

Hardening your Infrastructure with a Vault



whoami

Luís Duarte

Software Engineer - OSS contributor

BSc Degree @



driverpt @



What's a secret?

"Something not known or not to be seen by others"

How to store secrets

- Text Files
- Password Managers (KeePass, LastPass, etc...)
- Post-It Stickers
- Notebook handwriting (Book of Secrets)
- Git Repository

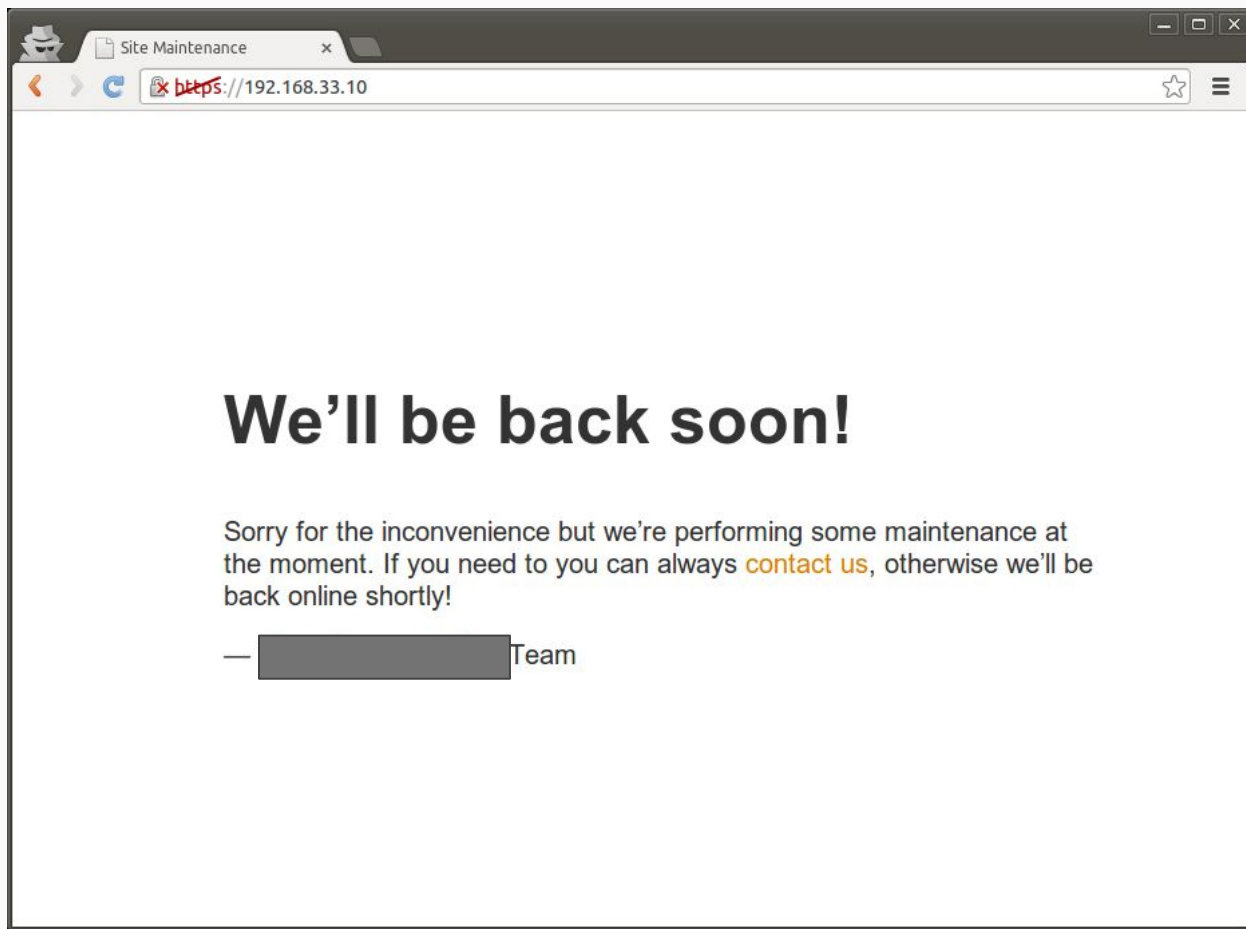
How do companies manage
secrets ?

How do companies manage secrets ?

