Introduction to the DANE Protocol

ICANN 47
July 17, 2013
Internet Society Deploy360 Programme

Providing real-world deployment info for IPv6, DNSSEC, routing 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 requests example.com.
2. DNS Svr.com responds with 10.1.1.123.
3. DNS Svr.example.com resolves example.com.
4. Web Browser connects to 10.1.1.123.
6. Web Browser presents TLS-encrypted web page.
The Typical TLS (SSL) Web Interaction

1. DNS Resolver sends a request for example.com.
2. DNS Resolver receives example.com from root DNS server.
3. DNS Resolver receives example.com from .com DNS server.
4. Web Browser connects to 10.1.1.123.
5. Web Browser connects to https://example.com/.
6. Web Server sends an encrypted message to the browser.

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

1. DNS Server
   - www.example.com?
   - 1.2.3.4

2. Web Server
   - https://www.example.com/

Web Browser
- TLS-encrypted web page with CORRECT certificate

Firewall (or attacker)
- https://www.example.com/
- TLS-encrypted web page with NEW certificate (re-signed by firewall)
Problems?

Web Server → https://www.example.com/

Firewall (or attacker) → https://www.example.com/

Web Browser → Web Server

TLS-encrypted web page with CORRECT certificate

DNS Server → www.example.com?

1.2.3.4

1

2

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

- **Web Server**:  
  - **DNS Server**
    - **Firewall** (or attacker)
      - **Web Browser**
        - **Log files or other servers**
          - **TLS-encrypted web page with CORRECT certificate**
            - **TLS-encrypted web page with NEW certificate (re-signed by firewall)**
              - **Potentially including personal information**

- **https://www.example.com/**
  - 1.2.3.4
  - www.example.com?
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.

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

• TLS = encryption + \textit{limited} integrity protection

• DNSSEC = strong integrity protection

• How to get encryption + strong integrity protection?

• TLS + DNSSEC = \textbf{DANE}
DNS-Based Authentication of Named Entities (DANE) – RFC 6698

• 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-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
  - VoIP
  - Jabber/XMPP
  - ?
DANE Resources

DANE Overview and Resources:


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!