




# **Software Architecture**

Secret Management




# Secret Management

## Use case: VAULT

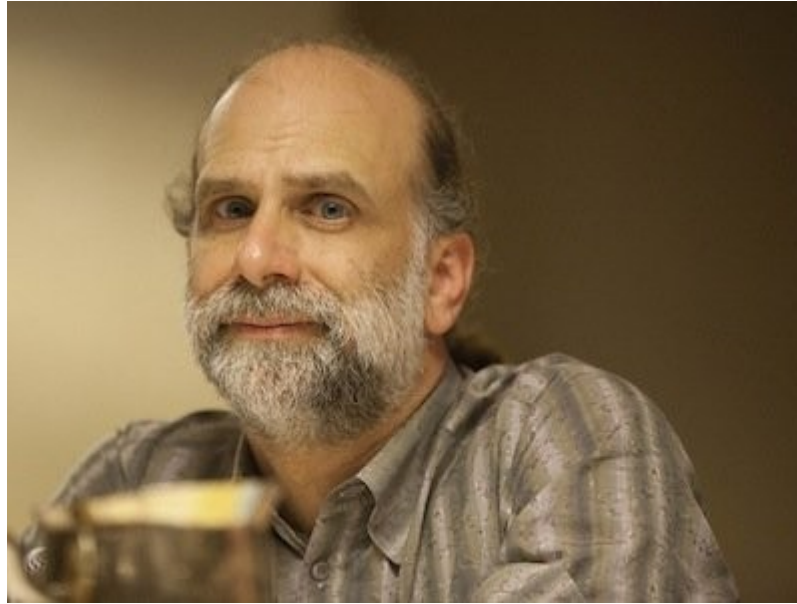


How are you storing your secrets today ?  
DB credentials, API keys, tokens, SSH ,...



How are you storing your secrets today ?  
DB credentials, API keys, tokens, SSH ,...

What can go wrong?



Cryptography is harder than it looks,  
primarily because it looks like math

Bruce Schneier



# What do we need ?

- Secure secret storage
  - Encryption of data at rest and transfer
- Audit trail
- Dynamic secrets!
  - Generated short term credentials
- Lease and revoke access
- ....



# What Vault offers

- Secure secret storage
  - Encryption of data at rest and transfer
- Audit trail
- Dynamic secrets!
  - Generated short term credentials
- Lease and revoke access

<https://www.vaultproject.io/>



# Vault

- Let's hear from the creator
- Introduction to HashiCorp Vault with Armon Dadgar
  - <https://www.youtube.com/watch?v=VYfl-DpZ5wM>

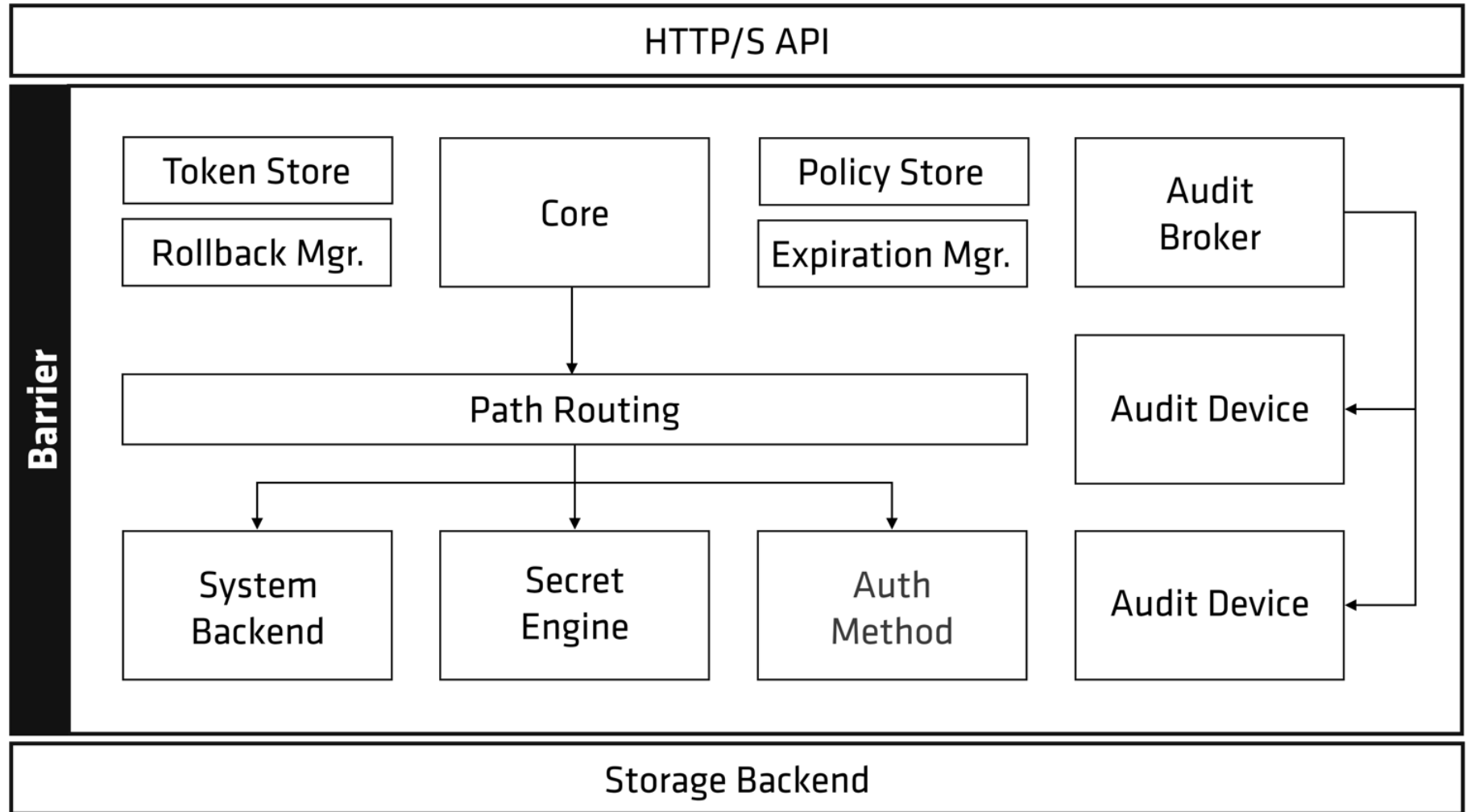




# Vault

- The storage back-end is not trusted
- Like a bank vault is sealed when it starts
  - To unseal we use a set of key shares
    - Master key is divided
    - Shamir's Secret Sharing scheme
- Encryption from inside to outside
  - Through a barrier

# Vault





# Vault

- Got time?, Let's read Architecture
  - <https://www.vaultproject.io/docs/internals/architecture.html>



# Final Thoughts

- Keeping secrets is tricky
  - You think of DYI security ?! .. think again
- Spring supports Vault