# Research Project 1: Implementing DANE

Pieter Lexis

System and Network Engineering

Wed, Feb 8 2012

# Table of contents

Basics

- DNS and DNSSEC
- PKIX and trust
- DANE

Research

- Swede
  - Features
  - Reactions
- Tests and results

Conclusion

# Question

- Who has a basic understanding of DNS?
- Who has a basic understanding of DNSSEC?
- Who has a basic understanding of PKI/SSL/Certificates?

# Domain Name Service

"It's everywhere!"

- Distributed, hierarchical database that stores:
  - IP-addresses (`A`, `AAAA`)
  - Servers that handle mail for the listed domains (`MX`)
  - Delegation information (`NS`)
  - Aliases (`CNAME`, `DNAME`)
  - More!
- Created in the early 80's
- Focus on speed, efficiency and flexibility, *not* security
- Everything is passed in-the-clear
- Multiple security issues (mostly spoofing)
- Control the DNS → control the Internet

# Domain Name Service Security Extensions

- Adds authenticity – ‘transparent sealed envelope’
- Uses new record types
- Backwards compatible
- Has a chain of trust from the root → TLD → somedomain.tld
- Not implemented broadly (no ‘killer’ application)

# Trust on the Internet

“Extended Validation means hotter air!”

- Trust infrastructure on the Internet based on TLS and PKIX (RFC 5280)
- Certificate Authorities verify a cryptographic keypair belongs to a named entity

# Trust on the Internet

“Extended Validation means hotter air!”

- Trust infrastructure on the Internet based on TLS and PKIX (RFC 5280)
- Certificate Authorities verify a cryptographic keypair belongs to a named entity
- All CA signatures are equally valid

# Trust on the Internet

“Extended Validation means hotter air!”

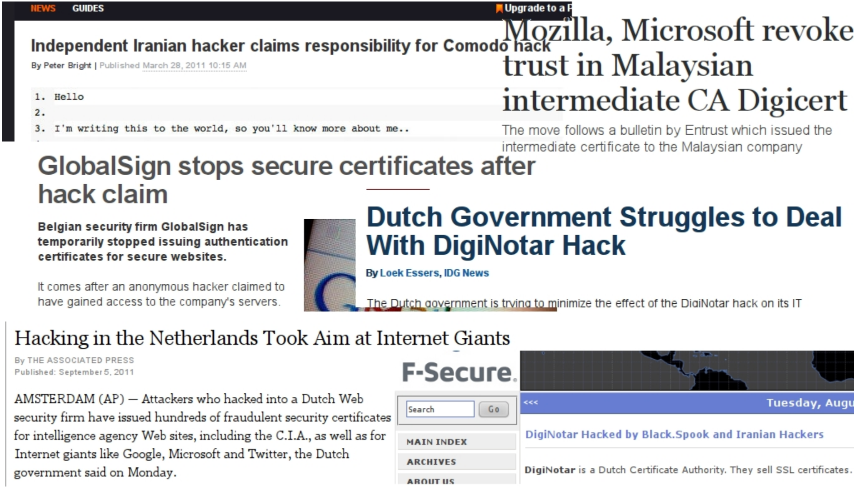
- Trust infrastructure on the Internet based on TLS and PKIX (RFC 5280)
- Certificate Authorities verify a cryptographic keypair belongs to a named entity
- All CA signatures are equally valid
- An average browser trusts 1500 of them

# Trust on the Internet

"Extended Validation means hotter air!"

- Trust infrastructure on the Internet based on TLS and PKIX (RFC 5280)
- Certificate Authorities verify a cryptographic keypair belongs to a named entity
- All CA signatures are equally valid
- An average browser trusts 1500 of them
- To eavesdrop/do nasty stuff, compromise 1 Certificate Authority

# Bad things never happen right?



NEWS GUIDES

Upgrade to a P

## Independent Iranian hacker claims responsibility for Comodo hack

By Peter Bright | Published March 28, 2011 10:15 AM

```
Hello

I'm writing this to the world, so you'll know more about me..
```

## Mozilla, Microsoft revoke trust in Malaysian intermediate CA Digicert

The move follows a bulletin by Entrust which issued the intermediate certificate to the Malaysian company

## GlobalSign stops secure certificates after hack claim

**Belgian security firm GlobalSign has temporarily stopped issuing authentication certificates for secure websites.**

It comes after an anonymous hacker claimed to have gained access to the company's servers.

