Perspectives on Deploying DNSSEC

ION Sao Paulo
December 5, 2012
Panelists

- Dan York, Internet Society
- Frederico Neves, NIC.BR
- Robert Martin-Legene, Packet Clearing House
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/
What Problem Is DNSSEC Trying To Solve?

DNSSEC = "DNS Security Extensions"

- Defined in RFCs 4033, 4034, 4035
- Operational Practices: RFC 4641

Ensures that the information entered into DNS by the domain name holder is the SAME information retrieved from DNS by an end user.

Let's walk through an example to explain…
A Normal DNS Interaction

Web Server

https://example.com/

Web Browser

example.com?

10.1.1.123

DNS Resolver

Resolver checks its local cache. If it has the answer, it sends it back.

example.com 10.1.1.123

If not…
A Normal DNS Interaction

1. DNS Resolver
2. DNS Svr root
3. 10.1.1.123
4. example.com
5. https://example.com/
6. web page

Web Server
Web Browser
DNS Svr .com
DNS Svr example.com
DNS Svr .com
DNS Svr root

example.com NS
10.1.1.123
example.com NS
DNS Works On Speed

• First result received by a DNS resolver is treated as the correct answer.

• Opportunity is there for an attacker to be the first one to get an answer to the DNS resolver, either by:
  • Getting to the correct point in the network to provide faster responses;
  • Blocking the responses from the legitimate servers (ex. executing a Denial of Service attack against the legitimate servers to slow their responses)
Attacking DNS

1. DNS Resolver
2. example.com?
3. 192.168.2.2
4. 192.168.2.2
5. https://example.com/
6. web page
A Poisoned Cache

Web Server

https://example.com/

Web Browser

192.168.2.2

example.com?

DNS Resolver

Resolver cache now has wrong data:
example.com 192.168.2.2

This stays in the cache until the Time-To-Live (TTL) expires!
How Does DNSSEC Help?

- DNSSEC introduces new DNS records for a domain:
  - **RRSIG** – a signature ("hash") of a set of DNS records
  - **DNSKEY** – a public key that a resolver can use to validate RRSIG

- A DNSSEC-validating DNS resolver:
  - Uses DNSKEY to perform a hash calculation on received DNS records
  - Compares result with RRSIG records. If results match, records are the same as those transmitted. If the results do NOT match, they were potentially changed during the travel from the DNS server.
A DNSSEC Interaction

Web Server

https://example.com/

Web Browser

example.com?

DNS Resolver

10.1.1.123

DNS Svr root

DNS Svr .com

DNS Svr example.com

web page
But Can DNSSEC Be Spoofed?

• But why can't an attacker simply insert DNSKEY and RRSIG records? What prevents DNSSEC from being spoofed?

• An additional was introduced, the "Delegation Signer (DS)" record

• It is a fingerprint of the DNSKEY record that is sent to the TLD registry

• Provides a global "chain of trust" from the root of DNS down to the domain

• Attackers would have to compromise the registry
A DNSSEC Interaction

1. The DNS Resolver queries the DNS server for example.com.
2. The DNS server returns the DNSKEY and RRSIGs.
3. The DNS Resolver verifies the DNSKEY and RRSIGs.
4. The DNS Resolver queries the DNS server for 10.1.1.123.
5. The Web Server returns the web page.
6. The Web Browser displays the web page.
The Global Chain of Trust

Web Server

https://example.com/

Web Browser

web page

DNS Resolver

example.com?

10.1.1.123

10.1.1.123

DNSKEY RRSIGs

DNS Svr example.com

DNS Svr .com

DNS Svr root
Attempting to Spoof DNS

Web Server

Web Browser

DNS Resolver

DNS Svr root

DNS Svr .com

DNS Svr example.com

Example DNS Svr example.com

10.1.1.123

DNSKEY RRSIGs

192.168.2.2

DNSKEY RRSIGs

1

2

3

6

5

https://example.com/

example.com?
Attempting to Spoof DNS

1. DNS Resolver requests DNS records for example.com.
2. DNS Svr returns DNSKEY RRSIGs.
3. DNS Svr returns SERVFAIL.
4. Web Browser receives SERVFAIL.
5. Web Browser requests https://example.com/.