<blank>



DON'T PANIC

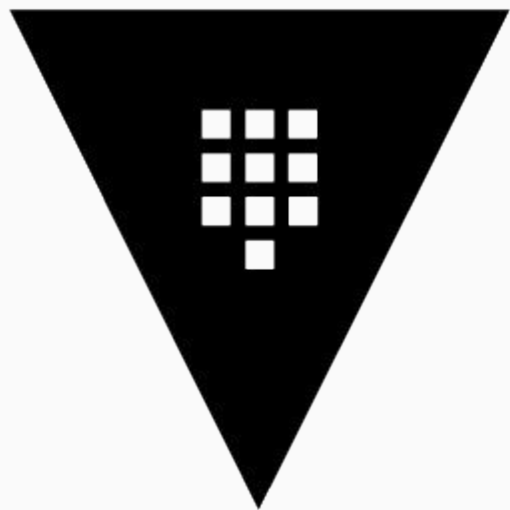


DATA BREACH

**IN EMERGENCY
BREAK GLASS**

What to do in case of Data Breach?

- Revoke all users and passwords
- Change database hostnames
- Create new users and passwords
- Reconfigure all infrastructure with new data (restart)

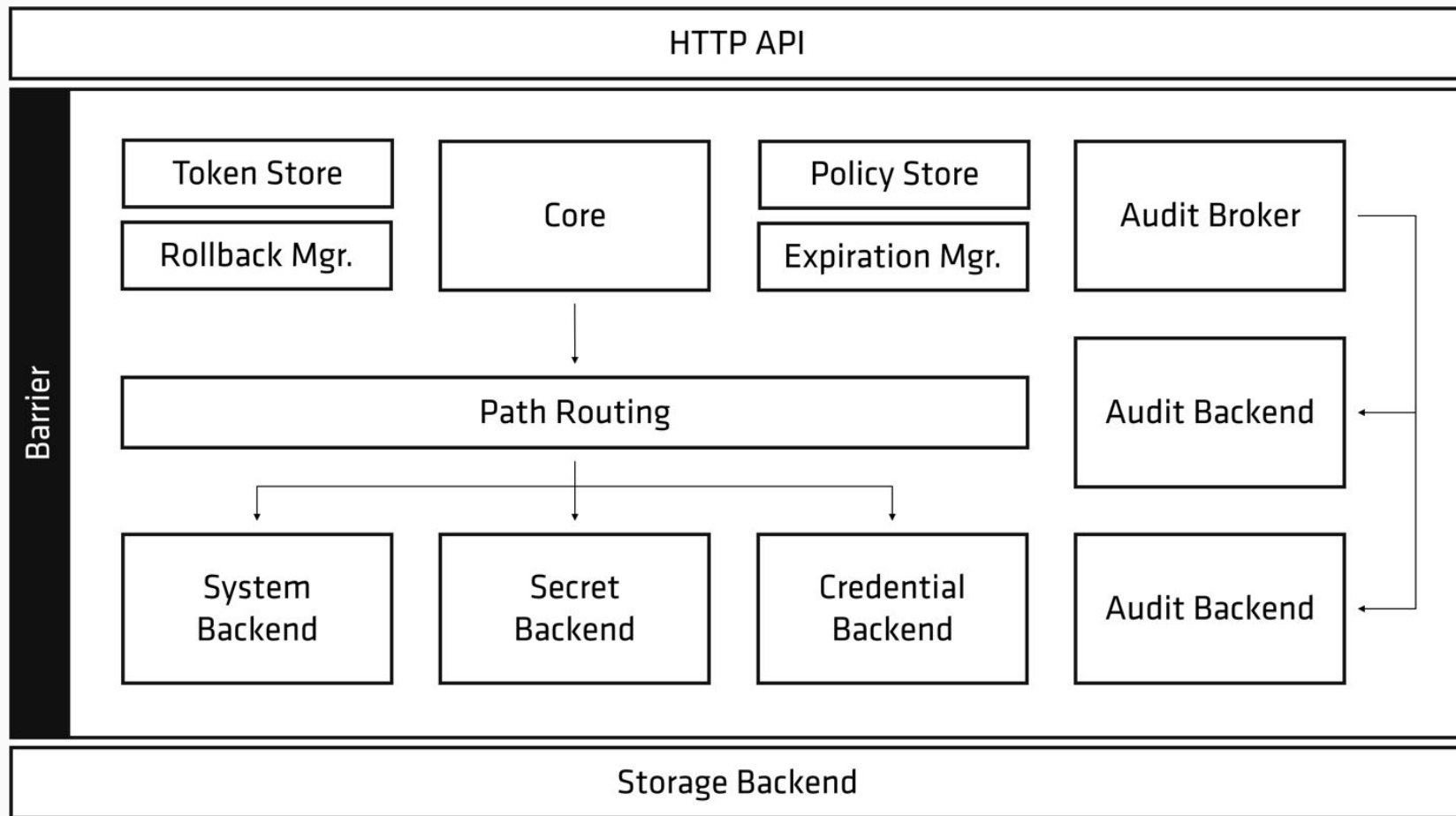


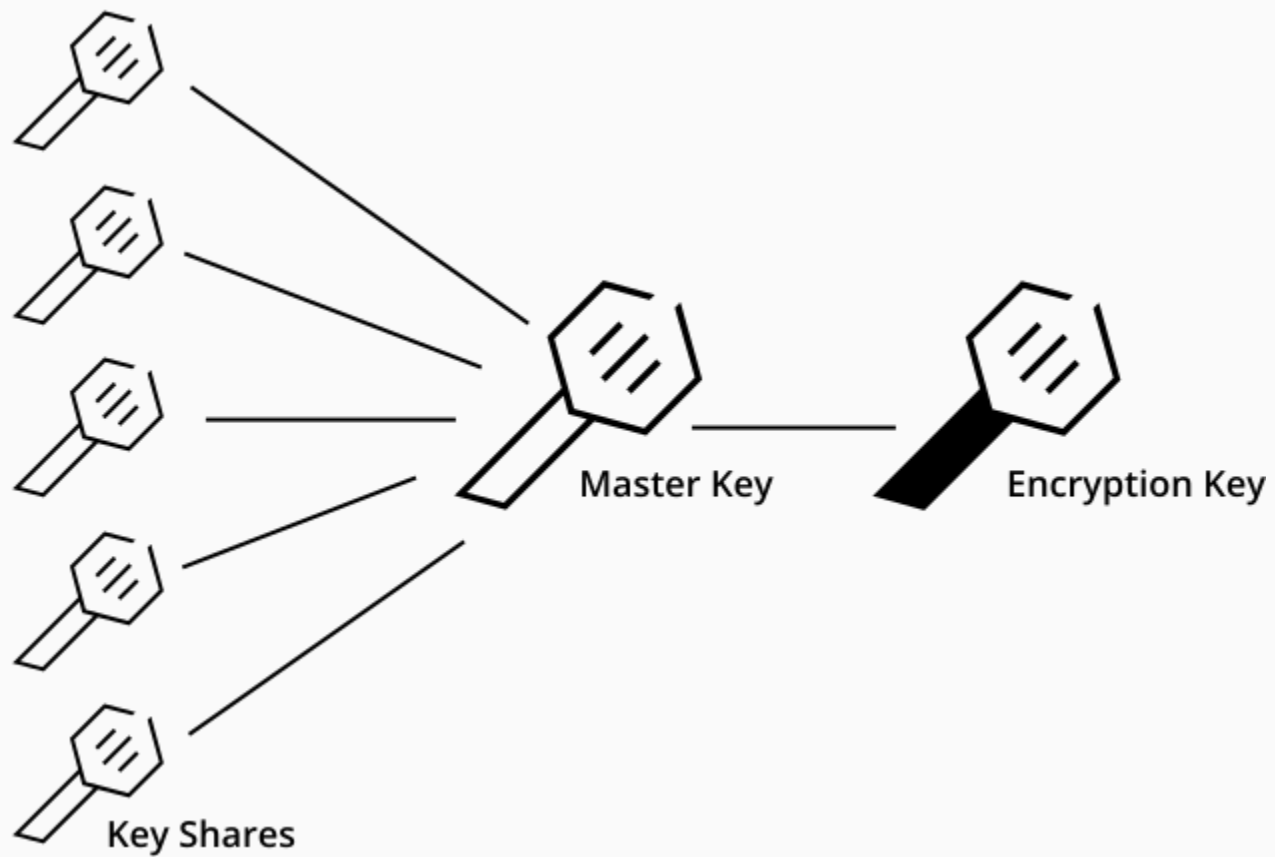
HashiCorp

Vault

Features

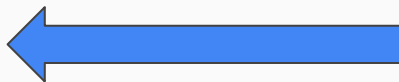
- Dynamic Secrets (Created on demand)
- Key Rolling
- Data Encryption
- ACL's
- Leasing, Renewing, Revocation
- Audit Log
- Multiple 3rd-party authentication plugins
- REST API





