Deploying DNSSEC: From Content to End-customer

InterOp Mumbai 2012
11 October 2012
richard.lamb@icann.org
Terminology

Registrant (Content) ← Registrar ←
  → Registry ← Root ←
  → ISP ← End User (Eyes)

Example:
tata.in (TATA) ← net4.in (Net4) ←
  → nixi.in (NIXI) ← icann.org (ICANN) ←
  → Airtel, Sify, etc.. ← ISP Customer
Creating a Chain of Trust

• Registrant generates, signs their records with and publishes key to Registrar.
• Registrar manages key at the Registry on behalf of the Registrant.
• Registry generates, signs Registrant key with and publishes its own key in root.
• The root generates, signs Registry key with and publishes its own key to public.
• ISP/End User validates Registrant DNS record with Registrant key then Registrant key with Registry key and finally Registry key with root key.
• This creates the chain of trust from content provider (Registrant) to end user.

Registrant ➔ Registrar ➔ Registry ➔ Root ➔ ISP ➔ End User
DNSSEC: We have passed the point of no return

- Fast pace of deployment at the TLD level
- Deployed at root
- Supported by software
- Growing support by ISPs
- Required by new gTLDs

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

- DNSChanger attack, calls for deployment by governments, etc...
- Technology and standards built on DNSSEC*
  - Improved Web TLS and certs for all
  - Secured e-mail (S/MIME) for all
  - SSH, IPSEC, ...
- ...and new applications
  - VoIP
  - Digital identity
  - Secured content delivery (e.g. configurations, updates)
  - Smart Grid
  - A global PKI
  - Increasing trust in e-commerce


*IETF standards complete or currently being developed*
DNSSEC interest from governments

• Sweden, Brazil, Netherlands and others encourage DNSSEC deployment to varying degrees

• Mar 2012 - AT&T, CenturyLink (Qwest), Comcast, Cox, Sprint, TimeWarner Cable, and Verizon have pledged to comply and abide by US FCC [1] recommendations that include DNSSEC. “A report by Gartner found 3.6 million Americans getting redirected to bogus websites in a single year, costing them $3.2 billion.”[2].

• 2008 US .gov mandate. >60% operational. [3]

DNSSEC: Where we are

- Deployed on 94/316 TLDs (.in, .lk, .my, .asia, .tw, 台湾, .kr, 한국, .jp, .kg, .tm, .am, .mm, .ua, .cr, .cz, .bi, .nl, .fr, .com, .tt, .net, .post, ...)
- Root signed** and audited
- >84% of domain names could have DNSSEC
- Growing ISP support*
- 3rd party signing solutions are appearing: GoDaddy, VeriSign, Binero, ...***
- S/W H/W support: NLNetLabs/NSD+Unbound, ISC/BIND, Microsoft, PowerDNS, Secure64, Xelerence, ...
- IETF standard on DNSSEC SSL certificates (DANE)

*COMCAST Internet (18M), TeliaSonera SE, Sprint, Vodafone CZ, Telefonica CZ, T-mobile NL, SurfNet NL, SANYO Information Technology Solutions JP, others..

**21 TCRs from: TT, BF, RU, CN, US, SE, NL, UG, BR, Benin, PT, NP, Mauritius, CZ, CA, JP, UK, NZ

*** Partial list of registrars: https://www.icann.org/en/news/in-focus/dnssec/deployment
But...

- But deployed on < 1% (~2M) of 2nd level domains. Many have plans. Few have taken the step (e.g., yandex.com, paypal.com*, comcast.com).
- DNSChanger and other attacks highlight today’s need. (e.g. end-2-end DNSSEC validation would have avoided the problems)
- Innovative security solutions (e.g., DANE) highlight tomorrow’s value.

DNSSEC: So what’s the problem?

• Not enough enterprise IT departments know about it or are busy putting out other fires.

• When they do look into it they hear FUD and lack of turnkey solutions.

• Registrars/DNS providers see no demand
How to implement DNSSEC?

- **For Companies:**
  - Sign your corporate domain names (ask Registrars to support DNSSEC)
  - Just turn on validation on corporate DNS resolvers
- **For Users:**
  - Ask ISP to turn on validation on their DNS resolvers
- Take advantage of ICANN, ISOC and other organizations offering education and training.
"What You Can Do"

• Raise awareness of DNSSEC and its security value in your enterprises. Deploy on your domain names – it is “a feature”.

• Start DNSSEC implementation early, combine with other upgrades. Later, offer hosting as a service.

• At minimum ensure network and resolvers pass DNSSEC responses to end users unscathed to allow validation to occur there.
Trustworthy Implementation
Building in security

• Getting the machinery for DNSSEC is easy (BIND, NSD/Unbound, OpenDNSSEC, etc.).

• Finding good security practices to run it is not.
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 (CR NIC)

Offline Laptop with TPM

Secure Off-line Environment

Transport KSK with TPM

Sign ZSKs with KSK

Generate KSK

Transport public half of ZSKs

Online/off-net DNSSEC Signer with TPM

Generate ZSKs

Sign zones with ZSK

unsigned zone

signed zone

Animated slide
...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
- signer
- firewall
- hidden master

FD with public ZSKs

FD with KSK signed DNSKEY RRsets
But all must have:

- Published practice statement
  - Overview of operations
  - Setting expectations
    - Normal
    - Emergency
  - Limiting liability
- Documented procedures
- Multi person access requirements
- Audit logs
- Monitoring (e.g., for signature expiry)
- Good Random Number Generators

Useful IETF RFCs:
Summary

DNSSEC has left the starting gate but without greater deployment by domain name holders, support from Registrars, and trustworthy deployment by operators, we may miss the opportunity to improve overall Internet security and develop innovative new security solutions.
DNS is a part of all IT ecosystems

OECS ID effort

Smart Electrical Grid

Trust frameworks are not new