Relatório Password Vault

Segurança da Informação – Analise e Desenvolvimento de Sistemas – CST

Jessé Ricardo Rogério
Kauê dos Santos Rocha

12 de junho de 2025

Sumário

Introdução

No mundo digital, a segurança de dados é um dos pilares mais críticos e em constante evolução. Porém, atualmente, múltiplos indivíduos utilizadores da internet ainda usam senhas fracas, repetem-nas em todas as suas credenciais e até armazenam-nas em locais inseguros, como localmente em arquivos de texto. Além disso, são possíveis vítimas de ataques cibernéticos e engenharia social.

Diante desse cenário, os *password vaults*, ou em português – **cofres de senhas**, surgem como uma solução relativamente eficiente para resolver tais problemas.

1.1 Objetivos

Esse relatório possui os seguintes objetivos:

- Explicar o funcionamento técnico por trás dos *password vaults,* apontado criptografia, autenticação e mais.
- Comparar diferentes tipos desses gerenciadores, exemplificando e demonstrando pontos positivos e negativos de cada.
- Analise de vulnerabilidades & um caso real (LastPass 2022), visando mostrar os impactos sobre essa tecnologia.
- E por fim, fornecer orientações praticas para utilização de um cofre de senhas em uma interação com uma simples aplicação *Java – Spring Boot.*

1.2 Justificativa

Este relatório busca conscientizar o publico geral a partir de recomendações de segurança, que foram baseadas no fato que para pessoas comuns, gerenciadores de senhas simplificam a vida digital, eliminando a necessidade de decorar múltiplas senhas, evitam senhas fracas e em geral, praticas de melhoram entropia & conveniência geral. Já para empresas, gerenciadores podem ser essenciais, isso devido a diferentes motivos como: leis de proteção de dados, vazamentos de dados e ate ataques de *phishing* e afins.

Fundamentação Teórica

2.1 Armazenamento Criptográfico

A criptografia AES-256 (Advanced Encryption Standard com chave de 256 bits) é amplamente reconhecida como um dos padrões mais seguros atualmente disponíveis para proteção de dados sensíveis. Ela é utilizada para garantir que todas as informações armazenadas em banco de dados — seja em servidores locais ou soluções em nuvem — estejam protegidas contra acessos não autorizados. Os dados são criptografados antes mesmo de serem gravados, assegurando sua confidencialidade em repouso. Mesmo que um invasor tenha acesso físico ao banco de dados, não poderá interpretar os dados sem a chave de criptografia correta.

2.2 Senha Mestra (Master Password)

A senha mestra é a única credencial necessária para desbloquear o acesso ao cofre de senhas do usuário. Por isso, ela é tratada com extrema cautela e nunca é armazenada diretamente, nem mesmo em formato criptografado. Em vez disso, técnicas de hashing robustas como PBKDF2, Argon2 ou bcrypt são utilizadas para derivar uma representação segura da senha, tornando impraticáveis ataques de força bruta. Além disso, aplica-se o conceito de *Zero-Knowledge Proof*, no qual o provedor do serviço nunca possui acesso à senha mestra, garantindo que, mesmo em caso de violação dos servidores, os dados criptografados permaneçam inacessíveis.

2.3 Autenticação Multi-Fator (MFA/2FA)

A autenticação multifator (MFA) adiciona uma camada adicional de proteção além da senha mestra, exigindo um segundo fator de verificação para acesso ao sistema. Esse segundo fator pode variar entre tokens gerados por aplicativos autenticadores (como Google Authenticator), códigos enviados por SMS, chaves físicas (como YubiKey) ou autenticação biométrica. Essa abordagem reduz drasticamente os riscos decorrentes de senhas comprometidas, pois um invasor precisaria também do segundo fator para obter acesso. A combinação de “algo que o usuário sabe” (senha) com “algo que ele possui” (token ou dispositivo), muitas vezes obrigatório.

2.4 Geração de Senhas Aleatórias

O sistema implementa a geração de senhas seguras por meio de algoritmos de geração pseudoaleatória criptograficamente seguros (CSPRNG), assegurando alta entropia e imprevisibilidade. Esse recurso é essencial para criar credenciais fortes e únicas para cada serviço utilizado pelo usuário, evitando o reuso de senhas. O processo de geração considera também a compatibilidade com requisitos específicos de plataformas, permitindo customizações como evitar caracteres ambíguos ou atender regras de complexidade. Essas senhas são copiadas muitas vezes, de forma autônoma para os requerimentos do sites.

2.5 Controle Central

O controle central em gerenciadores de senhas permite monitorar atividades como horários de acesso, IPs autorizados e políticas de segurança (ex.: exigir MFA para logins suspeitos). Tokens de acesso temporários e revogáveis garantem permissões granulares, enquanto “logs” detalhados facilitam auditorias. Isso assegura gestão e controle.

