Securing Security - DNSSEC and DANE

Patrick Koetter und Carsten Strotmann, sys4 AG

CREATED: 2023-10-19 THU 07:20

DNSSEC as the new Internet PKI

- The traditional Internet PKI with certification authorities (CA) has problems:
    - Users must have ultimate trust towards **all** CAs
    - There are too many CAs (2.000 +)
    - The security of the CA model is only as good as its weakest part

- Goal: Regain control over trust and policies

DNSSEC as the new Internet PKI

- DANE - DNS(SEC) Authenticated Named Entities replaces the CA model with DNSSEC
  - The owner of a DNS domain has the authority to publish content in the name of this domain
  - DNSSEC authenticates the content
  - The security level of DNSSEC is comparable to domain-validated (DV) x509 certificates
  - There is only one trust chain (the Internet DNS delegation chain) that Internet users already trust today for their DNS name resolution
  - The DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS) Protocol: TLSA

DNSSEC as the new Internet PKI

- The owner of a DNSSEC signed domain creates or receives a x509 certificate
- The owner publishes the hash of the certificate (or of the public key embedded inside the certificate) using a TLSA-DNS-record and configures the certificate on the service (server)

DNSSEC as the new Internet PKI

- Example of a TLSA-record (this is for a mail server for the GMX.DE domain):

```
% dig _25._tcp.mx01.emig.gmx.net tlsa +multi

; <<>> DiG 9.10.4-P4-RedHat-9.10.4-2.P4.fc25 <<>> _25._tcp.mx01.emig.gmx.net tlsa +multi
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 29351
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;_25._tcp.mx01.emig.gmx.net. IN TLSA

;; ANSWER SECTION:
_25._tcp.mx01.emig.gmx.net. 293 IN TLSA 3 1 1 (
                                9BDE51EA74128A327A6A4F3A4F21CBA855475DCF88BC
                                1532A2B45B35E16E6D61 )

;; WHEN: Mon Dec 19 07:41:58 CET 2016
;; MSG SIZE  rcvd: 102
```

DNSSEC as the new Internet PKI

- A DANE-enabled client program validates the x509 certificate received from the server with the information in the TLSA-record (hash)
- The domain name of the service will be matched with the domain name of the TLSA-record. The Common-Name (CN) or the domain names inside the certificate ***does not*** need to match with the server name of the service
- The certificate is seen as valid as long as a valid TLSA-record exist in DNS. The expire time inside the certificate will ***not*** be checked by DANE clients
- The certificate chain of the x509-certificate does ***not*** need to be validated by the client. The trust towards the certificate is established via DNSSEC and the TLSA-record.

DANE-TLSA

- DANE-TLSA is (currently) specified for
  - SMTP (E-Mail)
  - HTTPS (Web) (limited support for Client-Browser applications)
  - DNS-over-TLS / DNS-over-HTTPS (DNS encryption)
  - IRC
  - XMPP/Jabber
  - Generic services via SRV-Records (RFC 7673)

DANE-SMTP

- In Germany, the "Technische Richtlinie BSI TR-03108" ("Sicherer E-Mail-Transport") defines:
  - Requirements for secure email transport for email service provider
  - DANE/DNSSEC use is mandated
  - **`posteo.de`** was the 1st email provider certified in December 2016
  - **`mail.de`** was the 1st email provider receiving the "IT-Sicherheitskennzeichen" ("IT security badge") in 2022

DANE-SMTP

- Additional DANE-SMTP provider:
  - Mailbox.org
  - Web.de/Gmx.de
  - mail.de
  - bund.de
  - Microsoft
  - GMail (Inbound - for selected customers)
  - many universities

DANE @ Microsoft

27th September 2023: Breaking news, Microsoft is pulling the trigger on DANE next year: Implementing Inbound SMTP DANE with DNSSEC for Exchange Online Mail Flow - Microsoft Community Hub

https://techcommunity.microsoft.com/t5/exchange-team-blog/implementing-inbound-smtp-dane-with-dnssec-for-exchange-online/ba-p/3939694

DANE-SMTP

- DANE-SMTP users

gmx.at	lrz.de	ouderportaal.nl
travelbirdbelgie.be	mail.de	overheid.nl
travelbirdbelgique.be	posteo.de	pathe.nl
nic.br	ruhr-uni-bochum.de	uvt.nl
registro.br	tum.de	xs4all.nl
gmx.ch	uni-erlangen.de	domeneshop.no
open.ch	one.com	handelsbanken.no
switch.ch	sys4.de	webcruitermail.no
anubisnetworks.com	web.de	aegee.org
gmx.com	egmontpublishing.dk	debian.org
isavedialogue.com	netic.dk	freebsd.org
mail.com	tilburguniversity.edu	gentoo.org
solvinity.com	octopuce.fr	ietf.org
t-2.com	comcast.net	isc.org
trashmail.com	dd24.net	netbsd.org
xfinity.com	dns-oarc.net	openssl.org
xfinityhomesecurity.com	gmx.net	samba.org
xfinitymobile.com	hr-manager.net	torproject.org
nic.cz	mpssec.net	asf.com.pt
bayern.de	t-2.net	handelsbanken.se
bund.de	xs4all.net	t-2.si
fau.de	bhosted.nl	mail.co.uk
freenet.de	boozyshop.nl	govtrack.us
gmx.de	hierinloggen.nl	

DANE-SMTP Domain Count

- DANE-SMTP domains by countries (09/2023)

COUNTRY	DANE DOMAINS (TSND)
Germany	3553
USA	1894
Netherlands	1886
France	822
Swiss	556

DANE-SMTP Domain Count

- DANE secures user communication. The domain count is not relevant, the number of users behind the services on these domains are important
    - Some DANE secured domains are being used by millions of users

DANE-SMTP

- DANE-SMTP Implementations:
  - postfix (https://postfix.org)
  - exim (Exim DANE Wiki)
  - opensmtpd (https://www.opensmtpd.org/)
  - Port25
  - Halon (https://halon.io/)
  - MS Exchange via Add-On Filter (CryptoFilter)
  - MS Office 365 uses DANE outbound since 2022 and will enable inbound DANE in 2024. See outbound DANE.

End

Questions? Answers!