cryptdomainmgr

automating Cert, TLSA, DKIM and many more

Stefan Helmert

Chaostreff Chemnitz

30. April 2018

Content

Motivation

- fine
- not so fine

Basics

- SSL Certifcate
- TLSA
- DNSSEC
- DKIM

Solution

- cryptdomainmgr

cryptdomainmgr

- structure
- update cycle
- configuration

Motivation

→ **let's make a web app** ←

- DNS
- Webpage
- E-Mail
- Mailinglist
- **and the s for security**

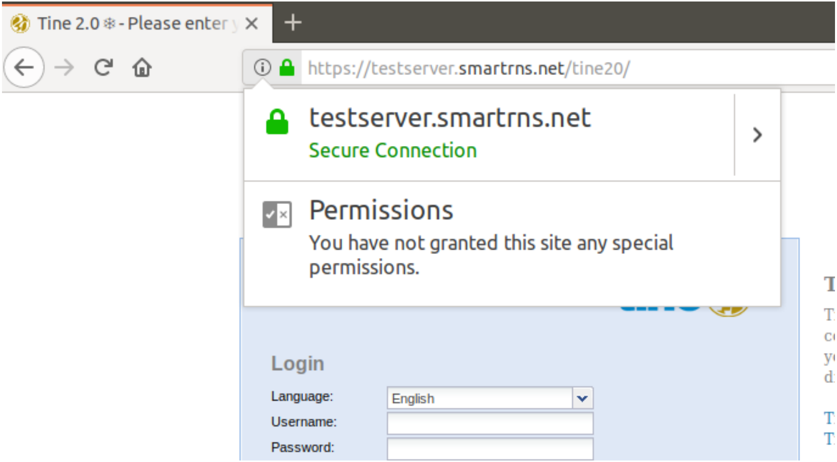
DeMotivation

→ let's make a web app ←

- DNS
  - SOA
  - DNSSEC
- Webpage
  - HTTPS
  - Certificate
  - HSTS
  - SRV
  - TLSA
- E-Mail
  - Spam
  - DKIM
  - SPF
  - ADSP
  - DMARC
  - SRV
- Mailinglist
  - SRS

DeMotivation

fine



https://testserver.smartrns.net/tine20/

testserver.smartrns.net

Secure Connection

Permissions

You have not granted this site any special permissions.

Login

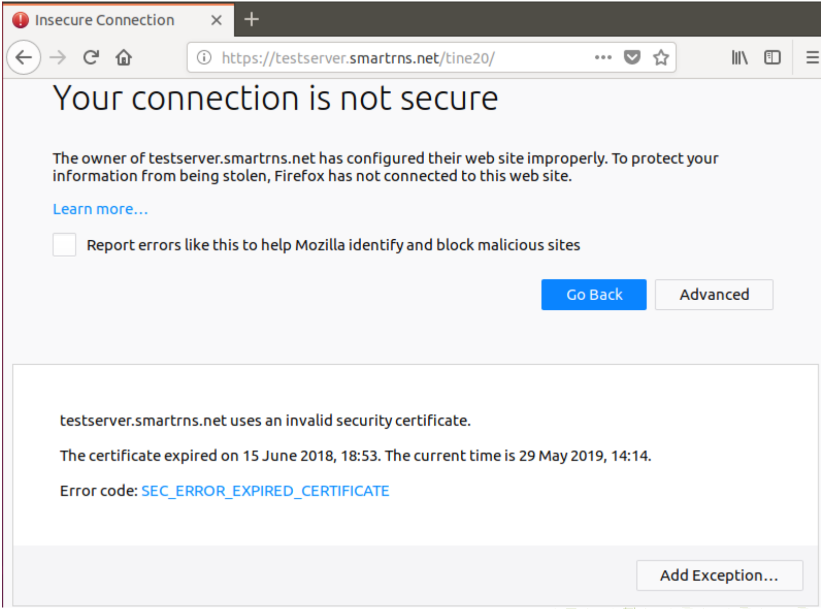
Language: English

Username:

Password:

DeMotivation

not so fine



Your connection is not secure

The owner of testserver.smartrns.net has configured their web site improperly. To protect your information from being stolen, Firefox has not connected to this web site.

