Intel SGX e Criptografia Homomórfica

Gabriel G. Milan[1], **Natã S. Carvalho**[1], **Brenno Rodrigues**[1]

[1]Departamento de Engenharia Eletrônica e de Computação – Universidade Federal do Rio de Janeiro (UFRJ)
21.941-909 – Rio de Janeiro – RJ – Brasil

Abstract. *This document is the report of a work of the discipline of "Information Security"(NCG020) at the Federal University of Rio de Janeiro (UFRJ). The work consists of conducting research on the Intel SGX platform and homomorphic cryptography, in order to obtain brief knowledge of these subjects.*

Resumo. *Esse documento é o relatório de um trabalho da disciplina de "Segurança da Informação" (NCG020) na Universidade Federal do Rio de Janeiro (UFRJ). O trabalho consiste em realizar uma pesquisa sobre a plataforma Intel SGX e criptografia homomórfica, a fim de obter breve conhecimento nesses assuntos.*

1. Introdução à Intel SGX

A Intel SGX consiste em particionar informações confidenciais em "enclaves", como denominado pela própria Intel, que são áreas de execução na memória com maior proteção.

A plataforma, que nasceu devido à dificuldade dos desenvolvedores de garantir segurança em suas aplicações, promete:

- Aumentar integridade e confidencialidade;
- Atestar e provisionar remotamente;
- Ajudar a reduzir significativamente maneiras de ataque;
- Baixa curva de aprendizado.

Denominando-se uma nova abordagem, embasa-se em incrementos na arquitetura do hardware, com instruções específicas para segurança de aplicações.

Como pode ser visto na Figura 1, em tempo de execução, as instruções constroem e executam os enclaves em uma região especial e cifrada da memória com acesso restrito definida pelo desenvolvedor. Isso ajuda a prevenir vazamento de dados, uma vez que tudo que está contido nos enclaves é cifrado e possui sua integridade verificada.

Na Figura 1, os números significam:

1. Aplicação construída com partes seguras (SGX) e partes não-seguras;
2. Quando o aplicativo roda, cria a enclave, que é colocada na área segura de memória;
3. Quando uma função segura é chamada, a execução transita para a enclave;
4. A enclave consegue visualizar todos os dados de maneira plana, ainda que impedindo acesso externo não autorizado;
5. A função retorna, mantendo os dados sensíveis na região protegida da memória;
6. A aplicação continua seu curso normal.

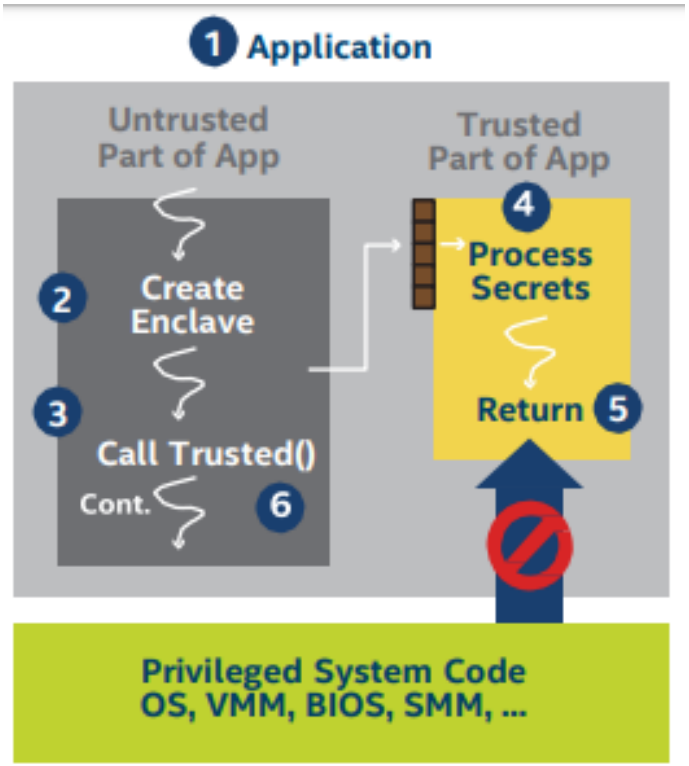

Figura 1. Execução

2. Casos de uso da Intel SGX

A Intel cita alguns casos de uso interessantes para sua plataforma, vistos a seguir:

2.1. Gerenciamento de chaves

Usar enclaves para ajudar a gerenciar chaves criptográficas e fornecer funcionalidades semelhantes a de um HSM.

