DNSSEC College

Arjen Zonneveld

Jelte Jansen

DHPA Techday, 21 mei 2015
Reach more buyers with Canada's performance media network.
DNS

Network Working Group
Request for Comments: 1035
Obsoletes: RFCs 882, 883, 973

DOMAIN NAMES - IMPLEMENTATION AND SPECIFICATION

1. STATUS OF THIS MEMO

This RFC describes the details of the domain system and protocol, and assumes that the reader is familiar with the concepts discussed in a companion RFC, “Domain Names: Concepts and Facilities” [RFC-1034].

The domain system is a mixture of functions and data types which are an official protocol and functions and data types which are still experimental. Since the domain system is intentionally extensible, new data types and experimental behavior should always be expected in parts of the system beyond the official protocol. The official protocol parts of the system include standard queries, responses and the Internet class RR data formats (e.g., host addresses). Since the previous RFC set, several definitions have changed, so some previous definitions are obsolete. Experimental or obsolete features are clearly marked in these RFCs, and such information should be used with caution.

The reader is especially cautioned not to depend on the values which appear in examples to be current or complete, since their purpose is primarily pedagogical. Distribution of this memo is unlimited.

Table of Contents
The Flaw at the Heart of the Internet

Dan Kaminsky discovered a fundamental security problem in the Internet and got people to care in time to fix it. It's a dramatic story with a happy ending...but we were lucky this time.

IN ELLA A MINE

DNS

As Kaminsky and others tell it, he was looking at a bug in his pagers one year when he happened upon a flaw in the core of the Internet. The security researcher was working for a company that measured performance of the Internet itself in terms of a slow-moving machine used to measure things. Kaminsky’s expertise is in the measurement of network performance (DNS), the protocol responsible for making online web sites and other network services available. The flaw he found was in the network of computers that makes the Internet work.

Normally, DNS is reliable but not nimble. When a computer asks a server to help direct traffic, the server looks up information associated with the given URL, determines the answer for a period of time known as “time to live,” and then forwards the request to another server. This helps the server respond to new requests a lot faster. Kaminsky found that the number of responses the server makes is limited, and that the response time increases as more requests are made. Consequently, the server overloads itself with a single request.

In his research, Kaminsky found that the network could be overloaded in this way and that the network itself could be overloaded by a single request. He then discovered the flaw that would cause the network to fail.

In the end, the flaw was discovered and fixed. Kaminsky saw the flaw in the network, and he saw the flaw in the network. The flaw was discovered and fixed.
Report Claims DNS Cache Poisoning Attack Against Brazilian Bank and ISP

By Larry Seltzer | Posted 2009-04-22  

OPINION: Attack shows the potential for serious spoofing attacks that could leave end users helpless. The only real solution is DNSSEC, which will take years to implement under the best of circumstances.
Report Claims DNS Cache Poisoning Attack Against Brazilian Bank and ISP

By Larry Seltzer | Posted 2009-04-22  

OPINION: Attack shows the potential for serious spoofing attacks that could leave end users helpless. The only real solution is DNSSEC, which will take years to implement under the best of circumstances.

DNS cache poisoning attack exploited in the wild

Summary: UPDATE: Arbor Networks have provided more details in their "30 Days of DNS" analysis, SANS confirmed HD Moore's statement on DNS cache poisoned AT&T servers. Numerous independent sources are starting to see evidence of DNS cache poisoning attempts on their local networks, in what appears to be an attempt to take advantage of "recent" DNS cache poisoning vulnerability. client 143.

By Dancho Danchev for Zero Day | July 29, 2006 -- 03:24 GMT (04:24 BST) | 
Get the ZDNet Security newsletter now

UPDATE: Arbor Networks have provided more details in their "30 Days of DNS" analysis, SANS confirmed HD Moore's statement on DNS cache poisoned AT&T servers. Numerous independent sources are starting to see evidence of DNS cache poisoning attempts on their local networks, in what appears to be an attempt to take advantage of "recent" DNS cache poisoning vulnerability. client 143.

