Instituto Superior de Engenharia de Lisboa

Cibersegurança

E-Wallet

Mestrado em Engenharia Informática de Multimédia

Pedro Gonçalves, 45890

Rodrigo Dias, 45881

Rúben Santos, 49063

Semestre de Inverno, 2021/2022

1. Introdução

O objetivo deste projeto consiste na atualização de uma aplicação de criação, gestão e edição de uma carteira virtual com itens, de forma a que todas as operações que interajam com dados sensíveis sejam feitas de forma segura, do ponto de vista do hardware, mais concretamente do **CPU**. Para isso, tirar-se-á partido da tecnologia **Enclave**. Um **Enclave** permite que o código de uma aplicação seja isolado de qualquer entidade com previlégios, e permite que a a memória associada seja encriptada.

A aplicação em si já está implementada e funciona. O objetivo é utilizar o **Enclave** para isolar todas as operações sensíveis, tornando-a mais segura.

2. Problema

Para que se possa definir devidamente as operações a passar para o lado do **Enclave**, dever-se-á, primeiro, analisar a aplicação e perceber que tipo de operações efetua, interpretando-as e concluindo se devem ser isoladas no **Enclave** ou não.

A aplicação não-segura permite as seguintes operações:

- Gerar password aleatória (especifica-se o tamanho) – Sensível: Os números aleatórios deverão ser gerados de forma segura, no lado do enclave, de forma a que os caracteres da password gerada não sejam intercetados e comprometidos;
- Alterar password da carteira (tem de ser fornecida a anterior) – Sensível: Envolve o acesso ao ficheiro **'ewallet.db'**, que contém informação sensível;
- Adicionar item - Sensível: Envolve o acesso ao ficheiro **'ewallet.db'**, que contém informação sensível;
- Remover item - Sensível: Envolve o acesso ao ficheiro **'ewallet.db'**, que contém informação sensível;
- Guardar carteira (para um ficheiro) – Sensível: Utilizando as bibliotecas ***standard*** do **C**, esta operação só pode ser realizada no lado da aplicação. Nos capítulos consequentes será abordada uma possível solução para este problema.
- Carregar carteira (de um ficheiro) – Sensível: Utilizando as bibliotecas ***standard*** do **C**, esta operação só pode ser realizada no lado da aplicação. Nos capítulos consequentes será abordada uma possível solução para este problema.
- Verificar se já existe uma carteira criada;
- Criar uma carteira – Sensível: Envolve o acesso ao ficheiro **'ewallet.db'**, que contém informação sensível;
- Mostrar carteira – Sensível: Envolve o acesso ao ficheiro **'ewallet.db'**, que contém informação sensível;
- Imprimir carteira – Sensível: A impressão de informação para a consola só pode ser realizada no lado da aplicação. Nos capítulos consequentes será abordada uma possível solução para este problema.
- Mostrar ajuda;
- Mostrar versão.

Todas as operações sensíveis deverão ser efetuadas no lado do **Enclave**.

3. Solução

De forma a utilizar as funções das bibliotecas ***standard*** do **C**, tanto para impressão de informação na consola, como para acesso a ficheiros, optou-se por utilizar as funções de ***sealing*** estudadas nas aulas teórico-práticas, para cifrar a carteira. Ou seja, sempre que se manuseia a carteira no lado da aplicação, esta deverá estar cifrada para que não seja comprometida. Assim, a informação que é escrita e lida do ficheiro **'ewallet.db'** estará sempre cifrada.

