DNSSEC Deployment: Where We Are (and where we need to be)

MENOG 10, Dubai
30 April 2012
richard.lamb@icann.org
DNSSEC: We have passed the point of no return

- Fast pace of deployment at the TLD level
- Stable deployment at root

→ Inevitable widespread deployment across core infrastructure
DNSSEC: Plenty of Motivation

• DNSChanger (10 Nov 2011), Brazilian ISP (7 Nov 2011), calls by government, etc...

• DANE
  – Improved Web TLS for all
  – Email S/MIME for all

• ...and
  – SSH, IPSEC, VoIP
  – Digital identity
  – Other content (e.g. configurations, XML, app updates)
  – Smart Grid
  – A global PKI

http://www.internetsociety.org/deploy360/dnssec/
The BAD: DNSChanger - ‘Biggest Cybercriminal Takedown in History’ – 4M machines, 100 countries, $14M

9 Nov 2011

The BAD: Brazilian ISP fall victim to a series of DNS attacks

7 Nov 2011

http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil
The BAD: Other DNS hijacks*

- 25 Dec 2010 - Russian e-Payment Giant ChronoPay Hacked
- 18 Dec 2009 – Twitter – “Iranian cyber army”
- 13 Aug 2010 - Chinese gmail phishing attack
- 25 Dec 2010 Tunisia DNS Hijack
- 2009-2012 google.*
  - April 28 2009 Google Puerto Rico sites redirected in DNS attack
  - May 9 2009 Morocco temporarily seize Google domain name
- 9 Sep 2011 - Diginotar certificate compromise for Iranian users
- SSL / TLS doesn't tell you if you've been sent to the correct site, it only tells you if the DNS matches the name in the certificate. Unfortunately, majority of Web site certificates rely on DNS to validate identity.
- DNS is relied on for unexpected things though insecure.

*A Brief History of DNS Hijacking - Google
DNSSEC support from government

• Sweden, Brazil, and others encourage DNSSEC deployment

• 22 Mar 2012 - AT&T, CenturyLink, Comcast, Cox, Sprint, TimeWarner Cable, and Verizon have pledged to comply and abide by US FCC recommendations .. “A report by Gartner found 3.6 million Americans getting redirected to bogus websites in a single year, costing them $3.2 billion.,”[1].

• 2009 .gov mandate [2]

DNSSEC: Where we are

- Deployed on 86/313 TLDs (.uk, .fr, .asia, .in, .lk, .kg, .tm, .am, .tw 台灣 台灣, .jp, .cr, .com,...)
- Root signed and audited
- 84% of domain names could have DNSSEC deployed on them
- Large ISP has turned DNSSEC validation “on”*
- A few 3rd party signing solutions (e.g., GoDaddy, VeriSign, Binero,...)
- Unbound, BIND, DNSSEC-trigger, vsResolver and other last mile. DANE standard almost done

*Jan 2012 - 18M COMCAST Internet customers. Others..TeliaSonera SE, Vodafone CZ,Telefonica, CZ, T-mobile NL, SurfNet NL, others..
DNSSEC: Where we are

- But deployed on < 1% of 2^{nd} level domains. Many have plans. Few have taken the step (e.g., paypal.com*).

- DNSChanger and other attacks highlight today’s need.

- Innovative security solutions (e.g., DANE) highlight tomorrow’s value.

What needs to happen

- ISPs need to support DNSSEC*.
- Domain name holders need to sign.
- ...all in a trustworthy fashion.

* Tools to test with https://labs.nic.cz/dnssec-validator/
Barriers to success

• Registrar support*
  – chicken and egg

• Ease of implementation
  – security/crypto/management cost/complexity
  – no click and sign

• Trust
  – insecure practices and processes
  – garbage in, garbage out

Solutions

• Create demand for DNSSEC: Raise awareness of domain holders (content) and users (eyes)
• Ease Implementation:
  – DNSSEC training drawn from existing implementations
  – Key management automation and monitoring
• Trust: Transparent and Secure processes and practices
  – Writing a DPS creates the right mindset for:
    • Separation of duties
    • Documented procedures
    • Audit logging
  – Opportunity to improve overall operations using DNSSEC as an excuse
Learn from CA successes (and mistakes)

• The good:
  – The people
  – The mindset
  – The practices
  – The legal framework
  – The audit against international accounting and technical standards

• The bad:
  – Diluted trust with a race to the bottom (>1400 CA’s)
  – DigiNotar
    • Weak and inconsistent polices and controls
    • Lack of compromise notification (non-transparent)
    • Audits don’t solve everything (ETSI audit)
An implementation can be this$
...or this
..or this (from .cr)

- Secure Off-line Environment
- Offline Laptop with TPM
- Transport public half of ZSKs
- Generate ZSKs
- Sign KSK
- Sign ZSKs with KSK
- Online/off-net DNSSEC Signer with TPM
- Transport KSK signed DNSKEY RRsets
- Sign zones with ZSK
- unsigned zone
- signed zone
- Generate KSK

 Registro de dominios bajo .cr
nic.cr
Academia Nacional de Ciencias
...or even this

**Off-line**

**DATA CENTER**

**CAGE**

**RACK**

**SAFE**

- All in tamper evident bags
- KSK on FD
- Live O/S DVD
- laptop
- RNG

**Off-net**

**DATA CENTER**

**CAGE**

**RACK**

- Zonefile
- ZSKs
- Signer
- Firewall
- Hidden master

- FD with public ZSKs
- FD with KSK signed DNSKEY RRs
But all must have:

• Published practice statement
  – Overview of operations
  – Setting expectations
    • Normal
    • Emergency
  – Limiting liability

• Documented procedures for each operation

• Multi person access requirements

• Audit logs

• Good Random Number Generators

15 Feb 12 – “Ron was wrong, Whit is right”
Summary

• DNSSEC has left the starting gate but without greater support by Registrars, ISPs and domain name holders and trustworthy deployment it...

• Building awareness amongst a larger audience based on recent attacks and pronouncements may be the solution.

• Drawing on lessons learned from certificate authorities makes sure DNSSEC becomes a source of opportunity and innovation floating all boats
Resultant Global PKI
SSL (DANE), E-mail, VOIP security...

CA Certificate roots ~1482

DNSSEC root - 1

Content security
Commercial SSL
Certificates for
Web and e-mail

Yet to be discovered
security innovations,
enhancements, and
synergies

Content security
“Free SSL”
certificates for Web
and e-mail and “trust
agility” (DANE)

Network security
IPSECKEY RFC4025

Securing VoIP

Domain Names

Cross-
organizational and
trans-national
identity and
authentication

E-mail security
DKIM RFC4871

Login security
SSHFP RFC4255

https://www.eff.org/observatory
DNS is a part of all ecosystems

OECS ID effort

Smart Electrical Grid

lamb@xtcn.com

+1-202-709-5262
VoIP

US-NSTIC

Google
OpenID

facebook

PayPal

amazon Prime

e-Passport symbol

PASSPORT

Country of Origin

ICP Brasil

DigiNotar

COMODO

Creating Trust Online

Trust frameworks are not new

Norton SECURED
powered by VeriSign

mydomainname.com