Opportunities For ccTLDs With DNSSEC

Dan York, CISSP
Senior Content Strategist, Internet Society

ccNSO Meeting, ICANN 45
Toronto, Canada
October 16, 2012
.EH
market to startups
Great success!
pl.eh
The next Facebook

THE social network
Pl.eh = 😊
ccTLD = 😊

Success = more .EH domains
disrupt
DNS cache poisoning
A Normal DNS Interaction

Web Server

Web Browser

DNS Resolver

1. Resolver checks its local cache. If it has the answer, it sends it back.
   pl.eh 10.1.1.123
   If not…

2. 10.1.1.123

3. https://pl.eh/

4. Web page
A Normal DNS Interaction

1. DNS Resolver queries root DNS server for .eh domain.
2. Root DNS server sends response to DNS Resolver.
3. DNS Resolver queries pl.eh DNS server.
4. DNS Resolver receives response with IP address for pl.eh.
5. Web Browser requests web page for https://pl.eh/.
DNS works on speed
First result wins
What if someone else responds first?
Attacking DNS

1. Request pl.eh from DNS Resolver
2. DNS Svr root lookup
3. DNS Svr pl.eh lookup
4. DNS Svr pl.eh returns 192.168.2.2
5. Web Browser requests https://pl.eh/
6. Web Server sends web page

DNS Svr root
DNS Svr .eh
DNS Svr pl.eh
Attacking DNS Svr pl.eh
A Poisoned Cache

Web Server

Web Browser

DNS Resolver

Resolver cache now has wrong data:
pl.eh 192.168.2.2

This stays in the cache until the Time-To-Live (TTL) expires!
Oops
Unhappy Users
Exposure of personal information
Pl.eh = 😞
Aha!
.eh TLD is signed with DNSSEC
pl.eh gets signed
A DNSSEC Interaction

1. Web Browser requests pl.eh/ from DNS Resolver.
2. DNS Resolver queries DNS Svr pl.eh.
3. DNS Svr pl.eh returns 10.1.1.123 DNSKEY RRSIGs.
4. DNS Resolver receives 10.1.1.123.
5. Web Browser receives https://pl.eh/.
6. Web Browser displays web page.

Web Server
Web Browser
DNS Resolver
DNS Svr root
DNS Svr .eh
DNS Svr pl.eh

www.internetsociety.org/deploy360/
DNS Resolver:

- Uses DNSKEY to perform calculation on DNS records
- Compares result with RRSIG records
If results match, all is good.

If not…
THESE ARE NOT THE IP ADDRESSES

YOU ARE LOOKING FOR
But wait...
Spoof DNSSEC?
They can try, but…
Delegation Signer (DS) Record
Fingerprint of DNSKEY sent to registry
A DNSSEC Interaction

Web Server

https://pl.eh/

Web Browser

DNS Resolver

pl.eh?

10.1.1.123

10.1.1.123

DNS Svr root

DNS Svr .eh

DNS Svr .eh

DNS Svr pl.eh

pl.eh

NS

DS

DNSKEY
RRSIGs
The Global Chain of Trust

Web Server

Web Browser

DNS Resolver

DNS Svr root

DNS Svr .eh

DNS Svr pl.eh

https://pl.eh/

10.1.1.123

DNSKEY RRSIGs

pl.eh?

DNS Svr root

DNS Svr .eh

DNS Svr pl.eh

Internet Society
Attempting to Spoof DNS

Web Server

Web Browser

DNS Resolver

1. Query for pl.eh
2. Resolve pl.eh
3. Redirect to 192.168.2.2
4. Forward to 10.1.1.123
5. Return web page
6. Load web page

DNS Svr

DNSKEY RR SIGs

10.1.1.123

DNSKEY RR SIGs

192.168.2.2

Attacking DNS Svr

www.internetsociety.org/deploy360/
Attempting to Spoof DNS

1. DNS Resolver
2. DNS Svr .eh
3. DNSKEY RRSIGs
4. SERVFAIL
5. Web Server
6. Web Browser

https://pl.eh/

DNS Svr root
DNS Svr .eh
DNS Svr pl.eh
Attacking DNS Svr pl.eh

192.168.1.2
DNSKEY RRSIGs
0.1.1.123
DNSKEY RRSIGs
pl.eh
DNS Svr pl.eh
.pl.eh
DNS Svr .eh
.eh NS DS
DNS Svr root
.pl.eh
DNS Svr pl.eh

www.internetsociety.org/deploy360/
Also addresses leaving out DNSSEC
If DS record exists, DNSKEY and RRSIGs must exist
Global "chain of trust"
THESE ARE NOT THE IP ADDRESSES

YOU ARE LOOKING FOR
Integrity of DNS answers
Ensuring info entered into DNS is the **SAME** info end user receives
NOT about encryption
These are not the IP addresses you are looking for.
But wait…
I've got SSL (TLS)
EV-SSL
Why do I need DNSSEC?
The Typical TLS (SSL) Web Interaction

1. DNS Resolver queries 10.1.1.123.
2. DNS Resolver receives DNS Svr .eh.
3. DNS Resolver queries 10.1.1.123.
4. DNS Resolver receives DNS Svr pl.eh.
5. DNS Resolver queries pl.eh.
6. DNS Resolver receives TLS-encrypted web page.

Is this encrypted with the CORRECT certificate?
TLS = encryption + limited integrity protection
Certificate Authority (CA)
1,500+ CAs
Any CA can generate a certificate for ANY domain
compromises
social engineering
weak link
or self-signed cert
signing cert
What About This?