2.2. Blockchain

Ajuda a aumentar a privacidade e segurança para o processamento de transações, consenso, contratos inteligentes e armazenamento de chaves.

2.3. Aplicações em tempo de execução

Permite executar aplicações sem nenhuma alteração dentro de enclaves.

2.4. Proteção de conteúdo aprimorada por hardware

Ajuda proprietário de conteúdo a proteger seus IPs por meio de streaming inalterado ou não modificado.

2.5. Carteiras digitais

Pode ser usada para garantir mais segurança em transações monetárias.

2.6. IoT

Pode permitir uma conexão mais segura com dispositivos IoT. [Intel 2019]

3. Criptografia Homomórfica

3.1. Motivação

Como o significativo aumento da capacidade computacional em nuvem, a demanda por estes serviço vem aumentando consideravelmente. Empresas usam estas soluções para viabilizar a infraestrutura uma vez que não é necessário investir em máquinas robustas que atendam os requisitos necessários para executar suas tarefas. Como citado pelo professor Cláudio Miceli diversas vezes em aula, hoje em dia, é perfeitamente plausível desenvolver em qualquer linguagem e para qualquer plataforma usando serviços em nuvem.

Mas e quanto ao sigilo dos dados que são executados em aplicações em nuvem? Eis aí a principal motivação para o desenvolvimento de uma tecnologia que permita que, por exemplo, dois números escolhidos por Alice sejam somados por Bob sem que ele conheça tais números.

Este é o conceito de criptografia homomórfica, "possibilitar que dados possam ser processados por computadores de terceiros sem correr o risco que estes sejam lido."[Filho 2010]

3.2. Criptossistemas parcialmente homomórfico e completamente homomórfico

Um criptossistema é dito parcialmente homomórfico se satisfizer a definição de homomorfismo para a operação de adição ou de multiplicação. Do inglês, Partially Homomorphic Encryption - PHE.[Alves 2014]

Um criptossistema é dito completamente homomórfico se satisfizer a definição de homomorfismo para as operações de adição e multiplicação. Do inglês, Fully Homomorphic Encryption - FHE.[Alves 2014]

3.3. Vantagens e desvantagens

Como foi dito anteriormente, uma das vantagens é poder armazenar ou processar dados em computadores de terceiros sem que os mesmos tenham acesso aos dados. Porém, outras aplicações podem ser beneficiadas por esta técnica como leilões eletrônicos, onde um participante pode dar lances mas não quer que os demais conheçam o valor do lance para não incentivar ofertas maiores. Através de um esquema totalmente homomórfico, o leiloeiro poderá saber quem ganhou o leilão. Com isso, é garantido a confidencialidade dos dados.

Em contrapartida, devido a capacidade computacional necessária para para realizar operações em grande escala, esta técnica enfrenta grandes desafios de implementação. Uma busca simples aumentaria o tempo computacional por volta de um trilhão de vezes.

Haverá também um discussão a cerca privacidade e Big Data visto que uma vez implementada a criptografia homomórfica, muitos dados gerados não serão visualizados pelas ferramentas de análise de dados. Garante a privacidade do usuário porém atrapalha por exemplo, a distribuição de conteúdo personalizado.[de Medeiros Paiva 2015]

3.4. Considerações finais

Trabalhos de pequisas vem sendo feitos ao longo dos anos para otimizar as cifras de encriptação na expectativa de acelerar a viabilidade da aplicação. Podemos destacar Victor Shoup e Shai Halevi membros do IBM T.J. Watson Reaserch Center que lançaram

um biblioteca chamada Helib que encontra-se disponível para pesquisadores sob licença pública.[de Medeiros Paiva 2015]

Referências

Alves, P. (2014). Aplicação conceitual de criptografia homomórfica.

de Medeiros Paiva, G. C. (2015). Criptografia homomorfica e suas aplicacoes.

Filho, P. (2010). O que é criptografia homomórfica.

Intel (2019). Enhanced security features for applications and data in-use.