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.

api keys

passwords

ssh keys

secrets are everywhere.

api keys

passwords

ssh keys

secrets are
everywhere.

rsa keys

api keys

passwords

ssh keys

secrets are
everywhere.

rsa keys

api keys

client secrets

auth tokens

passwords

ssh keys

secrets are everywhere.

rsa keys

api keys

client secrets

auth tokens

passwords

ssh keys

secrets are everywhere.

rsa keys

api keys

signing keys

client secrets

auth tokens

passwords

ssh keys

secrets are everywhere.

x.509

rsa keys

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

```
name      | secret
----------+---------------------
database  | d4t4BASE!
web       | sekrit
admin     | welcome1
(3 rows)
```

we could...

encrypt them in the database

```
name      | secret
----------+---------------------
database  | U2FsdGVkX18uN/SjleX1
web       | U2FsdGVkX19miyEam2rj
admin     | U2FsdGVkX1+oT5SP3/Ir
(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.

HashiCorp Vault

vaultproject.io

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

beahero@starkandwayne.com