PKI should go: A note on TLSA and DANE

Damjan Sirnik

March 9, 2016

Overview

1. Introduction
   - Problems with current PKI system
2. DANE
   - What is DANE, how does it work?
   - TLSA RR structure explained
     - Usage field
     - Selector field
     - Matching type field
   - Requirements
   - Similar solutions
3. Supported environments
   - Web Browsers
   - Server Software
   - Big Players
4. DANE in Action
   - E-mail server example (Postfix)
   - Web browser example
5. Future
6. Conclusion

Problems with current PKI system

- Everyone can become trusted CA for about $50k-$250k

Problems with current PKI system

- Everyone can become trusted CA for about $50k-$250k
- Every CA can issue certificates for any domain

Problems with current PKI system

- Everyone can become trusted CA for about $50k-$250k
- Every CA can issue certificates for any domain
- CA breaches:
  - DigiNotar (531 fake certificates issued)
  - Comodo
  - DigiCert Malaysia (22 issued certificates; subordinate CA of Entrust)
  - MCS Holdings (subordinate CA of CNNIC)

Problems with current PKI system

- Everyone can become trusted CA for about $50k-$250k
- Every CA can issue certificates for any domain
- CA breaches:
  - DigiNotar (531 fake certificates issued)
  - Comodo
  - DigiCert Malaysia (22 issued certificates; subordinate CA of Entrust)
  - MCS Holdings (subordinate CA of CNNIC)
- Problem with breaches: attackers issued certificates for pupular domains. MITM attack possible without anyone even noticing.

Problems with current PKI system

- Everyone can become trusted CA for about $50k-$250k
- Every CA can issue certificates for any domain
- CA breaches:
  - DigiNotar (531 fake certificates issued)
  - Comodo
  - DigiCert Malaysia (22 issued certificates; subordinate CA of Entrust)
  - MCS Holdings (subordinate CA of CNNIC)
- Problem with breaches: attackers issued certificates for pupular domains. MITM attack possible without anyone even noticing.

Do we have (possible) solution available for that? Yes! DANE

DANE

- DANE is not something new
- Some changes and progress recently regarding real life usage
- Similar soulutions do exist

What is DANE, how does it work?

Definition

DNS-Based Authentication of Named Entities

What is DANE, how does it work?

Definition

DNS-Based Authentication of Named Entities

DANE:

- offers option to use DNS for keys and certificates storage

What is DANE, how does it work?

Definition

DNS-Based Authentication of Named Entities

DANE:

- offers option to use DNS for keys and certificates storage
- offers option to bind keys and certificates to DNS names

What is DANE, how does it work?

Definition

DNS-Based Authentication of Named Entities

DANE:

- offers option to use DNS for keys and certificates storage
- offers option to bind keys and certificates to DNS names
- inherits all benefits and limitations of DNSSEC

TLSA RR structure explained

- DANE uses TLSA resource record to associate a TLS server certificate or public key with the domain name.

TLSA RR structure explained

- DANE uses TLSA resource record to associate a TLS server certificate or public key with the domain name.
- TLSA record consists of four fields:

TLSA RR structure explained

- DANE uses TLSA resource record to associate a TLS server certificate or public key with the domain name.
- TLSA record consists of four fields:
    - The Certificate Usage filed:
      0 = PKIX-TA, 1 = PKIX-EE , 2 = DANE-TA, 3 = DANE-EE

TLSA RR structure explained

- DANE uses TLSA resource record to associate a TLS server certificate or public key with the domain name.
- TLSA record consists of four fields:
  - The Certificate Usage filed:
    0 = PKIX-TA, 1 = PKIX-EE , 2 = DANE-TA, 3 = DANE-EE
  - The Selector field:
    0 = Cert, 1 = SPKI

TLSA RR structure explained

- DANE uses TLSA resource record to associate a TLS server certificate or public key with the domain name.
- TLSA record consists of four fields:
  - The Certificate Usage filed:
    0 = PKIX-TA, 1 = PKIX-EE , 2 = DANE-TA, 3 = DANE-EE
  - The Selector field:
    0 = Cert, 1 = SPKI
  - The Matching Type field:
    0 = Full, 1 = SHA2-256, 2 = SHA2-512

TLSA RR structure explained

- DANE uses TLSA resource record to associate a TLS server certificate or public key with the domain name.
- TLSA record consists of four fields:
  - The Certificate Usage filed:
    0 = PKIX-TA, 1 = PKIX-EE , 2 = DANE-TA, 3 = DANE-EE
  - The Selector field:
    0 = Cert, 1 = SPKI
  - The Matching Type field:
    0 = Full, 1 = SHA2-256, 2 = SHA2-512
  - The Certificate Association Data filed:
    full value or digest of the certificate or subject public key

