Universidade do Minho
Escola de Engenharia

Mestrado em Engenharia Informática

Ano letivo 2024/2025

Engenharia de Segurança

Cofre Digital - Trabalho Prático #1

Análise de ameaças

Grupo 04

Eduardo Cunha - PG55939
João Rodrigues - PG57880

Índice

1 Introdução 1
2 Descrição do Cofre Digital 1
2.1 Aspetos de Segurança 1
2.2 Arquitetura do Cofre Digital 2
2.3 Diagrama de Fluxo de Dados 2
3 Ameaças ao Cofre Digital 3
3.1 Spoofing (Falsificação de Identidade) 3
3.2 Tampering (Adulteração) 3
3.3 Repudiation (Repúdio) 3
3.4 Information Disclosure (Divulgação de Informação) 3
3.5 Denial of Service (Negação de Serviços) 3
3.6 Elevation of Privilege (Elevação de Privilégios) 3
3.7 Vulnerabilidades Associadas (OWASP Top 10) 4
4 Análise de risco 4
4.1 Metodologia de Análise 4
4.2 Análise detalhada das ameaças 5
4.2.1 Ameaças de Spoofing 5
4.2.2 Ameaças de Tampering (Adulteração) 5
4.2.3 Ameaças de Repudiation (Repúdio) 6
4.2.4 Ameaças de Information Disclosure (Divulgação de Informação) 7
4.2.5 Ameaças de Denial of Service (Negação de Serviço) 7
4.2.6 Ameaças de Elevation of Privilege (Elevação de Privilégios) 8
5 Referências 9

1 Introdução

O presente trabalho tem como objetivo o desenvolvimento de uma aplicação, um cofre digital, com foco especial na sua segurança. Está organizado em três documentos distintos: o presente documento, que descreve o funcionamento do cofre digital, a análise de ameaças e a avaliação de riscos; um segundo documento que apresenta os requisitos extraídos do sistema; e um terceiro que detalha a análise da solução proposta, já numa fase avançada de integração. A decisão de dividir o trabalho em vários documentos deu-se devido à natureza cíclica da metodologia adotada, uma vez que não existe uma ordem linear ou fixa para as etapas do processo, sendo este iterativo por definição.

Neste relatório, é inicialmente apresentada a aplicação em questão. De seguida, procede-se à identificação e análise de ameaças utilizando a metodologia STRIDE. Por fim, é realizada uma avaliação de risco com base num modelo quantitativo que cruza probabilidade e impacto.

2 Descrição do Cofre Digital

Este projeto tem como objetivo desenvolver um Cofre Digital, uma solução segura onde os utilizadores podem armazenar ficheiros com as respetivas políticas de acesso. A interação com o sistema será realizada através de uma aplicação cliente (CLI), que comunicará com um servidor responsável pela gestão das funcionalidades.

Para utilizar o sistema, os utilizadores devem registar-se, ficando associados a um identificador e um endereço de email, ambos únicos. Durante o registo, estabelecem as suas credenciais de acesso, que serão posteriormente utilizadas para autenticação e interação com o Cofre Digital.

Cada utilizador dispõe de um cofre pessoal, onde pode armazenar e gerir informação de forma segura. O sistema suporta dois tipos de recursos: ficheiros, que contêm informação arbitrária, e pastas, utilizadas para organizar os ficheiros e definir políticas de acesso hierárquicas. Cada recurso tem um único dono, que corresponde ao utilizador que o criou.

O controlo de acesso é gerido pelo proprietário do recurso, que define as permissões atribuídas a outros utilizadores. Por defeito, apenas o dono tem acesso, podendo este conceder diferentes níveis de permissão: read, que permite ler ficheiros ou listar o conteúdo de pastas; append, que possibilita adicionar conteúdo a um ficheiro ou inserir novos elementos numa pasta; e write, que autoriza a modificação de ficheiros ou a reestruturação de pastas.

A aplicação cliente fornece os comandos necessários para executar todas as operações no sistema, enquanto o servidor é responsável por processar os pedidos e garantir um funcionamento seguro e eficiente.

2.1 Aspetos de Segurança

A segurança do Cofre Digital assenta em vários princípios fundamentais. A comunicação entre o cliente e o servidor deve ser protegida, garantindo a confidencialidade e a integridade dos dados, de forma a impedir o acesso por entidades externas ou utilizadores não autorizados. O servidor é responsável por assegurar que as políticas de acesso são rigorosamente cumpridas, permitindo que apenas os utilizadores devidamente autorizados possam aceder ou modificar recursos, conforme as permissões definidas pelo seu proprietário.

