Proposta de Mestrado

Plataforma de computação confidencial com SGX

Orientador: André Zúquete (andre.zuquete@ua.pt)
Coorientador: Tomás Oliveira e Silva (tos@ua.pt)
Colaborador: José Neto Vieira (jnvieira@ua.pt)

Curso: MCS, MEI, MECT, MIECT

Enquadramento

As ligações à rede Wi-Fi da UA permitem saber com alguma precisão a localização dos seus utentes. Esta informação pode ser útil para vários fins, como maiores ou menores graus de invasão da privacidade dos utentes da rede. A extração de informação a partir dos dados originais (em bruto) levanta o problema do acesso aos mesmos para fins que não os desejados, ou mesmo abusivos. Este problema pode ser resolvido através do que se designa como computação confidencial. Esta usa ambientes especiais, como o SGX da Intel, onde código devidamente autorizado e autenticado pode receber dados cifrados de uma maneira que só ele consegue decifrar e produzir informação agregada útil que não viole garantias de privacidade.

Objetivos

Neste trabalho pretende-se usar a plataforma SGX e os seus enclaves para executar aplicações autorizadas para produzir informação agregada considerada útil para a UA a partir de dados em bruto de acessos à rede Wi-Fi. Um exemplo de informação agregada útil consiste no número de alunos por sala de aula, sem referência a quem são esses alunos. Outro poderá ser a distribuição do número de aulas efetivamente frequentadas por cada aluno de uma turma de uma UC ao longo de um semestre. A extração destes indicadores usando aplicações com computação confiável sobre SGX levantam alguns problemas, como os limites materiais da memória útil disponível para um enclave SGX, que não dispõe de swapping. Assim, o ambiente de execução a desenvolver deverá fornecer algumas primitivas úteis para vários programas, como sejam monitores de ocupação de memória, a ingestão de dados cifrados do exterior a partir de várias origens, a produção de dados resultantes para vários destinos, sendo que uma dessas origens e destinos poderá ser algo similar a uma área de *swap* (para lidar com problemas de escassez de memória interna do enclave) ou a um *snapshot* (por exemplo, para ir fazendo computações diárias com os registos desse dia ao longo de um semestre sem que o programa tenha de estar a funcionamento permanente).

Tarefas

1. Estudo do SGX e dos seus mecanismos de segurança.
2. Estudo de uma arquitetura genérica para processar muitos dados em bruto de uma vez ou ao longo de muito tempo.

3. Desenvolvimento de uma aplicação para prova de conceito.
4. Extração de informação usando dados em bruto e validação dos mesmos.
5. Escrita da dissertação.

[1] Intel® Software Guard Extensions (Intel® SGX), https://www.intel.com/content/www/us/en/products/docs/accelerator-engines/software-guard-extensions.html