One year of DANE
Tales and Lessons Learned
sys4.de
DANE secures Security
Why secure Security?
Encryption Models

Opportunistic Encryption

> Expect anything
> Proceed if absent
> Try if offered
> Proceed unencrypted on failure
> Silent on failure

Mandatory Encryption

> Expect encryption
> Fail and alarm if absent
> Identify other side
> Fail and alarm if identity mismatch
> Encrypt or fail
> Alarm on failure
Issues with opportunistic TLS

- CA model
- Downgrade Attack
- MITM attack
- Incomplete automation for certification rollover
Br0ken CA Model

- Any CA can issue certificates for any domain
- CAs have been compromised in the past
- CAs have issued wrong or unauthorized certificates
- Declining Trust in CA root-certificates since Snowden
Türktrust? Diginotar?
Session downgrade

> TLS comes without policy channel

> Client can't know server supports STARTTLS before SMTP Session starts

> MITM-Attacker may downgrade session to „Non-TLS“

220 mail.example.com ESMTP
EHLO client.example.com
250-mail.example.com
250-PIPELINING
250-SIZE 40960000
250-ETRN
250-STARTTLS
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
Session downgrade

ISPs Removing Their Customers' Email Encryption

Recently, Verizon was caught tampering with its customer's web requests to inject a tracking super-cookie. Another network-tampering threat to user safety has come to light from other providers. Email encryption downgrade attacks. In recent months, researchers have reported ISPs in the US and Thailand intercepting their customers' data to strip a security flag—called STARTTLS—from email traffic. The STARTTLS flag is an essential security and privacy protection used by an email server to request encryption when talking to another server or client.¹

By stripping out this flag, these ISPs prevent the email servers from successfully encrypting their conversation, and by default the servers will proceed to send email unencrypted. Some firewalls, including Cisco's PIX/ASA firewall do this in order to monitor for spam originating from within their network and prevent it from being sent. Unfortunately, this causes collateral damage: the sending server will proceed to transmit plaintext email over the public Internet, where it is subject to eavesdropping and interception.
MITM Attack

> Attacker can intercept TLS secured communication with a matching certificate (Common Name)

> Easily done since everyone accepts self signed certificates...
Automation. NOT!

- Certification Authority is warrantor
- Manual verification
- Verification requires knowledge
- Verification requires presence
- Need to monitor certificate change
Securing Security
The Plan

- Add a policy channel
- Add a trust layer
- Indicate encryption
- Indicate identity
Welcome to DANE!
DANE

"DNS-based Authentication of Named Entities" (RFC 6698)

> DANE uses/requires DNSSEC
  > DNS becomes policy channel
  > DNSSEC adds trust layer

> New Resource Records
  > Presence indicates service availability
  > Record carries service specific data
Current Use Cases

- HTTPS
  Connect service/server to a certificate

- SMTP
  Connect service/server to a certificate

- OpenPGP
  Associate Public Keys to email address

- S/MIME
  Associate Certificates with Domain Names and email addresses
| Port-- | | | | | | |
| Protocol-- | | | | | | |
| Host-------- | | | | | | |
| Resource type-------------------------- | | | | |
| Certificate Usage --------------------- | | | |
| Selector ----------------------------- | | |
| Matching Type ------------------------- | |
| Certificate Association Data ----------- |
$ dig +dnssec TLSA _443._tcp.www.sys4.de

_443._tcp.mail.sys4.de.3600 IN TLSA 3 0 1 (9273B4E9040C1B9EE7C946EFC0BA8AAF2C6E5F05A1B2C960C41655E32B15CBE0)

_443._tcp.mail.sys4.de.3600 IN RRSIG TLSA 8 5 3600 (20141124104604 20141117195102 19786 sys4.de.afEJbtmKZVn995XiI2BFQwYKC1ZfcsIK/j2JA9C8oYSppneBLVYuX8C0ZW9zTHCExtXS1kJrNf48sFRaOWhbZvPy1vRiB+c46QRG0kwceDUjzZGtpG3Al2LKBVKw4bxMMOzuDeqECrf/n1W8XF6UQcrB0PdTY81Y6IZTUovYhak=)
HTTPS