Sample record

```
_25._tcp.mail.example.com IN TLSA 3 0 1
      b6ae36240791655a753ba19546fc4e46c554d010124616deac4b72ba28a8009f
```

Usage field explained

- PKIX-TA (CA constraint):
  - Allows domain owner to publish which CAs are only allowed to issue certificates
  - Clients should only accept certificates issued by those CAs
  - Certificate is still checked against local trust store
  - Name and expiration checks are still performed
  - TLS server needs to send full certificate chain
  - Useful if you want to simplify TLSA RRs publishing
  - Usage of PKIX-TA is not recomended
  - PKIX-TA offers no additional security over DANE-TA

Usage field explained

- PKIX-EE (Service certificate constraint):
  - Exact TLS certificate that should be used
  - PKIX verification is required.

Usage field explained

- PKIX-EE (Service certificate constraint):
  - Exact TLS certificate that should be used
  - PKIX verification is required.
- DANE-TA (Trust anchor assertion):
  - Similar to PKIX-TA: server still needs full chain, certificate still needs to be valid (not expired), names still must match etc.
  - No checks against local trust store are performed

Usage field explained

- DANE-EE (Domain-issued certificate):
  - Exact TLS certificate that should be used
  - Simple check that the server's certificate matches with TLSA record
  - CommonName or SubjectAltName are disregarded
  - Certficate expiration date MUST be ignored
  - No need to include full certificate chain

Selector field explained

Defines which part of TLS certificate presented by the server will be matched against Certificate Association Data:

- Cert: Full certificate is matched
- SPKI: DER-encoded subjectPublicKeyInfo is matched

Matching type field explained

Defines how Certificate Association Data is presented:

- Full: Exact match of selected content
  Not recommended!
- SHA2-256: SHA2-256 hash of selected content
  Mandatory in clients!
- SHA2-512: SHA2-512 hash of selected content
  Do not use it exclusively!

Requirements

- DNSSEC capable DNS server

Requirements

- DNSSEC capable DNS server
- DNS server must support TLSA RR

Requirements

- DNSSEC capable DNS server
- DNS server must support TLSA RR
- TLD you are using must be DNSSEC signed

Requirements

- DNSSEC capable DNS server
- DNS server must support TLSA RR
- TLD you are using must be DNSSEC signed
- DNS servers that support both DNSSEC and TLSA RR:
  - BIND from version 9.9.x
  - NSD from version 3.2.11
  - PowerDNS from version 3.0
  - Microsoft DNS will support from Windows Server 2016
  - Knot DNS from version 1.0.4
  - YADIFA from version 2.0
  - ...

Similar solutions

- HPKP (RFC 7469):
  - Similar to DANE, but using HTTP headers
  - Hash is kept in browser's cache
  - Only for web

Similar solutions

- HPKP (RFC 7469):
    - Similar to DANE, but using HTTP headers
    - Hash is kept in browser's cache
    - Only for web
- CAA (RFC 6844):
    - Domain name holder can specify CAs authorized to issue certificates for his domain
    - Enables CA to check domain ownership

Similar solutions

- HPKP (RFC 7469):
  - Similar to DANE, but using HTTP headers
  - Hash is kept in browser's cache
  - Only for web
- CAA (RFC 6844):
  - Domain name holder can specify CAs authorized to issue certificates for his domain
  - Enables CA to check domain ownership
- SSHFP (RFC 4255):
  - Verification of SSH server's public key
  - Fingerprint of SSH server published in DNS
- ...

Web Browsers

- None of most popular browsers support DANE natively

Web Browsers

- None of most popular browsers support DANE natively
- HPKP might be on of the reasons

Web Browsers

- None of most popular browsers support DANE natively
- HPKP might be on of the reasons
- You can use DNSSEC/TLSA Validator plugin from CZ.NIC

Server Software

- Mail servers:
  - Postfix - support from 2.11; some changes from 3.1
  - Exim - 4.85
  - Sendmail - no support yet
  - Exchange Server - no support (3rd party solution: CryptoFilter gateway)

Server Software

- Mail servers:
  - Postfix - support from 2.11; some changes from 3.1
  - Exim - 4.85
  - Sendmail - no support yet
  - Exchange Server - no support (3rd party solution: CryptoFilter gateway)
- IM servers, etc.

Big Players

- Unfortunately none

Big Players

- Unfortunately none
- Not really example of DANE - German VDA recomendation

E-mail server example (Postfix)

Requirements:

- DNSSEC capable resolver. If possible on same box.
- Postfix version 2.11 or greater. Best option 3.1

E-mail server example (Postfix)

Required configuration changes:

- In `main.cf` add or change following paramteres to enable opportunistic DANE:

```
smtp_dns_support_level = dnssec
smtp_tls_security_level = dane
```

- If you want, you can use higher security level for some particular domains, use `tls_policy_maps`

E-mail server example (Postfix)

Postfix distinguishes between following security levels:

- Anonymous TLS connection
- Untrusted TLS connection
- Trusted TLS connection
- Verified TLS connection

Examples with valid TLSA record, invalid TLSA record, without TLSA record...