Além disso, a confidencialidade dos dados deve ser preservada, garantindo que o servidor não tem acesso ao conteúdo dos ficheiros armazenados. Para reforçar a segurança e permitir uma gestão transparente do sistema, é essencial assegurar a auditabilidade, garantindo que todas as operações realizadas possam ser rastreadas.

2.2 Arquitetura do Cofre Digital

Sem querer entrar em demasiados pormenores sobre a aplicação, de forma a evitar compromissos prematuros que possam não se concretizar, idealizamos essencialmente a aplicação como um servidor com uma única base de dados.

Temos consciência de que esta abordagem torna a base de dados um ponto único de falha. No entanto, acreditamos que a sua distribuição aumentaria significativamente a superfície de ataque. Assim, consideramos que este trade-off entre disponibilidade e segurança é vantajoso, dado que o foco principal é precisamente a segurança.

Outra abordagem estudada seria a utilização de uma base de dados em conjunto com um servidor de armazenamento, onde os ficheiros seriam guardados de forma cifrada e a base de dados conteria as respectivas chaves de cifra. Esta solução reforçaria a segurança, mas, devido à complexidade da sua implementação, nesta fase optamos por manter a abordagem inicial de uma base de dados única para armazenar todos os dados da aplicação.

2.3 Diagrama de Fluxo de Dados

Com base na arquitetura definida anteriormente, criámos um Diagrama de Fluxo de Dados (DFD) para representar de forma clara e visual o funcionamento da aplicação.

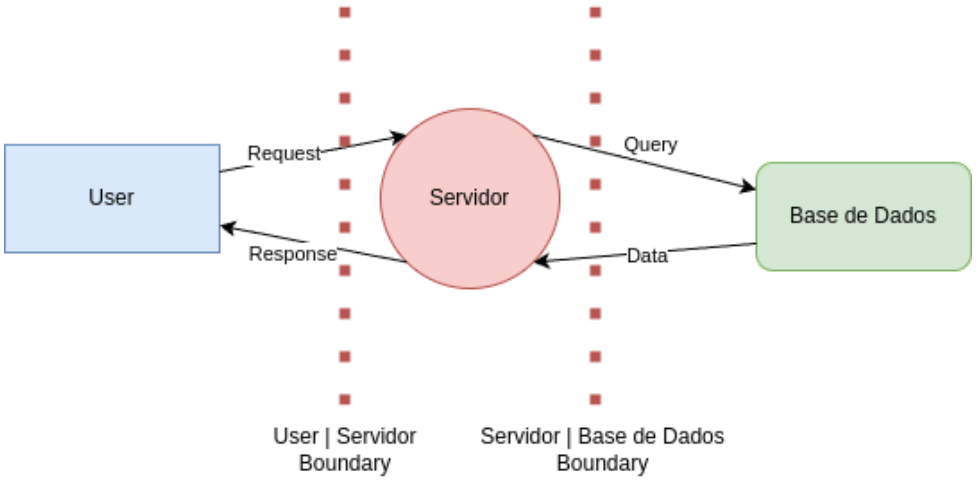

Figura 2: Diagrama de Fluxo do Sistema

Neste diagrama, é possível identificar os principais fluxos de informação e os componentes críticos da aplicação. Destacamos os seguintes aspetos essenciais:

- **Interação do Utilizador com o Servidor:** Envolve operações como autenticação, envio e recuperação de ficheiros, e gestão de permissões.
- **Comunicação entre o Servidor e a Base de Dados:** O servidor armazena e recupera informações essenciais, incluindo metadados dos ficheiros, credenciais cifradas e políticas de acesso.
- **Registo de Atividade:** Todas as interações relevantes são registadas para permitir auditoria e deteção de acessos indevidos.
- **Validação de Permissões:** Antes de qualquer operação, o servidor verifica se o utilizador tem as permissões adequadas para aceder ou modificar um recurso.

Este DFD ajuda a compreender as relações entre os diferentes componentes e realça a importância da segurança nas comunicações e no armazenamento de dados.