Wir sind ein Team namhafter Open-Source-Experten.
Browser Plugin

DNSSEC/TLSA Validator is a web browser add-on which allows you to check the existence and validity of DNS Security Extensions (DNSSEC) records and Transport Layer Security Association (TLSA) records related to domain names. Results of these checks are displayed by using icons and information texts in the page's address bar or browser tool-bar. Currently, Internet Explorer (IE), Mozilla Firefox (MF), Google Chrome/Chromium (GC), Opera (OP), Apple Safari (AS) are supported.

About

DNSSEC/TLSA Validator is a web browser add-on which allows you to check the existence and validity of DNSSEC signed DNS records. DNSSEC Validator shows whether the domain name is DNSSEC-signed. It also checks whether the browser is configured to use DNSSEC.

Description

DNSSEC/TLSA Validator is a web browser add-on which allows you to check the existence and validity of DNSSEC signed DNS records. DNSSEC Validator shows whether the domain name is DNSSEC-signed. It also checks whether the browser is configured to use DNSSEC.

News

Version: 2.2.0

New Features:
- New js-types-based implementation for Firefox.
- New validator implementation for Chromium/Chrome/Opera based on Native Messaging.
- Added new state notification about entering a non-existent (according to DNSSEC) web site.
- Polish localisation.

Bugfixes:
- Updated prefixes for DOM nodes in Firefox is-

DNS-Proxy issues, CPE-modem study over 15 common CPE devices sys4 for Unitymedia Deutschland, August 2014
TLSA Resource Record

_25._tcp.mail.sys4.de. IN TLSA 3 0 1 9273B4E9040C1B...
|   |   |    |
Port-- |   |    |
Protocol- |    |
Host-------    |
Resource type------------------    |
Certificate Usage ---------------    |
Selector -----------------    |
Matching Type -----------------    |
Certificate Association Data -------------
SMTP Security via Opportunistic DANE TLS

- Initial RFC draft published 2013
  Wes Hardaker, Viktor Dukhovni

- Currently in DANE WG „Last Call“ ends 2015-05-07

- First implementations
  - Postfix
  - OpenSMTPd
  - Exim

- In production @sys4 since 12/2013
„Verified“ makes all the difference

Today

Jul 14 11:03:31 mail postfix/smtp[6477]:
  Trusted TLS connection established to mx-ha03.web.de
  [213.165.67.104]:25: TLSv1.1 with cipher
  DHE-RSA-AES256-SHA (256/256 bits)

DANE

Jul 14 11:04:44 mail postfix/smtp[6409]:
  Verified TLS connection established to mail.sys4.de
  [194.126.158.139]:25: TLSv1 with cipher
  ECDHE-RSA-AES256-SHA (256/256 bits)
DANE over SMTP Adoption

Currently about 1.200 email domains

- posteo.de
- mailbox.org
- bund.de
- Unitymedia (UPC Germany)
- bayern.de
- SWITCH
- IETF
Top 10 DANE TLDs

- .de 121 39%
- .net 67 22%
- .org 35 11%
- .com 34 11%
- .eu 15 5%
- .uk 5 2%
- .ch 13 4%
- .cz 9 3%
- .info 5 2%
- .nl 5 2%

Viktor Dukhovni on IETF DANE mailinglist, 14.11.2014
OPENPGPKEY Resource Record

> Publish PGP/GPG public keys in DNS
> Local part of mail address hashed
> Replace or augment PGP-keyserver
> Benefits over current Keyservers:
  > Key removal!
  > Keys authenticated by DNSSEC domain ownership and web-of-trust
DANE OPENPGPKEY

Mail client

Mail server

(1) request for OPENPGPKEY record(s)