DNS Svr root.
DNS Svr .com.
DNS Svr example.com.

Internet Society

www.internetsociety.org/deploy360/
What DNSSEC Proves:

• "These ARE the IP addresses you are looking for." (or they are not)

• Ensures that information entered into DNS by the domain name holder (or the operator of the DNS hosting service for the domain) is the SAME information that is received by the end user.
The Two Parts of DNSSEC

- Signing
  - Registries
  - Registrars
  - DNS Hosting

- Validating
  - Applications
  - Enterprises
  - ISPs
DNSSEC Signing - The Individual Steps

- **Registry**
  - Signs TLD
  - Accepts DS records
  - Publishes/signs records

- **Registrar**
  - Accepts DS records
  - Sends DS to registry
  - Provides UI for mgmt

- **DNS Hosting Provider**
  - Signs zones
  - Publishes all records
  - Provides UI for mgmt

- **Domain Name Registrant**
  - Enables DNSSEC (unless automatic)
DNSSEC and SSL
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

Web Server

Web Browser

https://example.com/

DNS Resolver

DNS Svr root

DNS Svr .com

DNS Svr example.com

DNS Svr example.com

example.com?

10.1.1.123

10.1.1.123

TLS-encrypted web page

www.internetsociety.org/deploy360/
The Typical TLS (SSL) Web Interaction

Web Server

Web Browser

https://example.com/

DNS Resolver

example.com?

DNS Svr root

DNS Svr .com

DNS Svr example.com

10.1.1.123

1

4

10.1.1.123

5

https://example.com/

6

TLS-encrypted web page

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

Web Server

DNS Server

Firewall (or attacker)

Web Browser

https://www.example.com/

TLS-encrypted web page with CORRECT certificate

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

Web Server

Web Browser

DNS Server

---

https://www.example.com/

TLS-encrypted web page with CORRECT certificate

Firewall

1.2.3.4

1

2

Web Browser

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

www.example.com?
Problems?

- Web Server
- Web Browser
- DNS Server

HTTPS://www.example.com/

TLS-encrypted web page with CORRECT certificate

Firewall

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

Log files or other servers

Potentially including personal information
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

TLS-encrypted web page with CORRECT certificate

Firewall (or attacker)

Log files or other servers

DNS Server

.example.com?

10.1.1.123

DNSKEY RRSIGs TLSA

Web Browser w/DANE

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:

• http://tools.ietf.org/html/rfc6394

RFC 6698 – DANE Protocol:

• http://tools.ietf.org/html/rfc6698
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. hasheslinger]

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
Getting DNSSEC Deployed
Three Steps TLD Operators Can Take:

1. Sign your TLD!
   • Tools and services available to help automate process

2. Accept DS records
   • Make it as easy as possible (and accept multiple records)

3. Work with your registrars
   • Help them make it easy for DNS hosting providers and registrants

4. Help With Statistics
   • Can you help by providing statistics?

Implement DNSSEC and make your TLD more secure!
Three Requests For Network Operators

1. Deploy DNSSEC-validating DNS resolvers

2. Sign your own domains where possible

3. Help promote support of DANE protocol
   - Allow usage of TLSA record. Let browser vendors and others know you want to use DANE. Help raise awareness of how DANE and DNSSEC can make the Internet more secure.
Internet Society Deploy360 Programme

Can You Help Us With:

- Case Studies?
- Tutorials?
- Videos?

How Can We Help You?

www.internetsociety.org/deploy360/
Thank You!
Download A DNSSEC Whitepaper

“Challenges and Opportunities in Deploying DNSSEC”