Universidade do Minho
Escola de Engenharia

Mestrado em Engenharia Informática

Ano letivo 2024/2025

Engenharia de Segurança

Cofre Digital - Trabalho Prático #1

Requisitos do sistema

Grupo 04

Eduardo Cunha - PG55939
João Rodrigues - PG57880

Índice

1 Introdução

Este documento surge na sequência da descrição da aplicação Cofre Digital, assim como da identificação de ameaças e da análise de risco previamente realizadas. O seu principal objetivo é proceder ao levantamento dos requisitos do sistema, organizando-os em duas categorias: requisitos iniciais e requisitos refinados. Com base na ideia inicial do projeto, foi possível identificar um conjunto de requisitos preliminares, os quais foram posteriormente aprofundados e ajustados à medida que a solução técnica foi sendo desenvolvida.

É importante salientar que esta distinção não implica que os requisitos iniciais não tenham sido revistos. Tal como referido no documento anterior, este trabalho segue um processo de natureza cíclica e iterativa, pelo que o refinamento contínuo de ideias e requisitos é não só natural, como desejável. Foi precisamente essa característica iterativa que motivou a divisão do trabalho em documentos distintos, permitindo um acompanhamento mais claro e estruturado da evolução do projeto.

A metodologia adotada para o levantamento de requisitos baseou-se numa combinação de análise de caso, sessões de brainstorming colaborativo e validação contínua ao longo do desenvolvimento da solução. Esta abordagem permitiu identificar necessidades essenciais desde o início, bem como ajustar e integrar novos requisitos de forma consistente à medida que o projeto avançava.

2 Levantamento de requisitos inicias

Nesta etapa, identificamos e analisamos os requisitos, classificando-os em duas categorias essenciais: os requisitos funcionais, que definem as capacidades e comportamentos do sistema, servindo principalmente de referência para a fase seguinte de implementação do sistema, e os requisitos de segurança, que garantem a integridade, confidencialidade e proteção contra ameaças, sendo estes o foco principal do trabalho.

2.1 Requisitos funcionais

Gestão de Utilizadores

- RF1: O sistema deve permitir o registo de novos utilizadores
- RF2: Cada utilizador deve ser identificado por um ID único e um endereço de email único
- RF3: O sistema deve armazenar as credenciais de acesso definidas durante o registo
- RF4: O sistema deve permitir a autenticação de utilizadores existentes

Gestão de Dados

- RF5: O sistema deve permitir o armazenamento de dois tipos de recursos: ficheiros e pastas
- RF6: O sistema deve permitir a adição de ficheiros no cofre digital
- RF7: O sistema deve permitir a criação de pastas, as quais poderão ser utilizadas para armazenar e organizar recursos, como ficheiros ou subpastas.
- RF8: O sistema deve atribuir um único proprietário (owner) a cada recurso, correspondendo ao utilizador que o criou. Este será o detentor do recurso e terá controlo total sobre o mesmo, incluindo permissões de acesso, partilha e eliminação.
- RF9: O sistema deve permitir a leitura de ficheiros armazenados aos utilizadores que detenham permissão para tal.
- RF10: O sistema deve permitir a modificação de ficheiros armazenados aos utilizadores com permissão adequada para o fazer.
- RF11: O sistema deve permitir listar o conteúdo de pastas aos utilizadores que possuam permissão para aceder às mesmas.

- RF12: O sistema deve permitir adicionar novos recursos a pastas existentes, aos utilizadores que detenham permissões de escrita sobre essas pastas.

Controlo de Acesso

- RF13: O sistema deve implementar três níveis de permissões: leitura (read), extensão (append) e escrita (write)
- RF14: O sistema deve permitir ao proprietário de um recurso atribuir permissões de acesso a outros utilizadores, permitindo o controlo sobre quem pode visualizar ou modificar o recurso.
- RF15: O sistema deve permitir ao proprietário modificar as permissões atribuídas a outros utilizadores
- RF16: O sistema deve permitir ao proprietário remover permissões atribuídas a outros utilizadores

Interface de Utilizador

- RF17: O sistema deve fornecer uma aplicação cliente (CLI) para interação com o servidor
- RF18: A CLI deve suportar comandos para todas as operações disponibilizadas aos utilizadores
- RF19: O sistema deve fornecer feedback claro ao utilizador após a execução de operações, apresentando mensagens de sucesso em caso de conclusão bem-sucedida e mensagens de erro genéricas, sem revelar detalhes internos, em caso de falha.

2.2 Requisitos de segurança

Autenticação

- RS1: O sistema deve verificar as credenciais de autenticação do utilizador, garantindo que apenas utilizadores autenticados tenham acesso às suas contas.
- RS2: As credenciais de autenticação devem ser transmitidas de forma segura
- RS3: O sistema deve implementar mecanismos de segurança para prevenir ataques à autenticação, incluindo proteção contra força bruta e deteção de acessos suspeitos.