3 Ameaças ao Cofre Digital

No contexto do Cofre Digital, a identificação de ameaças é um passo fundamental para garantir que a aplicação é concebida e desenvolvida com um nível elevado de segurança desde a sua base. Para tal, recorremos à metodologia ***STRIDE***, uma abordagem amplamente reconhecida na área da segurança informática para a análise sistemática de ameaças em sistemas digitais.

3.1 Spoofing (Falsificação de Identidade)

- Falsificação de Credenciais: Roubo ou obtenção indevida de credenciais com o objetivo de aceder sem autorização e assumir a identidade de utilizadores legítimos, incluindo técnicas como phishing e ataques de força bruta.
- Sequestro de Sessão: Obtenção e utilização indevida de tokens de sessão válidos para personificar utilizadores autenticados

3.2 Tampering (Adulteração)

- Comprometimento da Integridade de Dados: Modificação não autorizada de ficheiros, estruturas de pastas e permissões de acesso
- Adulteração de Comunicações: Interceptação e modificação das comunicações entre cliente e servidor (MITM)
- Manipulação de Registos: Alteração ou eliminação de registos de auditoria para ocultar atividades maliciosas

3.3 Repudiation (Repúdio)

- Falhas de Responsabilização: Negação de operações realizadas devido a deficiências nos registos de auditoria.
- Assinaturas Digitais Inexistentes ou Ineficazes: Ausência ou utilização inadequada de mecanismos criptográficos que assegurem, de forma fiável, a autoria e a integridade de transações ou de alterações a dados sensíveis.

3.4 Information Disclosure (Divulgação de Informação)

- Acesso Não Autorizado a Dados Confidenciais: Acesso indevido a ficheiros sem permissões adequadas
- Comprometimento da Criptografia: Exposição ou roubo de chaves de cifragem usadas para proteger dados
- *Leak* de Dados: Exposição de informações sensíveis através de side-channels, comunicações inseguras ou metadados

3.5 Denial of Service (Negação de Serviços)

- Indisponibilidade do Sistema: Sobrecarga do servidor, esgotamento de recursos de armazenamento ou bloqueio de recursos
- Corrupção de Dados: Danos à integridade dos dados que podem comprometer o funcionamento do sistema ou resultar em perda de informações

3.6 Elevation of Privilege (Elevação de Privilégios)

- Contorno de Controlos de Acesso: Bypass de verificações de autorização ou manipulação de políticas de acesso

- Exploração de Vulnerabilidades: Utilização de falhas de segurança no servidor ou na aplicação para obter privilégios superiores aos originalmente atribuídos ao utilizador.
- Abuso de Funcionalidades: Injeção de comandos maliciosos ou uso indevido de privilégios administrativos

3.7 Vulnerabilidades Associadas (OWASP Top 10)

- A01:2021 - Falhas de Controlo de Acesso: Afeta políticas de acesso e proteção de dados
- A02:2021 - Falhas Criptográficas: Compromete a segurança de credenciais e dados confidenciais
- A03:2021 - Injeção: Permite manipulação de *input* de dados e comandos
- A05:2021 - Falhas de Configuração: Impactam a segurança da infraestrutura
- A06:2021 - Componentes Vulneráveis: Afetam a infraestrutura do servidor
- A07:2021 - Falhas de Autenticação: Compromete credenciais e sessões
- A09:2021 - Falhas de Registo e Monitorização: Dificulta a deteção de atividades maliciosas

4 Análise de risco

4.1 Metodologia de Análise

Para realizar a análise de risco do Cofre Digital, foi adotada uma abordagem quantitativa baseada na fórmula: **Risco = Probabilidade × Impacto**.

Esta metodologia permite avaliar de forma objetiva a gravidade de cada ameaça identificada, atribuindo-lhe um valor numérico resultante da combinação da probabilidade de ocorrência com o impacto que poderá ter no sistema.