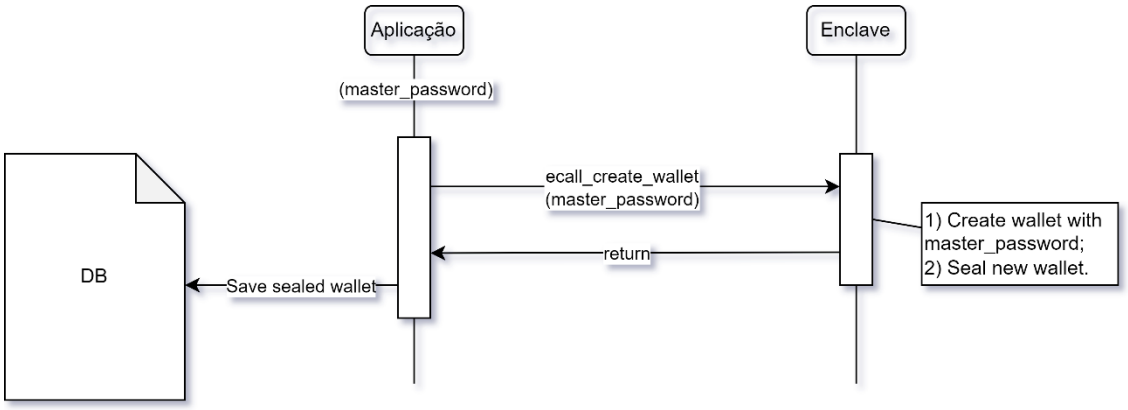
Sempre que seja pretendido criar, editar ou remover a carteira esta deve ser enviada (através de uma chamada **ECALL**) ao Enclave para que seja decifrada e manuseada. Depois, a função **ECALL** que manuseou a carteira deverá voltar a cifrá-la (já com os dados atualizados) para que seja novamente enviada para o lado da aplicação, onde será guardada novamente no ficheiro **'ewallet.db'**.

No que toca à impressão da informação contida na carteira, o Enclave irá efetuar uma chamada **OCALL** a uma função que realiza o ***printf()*** standard da linguagem **C**.

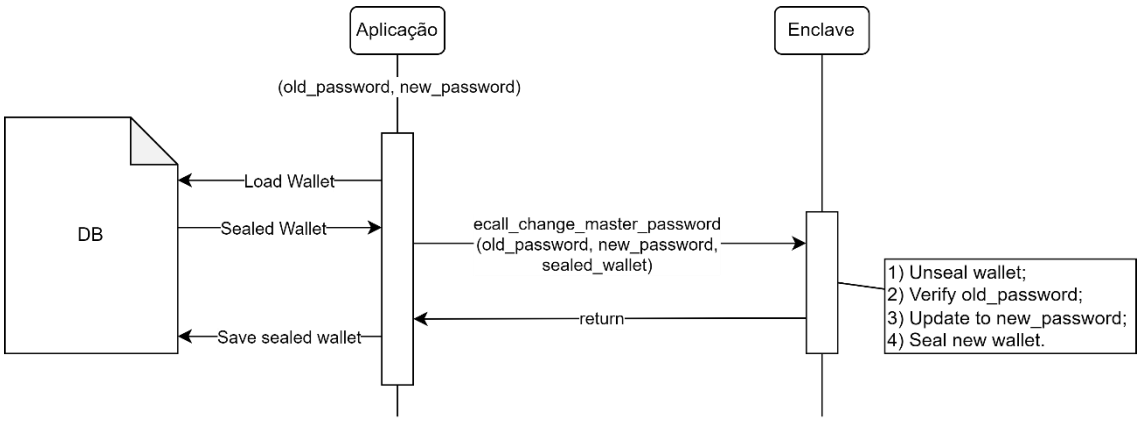
3.1. Casos de Utilização

Nos subcapítulos seguintes, ilustram-se alguns casos de utilização relativos a algumas das operações discutidas anteriormente. Pretende-se mostrar a parte do código que é efetuada do lado da aplicação (não-seguro) e do lado do Enclave (seguro).