Tipos de Password Vaults

Tipo	Exemplos	Vantagens	Desvantagens
Localmente	KeePass, Bitwarden	Controle total, imune a vazamentos	Sem sincronização entre dispositivos, necessita backup manual
Nuvem	LastPass, 1Password	Sincronização automática	Risco de vazamento em nuvem
Navegador	Google Password Manager	Integração fácil com navegadores & Conveniente	Criptografia menos robusta
Hardware	YubiKey, Trezor	Extremamente resistente a Malware	Custo elevado, perda física = perda de senhas & backup

3.1 Local

Utilizados geralmente por empresas de maneira interna. Escolha para empresas que preferem manter a arquitetura e o código seguros e com sigilo, como: empresas financeiras (bancos, fintechs). Desejável, pois não necessita de conexões estáveis com a internet pública, porém com custos iniciais mais altos, isso devido à manutenção, implementação, melhorias e ensino de uso. Soluções implementadas manualmente.

3.2 Nuvem

Extremamente popular com empresas, salvam dados já criptografados em servidores, permitindo acesso em qualquer localidade e dispositivo (autorizado), o que permite colaboração entre indivíduos de empresas digitais de diferentes locais. Geralmente envolve um modelo de pagamentos (mensais/anuais) e assinaturas. É facilmente escalável verticalmente (mais capacidade) e horizontalmente (mais máquinas/nós), pois utiliza recursos externos ao projeto. A segurança é terceirizada ao provedor e plano.

3.3 Navegador

Conveniente e usado em navegadores como: Firefox, Google Chrome e Safari. Foca principalmente no usuário, permitindo não apenas o salvamento de senhas, mas também de dados próprios como nome, endereço e mais. Não é usado por empresas e não tem custo ao usuário. Senhas não são sincronizadas entre navegadores. Inseguro para dispositivos compartilhados.

3.4 Hardware

Dispositivos físicos, geralmente “pen drives”. Têm um custo maior por incluir meios físicos. São vítimas de roubos, porém as credenciais podem ser retiradas/apagadas. Geralmente usados para acesso a contas/bancos de dados.

Metodologia

Este relatório adota uma metodologia mista, analisando tanto aspectos qualitativos (documentação da OWASP e estudos de caso como o incidente LastPass 2022) quanto testes práticos utilizando “Hashicorp Vault”, visando fornecer recomendações práticas para fortalecer a segurança digital para indivíduos não técnicos quanto os do mundo corporativo e técnicos.

Caso Real – LastPass 2022

Essa seção indica um exemplo real de como uma vulnerabilidade de *password vaults* foi utilizada para um ataque de acesso & prevenções/aprendizado por trás.

5.1. O Ataque

Detectado em agosto de 2022, a empresa “LastPass”, provedora de cofres de senhas, detectou uma série de atividades suspeitas, anunciando logo em seguida o vazamento de dados. De acordo com pesquisas internas, o “hacker” utilizou *phishing* (e-mails/mensagens que se passam por e-mails verdadeiros; funciona ao clicar e inserir credenciais em sites falsos) e, devido à falta de configuração de 2FA (MFA) por parte do engenheiro, conseguiu interagir com os dados salvos na nuvem e localmente. Porém, devido à estrutura de “Zero-Knowledge Proof”, apenas dados parcialmente não criptografados foram vazados.

5.2. Lições Aprendidas

A empresa enfatizou a utilização obrigatória de 2FA, indicando no mesmo relatório de ataque que senhas mestres devem ser entropicamente fortes. Definindo novas metas de segurança na empresa, essas sendo proteção contra falhas humanas (engenharia social):

- 2FA obrigatório
- Senhas mestres entropicamente fortes
- Proteção contra engenharia social

Atividades Praticas

As atividades praticas podem ser feitas através das instruções em: https://github.com/jesse-rr/pv

Conclusão

Concluindo, os *password vaults* são essenciais para segurança digital, permitindo gerenciar senhas complexas de forma centralizada, enquanto apenas exigem por uma senha mestra robusta e o uso de 2FA para máxima proteção. Embora não sejam perfeitos, reduzem significativamente os riscos de vazamentos por senhas fracas ou repetidas, a escolha de um serviço confiável com criptografia forte é crucial. Sua adoção é recomendação básica para qualquer usuário ou empresa preocupada com segurança cibernética.

Referências

OWASP. Password Storage Cheat Sheet. https://cheatsheetseries.owasp.org/.

Wikipedia. Password Manager. https://en.wikipedia.org/wiki/Password_manager.

1Password. Enterprise Password Vaults Guide. https://blog.1password.com/enterprisepassword-vaults-guide/.

Hashicorp/vault. https://hub.docker.com/r/hashicorp/vault

Hashicorp Developer. https://developer.hashicorp.com/vault

LastPass blog. https://blog.lastpass.com/posts/notice-of-recent-security-incident

Deepseek (LLM) – Auxilio em erros de português e formatação do relatório, slides & atividade pratica. https://www.deepseek.com/