Tendo em conta que o risco resulta diretamente da multiplicação entre a probabilidade e o impacto de uma ameaça, definimos uma metodologia de avaliação baseada numa escala de 1 a 5 para cada uma destas categorias (escala oficial do NIST), com os níveis descritos da seguinte forma:

Níveis de Probabilidade

- **Nível 1:** Praticamente impossível de ocorrer, requer condições extremamente específicas.
- **Nível 2:** Ocorrência extremamente improvável, barreira significativa para exploração.
- **Nível 3:** Possível sob certas circunstâncias, requer alguns recursos ou conhecimentos especializados.
- **Nível 4:** Provável de acontecer, condições relativamente acessíveis para exploração.
- **Nível 5:** Quase certo de ocorrer, condições amplamente disponíveis, múltiplos vetores de ataque

Níveis de Impacto

- **Nível 1:** Efeitos quase irrelevantes, sem prejuízo para utilizadores ou sistema.
- **Nível 2:** Efeitos limitados, afeta poucos componentes do sistema.
- **Nível 3:** Consequências relevantes, afeta processos importantes.
- **Nível 4:** Danos consideráveis, comprometimento de funcionalidades críticas.
- **Nível 5:** Danos extensivos, potencial colapso do sistema, consequências financeiras severas

Níveis de risco

Com base no valor resultante da multiplicação entre a probabilidade e o impacto (num intervalo de 1 a 25), o risco será classificado numa escala que varia de “Muito Baixo” a “Crítico”. Os níveis de risco

são distribuídos da seguinte forma: um valor entre 1 e 3 indica um risco muito baixo, entre 4 e 8 um risco baixo, entre 9 e 14 um risco médio, entre 15 e 19 um risco alto, e entre 20 e 25 um risco crítico.

Segue então a matriz de riscos:

Probabilidade/Impacto	1	2	3	4	5
1	1 (Muito Baixo)	2 (Muito Baixo)	3 (Muito Baixo)	4 (Baixo)	5 (Baixo)
2	2 (Muito Baixo)	4 (Baixo)	6 (Baixo)	8 (Médio)	10 (Médio)
3	3 (Muito Baixo)	6 (Baixo)	9 (Médio)	12 (Médio)	15 (Alto)
4	4 (Baixo)	8 (Médio)	12 (Médio)	16 (Alto)	20 (Crítico)
5	5 (Baixo)	10 (Médio)	15 (Alto)	20 (Crítico)	25 (Crítico)

Tabela 1: Matriz de níveis de risco.

4.2 Análise detalhada das ameaças

4.2.1 Ameaças de Spoofing

Falsificação de Credenciais
Probabilidade: 4 (Provável) • Ataques de phishing e força bruta são comuns e relativamente acessíveis • Credenciais fracas ou reutilizadas aumentam a vulnerabilidade
Impacto: 5 (Danos extensivos) • Acesso total aos dados confidenciais do utilizador • Potencial para comprometer todos os dados armazenados no cofre
Risco: 20 (Crítico)

Sequestro de Sessão
Probabilidade: 3 (Possível) • Requer conhecimentos especializados e condições específicas • Depende de vulnerabilidades na gestão de sessões
Impacto: 5 (Danos extensivos) • Permite acesso não autorizado sem necessidade de credenciais • Personificação completa do utilizador legítimo
Risco: 15 (Alto)

4.2.2 Ameaças de Tampering (Adulteração)

Comprometimento da Integridade de Dados
Probabilidade: 3 (Possível) • Requer acesso ao sistema com certos privilégios • Dependente de falhas nos mecanismos de controlo de acesso
Impacto: 4 (Danos consideráveis) • Modificação de ficheiros críticos • Desorganização da estrutura de dados
Risco: 12 (Médio)

Adulteração de Comunicações
Probabilidade: 3 (Possível) • Ataques MITM requerem posicionamento estratégico na rede • Mais difícil com protocolos seguros implementados corretamente
Impacto: 5 (Danos extensivos) • Intercepção de dados confidenciais em trânsito • Possibilidade de execução de comandos manipulados
Risco: 15 (Alto)

Manipulação de Registos
Probabilidade: 2 (Improvável) • Requer acesso privilegiado aos sistemas de logging • Sistemas de log bem projetados dificultam esta ameaça
Impacto: 4 (Danos consideráveis) • Eliminação de rastos de atividades maliciosas • Comprometimento da capacidade de auditoria
Risco: 8 (Baixo)

4.2.3 Ameaças de Repudiation (Repúdio)

Falhas de Responsabilização
Probabilidade: 2 (Improvável) • Sistemas modernos geralmente implementam registos robustos • Modificação de timestamps requer acesso privilegiado
Impacto: 3 (Consequências relevantes) • Dificuldade em atribuir responsabilidade por ações maliciosas • Problemas para reconstruir eventos em investigações
Risco: 6 (Baixo)