TLSA record generated using following command:

```
openssl x509 -in server.pem -outform DER | openssl sha256 | cut -d’=’ -f2 | awk ’{printf "IN
      TLSA 3 0 1 %s\n", $NF}’
IN TLSA 3 0 1 b6ae36240791655a753ba19546fc4e46c554d010124616deac4b72ba28a8009f
```

Valid TLSA record (using opportunistic DANE)

- TLSA record in DNS zone for lhns.org:

```
_25._tcp.dane IN TLSA 3 0 1
      b6ae36240791655a753ba19546fc4e46c554d010124616deac4b72ba28a8009f
```

- Postfix log:

```
postfix/smtp: Verified TLS connection established to dane.lhns.org[2001:db8:b51d:e5
      :510::2]:25: TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)
postfix/smtp: DD8748072B: to=<danetest@lhns.org>, relay=dane.lhns.org[2001:db8:b51d:e5
      :510::2]:25, delay=0.55, delays=0.09/0.02/0.25/0.1, dsn=2.0.0, status=sent (250
      2.0.0 Ok: queued as 84A6B3FD38)
```

- Connection to remote server is Verified (TLSA record and server certificate do match)

Invalid TLSA record (using opportunistic DANE)

- TLSA record in DNS zone for lhns.org:

```
_25._tcp.dane IN TLSA 3 0 1
      b6ae36240791655a753ba19546fc4e46c554d010124616deac4b72ba28a8009a
```

- Postfix log:

```
postfix/smtp: Trusted TLS connection established to dane.lhns.org[2001:db8:b51d:e5
      :510::2]:25: TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)
postfix/smtp: 730D78072B: to=<danetest@lhns.org>, relay=dane.lhns.org[2001:db8:b51d:e5
      :510::2]:25, delay=0.21, delays=0.09/0/0.12/0, dsn=4.7.5, status=deferred (Server
      certificate not verified)
```

- As server certificate is issued by trusted CA, connection is Trusted. But because server certifcate does not match with TLSA record, e-mail is `deffered`. Possible MITM attack prevented!

Without TLSA record (still using opportunistic DANE)

- Postfix log:

```
postfix/smtp: Trusted TLS connection established to dane.lhns.org[2001:db8:b51d:e5
      :510::2]:25: TLSv1.2 with cipher ECDHE-RSA-AES256-GCM-SHA384 (256/256 bits)
postfix/smtp: BFB6D8072B: to=<danetest@lhns.org>, relay=dane.lhns.org[2001:db8:b51d:e5
      :510::2]:25, delay=0.52, delays=0.06/0.02/0.29/0.14, dsn=2.0.0, status=sent (250
      2.0.0 Ok: queued as 95F623FD38)
```

- As there is no TLSA record, Postfix reverts to standard opportunistic TLS (`smtp_tls_security_level = may`)

Without TLSA record (using mandatory DANE)

- Using `tls_policy_maps` in Postfix to set `dane-only` policy for domain lhns.org:

```
echo "lhns.org dane-only" >> /etc/postfix/tls_policy
postmap /etc/postfix/tls_policy
```

- Postfix log:

```
postfix/smtp: warning: TLS policy lookup for lhns.org/dane.lhns.org: no TLSA records
      found
postfix/smtp: E9BCC8072B: to=<danetest@lhns.org>, relay=none, delay=0.15, delays
      =0.13/0.02/0/0, dsn=4.7.5, status=deferred (no TLSA records found)
```

- As there is no TLSA record and TLS policy for that domain is set to mandatory DANE, e-mail is `deffered`.

Web browser example

- Use DNSSEC/TLSA Validator plugin
- Visit test pages for all possible scenarios provided by Verisign Labs: `http://dane.verisignlabs.com/`

Future

- DANE with SRV records (RFC 7673) - DANE for IM protocols, VoIP services etc.

Future

- DANE with SRV records (RFC 7673) - DANE for IM protocols, VoIP services etc.
- DANE for S/MIME (RFC draft) - DANE for e-mail signing and encryption (SMIMEA RR).
- ...

Conclusion

- Use DANE

Conclusion

- Use DANE
- Main problem is lack of support in web browsers

Conclusion

- Use DANE
- Main problem is lack of support in web browsers
- Another problem - transperent proxies

Conclusion

- Use DANE
- Main problem is lack of support in web browsers
- Another problem - transperent proxies
- Don't be scared of DNSSEC

Q&A

Questions?

damjan<at>sirnik.si