Proteção de Dados

- RS4: O conteúdo dos ficheiros deve ser cifrado no cliente antes de ser enviado para o servidor
- RS5: O servidor não deve ter acesso ao conteúdo dos ficheiros armazenados
- RS6: O servidor deve verificar a integridade dos dados armazenados

Controlo de Acesso

- RS7: O servidor deve aplicar a política de controlo de acesso definida para cada recurso, garantindo que os utilizadores e entidades acedam apenas aos recursos para os quais têm permissão.
- RS8: O sistema deve validar as permissões antes de permitir qualquer operação sobre os recursos
- RS9: O sistema deve implementar mecanismos de monitorização e deteção de modificações não autorizadas nos recursos.

Auditoria

- RS10: O sistema deve registar todas as operações realizadas sobre os recursos.
- RS11: Os registos de auditoria devem, no mínimo, incluir as seguintes informações: o utilizador que realizou a operação, o timestamp (data e hora), a operação executada e, quando aplicável, o recurso afetado.
- RS12: Os registos de auditoria devem ser protegidos contra modificação não autorizada.

Gestão de Chaves

- RS14: O sistema deve implementar um mecanismo seguro para a geração, armazenamento e gestão de chaves criptográficas.

- RS15: O sistema deve implementar um mecanismo seguro para partilha de chaves entre utilizadores autorizados
- RS16: O sistema deve permitir a rotação de chaves para minimizar o impacto de possíveis comprometimentos

Comunicação Segura

- RS17: A comunicação entre a aplicação cliente e o servidor deve ser cifrada, garantindo confidencialidade e integridade dos dados transmitidos.

3 Requisitos adicionais refinados para implementação

Nesta secção serão apresentados requisitos levantados e refinados numa fase posterior ao levantamento dos apresentados anteriormente, inclusive durante o desenvolvimento do protótipo.

- Utilizar *multi-threading* para garantir consistência e desempenho em ambientes concorrentes.
- Utilizar o algoritmo bcrypt ou Argon2 para armazenar as palavras-passe de forma segura.
- Implementar um limite de tentativas de autenticação.
- O e-mail do utilizador deve ser validado como um endereço consistente e válido, por exemplo, através da utilização de uma expressão regular (regex).
- Adicionar pequenos atrasos após tentativas falhadas (utilizar sleep, tendo em conta que o servidor é multi-threaded), para dificultar ataques de força bruta.
- Implementar limpeza periódica dos registos de tentativas de login falhadas.
- Implementar um sistema de tempo limite (timeout) que encerra automaticamente sessões inativas após um período configurável, aumentando a segurança contra acessos não autorizados.
- Limitar o número de sessões ativas por utilizador.
- Estabelecer uma profundidade máxima para a estrutura de diretórios, evitando cenários excessivamente complexos que possam comprometer a eficiência do sistema.
- Estabelecer um tamanho máximo para ficheiros e pastas, de forma a não comprometer a eficiência e o desempenho do sistema.
- Apenas ficheiros de texto simples serão permitidos para upload, armazenamento e manipulação, garantindo compatibilidade, segurança e simplicidade na gestão de conteúdos.
- Garantir a validação adequada dos dados recebidos (por exemplo, utilizar psycopg2) para prevenir injeções de código SQL.
- Implementar rate limiting por utilizador e por endereço IP.
- Garantir que a palavra-passe introduzida no formulário de login é ofuscada (modo password/blur).
- Permitir ao utilizador remover a sua conta (exige verificação) mediante a confirmação do e-mail e palavra-passe. Esta ação deverá eliminar todos os ficheiros associados ao seu cofre, bem como todas as permissões atribuídas.
- Para conceder permissões, é necessário: o ID do ficheiro/pasta, o e-mail do utilizador e o nível de permissão. O sistema deve verificar a existência do utilizador e do ficheiro/pasta, bem como confirmar que quem está a conceder permissões é o proprietário do recurso.
- Os logs devem ser guardados em ficheiros cifrados. Apenas o servidor terá permissão para ler e escrever nestes ficheiros.

- Caminhos sensíveis e credenciais devem ser guardados como variáveis de ambiente.
- É permitida a entrada direta em pastas sem passar pela estrutura hierárquica completa. Isto permite atribuir permissões a subpastas específicas. No entanto, se um utilizador entrar diretamente numa subpasta, não poderá navegar para a pasta-mãe, uma vez que a entrada não foi feita pela hierarquia principal (como se a subpasta não tivesse pai).
- O sistema deverá impedir a tentativa de entrada em pastas onde o utilizador já se encontra.