The DNS server at AT&T is NOT overtly vulnerable, however, it may be subtly vulnerable in the near future.
DNS poisoning slams web traffic from millions in China into the wrong hole

ISP blames unspecified attack for morning outage

By John Leyden, 21 Jan 2014

A widespread DNS outage hit China on Tuesday, leaving millions of surfers adrift.
Report Claims DNS Cache Poisoning Attack Against Brazilian Bank and ISP

By Larry Seltzer | Posted 2009-04-22  Email  Print

OPINION: Attack shows the potential for serious spoofing attacks that could leave end users helpless. The only real solution is DNSSEC, which will take years to implement under the best of circumstances.

DNS cache poisoning attack exploited in the wild

Google’s Malaysian domains hit with DNS cache poisoning attack

Google’s Malaysian domains google.com.my and google.my were hijacked, redirecting users to a webpage that announced the attack was perpetrated by a Pakistani group called Madleets. MYNIC, the sole administrator for web addresses in Malaysia confirmed the attack in a statement.

“We can confirm there was unauthorised redirection of www.google.com.my and www.google.my to another IP address by a group which called themselves TeaM MADLEETS,” the MYNIC statement says.
DNSSEC in vogelvlucht: Signeren
DNSSEC in vogelvlucht: Signeren

RRSIG
example.dom. 7200 RRSIG SOA 5 3 7200
20131113113016 (20131014113016 57798 example.dom.
TWLzBuUgXWMA9cj+xe6YMjXy2/VdauWnONk7
uAP8JcdzsemcfWov4cFzXowS2YX291+5jBMp
m5AlwpM7ijbSBgAGz22yw1KN8JoOg3KtCM2Y
UX/c8/ATbYEBPKrjBs+YQKmY1NppwSjFi9Y0
1fVEBbrCnI0EP33c/VK97s8oNG8=)

I Have Come As One
Chats À Foucher
une Casserole
1170
RoggeHaus.com
DNSSEC in vogelvlucht: signen

• Maak een keypair aan

• Sign je zone(s)
  • BIND, NSD+Idns, PowerDNS, Secure64, Infoblox, etc.

• Publiceer gesignde zones

• Stuur public key naar parent
DNSSEC in vogelvlucht

- www.sidn.nl?
- 2001:7b8:c05::80:5
- www.sidn.nl?
- .nl at 2001:7b8:606::85
- www.sidn.nl?
- sidn.nl at 2001:610:0:800d::5
- www.sidn.nl?
- 2001:7b8:c05::80:5
- www.sidn.nl?
- .nl
- Root
- sidn.nl
DNSSEC in vogelvlucht

- Eerste bullet niveau
- Tweede bullet niveau

Titel: DNSSEC in vogelvlucht

2001:7b8:c05::80:5

www.sidn.nl?

Resolver

Root

.nl at 2001:610:0:800d::5

sidn.nl at 2001:610:0:800d::5

2001:7b8:c05::80:5

www.sidn.nl?
DNSSEC in vogelvlucht

![Diagram showing the process of DNSSEC.]
DNSSEC in vogelvlucht: chain of trust

• Chain of trust:
  • Vanaf een Trust Anchor (de root)
  • Via delegaties (.nl, sidn.nl)
  • Naar het antwoord (www.sidn.nl)
DNSSEC in .nl: zones
DNSSEC als basis

• DANE: verbindt X.509 (bekend van https) met DNS(SEC)
  • Aanvullend op CA
  • Maakt werkende self-signed certificates mogelijk

• In browser (met plugin; geen native support)

• Mail Transfer Agents
  • native support in Postfix (2.11)
  • Experimental support in Exim (4.85)
DANE voor SMTP

• Nu vaak opportunistic encryption
  • Want geen interactie met gebruiker
  • Biedt Weinig bescherming boven geen encryption

• Met DANE geef je certificaatkenmerken aan via DNSSEC
  • Verzender weet dat er encryption gebruikt kan worden
  • Niet meer opportunistic

• DNS Record:
  • `_25._tcp.<mailserver>_. 3600 TLSA 3 0 1 <fingerprint of cert>`
DANE voor SMTP

Zonder DNSSEC/TLSA:

