DNSSEC Explained

Marrakech, Morocco
June 28, 2006

Ram Mohan rmohan@afilias.info

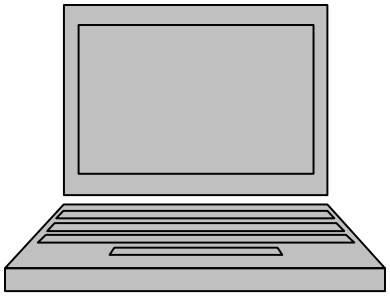
Afilias
GLOBAL REGISTRY SERVICES

Agenda

- Getting Started
  - Finding out what DNS does for you
  - What Can Go Wrong
- A Survival Guide to DNSSEC
  - Why Techies Created DNSSEC
  - What Can Happen Without DNSSEC
- Why Should Anyone Care
  - Consequences
  - Responsibilities of Network Operators (ISPs), Registrars, Registries, Root Operators, ICANN and others
- Q&A Session

What Does The DNS Do For You

- Tells machines where to go when you:
  - Type in a web address
  - Send an email



User

ISP

Name Server Operators

Resolver

Cache

Name Server

Am I online?
Where should I go to get my answer?
- My local Internet Service Provider

Do I already have the answer?
- Send the answer back to resolver

Else, contact Domain Name Server

Find the IP address
Send it back

DNSSEC

Why Attack the DNS

- Anti-Spam and anti-phishing technologies
  - Technologies that use the DNS to mitigate spam and phishing: $$$ value for the ‘Bad Guys’
- StockTickers, RSS feeds
  - Usually no source authentication but supplying false stock information via a stockticker or via a news feed can have $$$ benefit for attacker
- ENUM
  - Mapping telephone numbers to services in the DNS
    - As soon as there is some incentive

- Source: “DNS Security Technical Overview”, Russ Mundy

What Can Go Wrong

- Forgery
  - The DNS data being returned to your ISP can be forged
    - Especially easy on a wireless network
    - Result: You are transported where you did not mean to go
- Poisoning
  - The DNS data can be modified
    - Causes your ISP's cache to have valid but wrong information on where to go
- Eavesdropping
  - Can intercept your DNS data and just "listen" before passing on
- Other things that can go wrong:
  - Alteration of zone data - Impersonation of master/cache - Unauthorized updates

2005 ISP Attack

- In March-April 2005, users of an ISP had specific spyware, spam and pay-per-click trojans, from redirection sites
- The ISP's cache had hundreds of DNS names spoofed…
  - AmericanExpress.com
  - FedEx.com
  - CitiCards.com
  - DHL-USA.com
  - Sabre.com

Source: Allison Mankin

DNSSEC Explained

- DNSSEC is the Internet's answer to DNS Identity Theft
  - It protects users from DNS attacks
  - It makes systems detect DNS attacks
- Almost everything in DNSSEC is digitally signed
  - Allows authentication of the ORIGIN of the DNS data
  - Ensures INTEGRITY of the DNS data
- Digitally signed = "Public Key Cryptography"
  - Secret Private Key, Open Public Key
  - DNS Messages are scrambled using the Private Key – the Public Key is needed to unscramble it [a.k.a. "SIGNING"]
  - You now know WHO sent the message (since private key is unique)
- If data is MODIFIED, mangled, or otherwise compromised en-route…
  - The signature is no longer valid

- DNSSEC = DNS Security Extensions

The Chain of Trust

If I trust a public key from someone, I can use that key to verify the signature … and authenticate the source

- Make sure the root zone key can be trusted
  - Pointers in the root zone point to lower zones (com/org/info/de etc)
  - Each pointer is validated with the previous validated zone key
- Only the key for the root zone is needed to validate all the DNSSEC keys on the Internet
- How to update these keys and propagate them are not done yet

Technical Details behind DNSSEC

- **AUTHENTICATES** every set of DNS data – this is called a DNS Resource Record set, or RRs
  - (A records, MX records, DNAMEs, etc, etc)
- Authenticates **absence** of DNS data
  - xyz.icann.org does not exist
- Creates four **new** DNS record types
- Validates using **Chain Of Trust**
- **Each** answer is signed
- DNSSEC:
  - Provides no CONFIDENTIALITY of DNS data
  - No protection against Denial of Service attacks
- SSL, IPSec are not enough

Roles and Responsibilities

- Registrars, network operators, registries, ICANN, root server operators … large network must coordinate and interact
- Create DNSSEC Capable Name Servers for the TLD and lower level zones
- Put policies together
  - Zone walking
- How to handle key rollover
  - How can you ensure that when the key has to be changed, it is propagated securely, safely, and quickly?

DNSSEC Look-Aside Validation (DLV)

"Put simply, if the root isn't signed and TLDs are not signed, the IETF DNSSEC specification offers no way to start wide scale deployment. DLV, developed outside the IETF, offers such a way." – Paul Vixie, President ISC

- Interim approach to implementing DNSSEC
  - Compensates for no signed root or TLDs
- Provides a secure location to obtain DNSSEC validation information, absent a signed root zone
- DLV is a non-IETF extension to the DNSSEC protocol
- Implemented in BIND 9.3.2 and later
- Implemented and managed by Internet Systems Consortium (ISC)

What Next?

- Root must be signed!
- Sweden (.SE) first TLD to be signed
- DLV registry run by ISC allows “look-aside” mechanism for DNSSEC keys
- Evangelize the need for DNSSEC at industry – companies – organizations
- Policies must be established
- What to read:
  - Introductions: www.dnssec.net
  - Tutorials: http://www.ripe-ncc.org/training/dnssec/material/
  - Other material:
    - http://www.nlnetlabs.nl/dnssec/
    - http://www.ripe.net/disi/

Mailing Lists

- dnssec@cafax.se
  - operators and developers working on dnssec
- namedroppers@ops.ietf.org
  - DNSEXT IETF working group (DNS protocol development)
- dnsop@cafax.se
  - DNSOP IETF working group (operational DNS issues)
- techsec@ripe.net
  - RIPE Technical Security working group
- dns-wg@ripe.net
  - RIPE DNS working group

DNSSEC Explained

Marrakech, Morocco
June 28, 2006

Ram Mohan rmohan@afilias.info