Introduction to the DANE Protocol

ICANN 46
April 10, 2013
Internet Society Deploy360 Programme

Providing real-world deployment info for IPv6, DNSSEC and other Internet technologies:

- Case Studies
- Tutorials
- Videos
- Whitepapers
- News, information

English content, initially, but will be translated into other languages.

www.internetsociety.org/deploy360/
Why Do I Need DNSSEC If I Have SSL?

A common question:

• *why do I need DNSSEC if I already have a SSL certificate? (or an "EV-SSL" certificate?)*

• SSL (more formerly known today as Transport Layer Security (TLS)) solves a different issue – it provides encryption and protection of the communication between the browser and the web server
The Typical TLS (SSL) Web Interaction

1. DNS Resolver queries root DNS server for example.com.
2. Root DNS server returns .com DNS server.
3. Example.com DNS server returns 10.1.1.123.
4. DNS Resolver receives IP address and returns it to Web Browser.
5. Web Browser makes HTTPS request to example.com.

HTTPS://example.com/
The Typical TLS (SSL) Web Interaction

DNS Svr root

DNS Svr .com

DNS Svr example.com

10.1.1.123

1. DNS Request
2. DNS Response
3. DNS Response
4. DNS Request
5. Web Browser Request
6. TLS-encrypted web page

Web Server

Web Browser

example.com?

Is this encrypted with the CORRECT certificate?
What About This?

Web Server

https://www.example.com/

Firewall (or attacker)

1.2.3.4

1

2

Web Browser

DNS Server

www.example.com?

TLS-encrypted web page with CORRECT certificate

TLS-encrypted web page with NEW certificate (re-signed by firewall)
Problems?

DNS Server

Web Server

Web Browser

Firewall

1.2.3.4

1

www.example.com?

https://www.example.com/

TLS-encrypted web page with CORRECT certificate

TLS-encrypted web page with NEW certificate (re-signed by firewall)

www.internetsociety.org/deploy360/
Problems?

Web Server

DNS Server

https://www.example.com/

TLS-encrypted web page with CORRECT certificate

Firewall

1.2.3.4

1

2

Web Browser

www.example.com?

Log files or other servers

Potentially including personal information

TLS-encrypted web page with NEW certificate (re-signed by firewall)
Issues

A Certificate Authority (CA) can sign ANY domain.

Now over 1,500 CAs – there have been compromises where valid certs were issued for domains.

Middle-boxes such as firewalls can re-sign sessions.
A Powerful Combination

- TLS = encryption + *limited* integrity protection
- DNSSEC = strong integrity protection

- How to get encryption + strong integrity protection?

- TLS + DNSSEC = **DANE**
DNS-Based Authentication of Named Entities (DANE)

• Q: How do you know if the TLS (SSL) certificate is the correct one the site wants you to use?

• A: Store the certificate (or fingerprint) in DNS (new TLSA record) and sign them with DNSSEC.

A browser that understand DNSSEC and DANE will then know when the required certificate is NOT being used.

Certificate stored in DNS is controlled by the domain name holder. It could be a certificate signed by a CA – or a self-signed certificate.
DANE

Web Server

https://example.com/

Firewall
(or attacker)

https://example.com/

DNS Server

10.1.1.123 DNSKEY RRSIGs TLSA

Log files or other servers

TLS-encrypted web page with CORRECT certificate

Web Browser w/DANE

Log files or other servers

TLS-encrypted web page with NEW certificate (re-signed by firewall)

DANE-equipped browser compares TLS certificate with what DNS / DNSSEC says it should be.
DANE – Not Just For The Web

• DANE defines protocol for storing TLS certificates in DNS
• Securing Web transactions is the obvious use case
• Other uses also possible:
  • Email via S/MIME
  • VoIP
  • Jabber/XMPP
  • ?
DANE Resources

DANE Overview and Resources:

- http://www.internetsociety.org/deploy360/resources/dane/

IETF Journal article explaining DANE:


RFC 6394 - DANE Use Cases:


RFC 6698 – DANE Protocol:

How Do We Get DANE Deployed?

**Developers:**
- Add DANE support into applications (see list of libraries)

**DNS Hosting Providers:**
- Provide a way that customers can enter a “TLSA” record into DNS as defined in RFC 6698 (http://tools.ietf.org/html/rfc6698)
- This will start getting TLS certificates into DNS so that when browsers support DANE they will be able to do so.
- [More tools are needed to help create TLSA records – ex. hashslinger]

**Network Operators / Enterprises / Governments:**
- Start talking about need for DANE
- Express desire for DANE to app vendors (especially browsers)
Opportunities

• DANE is just *one* example of new opportunities brought about by DNSSEC

• Developers and others already exploring new ideas
Thank You!