Assinaturas Digitais Inexistentes ou Ineficazes
Probabilidade: 3 (Possível) • Algumas integrações podem não implementar mecanismos adequados de assinatura digital
Impacto: 4 (Elevado) • Permite que utilizadores neguem a autoria de ações importantes, como transações ou decisões, sem provas concretas. • Pode comprometer a integridade e a confiança nos registos digitais, dificultando a responsabilização em caso de incidentes.
Risco: 12 (Moderado)

4.2.4 Ameaças de Information Disclosure (Divulgação de Informação)

Acesso Não Autorizado a Dados Confidenciais
Probabilidade: 3 (Possível) • Requer exploração de vulnerabilidades específicas • Depende de falhas no controlo de acesso
Impacto: 5 (Danos extensivos) • Violação direta da confidencialidade dos dados protegidos • Potencial exposição de todas as informações armazenadas
Risco: 15 (Alto)

Comprometimento da Criptografia
Probabilidade: 2 (Improvável) • Requer conhecimentos especializados avançados • Sistemas bem projetados protegem adequadamente as chaves
Impacto: 5 (Danos extensivos) • Permite decifrar todos os dados confidenciais • Compromete completamente a segurança do sistema
Risco: 10 (Médio)

Leak de Dados
Probabilidade: 4 (Provável) • Side-channels e metadados são frequentemente negligenciados • Podem ocorrer mesmo em sistemas bem protegidos
Impacto: 4 (Danos consideráveis) • *Leak* potencial de informações sensíveis • Normalmente limitado a subconjuntos de dados ou metadados
Risco: 16 (Alto)

4.2.5 Ameaças de Denial of Service (Negação de Serviço)

Indisponibilidade do Sistema
Probabilidade: 4 (Provável) • Ataques DoS são relativamente comuns e acessíveis • Múltiplos vetores possíveis (sobrecarga, esgotamento de recursos)
Impacto: 3 (Danos relevantes) • Interrupção temporária do serviço • Perda de acesso aos dados durante o ataque
Risco: 12 (Médio)

Corrupção de Dados
Probabilidade: 2 (Improvável) • Sistemas modernos implementam medidas de proteção • Requer acesso privilegiado ou vulnerabilidades específicas
Impacto: 5 (Danos extensivos) • Perda potencial de dados críticos • Pode afetar a integridade de todo o sistema
Risco: 10 (Médio)

4.2.6 Ameaças de Elevation of Privilege (Elevação de Privilégios)

Contorno de Controlos de Acesso
Probabilidade: 3 (Possível) • Requer falhas específicas no sistema de autorização • Vulnerabilidades de configuração podem facilitar
Impacto: 4 (Danos consideráveis) • Acesso não autorizado a recursos protegidos • Violação das políticas de segurança estabelecidas
Risco: 12 (Médio)

Exploração de Vulnerabilidades
Probabilidade: 3 (Possível) • Depende da manutenção e atualização do sistema • Requer conhecimentos técnicos específicos
Impacto: 5 (Danos extensivos) • Controlo total potencial sobre o servidor • Possível acesso a todos os dados armazenados
Risco: 15 (Alto)

Abuso de Funcionalidades
Probabilidade: 3 (Possível) • Requer implementação inadequada de validação de entrada • Vulnerabilidades em interfaces de comando são comuns
Impacto: 4 (Danos consideráveis) • Execução de operações não autorizadas • Potencial para comprometer componentes críticos
Risco: 12 (Médio)

5 Referências

- National Institute of Standards and Technology (NIST). National Vulnerability Database (NVD). Disponível em: https://nvd.nist.gov
- MITRE Corporation. Common Vulnerabilities and Exposures (CVE). Disponível em: https://cve.mitre.org
- MITRE Corporation. Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK). Disponível em: https://attack.mitre.org
- OWASP Foundation. The Open Worldwide Application Security Project (OWASP). Disponível em: https://owasp.org
- National Institute of Standards and Technology (NIST). Computer Security Resource Center (CSRC). Disponível em: https://csrc.nist.gov
- OWASP Foundation. OWASP Cheat Sheet Series. Disponível em: https://cheatsheetseries.owasp.org
- Mozilla Foundation. Mozilla Web Security Guidelines. Disponível em: https://infosec.mozilla.org/guidelines/web_security
- OWASP Foundation. OWASP GitHub Repository. Disponível em: https://github.com/OWASP