Password Vaults - HashiCorp Vault

Jessé Rogério, Kauê Rocha

O que é um Password Vault?

Também chamado de Password Manager, são ferramentas para armazenar múltiplas senhas de forma segura, usando apenas **uma senha mestra.**

O termo se aplica a desde aplicações standalone locais simples até soluções empresariais compreensivas.

Para nossa apresentação, estudamos o **HashiCorp Vault.**

Por que usar um Password Vault?

- Evitar fadiga de senha
- Geração de senhas fortes
- Armazenamento seguro e criptografado de senhas
- Acesso de senhas em múltiplos dispositivos
- Preenchimento automático de senhas em sites/apps

Tipos diferentes 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

Sobre a HashiCorp

A HashiCorp é uma empresa fundada em 2012, e oferece uma gama compreensiva de produtos para para infraestrutura de TI.

Em 2021 a HashiCorp foi publicada pela primeira vez na bolsa de valores, avaliada em 13 bilhões de dólares, e posteriormente adquirida pela IBM em 2024 por 6.4 bilhões.

Em 2015, é lançada a primeira versão do Vault: um software open-source e gratuito com features empresariais pagas.

HashiCorp Vault - Modos de armazenamento

Permite múltiplos tipos de armazenamento:

- Integrado (o padrão, baseado em um backend distribuído com clusters de dados replicados via o algoritmo de consenso Raft para alta disponibilidade e escalabilidade)
- No sistema de arquivos, armazenado localmente
- Externo (hospedado em cloud)
- Em memória (sem persistência, usado para desenvolvimento)

HashiCorp Vault - Autenticação

- Segredos dinâmicos: credenciais temporárias com tempo de vida curto
- Suporta diversos métodos de autenticação baseada em identidade para usuários humanos (LDAP, GitHub, TLS, OpenID Connect, Radius)
- ...e também para aplicações (Microsoft Azure, Kubernetes, Google Cloud Platform, AWS IAM)
- Para qualquer acesso de leitura/escrita, bem-sucedido ou não, há logs de auditoria.

HashiCorp Vault - Criptografia

Criptografia como Password Manager:

- Para Dados em Repouso (Data at Rest), usa AES-256, modo GCM
- Para Dados em Trânsito (Data in Transit): usa TLS (Transport Layer Security)

Criptografia como Serviço (CaaS):

- Transit Secrets Engine: usado em desenvolvimento como provedor criptográfico, sem acesso da aplicação às chaves (que ficam no Vault).
- Suporta uma gama mais ampla de algoritmos simétricos (AES-GCM, ChaCha20-Poly1305), assimétricos para assinatura (Ed25519, ECDSA, RSA) e funções de hashing (SHA, HMAC).

HashiCorp Vault - Chave mestra

- Nunca é armazenada de forma persistente: só em RAM quando “unsealed”
- Gerenciada de forma fragmentada: Shamir's Secret Sharing (manual)
  - Criam-se fragmentos da chave mestra, a serem distribuidos a administradores distintos
  - Usa-se um número mínimo de fragmentos para deslacrar o vault
- Ou unsealing automático (Auto-Unseal)
  - Não fragmenta a senha para maior automação/velocidade de retorno do serviço
  - Usa um KMS (Key Manager Service) OU um HSM (Hardware Security Module)
  - Chave mestra Nunca armazenado no próprio vault de maneira persistente

Vulnerabilidades de Password Vaults - LastPass 2022

Contexto

Em agosto de 2022, atividades suspeitas e vazamento de dados reportados pela empresa LastPass.

Causa & Vulnerabilidade

Phishing (e-mails falsos) e ausência de 2FA no acesso de um engenheiro.

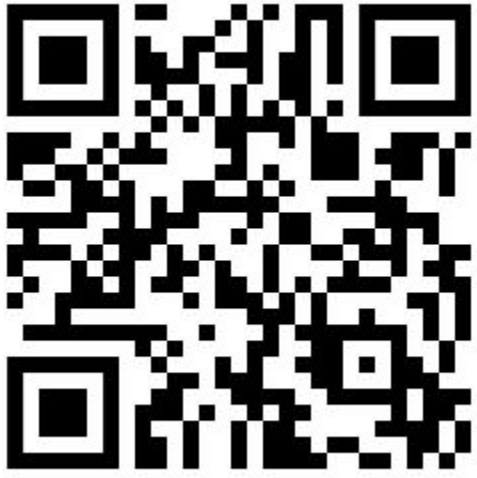
Consequências

2FA obrigatório e treinamento contra engenharia social

Atividade Prática

Instruções para a demonstração estão no nosso readme:

https://github.com/ifsc-seg-classroom/grupo-8



Conclusão

- Password Vaults ajudam a evitar problemas na parte mais vulnerável de um sistema de segurança: os usuários
  - Seja por compartilhamento seguro de segredos, ou evitando fadiga de senhas
- Podem ser usados para mais do que apenas guardar senhas
- Alguns permitem uso de Criptography as a Service, para abstrair esta parte durante o desenvolvimento
- Porém sua segurança é apenas tão boa quanto a entropia de sua senha-mestra

Referências I

https://www.hashicorp.com/pt - Hashicorp Site

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

https://github.com/hashicorp/vault - Hashicorp Github Guide

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

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

https://developer.hashicorp.com/vault/tutorials - Hashicorp Tutorials

Referências II

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

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

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