THE VAULT OF SECRETS



James Hunt @iamjameshunt

author of safe, spruce, vault-broker maintainer, vault / safe BOSH releases Stark & Wayne

secrets are everywhere.

ssh keys

secrets are everywhere.

ssh keys

secrets are everywhere. apikeys

ssh keys

passwords

secrets are

everywhere. api keys

passwords

ssh keys

secrets are

rsa keys everywhere api keys

passwords

ssh keys

secrets are

rsa keys everywhere. api keys

client secrets

auth tokens passwords ssh keys secrets are

rsa keys everywhere api keys

client secrets

auth tokens passwords ssh keys secrets are

rsa keys everywhere. api keys signing keys client secrets

auth tokens passwords ssh keys secrets are x.509 rsa keys everywhere api keys signing keys client secrets

where do we store them?

we could... hard-code them

```
import (
  "db"
const secret = "foo"
func main() {
 db.Connect("app", secret)
 // ... etc ...
```

we could... put them in env vars

\$ cf env my-app

User-Provided:
SECRET: oops

we could... put them in the database

secret name d4t4BASE! database sekrit web admin welcome1 (3 rows)

we could... encrypt them in the database

secret name U2FsdGVkX18uN/SjleX1 database U2FsdGVkX19miyEam2rj web U2FsdGVkX1+oT5SP3/Ir admin (3 rows)

so now we have an encryption key

where do we store it?

we could... hard-code it

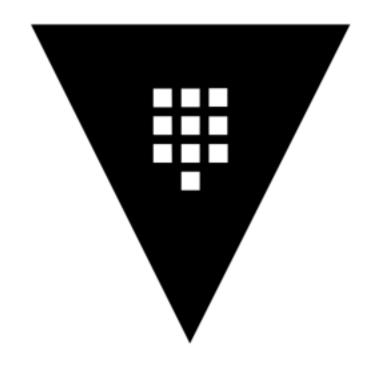
we could... put it in an env var

we could... put it in the database

we could... encrypt it in the database

we have a dilemma

secrets are tough.



Vault

what about cf?

there's a broker for that

https://github.com/cloudfoundry-community/vault-broker

(demo)

we also have a ui

https://github.com/jhunt/cf-vault-ui

(other demo)

an example app

https://github.com/jhunt/cf-apigen

(other other demo)

starkandwayne.com

