

# One year of DANE

(some)

# Lessons Learned

Jaap Akkerhuis  
NLnet Labs

# Disclaimer

Original work by sys4.de

All errors are mine

# DNSSEC & Dane

- DNSSEC is not an application
- Authenticated data enables other use
- Dane (DNSSEC Authenticated Name Entities)
- Secure and Verify

# Encryption models

## Opportunistic

- Expect anything
- Downgrade of not offered
- Silent on failure

## Mandatory

- Expect encryption
- Identify other side
- Force
- Alarm on failure

(What is the priority: message security?)

# Opportunistic TLS ISSUES

- 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?

The screenshot shows a Google Chrome browser window with the address bar displaying [www.heise.de/thema/DigiNotar](http://www.heise.de/thema/DigiNotar). The page content includes:

- DigiNotar** logo and navigation links.
- Fatale Panne bei Zertifikatsherausgeber Türktrust**  
04. Januar 2013, 12:32 Uhr | 195 | heise Security  
Zwei für Kunden ausgestellte SSL-Zertifikate eigneten sich dazu, Zertifikate für beliebige Domains auszustellen. Mit einem der beiden wurde ein Wildcard-Zertifikat für Google.com erzeugt. Mehr...
- 29C3: "Das SSL-System ist grundlegend defekt - und jemand muss es reparieren"**  
28. Dezember 2012, 21:00 Uhr | 162 | heise online  
Nach den Vorfällen um den Zertifikats-Anbieter Diginotar plant die EU-Kommission durch eine Regulierung das Vertrauen in die Verschlüsselung wieder herzustellen. Doch die Regelung greife viel zu kurz, meint der Forscher Axel Ambak auf dem 29C3. Mehr...
- Protokoll eines Verbrechens: DigiNotar-Einbruch weitgehend aufgeklärt**  
02. November 2012, 07:00 Uhr | 80 | heise Security  
Auf rund 100 Seiten hat das mit der Untersuchung des SSL-GAU's beauftragte Unternehmen Fox-IT seine Ergebnisse zusammengetragen. Eine spannende Lektüre – nicht nur für Admins. Mehr...
- EU-Behörde für IT-Sicherheit kritisiert Zertifizierungsstellen**  
07. Dezember 2011, 17:55 Uhr | 22 | heise Security

On the right side, there is a 'Top-News' section with articles like 'Gesellschaft für Informatik: BSI soll Lücken veröffentlichen' and 'Internetkonzerne wollen NSA-Befugnisse beschneiden lassen'. Below that is a 'neue Videos' section with a video titled 'nachgehakt: Online-Banking'.

# MITM Attack

- Attacker can intercept TLS secured communication with a matching certificate (Common Name)
- Easily done since everyone accepts self signed certificates...



# Session downgrade

The screenshot shows a web browser window with the URL <https://www.eff.org/deeplinks/2014/11/starttls-downgrade-attacks>. The page features the Electronic Frontier Foundation (EFF) logo and navigation menu. The main content area displays the article title "ISPs Removing Their Customers' Email Encryption" by Jacob Hoffman-Andrews, dated November 11, 2014. The article text discusses how ISPs like Verizon tamper with web requests to inject tracking cookies and strip the STARTTLS security flag from email traffic, leading to unencrypted email transmission. A sidebar on the right contains a "Donate to EFF" button, a "Stay in Touch" sign-up form, and a link to "NSA Spying" resources.

ISPs Removing Their Customers' Email Encryption | Electronic Frontier Foundation - Google Chrome

<https://www.eff.org/deeplinks/2014/11/starttls-downgrade-attacks>

**EFF** ELECTRONIC FRONTIER FOUNDATION  
DEFENDING YOUR RIGHTS IN THE DIGITAL WORLD

HOME ABOUT OUR WORK **DEEPLINKS BLOG** PRESS ROOM TAKE ACTION SHOP

NOVEMBER 11, 2014 | BY JACOB HOFFMAN-ANDREWS

## 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.<sup>1</sup>

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.

This type of STARTTLS stripping attack has mostly gone unnoticed because it tends to be applied to residential networks, where it is uncommon to run an email server<sup>2</sup>. STARTTLS was also relatively

Donate to EFF

Stay in Touch

Email Address

Postal Code (optional)

SIGN UP NOW

NSA Spying

[eff.org/nsa-spying](http://eff.org/nsa-spying)

EFF is leading the fight against the NSA's illegal mass surveillance program. [Learn](#)

# 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
```

# Automation? NOT!

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



# Trust but Verify!

# The Plan

- Add a policy channel
- Add a trust layer
- Indicate encryption
- Indicate identity

# 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**

1010110010100101011000000101100001000000111  
0011010111111100011110110100001111110111  
11110101000011110101010010010011111011011  
001010010111000001101000010000001000001  
0000111011010011101001011011000010111  
10001011011001011000010001100100001  
0001110101101001101100011111101011  
0010110100100110001001100011110111  
0101100100100100010110110110111  
10010100100001100001001100  
00100100011111001010101  
11100010111001110100111  
10110110111011101101101  
0001010010100101001  
10001100100100101  
111011011001101101101101  
10111100011101  
00110101100  
00101000  
111  
101

# HTTPS



# TLSA Resource Record