Mar 16 19:11:03 m3 postfix/smtp[25929]: Untrusted TLS connection established to mail1.example.de[2001:db8:100::25]:25: TLSv1 with cipher ECDHE-RSA-AES256-SHA (256/256 bits)

Met DNSSEC/TLSA:

Mar 16 19:20:01 m3 postfix/smtp[26131]: Verified TLS connection established to mail.example.de[2001:db8:100::25]:25: TLSv1 with cipher ECDHE-RSA-AES256-SHA (256/256 bits)
SSHFP

DNS:

<hostname> 3600 IN SSHFP 1 1 9CF43AD8D319F3854F84B841594101A82EF8227C

SSH client config:

VerifyHostKeyDNS yes
SSHFP

Zonder SSHFP:

debug1: Server host key: RSA
The **authenticity** of host 'tjeb.nl (2a02:348:55:5250::80)'
can't be established.
Are you sure you want to continue connecting (yes/no)?

Met SSHFP:

debug1: Server host key: RSA
debug1: found 1 secure fingerprints in DNS
debug1: **matching host key fingerprint found in DNS**
debug1: ssh_rsa_verify: signature correct
Signing methods

- **Offline signing**
  - BIND
  - OpenDNSSEC
  - ldns

- **Online signing**
  - BIND
  - Powerdns
  - Knot

- **Automatic key rolling**
  - BIND
  - OpenDNSSEC

- **Plesk plugin 'Admin-ahead DNSSEC'**
PowerDNS voorbeeld

Sign zone:
  pdnssec secure-zone powerdnssec.org
  pdnssec rectify-zone powerdnssec.org

Vraag DNSKEY (of DS) om naar parent te sturen:
  pdnssec show-zone powerdnssec.org
BIND voorbeeld

Live demo
Valkuilen

• Verhuizingen

• Minder vergevingsgezind dan DNS
  • Alle delegaties moeten expliciet zijn
  • Let op met wildcards en empty-nonterminals

• Wel DS, geen DNSKEY

• Verloopen RRSIGs

• Antwoorden worden groter
  • Gebruik RRL if supported

• Controleer!
Monitoring / Debugging

• Plugins
  • Nagios
  • Zabbix

• Online tools
  • DNSViz
  • SIDN DNSSEC portfolio checker
  • DNSCheck
  • internet.nl

• CLI debugging
  • dig (BIND)
  • drill (ldns)
  • logging
DNSSEC Test sites

- Signeren:
  - http://portfolio.sidnlabs.nl:8080/form
DNSSEC Test sites

• Signeren:
  • http://portfolio.sidnlabs.nl:8080/form
DNSSEC validatie monitor

- Validating resolvers at ISP
  - 4 ISPs SIDN
  - UNBOUND resolver
  - Validation errors
  - .nl Registry Support Desk
    - Email (overview)
    - Phone call
    - Check
  - .nl Registrar Support Desk
    - Email (per registrar)
Validatie errors
Validatie errors

Number of DNSSEC zones with errors
Validatie errors

Number of DNSSEC zones with errors
Validatie errors

Number of DNSSEC zones with errors

Mav
DNSSEC in vogelvlucht
DNSSEC in vogelvlucht

www.sidn.nl?

2001:7b8:c05::80:5

Resolver

www.sidn.nl?

root.nl

sidn.nl

www.sidn.nl?

2001:610:0:800d::5

sidn.nl at 2001:610:0:800d::5

www.sidn.nl?

2001:7b8:c05::80:5

www.sidn.nl?
DNSSEC Test sites

- Validatie:
  - https://dnssectest.sidnlabs.nl
DNSSEC Test sites

- Validatie:
  - https://dnssectest.sidnlabs.nl
DNSSEC Test sites

• Validatie:
  • https://dnssectest.sidnlabs.nl
DNSSEC Informatiesites

- http://www.dnssec.nl
- http://www.dnsseccursus.nl
Prijsvraag!

Beantwoord de vraag:

“Hoe denk jij dat de internetsector het gebruik van DNSSEC(-validatie) zou kunnen versnellen?

en maak kans op een GL-iNet device!
DNSSEC Informatiesites

- http://www.dnssec.nl
- http://www.dnsseccursus.nl