Privacy and Security in the DNS

Peter van Dijk
Senior Engineer

POWERDNS
Client requests
Client requests

$ cat /etc/resolv.conf
nameserver 8.8.8.8
Client requests

Client

$ cat /etc/resolv.conf
nameserver 8.8.8.8
Client requests

Client

Recursor

$ cat /etc/resolv.conf
nameserver 8.8.8.8
Client requests

Client requests for www.google.com/A are handled by the Recursor.

```bash
$ cat /etc/resolv.conf
nameserver 8.8.8.8
```
Client requests

$ cat /etc/resolv.conf
nameserver 8.8.8.8
Client requests

$ cat /etc/resolv.conf
nameserver 8.8.8.8
Recursion

Recursor

Root

.com

google.com
Recursion

Recursor

Root

.com

google.com
Recursion

Recursor

www.google.com/A

Root

.com

google.com
Recursion
Recursion
Recursion

www.google.com/A

Recursor

Root

.com

google.com
Recursion

Recursor

Root

.com

google.com

www.google.com/A

www.google.com/A

www.google.com/A

www.google.com/A
Who sees your queries?
A Faster Internet
The Global Internet Speedup
Client Subnet in DNS Requests

draft-ietf-dnsop-edns-client-subnet-00

Abstract

This draft defines an EDNS0 extension to carry information about the network that originated a DNS query, and the network for which the subsequent reply can be cached.
Recursion

Recursor

Root

.com

google.com
Recursion
Recursion

Recursor

www.google.com/A

Root

.com

google.com
Recursion

Recursor  →  www.google.com/A  →  Root  →  .com  →  google.com
Recursion

Recursor

www.google.com/A

Root

www.google.com/A

.com

google.com
Recursion
Recursion

Recursor

Root

.com

google.com

www.google.com/A

www.google.com/A

www.google.com/A/192.0.2.0/24
qname minimisation
DNS query name minimisation to improve privacy

draft-ietf-dnsop-qname-minimisation-05

Sending the full QNAME to the authoritative name server is a tradition, not a protocol requirement.

The idea is to minimise the amount of data sent from the DNS resolver to the authoritative name server.
qname minimisation

Recurser

Root

.com

google.com
qname minimisation

Recursor → Root

Root → .com

Root → google.com
qname minimisation

Recursor

com/NS

Root

.com

google.com
qname minimisation

Recursor → .com

.com → Root

Root → google.com

com/NS
qname minimisation

Recursor -> google.com.com/NS -> Root

com/NS

Root -> .com

google.com
qname minimisation

Recursor

com/NS

google.com/NS

Root

.com

google.com
qname minimisation
DNS Privacy Considerations

Abstract

This document describes the privacy issues associated with the use of the DNS by Internet users. It is intended to be an analysis of the present situation and does not prescribe solutions.
Spoofing

Recursor

Auth
Spoofing

Recursor -> Auth
Spoofing

www.google.com/A
Spoofing

www.google.com/A

Recursor → Auth

Attacker
Spoofing

www.google.com/A

204.79.197.200
Spoofing

www.google.com/A

204.79.197.200

Recursor

Auth

Attacker
Spoofing

Recursor

www.google.com/A

173.194.65.147
173.194.65.104

Attacker

204.79.197.200
Spoofing squared

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 is a dramatic story with a happy ending ... but we were lucky this time.

By Erica Naone

Dan Kaminsky, uncharacteristically, was not looking for a bug. Earlier this year when he happened upon a flaw in the core of the Internet, he was simply trying to fix a client's problem. Kaminsky's expertise is in the Internet's domain name system (DNS), the protocol responsible for matching websites' URLs with the numeric addresses of the servers that host them. The same concept can be extended to multiple servers with several addresses, and Kaminsky thought he could simplify the process for directing users to the servers best able to handle their requests at any given moment.

Normally, DNS is reliable but not nimble. When a computer — say, a server that helps direct traffic across Comcast's network — receives a request for a URL, it stores the answer for a period of time known as "time-to-live," which can be anywhere from seconds to days. This helps to reduce the number of requests the server makes. Kaminsky's idea was to bypass the time-to-live, allowing the server to get a fresh answer every time it wanted to know a site's address. Consequently, traffic on Comcast's network would be sent to the optimal address at every moment, rather than to whatever address had already been stored.

Kaminsky was sure that the strategy could significantly speed up content distribution.

It was only later, after talking casually about the idea with a friend, that Kaminsky realized his "trick" could completely break the security of the domain name system and, therefore, of the Internet itself. The time to live, it turns out, was at the core of DNS security: being able to bypass it allowed for a wide variety

Photograph by JOHN KEATLEY

POWERDNS

POWERDNS

POWERDNS

POWERDNS

POWERDNS

POWERDNS

POWERDNS

POWERDNS
Preventing spoofing

Sequential access

Random access
Preventing spoofing

Network Working Group
Request for Comments: 5452
Updates: 2181
Category: Standards Track

A. Hubert
Netherlabs Computer Consulting BV.
R. van Mook
Equinix
January 2009

Measures for Making DNS More Resilient against Forged Answers
Use of Bit 0x20 in DNS Labels to Improve Transaction Identity
Domain Name System (DNS) Cookies
<draft-ietf-dnsop-cookies-05.txt>

Abstract

DNS cookies are a lightweight DNS transaction security mechanism that provides limited protection to DNS servers and clients against a variety of increasingly common denial-of-service and amplification / forgery or cache poisoning attacks by off-path attackers. DNS Cookies are tolerant of NAT, NAT-PT, and anycast and can be incrementally deployed.
Total number of DNSSEC delegations in the .NL zone: 2438506
Questions?
Questions?
Privacy and Security in the DNS

Peter van Dijk
Senior Engineer

POWERDNS