Managing server secrets at scale with a vaultless password manager

Ignat Korchagin
@secumod
$ whoami

- Platform engineer at Cloudflare
- Passionate about security and crypto
- Enjoy low level programming
Disclaimer

There is no cloud
it’s just someone else’s computer
So you have a server
So you have a server

You need:

- server SSH key
So you have a server

You need:

- server SSH key
- configuration management key
So you have a server

You need:

- server SSH key
- configuration management key
- disk encryption key
So you have a server

You need:

- server SSH key
- configuration management key
- disk encryption key
- some server credentials
So you have a server

You need:

● server SSH key
● configuration management key
● disk encryption key
● some server credentials
● probably more...
So you have a server

You need:
- server SSH key
- configuration management key
- disk encryption key
- some server credentials
- probably more...

... so at least 5 keys... and that’s per server
So you have a datacentre
So you have a datacentre(s)
So you have a datacentre(s)
Cloudflare network today
So you have a datacentre(s)
Where do keys live?
Where do keys live?
Where do keys live?
# Keys in configuration management

```
# !yaml | gpg

root-password: |
    -----BEGIN PGP MESSAGE-----
    Version: GnuPG v1

    hQIMA221up1ZY1MdARAA583Z4o3xZawWzK8yUYJKBEkMQD/i+RRn7A0+h8SEmsov
    QkrxgeaCWFIZ5pRCPv0K1SWZGi0dzWkWe1DeNisawv5X/VUG3d5ej1xtAD4kBTy
    AzcnFft7QfIsV8C+juHYGITU++pFVAgEdGrb09mf6SEDaAGJhOq01BmHccw0Pat
    rBH/+gvD155F7sxM/BBQwL25ZjtC+8jUsp1bUcTQVofsy6kTVRNSS4hO4UNtMuMQ
    hYf6UAPaJv3PhFXKYYu0tEp2THZVT1UtTjyKAZrNiKyRpC/0exbJjJMQkJmmUG9r
    yP1CvubJnmHda2u42981dK3pz5T1LEO4MrBry6vynN0TJfXwn1nt7YMVatiViQb9
    UK5NDbjVKBBe6KkN28kJtsTkCOM7+RztjLdf+7ZWzxvF5EkM+2SLPIhQFCMjRG
...```
Keys in configuration management
Keys in configuration management

- Bootstrap configuration management
Keys in configuration management

- Bootstrap configuration management
- Does not scale for unique keys
Keys in configuration management

- Bootstrap configuration management
- Does not scale for unique keys

```yaml
#!/yaml|gpg
root-password: |
{% if grains[‘hostname’] == ‘baredog’ %}
    -----BEGIN PGP MESSAGE-----
    ...
{% elif grains[‘hostname’] == ‘cheesyonion’ %}
    -----BEGIN PGP MESSAGE-----
    ...
{% elif grains[‘hostname’] == ‘...’ %}
    ...
{% endif %}
```
Keys on local disk
# super nitty startup script, fully automated !!!
if [ ! -f /etc/server_key ]; then
  dd if=/dev/urandom of=/etc/server_key bs=1 count=32
fi

# don’t forget SSH
if [ ! -f /etc/ssh/id_rsa ]; then
  ssh-keygen -f /etc/ssh/id_rsa
fi
Entropy

WHAT IF I TOLD YOU

ENTROPY IS LOW RIGHT AFTER SYSTEM BOOT
Keys on local disk
Keys on local disk

- Not suitable for some key types
Keys on local disk

- Not suitable for some key types
  - root passwords
Keys on local disk

- Not suitable for some key types
  - root passwords
- Does not play well with disk encryption
Keys on local disk

- Not suitable for some key types
  - root passwords
- Does not play well with disk encryption
  - decrypt configuration management key
Keys on local disk

- Not suitable for some key types
  - root passwords
- Does not play well with disk encryption
  - decrypt configuration management key
- What about diskless/stateless systems?
Encrypted disks

server

store

disk 1

crypt

disk 2

disk N
Unified Extensible Firmware Interface
Unified Extensible Firmware Interface

- Aka BIOS 2.0
Unified Extensible Firmware Interface

- Aka BIOS 2.0
- Standard pre-OS environment
Unified Extensible Firmware Interface

- Aka BIOS 2.0
- Standard pre-OS environment
- Extensible (you can write your own apps)
Unified Extensible Firmware Interface

- Aka BIOS 2.0
- Standard pre-OS environment
- Extensible (you can write your own apps)
- Supported by most major OSes
Unified Extensible Firmware Interface

- Aka BIOS 2.0
- Standard pre-OS environment
- Extensible (you can write your own apps)
- Supported by most major OSes
- Provides many advanced features
Unified Extensible Firmware Interface

- Aka BIOS 2.0
- Standard pre-OS environment
- Extensible (you can write your own apps)
- Supported by most major OSes
- Provides many advanced features
  - UEFI variables
UEFI variables

- Backed by flash memory on platform firmware chip
UEFI variables

- Backed by flash memory on platform firmware chip
- Can store standard and custom (OEM/user) data
UEFI variables

- Backed by flash memory on platform firmware chip
- Can store standard and custom (OEM/user) data
- Can be accessed after OS kernel booted
UEFI variables

- Backed by flash memory on platform firmware chip
- Can store standard and custom (OEM/user) data
- Can be accessed after OS kernel booted
- Have built-in support in Linux
UEFI variables in Linux

# not needed for systemd-based Linux distributions
mount -t efivarfs efivarfs /sys/firmware/efi/efi/efivars

# need to prepend data with 4 byte attr and put an "owner" GUID
cat <(printf '\x07\x00\x00\x00') <(cat mydata.bin) > /sys/firmware/efi/efi/efivars/mydata-<some GUID>
UEFI variables in Linux

# not needed for systemd-based Linux distributions
mount -t efivarfs efivarfs /sys/firmware/efi/efi/efivars

# need to prepend data with 4 byte attr and put an “owner” GUID
cat <(printf "\07\00\00\00") <(cat mydata.bin) > /sys/firmware/efi/efi/efivars/mydata-<some GUID>

- always available
UEFI variables in Linux

# not needed for systemd-based Linux distributions