## Dutch Government Struggles to Deal With DigiNotar Hack

By Loek Essers, IDG News

The Dutch government is trying to minimize the effect of the DigiNotar hack on its IT

## Hacking in the Netherlands Took Aim at Internet Giants

By THE ASSOCIATED PRESS
Published: September 5, 2011

AMSTERDAM (AP) — Attackers who hacked into a Dutch Web security firm have issued hundreds of fraudulent security certificates for intelligence agency Web sites, including the C.I.A., as well as for Internet giants like Google, Microsoft and Twitter, the Dutch government said on Monday.

F-Secure.

Search Go

MAIN INDEX

ARCHIVES

ABOUT US

<<< Tuesday, Augu

DigiNotar Hacked by Black.Spook and Iranian Hackers

**DigiNotar** is a Dutch Certificate Authority. They sell SSL certificates.

# Solutions to this mess?

- Sovereign Keys by the Electronic Frontier Foundation[1]
- Multi-path probing
  - Perspectives by the Carnegie Mellon University[2]
  - Convergence by Moxie Marlinspike[3]
- Out of band pinning of (CA-)certificates to names
  - Chrome's pinning of certificates of high-value websites
  - Tethered Assertions for Certificate Keys (TACK)
  - DNS-based Authentication of Named Entities by the IETF

[1] `https://www.eff.org/sovereign-keys`

[2] `http://perspectives-project.org/`

[3] `http://convergence.io`

# DNS-based Authentication of Named Entities

“DANE, like the dudes from Denmark”

## Why?

- ‘Pin’ a certificate to a named service outside of TLS-sessions
- Allow only 1 CA to issue certificates for an organization
- Create your own CA
- Self-signed certificates

## How?

- Publishing the certificate data in DNS
- Using the DNSSEC Chain of Trust for authentication
- Uses a new DNS resource record (`TLSA`)

# The TLSA record

## Example

```
_443._tcp.www.os3.nl IN TLSA ( 1 0 1
           5819d4c63da043785bf88a9c1ae6f4d3
           f56a4072376d64d7fb89be242bce65b1 )
```