DNS(SEC) resolver

(1) request for OPENPGPKEY record(s)

authoritative DNS
DANE OPENPGPKEY

Mail client

Mail server

DNSSEC resolver

DNSSEC validation

(2) public PGP key(s) for recipient email address

(3) DNSSEC validation

Authoritative DNS
DANE OPENPGPKEY

Mail client

Mail server

DNS(SEC) resolver

authoritative DNS

(4) mail encrypted with public key

(5) encrypted email is sent
SMIMEA Resource Record

- Authenticates email x509 certificates for S/MIME
- Store hash or certificate in DNSSEC secured domain
- Email localpart hashed
  - email clients (MUA, mail user agent) validate x509 certificate/public-key in incoming email
  - email clients fetch x509 public key certificates from DNS
(1) Bob sends Alice email with S/MIME cert attached
DANE S/MIME

Alice

(2) request for SMIMEA records

DNS(SEC) resolver

(2) request for SMIMEA records

Bob

authoritative DNS
DANE S/MIME

(3) S/MIME x509 cert (or hash)

(4) DNSSEC validation

(5) S/MIME x509 cert (or hash) + AD

Alice

Bob

DNS(SEC) resolver

authoritative DNS
DANE S/MIME

(6) Alice encrypts email with Bob's public key

(7) Encrypted email sent

Alice

Bob

DNS(SEC) resolver

authoritative DNS
smilla

- SMIMEA aware Milter
- „Smilla's Sense of Snowden“
- Transparent for users
- In- and outbound encryption
- To be released as Open Source as soon as RFC becomes standard at https://github.com/sys4/
Next Steps DANE WG

> raw-Certificates

> Mutual Authentication
  client-side authentication via TLSA RR

> Payment Association Records
  Link account information/bitcoin wallet to a email adress
Markets for DANE
Who benefits from DANE?

> „Security services“ providers
> Email users with „defined“ security requirements
> Online-Payment, insurance, banks
> Enterprises
> Subcontractor
TLS in .de

- STARTTLS 55%
- Plaintext 45%

2,7 Mio. MX RR > 275.000 MTAs with 12,092 IPv6 \o/ MTAs
DNSSEC in .DE

- signed 1%
- unsigned 99%

“SMTP, STARTTLS, DANE - Wer spielt mit wem?”, Peter Koch, DENIC eG
DENIC – Technisches Meeting, Frankfurt, 2014-09-30
DNSSEC growth in .de

„SMTP, STARTTLS, DANE - Wer spielt mit wem?“, Peter Koch, DENIC eG
DENIC – Technisches Meeting, Frankfurt, 2014-09-30
DNSSEC growth in .NL

PowerDNS DNSSEC deployment graph:
https://xs.powerdns.com/dnssec-nl-graph/
DANE road-blocks?
What people tell

- DNS provider with incomplete or non-existent DNSSEC-support
- DNSSEC is technology but not a use case
- With DNSSEC issues become mission critical
- Missing DNSSEC/DANE monitoring and alarming
- Missing know-how for automated certificate-management and DNSSEC signing
- Missing toolchain for automated management
Registrars

> Major registrars do not offer DNSSEC
> Costs/risks of moving domains between registrars
Coordination

> x509 certs, PGP keys in DNS

> DNS is a loosely consistent database

> don't forget about the caches!

- new cert created, new TLSA record published
- Zonetransfer + TTL of TLSA RRset
- old cert removed from mail-server, TLSA of old cert deleted from DNS zone
DNSSEC is Mission Critical

- DNS is the “ugly duckling“ of network management
- DNSSEC might require a new/better DNS design
- DNSSEC requires „trusted peers“
- Expired DNSSEC signatures can make domain „vanish“ (until the SIGs are renewed)
DANE Validator

ripe.net  DNSSEC ✅  TLSA ✅  SMTP ✅

The domain lists the following MX entries:

200 koko.ripe.net

No TLSA records.

250 kaka.ripe.net

This MX host has been ignored due to a problem with a higher-priority host.
Takeaway

- DNSSEC as a „one-time-cost“
- Open standard
- DANE allows scalable and secure trust-management
- Reduces management costs
- Automates rollover
- Software support is here: Postfix, Exim, OpenSMTPd, OpenPGPKEY milter, smilla