The Business Case for DNSSEC

• Cyber security is becoming a greater concern to government, enterprises and end users. DNSSEC is a key tool and differentiator.
• DNSSEC is the biggest security upgrade to Internet infrastructure in over 20 years.
• DNSSEC is a critical tool in combating the global nature of cyber crime providing a cross-organizational and trans-national platform for innovative security solutions and authentication.
• DNSSEC infrastructure deployment has been brisk but requires expertise. Getting ahead of the curve is a competitive advantage.
Where DNSSEC fits in

• DNS converts names (www.tata.in) to numbers (64.37.102.54)
• ..to identify services such as www and e-mail
• ..that identify and link customers to business and visa versa
Where DNSSEC fits in

• ..but CPU and bandwidth advances make legacy DNS vulnerable to MITM attacks
• DNS Security Extensions (DNSSEC) introduces digital signatures into DNS to cryptographically protect contents from modification
• With DNSSEC fully deployed a entities can be sure the customer gets un-modified data (and visa versa)
The Original Problem: DNS Cache Poisoning Attack

www.majorbank.se=5.6.7.8

DNS Resolver

Get page
Login page
Username / Password
Error

ISP / ENTERPRISE / END NODE

Password database

DNS Server

www.majorbank.se = 1.2.3.4

Attacker
www.majorbank.se = 5.6.7.8

Attacker
webserver
www @ 5.6.7.8

Animated slide in .ppt
detailed description at: http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html
Argghhh! Now all ISP customers get sent to attacker.

www.majorbank.se =? 5.6.7.8 → DNS Resolver → www.majorbank.se = 1.2.3.4

Get page → Attacker webserver www @ 5.6.7.8
Login page
Username / Password
Error

Password database

Animated slide in .ppt
The Bad: DNSChanger - ‘Biggest Cybercriminal Takedown in History’ – 4M machines, 100 countries, $14M

DNS Malware: Is Your Computer Infected?

DNS—Domain Name System—is an Internet service that converts user-friendly domain names, such as www.fbi.gov, into numerical addresses that allow computers to talk to each other. Without DNS and the DNS servers operated by Internet service providers, computer users would not be able to browse websites, send email, or connect to any Internet services.

Criminals have infected millions of computers around the world with malware called DNSChanger which allows them to control DNS servers. As a result, the cyber thieves have forced unsuspecting users to fraudulent websites, interfered with their web browsing, and made their computers vulnerable to other kinds of malicious software.

End-2-end DNSSEC validation would have avoided the problems


End-2-end DNSSEC validation would have avoided the problems
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
The Good: Securing DNS with DNSSEC

www.majorbank.se = ?
1.2.3.4

DNS Resolver with DNSSEC

DNS Server with DNSSEC

Attacker’s record does not validate – drop it
www.majorbank.se = 1.2.3.4
Attacker
www.majorbank.se = 5.6.7.8

Get page
Login page

Username / Password
Account Data

webserver
www @ 1.2.3.4

Animated slide in .ppt
The Good: Resolver only caches validated records

www.majorbank.se =?
1.2.3.4

DNS Resolver with DNSSEC

www.majorbank.se = 1.2.3.4

DNS Server with DNSSEC

Get page
Login page

Username / Password
Account Data

ISP / ENTERPRISE / END NODE

webserver www @ 1.2.3.4

ENTERPRISE

Animated slide in .ppt
DNSSEC interest from governments

• Sweden, Brazil, Czech Republic 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. ~70% operational. [3]

DNSSEC: Where we are

- Deployed on 95/316 TLDs (.br, .cz, .co, .ua, .nl, .bg, .kg, .am, .lv, .ug, .mm, .mn, .de, .eu, .uk, .tt, .pl, .in, .lk, .com, .my ماليزيا, .asia, .tw 台湾, .kr 한국, .jp, .fr, .post, …)
- Root signed** and audited
- New gTLDs require it
- >84% of domain names could have DNSSEC
- Growing ISP support*
- 3rd party signing solutions: GoDaddy, Binero, VeriSign...***
- Vendors support it: ISC/Bind, Microsoft, ...
- New standards being developed on DNSSEC (e.g., IETF RFC6698 SSL Certificates)
- Growing interest from others major players...

*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
The Bad: SSL Dilution of Trust
The Good: DNSSEC = Global “free” PKI

CA Certificate roots ~1482

Content security
Commercial SSL
Certificates for
Web and e-mail

DANE and other yet to be
discovered security
innovations, enhancements,
and synergies

DNSSEC root - 1

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

Network security
IPSECKEY RFC4025

E-mail security
DKIM RFC4871

Cross-
organizational and
trans-national
identity and
authentication

Securing VoIP

Domain Names

Login security
SSHFP RFC4255

https://www.eff.org/observatory
Opportunity: New Security Products

- Improved Web SSL and certificates for all*
- Secured e-mail (S/MIME) for all*
- Validated remote login SSH, IPSEC*
- Securing VoIP
- Cross organizational digital identity systems
- Secured content delivery (e.g. configurations, updates, keys)
- Securing Smart Grid efforts
- A global PKI
- Increasing trust in e-commerce


*IETF standards complete or currently being developed RFC6698
DNS is a part of all IT ecosystems

US-NSTIC effort

OECS ID effort

Smart Electrical Grid

Trust frameworks are not new
DNSSEC: Classic bottom-up, multi-stakeholder built Internet infrastructure upgrade to help address today’s needs and create tomorrow’s opportunity.
DNSSEC @ the root: A bottom-up, multi-stakeholder operation
Community driven

• Listened to calls from global community for deployment:
  – Internet community (e.g., RIPE, APNIC, ccNSO...)
  – Governments
  – Business (e.g., Kaminsky 2008, Press)
Deploying it

• Problem
  – Bureaucracy and Fear: Hard to change anything that has not changed since 1983. Many excuses not to.
  – root - An internationally agreed to single key – right
  – Trust me - I will manage the root key. ..uh huh.
Approach

• Eliminate excuses and lead by example – start at root

• Solution
  – Multi-stakeholder – get buy in up front
  – Bottom up – like the Internet itself
  – Transparency and Choice
  – Draw from existing secure practices and trusted models
DNSSEC at the root: result

• Deployed 15 July 2010
• Completed in ~2years
• Biggest upgrade to the Internet’s core infrastructure in 20 years
• Set the stage for deployment in rest of hierarchy (e.g., top level domains, end user domains)
• Got global buy in
• Direct stakeholder participation in key management – 21 Trusted Community Representatives made up of respected members of Internet community from 18 countries
  • Currently: URUGUAY, BRAZIL, TRINIDAD AND TOBAGO, CANADA, BENIN, SWEDEN, NEPAL, NETHERLANDS, NEW ZEALAND, RUSSIAN FEDERATION, PORTUGAL, JAPAN, MAURITIUS, CHINA, BURKINA FASO, CZECH REPUBLIC, UNITED KINGDOM, USA
• Enabled DNSSEC deployment throughout hierarchy – need just one key to validate all
• Publish, broadcast everything.
• Pass 3rd party annual SysTrust audit
• ICANN Secure Key Management Facilities in Culpepper, VA and El Segundo, CA. FIPS 140-2 Level 4 crypto, GSA Class 5 safes, multiple tiers, biometrics, etc.
See root-dnssec at http://dns.icann.org/
Documentation - Root

91 Pages and tree of other documents!

Root DPS
Summary

DNSSEC multi stakeholder effort from start and at root is a concrete operational example of how successful the bottom-up multi-stakeholder approach can be.