The Business Case for DNSSEC

InterOp/ION Mumbai 2012
11 October 2012
richard.lamb@icann.org
The Business Case for DNSSEC

- Cyber security is becoming a greater concern to enterprises, government, and end users. DNSSEC is a key tool and differentiator.
- DNSSEC is the biggest security upgrade to Internet infrastructure in over 20 years. It is a platform for new security applications (for those that see the opportunity).
- 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
• With DNSSEC fully deployed a business can be sure a customer gets un-modified data (and visa versa)
The Original Problem: DNS Cache Poisoning Attack

www.majorbank.se = ?
5.6.7.8

DNS Resolver

DNS Server

ISP / ENTERPRISE / END NODE

Attacker webserver www @ 5.6.7.8

Password database

Get page
Login page

Username / Password
Error

www.majorbank.se = 1.2.3.4

ENTERPRISE

Attacker
www.majorbank.se = 5.6.7.8

Detailed description at: http://unixwiz.net/techtips/iguide-kaminsky-dns-vuln.html
Argghh! Now all ISP customers get sent to attacker.

www.majorbank.se = 5.6.7.8

DNS Resolver

www.majorbank.se = 1.2.3.4

DNS Server

GET page
Login page

Username / Password
Error

Attacker

webserver
www @ 5.6.7.8

Password database
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 web sites, send e-mail, 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

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

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

Attacker’s record does not validate – drop it

www.majorbank.se = 5.6.7.8

Username / Password
Login page

Get page
DNS Resolver with DNSSEC

DNS Server with DNSSEC

webserver
www @ 1.2.3.4

Animated slide
The Good: Resolver only caches validated records

www.majorbank.se=?
1.2.3.4

DNS Resolver with DNSSEC

Get page
Login page
Username / Password
Account Data

ISP / ENTERPRISE / END NODE

webserver www @ 1.2.3.4

ENTERPRISE

DNS Server with DNSSEC

www.majorbank.se = 1.2.3.4

Animated slide
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]

Security as Differentiator and Edge

- **Differentiator**
  - Increased cyber security awareness for govts and industry
  - Major ISP says security now on checklist for customers

- **DNSSEC Service and Support**
  - 94/316 TLDs (e.g., .com,.in,.nl,..)
  - Growing ISPs adoption*
  - Available to 84% of domains
  - Vendor support (ISC/BIND, Microsoft..)
  - gTLDs (e.g., .bank, .search) require it

*COMCAST Internet (18M), TeliaSonera SE, Sprint, Vodafone CZ, Telefonica CZ, T-mobile NL, SurfNet NL, SANYO Information Technology Solutions JP, others..
DNS is a part of all IT ecosystems

Smart Electrical Grid

OECS ID effort

US-NSTIC effort

Trust frameworks are not new
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
- 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
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
DNSSEC: Internet infrastructure upgrade to help address today’s needs and create tomorrow’s opportunity.
The Internet’s Phone Book - Domain Name System (DNS+DNSSEC)

www.majorbank.se = 1.2.3.4

Get page
Login page
Username / Password
Account Data

ISP / HotSpot / Enterprise / End Node

Majorbank.se (Registrant)

DNS Server

.se ( Registry)

DNS Server

.( Root)

Animated slide