- **Web Server**
  - https://pl.eh/
  - TLS-encrypted web page with CORRECT certificate

- **Firewall** (or attacker)
  - https://pl.eh/
  - TLS-encrypted web page with NEW certificate (re-signed by firewall)
  - 10.1.1.123
  - pl.eh?

- **DNS Server**
  - 10.1.1.123
  - pl.eh?

- **Web Browser**
Oops

Web Server

https://pl.eh/

Firewall (or attacker)

TLS-encrypted web page with CORRECT certificate

https://pl.eh/

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

Web Browser

DNS Server

pl.eh?

10.1.1.123

1

2

www.internetsociety.org/deploy360/
Oops

Web Server

DNS Server

Firewall (or attacker)

Log files or other servers

TLS-encrypted web page with CORRECT certificate

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

Web Browser

Log files or other servers

Potentially including personal information

https://pl.eh/

10.1.1.123

pl.eh?
Hmmm...
TLS = encryption + limited integrity protection
DNSSEC = strong integrity protection
encryption + strong integrity protection?
TLS + DNSSEC ?
TLS + DNSSEC = DANE
"stuff a TLS cert (or a fingerprint) into DNS"
new TLSA record
secured by DNSSEC
Hurrah!

- **Web Server**: TLS-encrypted web page with CORRECT certificate
- **Firewall (or attacker)**: TLS-encrypted web page with NEW certificate (re-signed by firewall)
- **DNS Server**: 10.1.1.123, DNSKEY RRSIGs, TLSA
- **Web Browser w/DANE**: DANE-equipped browser compares TLS certificate with what DNS / DNSSEC says it should be.
- **Log files or other servers**

HTTPS://pl.eh/
THIS IS NOT THE TLS CERTIFICATE

YOU ARE LOOKING FOR
RFC 6698
DANE not just for web
Email – S/MIME
VoIP
Jabber/XMPP
? (anything with certs)
DANE not just for CA-signed certs
Also for self-signed certs!
Beyond DNSSEC and DANE...
Developers are just starting to explore the opportunities!
So...
DNSSEC ensures your ccTLD DNS info isn't modified
DANE upgrades security of Internet services
Together they open up a world of opportunity
Sign your ccTLD…
Profit! 😊
Pretty picture, eh?
The Two Parts of DNSSEC

- Signing
  - Registries
  - Registrars
  - DNS Hosting

- Validating
  - Applications
  - Enterprises
  - ISPs
Today’s Focus

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 Signing - The Players

- Registries
- Registrars
- DNS Hosting Providers
- Domain Name Registrants

Registrar also provides DNS hosting services
DNSSEC Signing - The Players

- Registries
- Registrars
- DNS Hosting Providers
- Domain Name Registrants

Registrant hosts own DNS
Three General Points:

1. **Registries** need to make it as simple as possible for registrars to upload Delegation Signer (DS) records

2. **Registrars** need to make it as simple as possible for DNS hosting providers (including domain name registrants who self-host their DNS) to upload DS records

3. **DNS hosting providers** need to make it as simple - and as automated - as possible for domain name registrants to sign domains
Simplify The Registrar/Hosting Experience

We need to make the DNSSEC-signing process at domain name registrars easy for domain name registrants / holders. Examples:

- Binero in Sweden signs all domains by default
- GoDaddy provides a “one-click” button as part of “Premium DNS” offering
- All keys automatically generated and handled for the domain name holder

www.internetsociety.org/deploy360/
Simplify The DNS Hosting Experience

Another example, Dyn, Inc:

- Provides a simple experience – just click “Add DNSSEC” at the bottom
- Availability of options may be good for technical users but confusing / intimidating for new users

Need this kind of simple interface at more DNS hosting providers
Simplify/Automate Transfer of DS Records

If DNS is hosted with one provider (including self-hosted), process of getting Delegation Signer (DS) record to registrar is primarily copy / paste between web forms.

- Ideally needs to be automated to remove this extra step

Some registrars offering API. Example:

- www.gkg.net/ws/ds.html
Registrars / DNS Hosting Providers

Two technical issues:

- **REGISTRAR TO REGISTRY**
  - Upload of DS records
  - Multiple DS records (to support key rollover)
  - Use of EPP?

- **DNS HOSTING PROVIDER TO REGISTRAR**
  - Upload of DS records
  - No standardized API – mainly propriety APIs or web UI copy/paste
Increase Number of Domain Name Registrars

Need to increase number of domain name registrars supporting DNSSEC

• Good news is that the list keeps increasing!

List from ICANN at:

• www.icann.org/en/news/in-focus/dnssec/deployment

If you are a registrar and support DNSSEC, you can ask to be added to ICANN’s list.

Source: www.icann.org/en/news/in-focus/dnssec/deployment
Next steps...
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/
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!
Thank You!

Want more info?
Attend the "DNSSEC Deployment Workshop" tomorrow or watch the archived recording later.
Additional Material
Review Our DNSSEC Content Roadmap

We have posted a roadmap of the content we believe we need to add to Deploy360 site related to DNSSEC (and IPv6):

www.internetsociety.org/deploy360/roadmap/

We would greatly appreciate feedback:

• Anything missing? Are there additional topics we should consider?
• Will this content help you deploy DNSSEC?
• Please send comments to deploy360@isoc.org
Download A DNSSEC Whitepaper

“Challenges and Opportunities in Deploying DNSSEC”

Other Areas (Beyond Those Mentioned Earlier)

- Tools exist to help automate key signing (ex. OpenDNSSEC)
- The “key rollover” process needs to be well-documented (ex. NASA/Comcast issue)
- Guidance can be found in “DNSSEC Policy & Practice Statements” (often abbreviated “DPS”)
  - http://www.internetsociety.org/deploy360/resources/dnssec-practice-statements/
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. hashslinger]

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