# Securing DNS Infrastructure Using DNSSEC

Ram Mohan

Executive Vice President, Afilias

rmohan@afilias.info

February 28, 2009

ICANN
AT-LARGE SUMMIT
28 FEBRUARY – 5 MARCH 2009

Ciudad de
MÉXiCO

# 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
- The Road Ahead
  - Signing the root
  - What domain name owners can do
- Q&A Session

# What the DNS is used for

- Web, Email, Streaming Media, Instant Messaging – the Internet depends on the DNS
  - DNS decides if your site can be reached
  - DNS determines if your email can be delivered
- DNS is the Internet directory and phone book
  - Provides directions on where computers are for each domain name
- DNS Prevents Outages and Provides Redundancy
  - DNS mismanagement can result in "Internet outages" even if your Internet connection is working

# What Does The DNS Do For You

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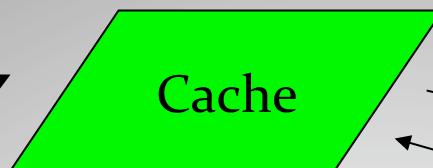  - Type in a web address
  - Send an email

*User*

*ISP*

*Name Server Operators*

**Cache**

**Resolver**

Do I already have the answer?
- Send the answer back to resolver
Else, contact Domain Name Server

**Name Server**

Find the IP address
Send it back

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

mohan_dnssec

Ciudad de
**México**

# Why Attack the DNS

- Money
  - Lot of money waiting to be made (stolen) when ecommerce and banking is compromised
- Power
  - ISPs, Network operators and the Danish Internet user can be hijacked and forcibly redirected
  - Reduces credibility and erodes trust
- Control
  - Allows spying on users without their knowledge or control

# 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

# The Kaminsky Attack

- July 2008 - researcher Dan Kaminsky discloses evidence of massive Internet vulnerability
  - Easy "cache poisoning"
  - Exposes all recursive DNS resolvers to takeover
- Allows all Internet traffic to be hijacked on compromised DNS resolvers
  - Less than one second to compromise a vulnerable server
  - Completely transparent to Internet user

***Worldwide critical problem: DNS vendors and other companies issued emergency patches***

# What Did The Attack Allow

1) Break past most username/password prompts on websites, no matter how the site is built.

2) Break the Certificate Authority system used by SSL, because Domain Validation sends an email and email is insecure.

3) Expose the traffic of SSL VPNs, because the certificate check is now circumvented

4) Force malicious automatic updates to be accepted

5) Cause millions of lines of totally untested network code to be exposed to attack

6) Leak TCP and UDP connectivity behind the firewall, to any website, in an attack we thought we already fixed *twice*

7) Expose the traffic of tools that don't even pretend to be secure, because "it's behind the firewall" or "protected by a split-tunneling IPsec VPN".

Source: http://www.doxpara.com/

mohan_dnssec

# 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

Ciudad de MéXiCo

# 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 Trust Anchor Repositories (TAR)

*A Trust Anchor Repository (TAR) can be defined as a repository or set of repositories that may be used for storing Secure Entry Point (SEP) aka zone keys for one or more DNS zones*

- Interim approach to implementing DNSSEC
  - Compensates for no signed root or TLDs
- Provides secure locations to obtain DNSSEC validation information, absent a signed root zone
- Proposed types of TARs:
  - Global TARs
  - Community of Interest (CoI) TARs
  - Local TARs

# Summary

- Root must be signed!

- 6-7 ccTLDs already signed

- .ORG has announced plans to sign in 1H 2009

- Trust Anchor Repositories allow "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/

# The Road Ahead

## Make the DNS immune to DNS Identity Theft

- **Implement DNSSEC at the root and TLD zones**
  - Immunization against DNS hijacking
- **Proven "Chain of Trust" model protection**
  - Public key cryptography with strong encryption will protect DNS system
- **Secure storage of keys in Trust Anchor Repository**
  - Results in guaranteed lookups in a safe environment
- **Build a strong foundation for domain name owners**
  - Allows domain name owners to digitally sign their domains -- protects their names from hijacking

mohan_dnssec

# What You Can Do

- Talk to your web site host provider or technical provider about "Signing your zone" with a DNSSEC key
  - This will <u>automatically</u> protect visitors to your website from being hijacked
  - It will increase the perception and reality of security for your organization
- Sign up with mailing lists to understand more about implementing DNSSEC
  - Eliminate DNS identity theft
  - Ensure safety for your clients
  - Improve your branding

# 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