```
      _443._tcp.www.sys4.de. IN TLSA 3 0 1 9273B4E9040C1B...
      |      |      |
Port--      |      |
Protocol--   |      |
Host-----
Resource type-----
Certificate Usage -----
Selector -----
Matching Type -----
Certificate Association Data -----
```

Mo... ▾ CircleID: News B... ▾ Latest f... ▾

**[\*]sys4**

Deutsch About us

Messaging Automation Sc... Security Management

**sys4 is a group of well-known open source experts.**

**We excel at building interdisciplinary systems.**

**You get custom-fit solutions.**

The screenshot shows a web browser window with the URL <https://www.dnssec-validator.cz>. The browser's address bar and tabs are visible. The website's navigation menu includes [HOME](#), [DOWNLOAD](#), [DOCUMENTATION](#), and [DEVELOPMENT](#). The main content area features a large graphic with a green key icon and an orange padlock icon, with the text "DNSSEC TLSA VALIDATOR" and "DNSSEC/TLSA Validator add-on for Web Browsers". A blue "Download" button is positioned to the right of the graphic. Below the graphic, there are sections for "About", "Description", and "News".

**About**

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.

**Description**

DNSSEC/TLSA Validator 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 connecting to the correct IP address assigned for this domain name. If a valid DNSSEC chain related to the domain is found the plug-in will also check for the existence of TLSA records. TLSA records store hashes of remote server TLS/SSL certificates. The authenticity of a TLS/SSL certificate for a domain name is verified by **DANE** protocol (RFC 6698). DNSSEC and TLSA validation results are displayed by using several icons.

**News**

**Version: 2.2.0**

**New Features:**

- New js-ctypes-based interface for Firefox.
- New validator implementation for Chromium/Chrome/Opera Messaging.
- Added new state notification for non-existent (according to DNSSEC) records.
- Polish localisation.

**Bugfixes:**

- Updated prefixes for DNSSEC records for js-ctypes extension.
- Fixed bug in type 2 TLSA records.
- Fixed some warnings in the browser tool-bar.
- Build mechanism fixes.
- Added name-spaces to the configuration file.

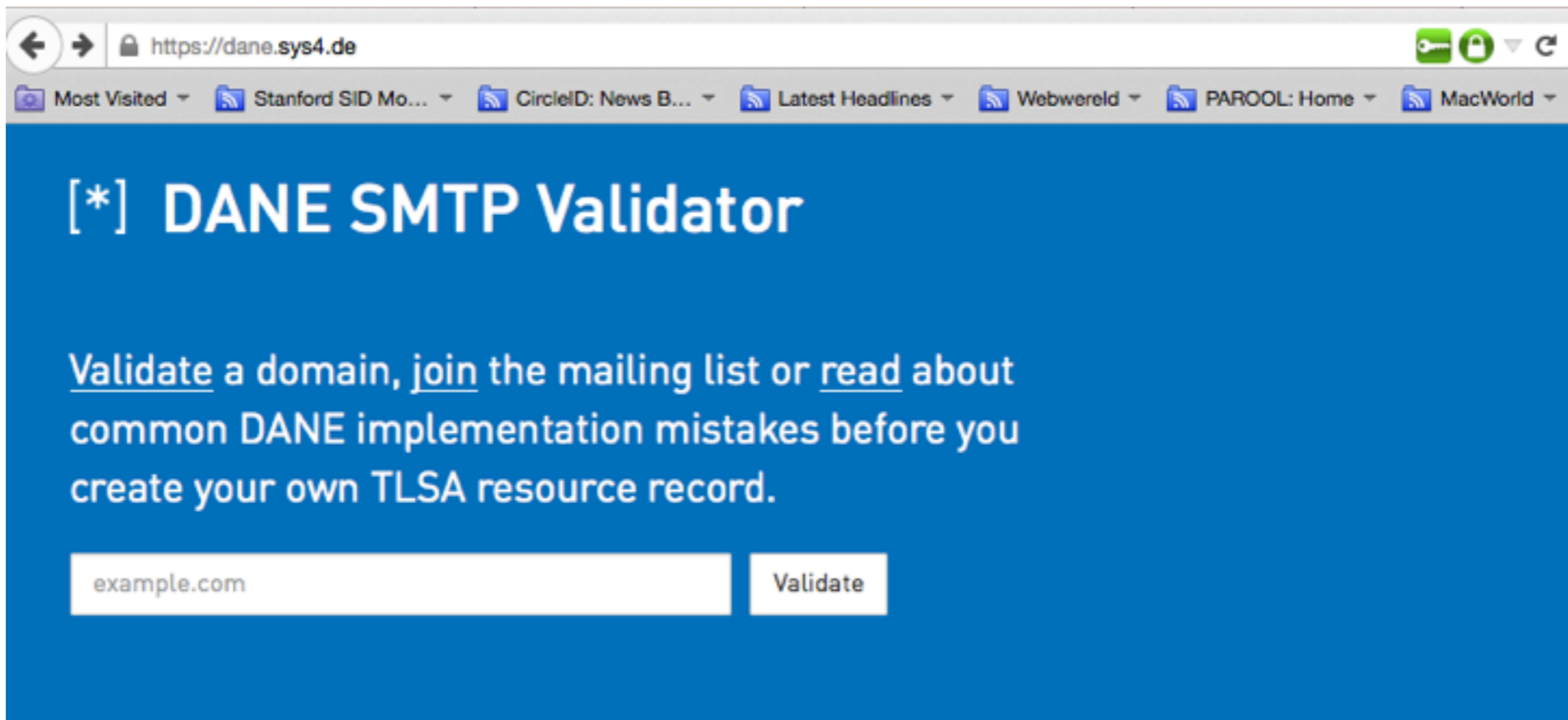
# SMTTP

# TLSA Resource Record

