DANE

Killer app for DNSSEC?

Warren Kumari, Google
&
Ondřej Surý, CZ.NIC

What's wrong with PKI?

- You have no way of knowing which the "right one" CA is...
    - And they are all equally trusted...
        - And there are lots of them...
- Extended Validation (EV), Organization Validated (OV), Domain Validated (DV)
- Domain Validated (DV) certs based on email/whois information.

Question for you:

Do you know which CA your bank uses?

Do you know if it uses EV or OV or DV certs?

DANE

- The domain owner should know!
- Put fingerprint (or cert) in DNS
- Sign it with DNSSEC
- (Add some magic dust)
- Use that as new “trust path” for certificate

DANE protocol

- DANE Use Cases and Requirements, RFC 6394, October 2011 (R. Barnes)
- DANE / TLSA Protocol, RFC6698, August 2012 (P. Hoffman, J. Schlyter)
- TLSA RR Type (TLS Association)
- *_port._proto.example IN TLSA usage selector matching data*
    - `_443._tcp.www.tlsa.cz. IN TLSA 3 0 1 2f4af1513d4457c0e97f7ebb14ea...`

Certificate usage

- Must pass the PKIX validation (Usage 0/1)
  - Pin the CA
    (e.g. I use only “DigiNotar”!)
  - Pin the certificate
    (e.g. I use only this specific certificate from ...)
- Insert new trust anchor (Usage 2/3)
  - Insert new CA
    (e.g. I created my company CA and want to trust it)
  - Insert new EE
    (e.g. what you would call self-signed certificate)

Selector & Matching Type

- Selector
  - Fingerprint whole certificate
  - Fingerprint just the subjectPublicKeyInfo (no need to change TLSA record when changing the validity of cert, etc.)
- Matching Type (use hashing or not?)
  - Full certificate or SHA256 or SHA512

Security of DANE

- Depends on DNS
  - But you **already do**!

DANE and DNSSEC

- Depends on DNSSEC and need secure path from resolver to end application
  - DNSSEC-Trigger - http://www.nlnetlabs.nl/projects/dnssec-trigger/

Go and play

- Swede tool (https://github.com/pieterlexis/swede)

```
usage: swede create [-h] [--port PORT] [--protocol {tcp,udp,sctp}]
                    [--certificate CERTIFICATE] [--output {generic,rfc,both}]
                    [--usage {0,1,2,3}] [--selector {0,1}] [--mtype {0,1,2}]

# swede create -p 443 -o rfc -u 1 -s 1 -c www.nic.cz.pem -m 2 www.nic.cz
_443._tcp.www.nic.cz. IN TLSA 1 1 2 b43dd88534c0a26859d19a26a54a50205518
                                    7de2099f6d35564c55a659525a52dcb5163c
                                    961e233578a3408d57e7c842db2234796705
                                    8c2396c88e7cd367a978
```

Future of DANE

- Other protocols with complex lookups (aka fix the protocols)
  - S/MIME – draft-ietf-dane-smime
  - SMTP – draft-fanf-dane-smtp
  - MUA – draft-fanf-dane-mua
  - XMPP – draft-miller-xmpp-dnssec-prooftype
- Implementations
  - Firefox Add-On: DanePatrol (fork of Certificate Patrol)
  - Chicken & Egg problem – no users thus no consumers and vice versa

QUESTIONS?