Behind Closed Doors

Managing Passwords in a Dangerous World

Noah Kantrowitz

Me

- Chef dude
- Likes making things
- Fights for the user

Secrets

Definition

- Small
- Radioactive
- Required

Secrets

- Passwords
- Keys
- Tokens
- Other

Passwords

- Computer to computer
- 1 to ~1024 bytes
- "Internal" or human-y

Tokens

- "External" or API
- Like passwords

Keys

- Whole files
- Bigger, chunkier

Other

- Kerberos tickets
- PCI log files
- HIPAA records

Temperature

Hot / Online

- Autonomous access
- Used a lot
- Humans need not apply

Cold / Offline

- Used rarely
- Humans required

Spectrum

Speed

Slow

- "Static"
- Change is "big"
- Less safe

Fast

- Changes constantly
- Automatic rotation
- More safe

Properties of a Secrets Management System

“Every program and every privileged user of the system should operate using the least amount of privilege necessary to complete the job.”

– Jerome Saltzer, Communications of the ACM

Properties

- Least privilege
- Audit trail

Let's do it!

```
$ echo "P@s5wd" > secret.txt
$ git commit -a -m "yolo!"
$ git push origin master
To git@github.com:me/myapp.git
f35a8c0..c2f0adf  master -> master
```

Attack Surfaces

Surfaces

- Brute force
- Code leak
- Backup leak
- Traversal
- Code exec
- Root exec
- Laptop theft
- Higher power

Brute Force

- Always be wary
- Rate-limit, restrict, rotate
- Make it impossible

Code Leak

- Read-only access
- No data
- "GitHub oops"

Backup Leak

- Still read-only
- With database, et al

Traversal

- /show?n=about
- /show?n=../../passwd
- /search?q=;select…

An Aside

- Environment variables
- Logged, inherited, etc
- Unsafe at any speed

Code Exec

- Beyond app security
- Infrastructure hygiene
- Service users

Root Exec

Lasciate ogne speranza,
voi ch'intrate.

Laptop Theft

- Use disk encryption
- Rotate everything

Higher Power

- Government
- Advanced threat
- Natural disaster

Tools

Text Files

- git add …
- scp …
- Interns

Chef Encrypted Bags

- Symmetric, AES-256-GCM
- Server vs git
- Turtles all the day down

Ansible Vault

- AES-256-CTR + SHA-256
- Still turtles

Hiera Eyaml

- PKCS7 (or GPG)
- Trusted Third Party

Chef Vault

- RSA(encrypted bags)
- Asymmetric pre-encrypt
- Kind of still turtle-y

An Aside

- Pre-encryption
- Symmetric key distribution
- Asymmetric key identity

Hashicorp Vault

- TTP service
- New bar for fast secrets
- Modular design

Keywhiz

- TTP
- TLS keys, files
- Battle tested

Amazon KMS

- Kool-aid-tastic
- Key escrow
- Hosted encrypt/decrypt

Sneaker

- KMS + S3
- Still kool

Confidant

- KMS + DynamoDB
- Web-based
- Versioned w/ history

Trousseau

- Asymmetric pre-encrypt
- GPG + modular storage
- S3, GPG, GitHub

Sops

- KMS or GPG
- Manual storage

Red October

- Cold secrets
- N of M storage

Barbican

Pining for the fjords

Conjur

- And other closed source
- Trust but verify

HSMs

- $$$
- Dedicated hardware
- Bugs not unheard of

The Hard Problem

Identity

- Who are you?
- Who am I?
- Why are we in this hand basket?

Pure Identity

- TLS client certificates
- MySQL, Postgres
- Internal APIs

Integration

API Clients

- Vault: HVAC, vault-rails
- KMS: botocore, aws-sdk

Config Management

- Templates/commands
- hiera-vault
- Ruby/Python APIs

KeywhizFS

- FUSE filesystem
- Direct key usage
- In-memory

Consul Templates

- Standalone daemon
- Sync Vault data to files
- CM → Templates → files

envconsul

- Vault data in $ENV
- Beware of logging

Summon

- Secrets in $ENV
- Modular providers
- S3, Keyring, Conjur

Thank You

Questions?

@kantrn
coderanger.net