```
mount -t efivarfs efivarfs /sys/firmware/efi/efi/efivars
```

# need to prepend data with 4 byte attr and put an "owner" GUID
```
cat <(printf "\x07\x00\x00\x00") <(cat mydata.bin) > /sys/firmware/efi/efi/efivars/mydata-<some GUID>
```

- always available
- can be accessed in early boot stages
UEFI variables in Linux

# not needed for systemd-based Linux distributions
mount -t efivarfs efivarfs /sys/firmware/efi/efi/efivars

# need to prepend data with 4 byte attr and put an “owner” GUID
\n\ncat <(printf "\x07\x00\x00\x00") <(cat mydata.bin) > /sys/firmware/efi/efi/efivars/mydata-<some GUID>

• always available
• can be accessed in early boot stages
• however, may have limited storage
Keys in cryptography
Keys in cryptography

derive
Keys in cryptography
Key derivation functions

master key

KDF
Key derivation functions
Key derivation functions

string1 -> master key

master key -> KDF
Key derivation functions
Key derivation functions

- string1
- master key
- string2
- key1

KDF
Key derivation functions
Generating key pairs

Deterministic CSPRNG
Generating key pairs

seed1

Deterministic CSPRNG
Generating key pairs

1. seed1
2. Deterministic CSPRNG
3. keypair1
Generating key pairs

- seed1
- seed2
- Deterministic CSPRNG
- keypair1
Generating key pairs

seed1 → Deterministic CSPRNG → keypair1

seed2 → Deterministic CSPRNG → keypair2
Introducing gokey tool

master seed

realm

*For example*  
“ssh”, “saltstack”,  
“disk encryption”  
etc
Introducing gokey tool

master seed → HKDF → realm

For example “ssh”, “saltstack”, “disk encryption” etc
Introducing gokey tool

HKDF

master seed

Deterministic CSPRNG

realm

For example "ssh", "saltstack", "disk encryption" etc
Introducing gokey tool

For example "ssh", "saltstack", "disk encryption" etc
Introducing gokey tool

For example "ssh", "saltstack", "disk encryption" etc
Introducing gokey tool

- **master seed**
- **HKDF**
- **realm**
- **Deterministic CSPRNG**
  - saltstack key
  - ssh key

For example, “ssh”, “saltstack”, “disk encryption” etc
Key management

- Provisioning process ensures a master seed is generated and stored in UEFI on first boot
Key management

- Provisioning process ensures a master seed is generated and stored in UEFI on first boot
- Startup scripts “recover” (derive from master seed) configuration management credential (key)
Key management

● Provisioning process ensures a master seed is generated and stored in UEFI on first boot

● Startup scripts “recover” (derive from master seed) configuration management credential (key)

● Configuration management “recovers” all other keys
root-password: |
{% if grains['hostname'] == 'baredog' %}
    -----BEGIN PGP MESSAGE-----
    ...
{% elif grains['hostname'] == 'cheesyonion' %}
    -----BEGIN PGP MESSAGE-----
Key management

root-password: |
{% if grains['hostname'] == 'baredog' %}
    -----BEGIN PGP MESSAGE-----
    ...
{% endif %}
{% elif grains['hostname'] == 'cheesyonion' %}
    -----BEGIN PGP MESSAGE-----

root-password: {% gokey('root-password') %}
ssh-key: {% gokey('ssh') %}

Adding a server
Adding a server
Adding a server
Rotate a specific service key
Rotate a specific service key

server

server

server

ssh-key: `{% gokey('ssh') %}`

ssh-key: `{% gokey('ssh-v2') %}`
Rotate a specific service key

```
ssh-key: {% gokey('ssh') %}
```

```
ssh-key: {% gokey('ssh-v2') %}
```
Rotate all key on a server
Rotate all key on a server

rotate EFI seed
Rotate all key on a server

rotate EFI seed
Encrypted disks (previously)
Encrypted disks

server

encrypt

disk 1

encrypt

disk 2

encrypt

disk N
Conclusions
Conclusions

- Decouple key storage from regular storage
Conclusions

● Decouple key storage from regular storage
● Decouple key contents from key management
Conclusions

- Decouple key storage from regular storage
- Decouple key contents from key management
- Easy to add new or rotate existing keys
Conclusions

● Decouple key storage from regular storage
● Decouple key contents from key management
● Easy to add new or rotate existing keys
● Better security guarantees
Conclusions

- Decouple key storage from regular storage
- Decouple key contents from key management
- Easy to add new or rotate existing keys
- Better security guarantees

https://github.com/cloudflare/gokey
Thank you