CYPHERLOCK – Secrets & Time

How much torture can you endure before your secrets expire?

Jonathan “smuggler” Logan

About

- Black IT (IT projects nobody wants to admit to)
- Covert Communications
- Going to the good side… protecting journalists

The Problem (tm)

- Client project: Carry secret data over borders
- Being held & forced to decrypt
- Go to jail if you refuse **OR** prove that you can’t
- Situation in Australia, UK, US...

Insert NDA problem here…….

Analysis

- You cannot (intentionally) forget a secret
- => Never know the secret
- => Never share the secret

Layman solution

- Create random secret (blindly)
- Encrypt to third party
- Ask third party to decrypt
- Use secret

But….

DO NOT SHARE YOUR SECRET

Oracles...

- Encrypt secret to random key
- Encrypt THAT key to third party

Oracles & Time

Expire secrets by expiring Oracle keys

WHY?

You cannot resist forever!

Process

- Encrypt secret to random key
- Encrypt random key to “time lock key”
- Encrypt result to Oracle long-term key

Time Lock Keys

- Asymmetric Ratchet Algorithm
- Pregenerate (public&private) keypairs for each timeframe
- Repeat ratchet in real time. Throw away state.
- => Irrecoverable (like Signal PFS)

Use case

- Laptop with “network” and encrypted “secret” partition
- Raspberry Pi with **cypherlockd** at home (via Tor)
- Create **cypherlock** on laptop for secret partition

Usecase (cont.)

IFF all goes well: Unlock

Or

Under distress: Wait until lock expires

Security best practice

- DO NOT HAVE YOUR Raspberry PI SSH key on non-cypherlocked partition
- ONLY use over TOR (or TLS)

Show, don’t tell

```
$ cypherlockd -create
Server created.
SignatureKey: 08e687303df497......
$

$ cypherlockd -serve
Serving...
SignatureKey: 08e687303df497......

$
```

Client...

```
$ exec 3<secret ; cypherlock  -create -sigkey 08e687... -fd 3
Please enter passphrase (no echo):
Please repeat passphrase (no echo):
Lock created. From "Sat Sep 15 01:54:09 +0000 UTC 2018"
to "Sat Sep 15 02:24:09 +0000 UTC 2018"
$

$ exec 3>secret2 ; cypherlock  -unlock -sigkey 08e687... -fd 3
Please enter passphrase (no echo):

$
```

Options…

-create -unlock -extend
-from -to
-path -server -sigkey -help

CODE

In go…
Linux (arm64/amd64), OpenBSD (amd64)

http://opaque.link/files/cypherlock-release-v0.1.tar.bz2

….the end

Thank YOU!!!!
And
Frank Braun (co-conspirator on Cypherlock)
Tatjana Adamov (training journalists)
Frank Rieger (journalist contacts and usecases)