Supported Secret Backends

- SSH
- Databases (Postgres, Oracle, MySQL, etc...)
- PKI
- Key-Value Store
- AWS
- RabbitMQ



Example

Via CLI:

```
vault write secret/foo value=bar value2=baz
```

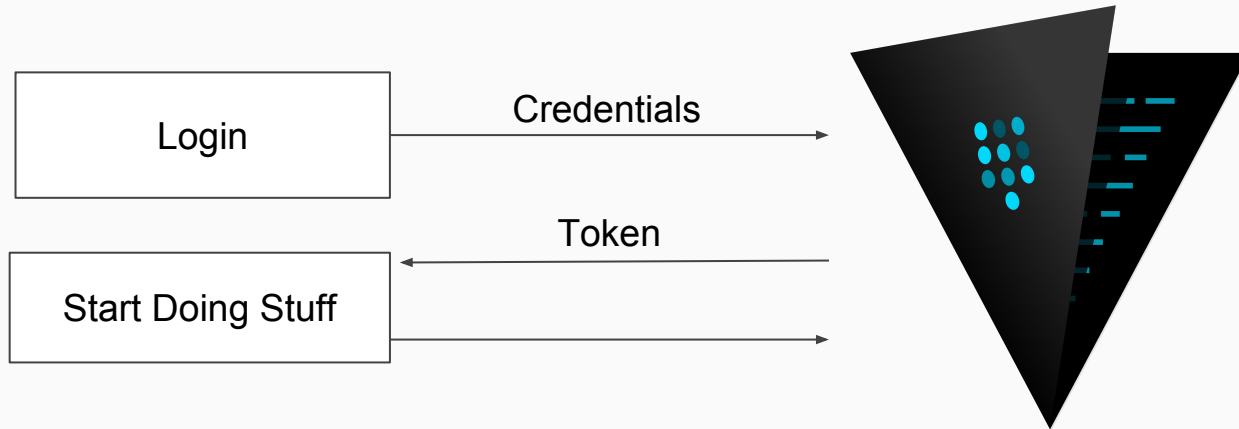
```
vault read secret/foo
```

Via REST API

```
curl --request POST  
https://vault.local:8200/v1/secret/foo --data  
"value=bar&value2=baz"
```

```
curl https://vault.local:8200/v1/secret/foo
```


How to spin this off?





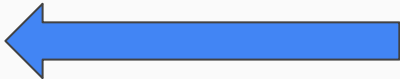
Fundamental Theorem of Software Engineering

"We can solve any problem by introducing an extra level of indirection."

DEMO

How to control access to what
and for how long?

Features

- Dynamic Secrets (Created on demand)
- Data Encryption
- Key Rolling
- ACL's 
- Leasing, Renewing, Revocation
- Audit Log
- Multiple 3rd-party authentication plugins
- REST API

Access Control Lists (ACL)

- Written in JSON or HCL
- Default Policy is **ALWAYS** Deny by default
- All Token policies are atomic
- Fine-grained Control

Policy Example (HCL)

```
path "secret/foo" {  
  capabilities = ["create", "update", "read", "delete"]  
  denied_parameters = {  
    "bar" = []  
  }  
  allowed_parameters = {  
    "*" = ["foo-*"]  
  }  
}
```


DEMO 2

What to do in case of Data Breach?

- **DO NOT PANIC!**
- Seal Vault (If you suspect if hackers are deep inside)
- Revoke all Tokens
- Generate new Tokens (Re-Login into Vault)

Best-Practices

- Keep ACL's Small
- Use token-create to test out new policies
- Restart App Containers on Policy Changes (New Tokens)
- Destroy Root Token in Production
- Make sure default policy has minimal access

Source Code for this Presentation



<https://github.com/driverpt/pixelscamp-hardening-infrastructure-with-vault>

ANY QUESTIONS?