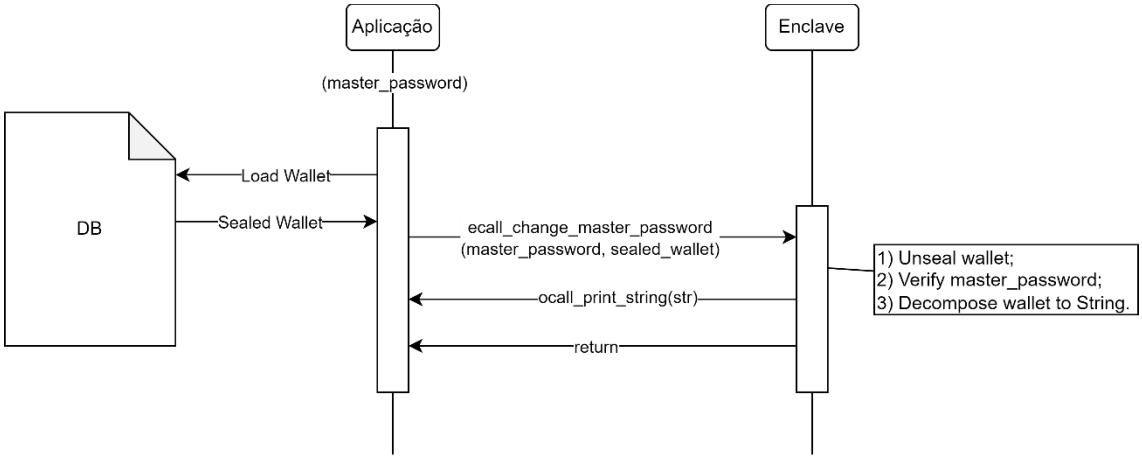
3.1.1. Criar Carteira



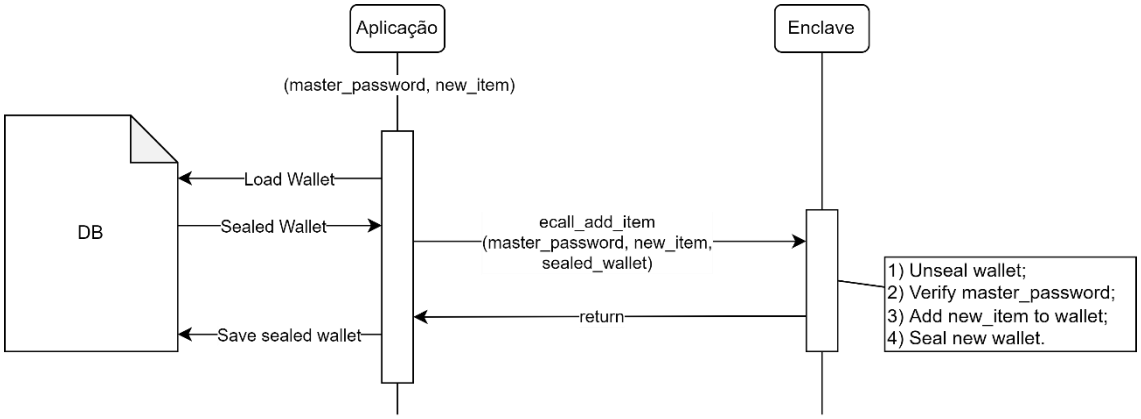
3.1.2. Atualizar Password da Carteira



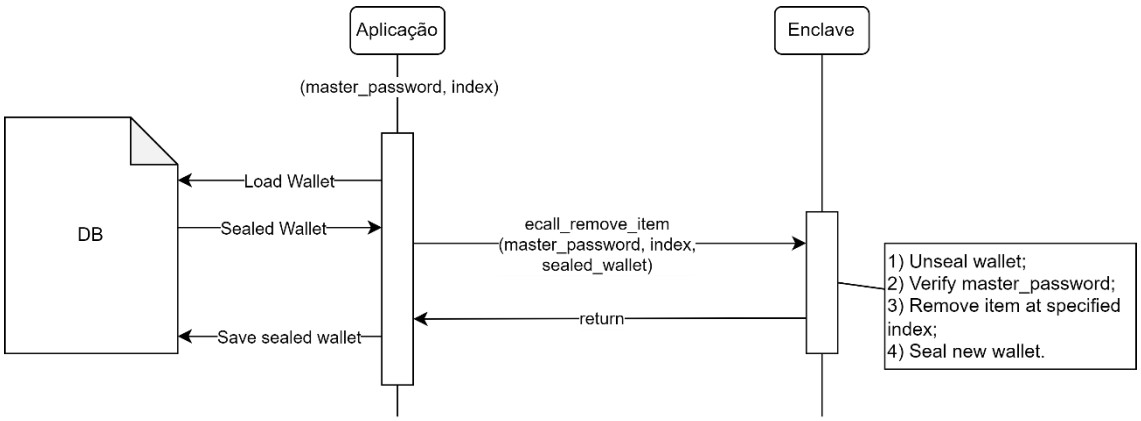
3.1.3. Mostrar Carteira



3.1.4. Adicionar Item



3.1.5. Remover Item



4. Conclusão

A segurança e persistência de informação sensível em aplicações não é garantida apenas com base em métodos de segurança do software, bibliotecas e sistema operativo. A ciência da cibersegurança deverá cobrir também outras superfícies de ataque como o próprio hardware. A aplicação **E-Wallet** tornou-se mais segura, visto que a superfície de ataque foi reduzida.