Hello World

zhuangh7

2019 年 12 月 13 日

1 Introduction

Intel SGX 技术提供了一系列的硬件特性, 帮助保护应用免受操作系统、hypervisor、BIOS 和其他软件的伤害。应用程序可以整个或者部分的放入到 enclave 中运行

2 威胁模型

Graphene-SGX 的威胁模型与典型的 SGX 应用的威胁模型类似。下列的组件是不被信任的:

1) 除 CPU 之外的硬件。

2) 操作系统、hypervisor 和其他的系统软件。

3) 在 enclave 之外跟其他 enclave 之内运行的应用程序。

4) 同一应用程序的 enclave 之外的部分。

Graphene-SGX 只信任 CPU, 还有 enclave 内部的代码。还必须信任 Intel 的 SGX SDK 中的 aesmd 工具，该工具验证 enclave 签名中的属性并批准 enclave 的创建。这是现在利用 SGX 技术的所有工作都必须信任的。除此之外，Graphene-SGX 还使用了 Intel SGX 的驱动程序，但是不信任他。Graphene-SGX 不使用 SDK 中的其他部分。

3 保证的安全性质和能够防御的一些具体攻击

3.1 保证的安全性质

3.2 能防御的具体攻击

4 性能、可扩展性（scalability）、灵活性等分析

4.1 灵活性

由于 Graphene-SGX 可以直接在 enclave 上运行没有经过修改的 Linux 程序，因此，通过 Graphene-SGX 可以快速的帮助现有应用利用到 SGX 的 enclave 这一特性，提高已有应用的安全性，而同时不需要付出太大的开发成本。

4.2 性能分析

4.3 scalability

5 不足（至少包含两点）

无法防御一些攻击 Denial of service,sidechannels,controlled-channel attacks 这些攻击是目前所有的 SGX 平台都难以防御的，Graphene-SGX 同样无法处理。