## Wire format

```
                     1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2 2 2 2 3 3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Usage     |   Selector    | Matching Type |               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+               /
/                                                               /
/                 Certificate Association Data                  /
/                                                               /
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

# TLSA fields

## Usage – Describes *how* the matched certificate should be used

| **Value** | **Meaning** |
|---|---|
| 0 | CA certificate |
| 1 | End Entity, must chain to a CA certificate |
| 2 | Use this as a trust anchor |
| 3 | End Entity |

## Selector – Describes *what part* should be matched

| **Value** | **Meaning** |
|---|---|
| 0 | Full certificate |
| 1 | SubjectPublicKeyInfo |

# TLSA fields (cont.)

Matching Type – Describes *how* the association data is matched

| **Value** | **Meaning** |
|---|---|
| 0 | Full data |
| 1 | SHA-256 hash |
| 2 | SHA-512 hash |

Certificate Association Data

The exact bytes to be matched, represented in hex

# Research question

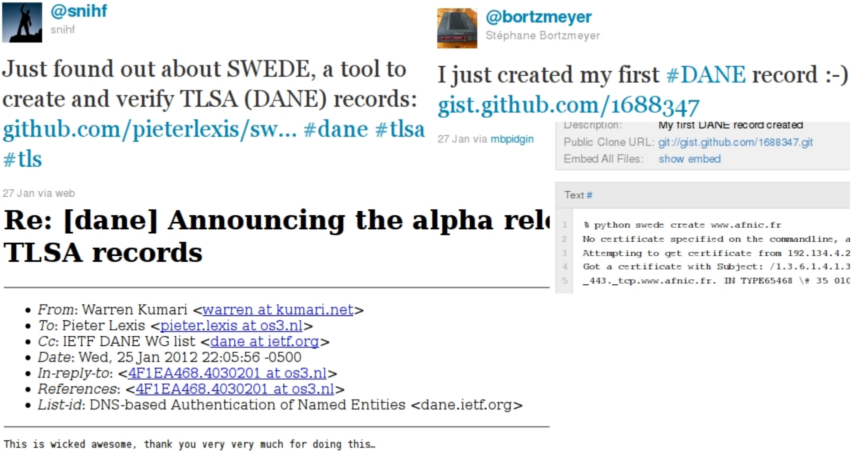
“Is DANE in its current form implementable and does it achieve its goal of securely binding DNS names to TLS certificates?”

# swede – A tool to create and verify TLSA records

"DANE. . . swede, get it?"

- DNSSEC validation for all lookups
- Creation
  - Creates all 24 permutations of TLSA records
  - Loads certificates from the SSL/TLS service or from disk
- Verification
  - Handles multiple TLSA records for the same service
  - Handles CNAME redirections

# Reactions



@snihf
snihf

Just found out about SWEDE, a tool to create and verify TLSA (DANE) records: github.com/pieterlexis/sw... #dane #tlsa #tls

27 Jan via web

@bortzmeyer
Stéphane Bortzmeyer

I just created my first #DANE record :-) gist.github.com/1688347

27 Jan via mbpidgin

Description: My first DANE record created
Public Clone URL: git://gist.github.com/1688347.git
Embed All Files: show embed

Text #

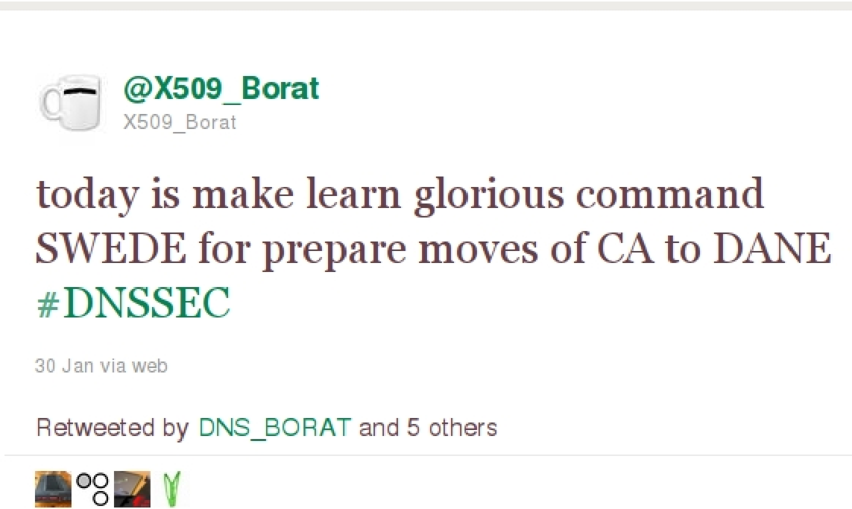
```
% python swede create www.afnic.fr
No certificate specified on the commandline, a
Attempting to get certificate from 192.134.4.2
Got a certificate with Subject: /1.3.6.1.4.1.3
_443._tcp.www.afnic.fr. IN TYPE65468 \# 35 010
```

**Re: [dane] Announcing the alpha rel**
**TLSA records**

- *From*: Warren Kumari <warren at kumari.net>
- *To*: Pieter Lexis <pieter.lexis at os3.nl>
- *Cc*: IETF DANE WG list <dane at ietf.org>
- *Date*: Wed, 25 Jan 2012 22:05:56 -0500
- *In-reply-to*: <4F1EA468.4030201 at os3.nl>
- *References*: <4F1EA468.4030201 at os3.nl>
- *List-id*: DNS-based Authentication of Named Entities <dane.ietf.org>

This is wicked awesome, thank you very very much for doing this…

# It doesn’t count until Borat knows it



@X509_Borat
X509_Borat

today is make learn glorious command SWEDE for prepare moves of CA to DANE #DNSSEC

30 Jan via web

Retweeted by DNS_BORAT and 5 others

# Real-world test

## Setup

- PowerDNS 3.1-pre + `TLSA` patch
- Apache with SSL ports open for:
  - 18 permutations of `TLSA` records
  - 2 `TLSA` records for 1 hostname
  - 2 types of CNAME redirection
  - 1 Wrong record
  - 1 Private CA usage 2 record
  - 1 Usage 3 record

## Method

- Verify (using swede) all records and certificates
- Verify (using swede) records posted on the DANE mailinglist

# Results

“I love results!” – Adam Savage

- All records can be validated (=win!)
- Patched PowerDNS to support the latest `TLSA` format
- `swede` might be included in a ‘secdns’ package with `sshfp`

# Helped the specification forward

- Fixed some typos, included in the current draft
- Re-added certificate encoding obligation to the specification
- Created a test-bed for the Working Group to test against
- Busy creating test-vectors for inclusion in the final draft
- `swede`, obviously

# Conclusion

- DANE can be implemented in its current form
- Some issues remain, but are discussed
- But it could be the ‘killer application’ DNSSEC needs

# QUESTIONS?

DEMO?

Get swede from:
`https://github.com/pieterlexis/swede`