Overview of DNSSEC

17 January 2012
Roseau Dominica
richard.lamb@icann.org
• The Internet did not have security designed into it.

• But has demonstrated time and again that it is a platform for innovation - good and bad.
Recent News

• 9 Nov 2011 - DNSChanger/Ghost Click: 4M PCs across 100 countries

• 7 Nov 2011 - Large scale Brazilian ISP DNS poisoning attack

• 3 Aug 2008 - Dan Kaminsky reveals DNS cache poisoning shortcut

• Highlights need for securing DNS

http://www.securelist.com/en/blog/208193214/Massive_DNS_poisoning_attacks_in_Brazil
The Internet's Phone Book - Domain Name System (DNS)

www.majorbank.se =? 1.2.3.4
Get page
Login page
Username / Password
Account Data

DNS Hierarchy
root
se
com
majorbank.se

DNS Resolver

DNS Server

ISP

majorbank

webserver www @ 1.2.3.4
The Problem: DNS Cache Poisoning Attack

DNS Resolver

www.majorbank.se =? 5.6.7.8

Get page
Login page
Username / Password
Error

DNS Server

www.majorbank.se = 1.2.3.4
Attacker
www.majorbank.se = 5.6.7.8

Attacker webserver
www @ 5.6.7.8

Password database
Argghh! Now all ISP customers get sent to attacker.

www.majorbank.se = 1.2.3.4

DNS Resolver

www.majorbank.se = 5.6.7.8

Get page
Login page
Username / Password
Error

Attacker webserver
www @ 5.6.7.8

Password database
Securing The Phone Book - DNS Security Extensions (DNSSEC)

- Add keys to hierarchy; 15+ years of standards work; backwards compatible

www.majorbank.se = ?
1.2.3.4

DNS Resolver with DNSSEC

Get page
Login page
Username / Password
Account Data

www.majorbank.se = 1.2.3.4

Attacker’s record does not validate – drop it

Attacker www.majorbank.se = 5.6.7.8

webserver www @ 1.2.3.4
Resolver only caches validated records

www.majorbank.se = 1.2.3.4

DNS Resolver with DNSSEC

Get page
Login page
Username / Password
Account Data

DNS Server with DNSSEC

webserver www @ 1.2.3.4
DNSSEC Deployment
Where we are now

- < 1% DNSSEC still needs to be deployed on more domain names.
- 82/312 top level domain (e.g., .se) have DNSSEC deployed. Multi-stakeholder managed root key.
- 82% of domain names can have DNSSEC deployed on them. Large ISP in US has turned DNSSEC “on”.
- Supported by DNS implementations

Last week ALL 17.8 M COMCAST Internet customers. Vodafone, Telefonica CZ
Deploying DNSSEC at the top (root)
An International Multi-Stakeholder, Bottom-up, Cooperative effort

• **Bottom-up**: Responding to calls for deployment at root by Internet Community, IT security researchers, and Governments. Based on 15+ years of development in IETF and experience from early deployments by ccTLDs (SE, BR, PR, etc.).

• **Multi-Stakeholder**: “root signed” 15 July 2010 and managed with direct participation by 21 respected Internet representatives from 17 countries.

• **Transparent**: We publish and broadcast everything and have annual 3rd party audit.
Result

- Biggest upgrade to the Internet’s core infrastructure in 20 years
- Enabled DNSSEC deployment throughout hierarchy
- Who is this guy?
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 and other organizations offering education and training.
But wait, there’s more...

• Looks like we now have a global, secure database for “free”!
• A globally trusted Public Key Infrastructure
• Enabler for global security applications
• An authentication platform for identification
• Cross-organizational and trans-national
• .. A global platform for innovation
Another Source of Trust on the Internet

CA Certificate roots ~1482

Content security
Commercial SSL
Certificates for
Web and e-mail

Yet to be discovered
security innovations,
enhancements, and
synergies

Domain Names

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

Network security
IPSECKEY RFC4025

VoIP securing SIP

Cross-organizational and
trans-national
identity and
authentication

E-mail security
DKIM RFC4871

Login security
SSHFP RFC4255

https://www.eff.org/observatory
Potential Applications

• Build and improve on established trust models, e.g., CAs
• Greatly expanded SSL usage (currently ~4M/200M)
• Make SMIME a reality
• May work in concert with in enhancing or extending other cyber security efforts like digital Identities, WebID, BrowserID, CAs, ..
• Securing VoIP
• Simplify WiFi roaming security
• Secure distribution of configurations (e.g., blacklists, anti-virus sigs)
Opportunity for Indigenous Certification Authorities

• CAs located in only 52 countries

• Even then, some countries are not using their own CAs.

• Synergy: Reduced barriers, Alignment with TLD, DNSSEC operations
DNS is a part of all ecosystems
What needs to still happen

• Needs to be widely deployed across more domain names
• Registrars, ISPs, and hosting providers need to support it in a trustworthy fashion
• DNSSEC validation needs to be pushed to the end user
• Raise awareness of the security benefits of DNSSEC and its secure deployment.
Summary

- DNSSEC is a platform for cyber security innovation and international cooperation.
- DNSSEC does not solve all the ills of the Internet but can become a powerful tool in improving the security of the Internet.
- DNSSEC will be a critical tool in combating the global nature of cyber crime allowing cross-organizational and trans-national authentication.
- DNSSEC is a game changing example of what can result from the bottom-up, multi-stakeholder process the Internet has come to be known for.
- In order to realize the full benefits of DNSSEC, greater end user and domain name owner awareness is needed to drive a virtuous cycle for effective deployment.