ISEL
DEETC
Departamento de Engenharia Electrónica e Telecomunicações e de Computadores

Mestrado em Engenharia de Eletrónica e Telecomunicações
Mestrado em Engenharia Informática e de Computadores
Mestrado em Engenharia Informática e Multimédia
Ano letivo 2021/2022 – Semestre de Inverno

Cibersegurança

Módulo 3 - Segurança no Hardware

Trabalho de Avaliação

Objetivo

Este trabalho tem como objetivo a exploração da tecnologia Intel Software Guard Extensions (SGX) para a realização de uma carteira eletrónica (e-walllet) simples, destinada ao armazenamento seguro das credenciais de acesso a plataformas informáticas.

Especificação

Pretende-se que a aplicação a desenvolver permita a gestão de até 100 credenciais de acesso diferentes, para o que deverá disponibilizar ao utilizador, no mínimo, as seguintes funcionalidades: 1) criar uma carteira, 2) mostrar o conteúdo da carteira; 3) adicionar credenciais à carteira, 4) eliminar credenciais da carteira e 5) gerar senhas de acesso, com um número de caracteres compreendido no intervalo 8 a 100.

Considera-se que uma credencial de acesso é constituída por um nome de utilizador, no máximo com 100 caracteres, a correspondente senha de acesso, com um número de caracteres compreendido no intervalo 8 a 100, e uma descrição identificativa do seu cenário de utilização, no máximo com 100 caracteres.

Para garantir a persistência da informação gerida pela carteira, todos os dados deverão ficar armazenados em ficheiro. Dada a natureza sensível desta informação, o acesso à carteira deverá ser protegido por uma senha de acesso, com um número de caracteres compreendido também no intervalo 8 a 100, e todos os dados armazenados no ficheiro, incluindo a senha de acesso, devem ser cifrados com cifra AES-GCM de 128-bits.

Realização

O trabalho a realizar deve ser baseado na aplicação disponibilizada [1], desenvolvida em linguagem C, que deverá ser alterada para garantir a confidencialidade e a integridade dos dados guardados na carteira recorrendo à tecnologia Intel SGX. Para tal, pretende-se que as partes da aplicação que lidam com os dados sensíveis sejam executadas num enclave SGX e utilizar a funcionalidade de selagem para o armazenamento da carteira em ficheiro [2].

Recomenda-se a minimização da base de computação confiável (em inglês, a *Trusted Computing Base* – TCB) da aplicação, por forma a reduzir a sua superfície de ataque e, dessa forma, restringir-se as possibilidades de ataque e aumentar-se a segurança da aplicação.

Nota: Na realização deste trabalho pode utilizar o código analisado e desenvolvido nas aulas teórico-práticas.

Entrega

O trabalho deve ser entregue via plataforma Moodle até às 23:59:59 do dia 10 de janeiro de 2022.

Aquando da submissão do trabalho deverão ser entregues os seguintes dois elementos: 1) o relatório do trabalho, em formato PDF, com uma descrição, sucinta, dos elementos relevantes para a compreensão do trabalho realizado e as conclusões extraídas; e 2) um ficheiro ZIP com todo o código fonte do programa desenvolvido, devidamente indentado e comentado.

Referências

[1] Dias, T. M. (2020). *Wallet* [Computer software]. https://2122moodle.isel.pt/pluginfile.php/1140606/mod_assign/introattachment/0/ewallet.zip

[2] Intel Corporation. (2020). Intel Software Guard Extensions (Intel SGX) SDK for Linux OS - Developer Reference. Santa Clara, CA: Intel Corporation.