Learn more…

□ Report errors like this to help Mozilla identify and block malicious sites

testserver.smartrns.net uses an invalid security certificate.

The certificate expired on 15 June 2018, 18:53. The current time is 29 May 2019, 14:14.

Error code: SEC_ERROR_EXPIRED_CERTIFICATE

Basics

SSL Certifcate

- authentication (phishing)
- integrity (man in the middle)
- privacy (spy)

→ certbot renew

Basics

TLSA

DANE – DNS-based Authentication of Named Entities
Transport Layer Security Authentication

- locks certificate to domain/DNS (fraudulent CA, stolen cert)

→ to do

Basics

DNSSEC

Domain Name System Security Extensions

- authenticate domain owner
- integrity (DNS cache poisoning)

→ done by domain provider

Basics

DKIM

DomainKeys Identified Mail

- authenticate MTA (fake/spam server)
- integrity (man in the middle)

→ to do

Solution

cryptdomainmgr

autorenew

- prepare
  - generate certificate
  - calculate TLSA from certificate
  - add TLSA RR
  - generate key pair for DKIM
  - calculate DKIM
  - add DKIM RR
- rollover
  - use new certificate
  - use new DKIM key
- cleanup
  - remove old TLSA RR
  - remove old DKIM RR
  - delete old certificates
  - delete old DKIM keys

cryptdomainmgr

structure

- cryptdomainmgr
    - dnsuptools
        - domrobot
    - certbot

cryptdomainmgr

update cycle

update – set a, aaaa, srv, dmarc, spf, adsp

```
~/cryptdomainmgr$ ./update.py inwxcred.conf example.conf
```

prepare cycle – generate Cert, TLSA, DKIM

```
~/cryptdomainmgr$ ./prepare.py inwxcred.conf example.conf
```

rollover cycle – use Cert, TLSA, DKIM

```
~/cryptdomainmgr$ ./rollover.py inwxcred.conf example.conf
```

cleanup cycle – remove outdated

```
~/cryptdomainmgr$ ./cleanup.py inwxcred.conf example.conf
```

cryptdomainmgr

configuration

DNS credential

```
~/cryptdomainmgr$ cat inwxcred.conf

[domain]
user = myusername
passwd = mypassword
```

cryptdomainmgr

configuration

certificate configuration

```
~/cryptdomainmgr$ cat example.conf

[certificate]
generator = certbot
email = stefan.helmert@t-online.de
keysize = 4096

[certificate:maincert]
destination = /etc/ssl
extraflags = --staging, --renew-with-new-domains, --hsts
certname = fullchain.pem
```

cryptdomainmgr

configuration

dkim configuration

```
~/cryptdomainmgr$ cat example.conf

[dkim]
generator = rspamd

[dkim:maindkim]
signingConfTemplateFile = ~/cryptdomainmgr/dkim_signing_te
signingConfTemporaryFile = /etc/rspamd/dkim_signing_new.co
signingConfDestinationFile = /etc/rspamd/local.d/dkim_sign
```

cryptdomainmgr

configuration

domain configuration

```
~/cryptdomainmgr$ cat example.conf

[domain]
user = myusername
handler = dnsuptools

[domain:domain.example]
soa.hostmaster = stefan.helmert@t-online.de
soa.refresh = 7200

[domain:sub.domain.example]
ip4 = auto, 192.168.0.1
ip6+ = auto, 0ffc::0030
mx = mail20.domain.example:20, mail30.domain.example:30
mx.40 = mail40.domain.example, mail50.domain.example:50
mx.10+= mail10.domain.example
```

cryptdomainmgr

configuration

domain configuration – combine stuff

```
~/cryptdomainmgr$ cat example.conf

[domain:sub.domain.example]
tlsa = 3 0 1, 3 1 1
certificate = maincert
dkim = maindkim
```