TWNIC’s Experience on DANE (DNS-Based Authentication of Named Entities)

TWNIC
Tsz-Heng Guo
Abstract

* DANE(The DNS-Based Authentication of Named Entities) is a protocol releases at 2012.
* HTTP over TLS(https) is widely used to ensure that the communication is safe and trusted. However, in recent years, several CAs leak and spamming incidents make it different, can we still trust the web site we are visited?
* DANE is a protocol with DNSSEC to ensure that the certificate are owned by the domain owner and can be trusted.
The authentication process of HTTP over TLS
The risk of HTTP over TLS
How to setting up DANE and TLSA record ensure certificate is safe
The setting of browser’s plugin
Q&A
HTTP over TLS

1. Get a certificate from ca
2. Connect web
3. Return twnic Certificate
4. Check certificate is correct by CA’s public key
HTTP over TLS

1. Get a certificate from CA
2. Connect request
3. Return twnic Certificate
4. Check certificate is correct by CA’s public key

Twnic Web server

CA been trusted

CA2 been trusted

Phishing web site

twnic Certificate

User
HTTP over TLS risk

* The CA、Intermediate CA is safe?
  * 2011 comodo 9 domain CA leak.
  * 2018 dlink、netscape CA had been stolen.
* The CA、Intermediate CA abuse
  * 2017 Symantec issued more than 20,000 wrong certification, and to lead to the security level was lowered.
How to set up tlsa

* The domain zone must enable DNSSEC
* Set tlsa record for your application (www, mail...)
* For example TWNIC set two tlsa record
  * rs.twnic.net.tw
  * www.twnic.net.tw
How to set up tlsa

- Certificate usage: 0~3
- Selector: 0~1
- Matching type: 0~2
- Certificate association data

```bash
tszheng@Tszheng-test:~$ dig 443._tcp.www.twnic.net.tw tlsa
; <<>> DiG 9.9.6 <<>> _443._tcp.www.twnic.net.tw tlsa
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 38552
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 3072
;; QUESTION SECTION:
;_443._tcp.www.twnic.net.tw. IN TLSA

;; ANSWER SECTION:
_443._tcp.www.twnic.net.tw. 60 IN TLSA 3 1 1 D216BF00A15E2D4BC9DB4AB1CE1E
C112A746E28E1E35510F161433E8_BBAE2752
```
How to set up tlsa

* Get public key from certification
  * openssl s_client -showcerts -servername www.twnic.net.tw -connect www.twnic.net.tw:443 | openssl x509 -text | openssl x509 -noout -pubkey

```
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAl2wLxVeZFeCQkWvXY2
OJk7r7JK3o5sMHA6cA4V2Xk3OyCh+pJQ8n/kVwL8n57fG3c98gywD4o6f
-----END PUBLIC KEY-----
```
How to set up tlsa

* Convert public key to binary file and hash by sha256
  * openssl rsa -in twnic.key -pubin -outform DER > twnic.bin
  * sha256sum twnic.bin
Google chrome plugin setting

![Image of Google Chrome plugin search for DNSSEC Validator and TLSA Validator](https://chrome.google.com/webstore/search/DNSSEC?hl=zh-TW)
Google chrome plugin setting

* Install windows application
* https://secure.nic.cz/files/dnssec-validator/2.2.0/dnssec-plugin-2.2.0.x-windows-x86.exe
* https://secure.nic.cz/files/dnssec-validator/2.2.0/tlsa-plugin-2.2.0.x-windows-x86.exe
Google chrome plugin setting

* Setting a cache server which enable dnssec

Google dns server 8.8.8.8
Cloudflare dns server 1.1.1.1
Google chrome plugin setting

* Windows will ask and allow application to access the firewall
Google chrome plugin setting

* Testing the plugin is workable.
Thanks for your listen