```
      _25._tcp.open.nl.netlabs.nl. IN TLSA 3 1 1 544F284D6..
      |   |   |
Port--   |   |
Protocol--|
Host-----
Resource type-----
Certificate Usage-----
Selector -----
Matching Type -----
Certificate Association Data -----
```

# SMTP Security via DANE TLS

- Initial RFC draft published 2013 Wes Hardaker, Viktor Dukhovni
- Currently for IESG DANE
- First implementations
  - Postfix
  - OpenSMTPd
  - Exim



nlnetlabs.nl

DNSSEC

TLSA

SMTP

The domain lists the following MX entries:

### 50 open.nlnetlabs.nl

DNSSEC

TLSA

SMTP

[Show Details](#)

#### IP Addresses

185.49.140.10

2a04:b900:0:0:1:0:0:10

#### Usable TLSA Records

3, 1, 1 544f284d66af2de0[...]a62b55ab7ac269be

3, 1, 1 f7db964ed80ed077[...]37ad0ccfbfe2359f - certificate not trusted: [27] - certificate not trusted: [27]

### 90 mcvox.nlnet.nl

DNSSEC

TLSA

SMTP

[Show Details](#)



# OpenPGP & S/MIME

# OpenPGP & S/MIME

*Under Construction*

- Local email parts are a mess
- “Local Part”@email.example.org
- Non RFC-compliant behaviour
- Non standard Variations
- Foo.Bar synonym for foobar?
- Déjà vu all over again...

# Some Lessons

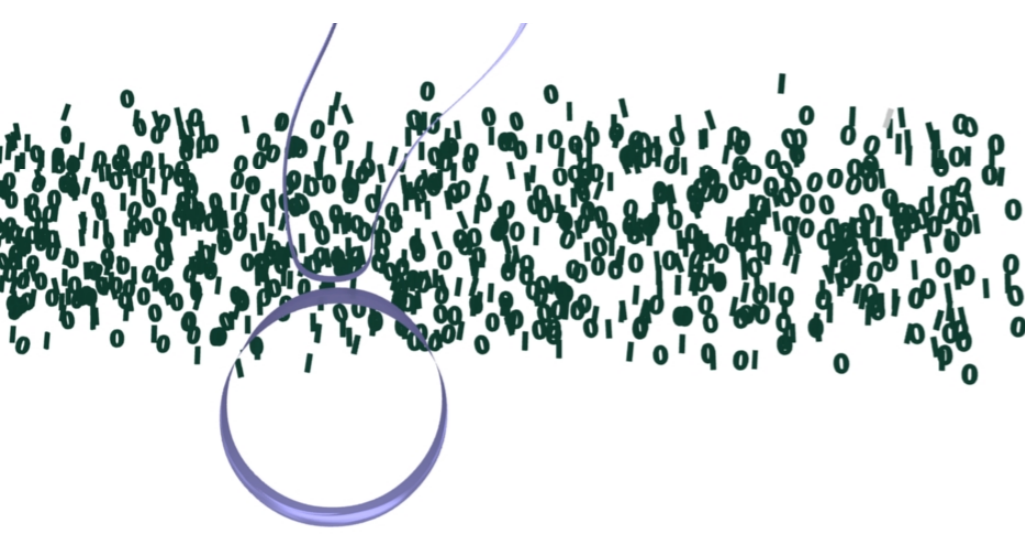
- DNS is infrastructure to build upon
- DNSSEC is an security enabling technology
- DANE verifies “trustworthiness” level

# What people tell

- DNS provider with incomplete or non-existent DNSSEC-support
- 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

# “Takeaways”

- DNSSEC as a „one-time-cost“ infrastructure
- Open standard
- DANE allows scalable and secure trust-management
- Reduces management costs
- Automates rollover



# Questions

