy Certification Authority (Privacy CA) is a trusted third-party entity that issues digital certificates in a privacy-preserving manner. Privacy CAs play a crucial role in remote attestation processes for secure hardware platforms, such as

Intel SGX (Software Guard Extensions) and Trusted Platform Modules (TPMs).

The main purpose of a Privacy CA is to verify the authenticity and integrity of a secure hardware platform or an enclave (in the case of Intel SGX) without revealing sensitive information about the platform or enclave to other parties. The Privacy CA is responsible for validating the identity and measurements of the secure platform, and then issuing a digital certificate as proof of the platform's trustworthiness.

In this process, the Privacy CA acts as an intermediary between the secure platform and the external party seeking to establish a trusted communication channel. The Privacy CA helps to maintain the confidentiality of the platform's sensitive information while still providing the necessary level of assurance to the external party.

For example, in the context of Intel SGX, the Privacy CA is the Intel Attestation Service (IAS). The IAS issues digital certificates for Intel SGX enclaves after verifying their authenticity and integrity based on measurements provided by the enclave during the remote attestation process.

Question: How does the Solution 1 "Privacy CA for provisioning ak" work? Please list the steps. `(Slides.SGX.0420.md)`

Answer:

"Privacy CA for provisioning ak" refers to using a Privacy Certification Authority (Privacy CA) to provision an Attestation Key (ak) for a TPM (Trusted Platform Module) while maintaining the privacy of the device. The process allows a TPM to interact with third parties without disclosing its unique identity. Here are the steps involved in this solution:

1. TPM generates an Attestation Key (ak) pair: The TPM generates a public-private key pair intended for use in attestation. The private part of the key remains within the TPM, while the public part is shared externally.
2. TPM creates an Attestation Key Certificate Request: The TPM generates a certificate signing request (CSR) for the public portion of the Attestation Key. This request typically includes information about the TPM, such as its public Endorsement Key (EK) and the desired ak.
3. Privacy CA verifies TPM identity: The Privacy CA receives the CSR and verifies the authenticity of the TPM using the provided public EK and the corresponding endorsement certificate issued by the TPM manufacturer. The Privacy CA may also check other information, such as the platform's conformance to certain security standards.
4. Privacy CA issues an Attestation Key Certificate: Once the Privacy CA is satisfied with the TPM's authenticity, it signs the CSR and generates an Attestation Key Certificate. This certificate is then sent back to the TPM.
5. TPM receives and stores the Attestation Key Certificate: The TPM securely stores the Attestation Key Certificate, linking the ak to a trusted Privacy CA. This certificate can be used in future attestation processes to establish trust with third parties.

In summary, using a Privacy CA for provisioning an Attestation Key (ak) involves generating an ak pair within the TPM, creating a CSR for the public ak, verifying the TPM's identity by the Privacy CA, issuing an Attestation Key Certificate, and securely storing this certificate in the TPM. This process allows the TPM to prove its authenticity and integrity while preserving its privacy.

Launch Enclave

Question: What is "Launch Enclave"? `(Slides.SGX.0420.md)`

Answer:

A Launch Enclave is a secure environment in the context of Intel Software Guard Extensions (SGX), a set of security-related instruction codes that are built into some Intel processors. The Launch Enclave is responsible for verifying and controlling the launch of other secure enclaves within the SGX environment.

In Intel SGX, enclaves are isolated, protected memory regions that run sensitive code and store sensitive data. They are designed to protect the confidentiality and integrity of this information from external threats, even in the presence of compromised operating systems or hardware.

The Launch Enclave is a special enclave provided by Intel that plays a crucial role in the SGX ecosystem. When an application wants to create and run a new enclave, it must first request the Launch Enclave to create a launch token. The

Launch Enclave verifies the new enclave's identity and attributes, and if everything is in order, it creates the launch token. This token is then used by the application to launch the new enclave.

By controlling the launch of other enclaves, the Launch Enclave helps maintain the security and integrity of the SGX environment. It ensures that only trusted and authorized enclaves can be created and executed, thus preventing rogue enclaves from compromising the security of the system.

Question: Is Launch Enclave a software? `(Slides.SGX.0420.md)`

Answer:

Yes, the Launch Enclave is a software component provided by Intel as part of the Intel Software Guard Extensions (SGX) framework. It is designed to run within the secure environment of an Intel SGX-enabled processor.

The Launch Enclave is a specific enclave with predefined functionality that manages the creation and launch of other secure enclaves within the SGX environment. By acting as a gatekeeper, the Launch Enclave helps ensure that only authorized and trusted enclaves are executed, maintaining the overall security of the system.

Question: Does Launch Enclave run in OS? `(Slides.SGX.0420.md)`

Answer:

The Launch Enclave runs within the secure environment provided by Intel SGX, which is a set of security-related instruction codes built into Intel processors. While it is not part of the operating system (OS) itself, it does interact with the OS through a set of APIs and drivers.

The OS plays a role in managing the resources and interactions between the untrusted, non-secure part of the system and the secure enclave environment. In this sense, the Launch Enclave does run on a system with an OS, but it operates within the protected enclave environment provided by the Intel SGX, isolated from the untrusted portion of the OS.

Question: Does the binary of Launch Enclave reside in BIOS or ME? `[title]` `(Slides.SGX.0420.md)`

Answer:

The binary of the Launch Enclave does not reside in the BIOS or the Intel Management Engine (ME). The Launch Enclave is a part of the Intel SGX software stack, which is installed on the operating system. The Intel SGX software stack includes the Intel SGX SDK and Platform Software (PSW).

The Launch Enclave is loaded as part of the Intel SGX runtime system when an application wants to create a new enclave. The Launch Enclave binary is signed by Intel, and its primary purpose is to verify and manage the launch of other enclaves, ensuring that they have been signed with an authorized launch key.

While the Launch Enclave is not directly part of the BIOS or ME, both the BIOS and ME play a role in enabling Intel SGX on the system. The BIOS must support and properly configure the hardware for Intel SGX, and the Intel ME is responsible for managing security features and providing cryptographic services to the system, including those related to Intel SGX.

Question: Is Launch Enclave provided by another vendor (No Intel)? `(Slides.SGX.0420.md)`

Answer:

No, the Launch Enclave is provided by Intel as part of the Intel SGX software stack. Intel is responsible for signing the Launch Enclave binary and distributing it as a part of the Intel SGX SDK and Platform Software (PSW). This is an important aspect of the SGX security model, as it allows Intel to maintain control over the trustworthiness of the Launch Enclave and ensure that only authorized enclaves can be launched on SGX-enabled systems.
