

Introducing Certgrinder

Thomas Steen Rasmussen
BornHack 2018

Agenda

- Background
- How does it work?
- What else does it do?
- What doesn't it do? / help needed

Background

- LetsEncrypt is nice! But sometimes...
- Load balanced web servers
- Server migrations
- Alternative software

How does it work?

- A LetsEncrypt “SSH proxy”
- One Certgrinder server & many clients
- Certgrinder.py & csrgrinder.sh
- Uses certbot behind the scenes

Files

```
[certgrinder@znc ~]$ ls -l
```

```
total 43
```

```
drwxr-xr-x  3 root          certgrinder  11 Jan 17 11:59 certgrinder
-rw-r--r--  1 certgrinder  wheel          649 Jan 17 12:31 certgrinder.yml
drwxr-x---  2 certgrinder  certgrinder    6 Jan 17 12:31 certificates
drwxr-xr-x  5 root          certgrinder    6 Oct  9 09:31 virtualenv
```

```
[certgrinder@znc ~]$ ls -l certificates/
```

```
total 32
```

```
-rw-r-----  1 certgrinder  certgrinder  7058 Dec  9 02:49 znc.tyknet.dk-concat.pem
-rw-r--r--  1 certgrinder  certgrinder  3786 Dec  9 02:49 znc.tyknet.dk.crt
-rw-r--r--  1 certgrinder  certgrinder  1647 Dec  9 02:49 znc.tyknet.dk.csr
-rw-r-----  1 certgrinder  certgrinder  3272 Oct  9 09:32 znc.tyknet.dk.key
```

```
[certgrinder@znc ~]$
```

Challenge Types

- HTTP-01

```
# letsencrypt ACME redirect to Certgrinder server
location '/.well-known/acme-challenge' {
    return 301 http://certgrinder.bornhack.org$request_uri;
}
```

- DNS-01

_acme-challenge.imap.bornhack.org. 43200 IN
CNAME imap.bornhack.org.acme.bornhack.org.

How does it work?

- 1) Generate keypair
- 2) Generate CSR
- 3) SSH to Certgrinder server
- 4) `cat example.org.csr | ssh
certgrinder.example.com > example.org.crt`
- 5) Profit!

What else does it do?

A few handy little features:

- `--showtlsa`
 - Reads public keys and outputs TLSA records for the given service, say `_443._tcp`
- `--checktlsa`
 - Reads public keys and checks DNS for TLSA records. Outputs what needs to be done (if anything).
- `Showspki`
 - Reads public keys and outputs pin-sha256 spki pins

What doesn't it do?

- For 1.0:
 - Limit allowed domains per SSH key
- Future / 2.0:
 - pip package & OS package managers (help)
 - Switch from py-openssl to cryptography
 - Switch from using Certbot to using acme directly
 - Rewrite csrgrinder in Python

Questions

?