# Privacy and Security in the DNS

Peter van Dijk Senior Engineer



#### **POWERDNS**



### **POWERDNS**





#### **POWERDNS**



#### **POWERDNS**



#### **POWERDNS**



#### **POWERDNS**



Recursor

















### Who sees your queries? powerdns:::



### edns-client-subnet



# **A Faster Internet** *The Global Internet Speedup*

### edns-client-subnet

### **POWERDNS**

dnsop Internet-Draft Intended status: Informational Expires: May 19, 2015 C. Contavalli W. van der Gaast Google D. Lawrence Akamai Technologies W. Kumari Google November 15, 2014

#### Client Subnet in DNS Requests draft-ietf-dnsop-edns-client-subnet-00

#### Abstract

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

Recursor



















### **POWERDNS**

Domain Name System Operations (dnsop) Working Group S. Bortzmeyer Internet-Draft AFNIC Intended status: Experimental August 1, 2015 Expires: February 2, 2016

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.









#### **POWERDNS**

Root





.com

#### google.com

comINS

#### **POWERDNS**





Root



comINS

#### **POWERDNS**

Root



google.com

.com







### DPRIVE

**POWERDNS** 

Internet Engineering Task Force (IETF)
Request for Comments: 7626
Category: Informational

S. Bortzmeyer AFNIC August 2015

ISSN: 2070-1721

#### 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.

### **DNSCurve&DNSCrypt**






Recursor

































# Spoofing squared

### **POWERDNS**



#### The Flaw at the Heart of the Internet

DAN KAMINSKY DISCOVERED A FUNDAMEN-TAL SECURITY PROBLEM IN THE INTERNET AND GOT PEOPLE TO CARE IN TIME TO FIX IT. IT'S A DRAMATIC STORY WITH A HAPPY END-ING ... BUT WE WERE LUCKY THIS TIME.

By ERICA NAONE

an Kaminsky, uncharacteristically, was not looking for bugs earlier this year when he happened upon a flaw at the core of the Internet. The security researcher was using his knowledge of Internet infrastructure to come up with a better way to stream videos to users. 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 content can be hosted by multiple servers with several addresses, and Kaminsky though the had a great trick 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 computersay, a server that helps direct traffic across Comcast's networkrequests the numerical address associated with a given 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

of attacks. Kaminsky wrote a little code to make sur was as bad as he thought it was. "Once I saw it work dropped." he says. "I thought, "What the heck am about this? This affects everything."

Kaminsky'stechnique could be used to direct Web Web page an attacker chose. The most obvious use is to phishing sites (websites designed to trick people banking passwords and other personal informatio attacker to steal their identities) or other fake ver pages. But the danger is even worse: protocols such to deliver e-mail or for secure communications ove ultimately rely on DNS. A creative attacker could us technique to intercept sensitive e-mail, or to creasions of the certificates that ensure secure transact users and banking websites. "Every day I find ano Kaminsky says." Another thing falls over if DNS is literally, you look around and see anything that's usiorything dhat's using a network – and it's probably u

Kaminsky called Paul Vixie, president of the Inte Consortium, anonprofit corporation that supportss of Internet infrastructure, including the software me used in the domain name system. "Usually, if somel report a problem, you expect that it's going to take at time for them to explain it-maybe a whiteboard, it document or two," Vixie says. "In this case, it took a him to explain the problem, and another ao secon answer my objections. After that, I said, 'Dun, I amon over an unsecure cell phone. Please do not ever say to you just said to me over an unsecure cell phone aga

Perhaps most frightening was that because the was not located in any particular hardware or softw design of the DNS protocol itself, it wasn't clear h secret, Kaminsky and Vixie gathered together so DNS experts in the world: people from the U.S. go

# Preventing spoofing powerDNS:: Sequential access







## **Preventing spoofing**

### **POWERDNS**

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

## **Preventing spoofing**

### **POWERDNS**

DNSOP Working Group INTERNET-DRAFT <draft-vixie-dnsext-dns0x20-00.txt> Intended Status: Full Standard Creation Date: March 17, 2008 P. Vixie, ISC D. Dagon, GaTech

Use of Bit 0x20 in DNS Labels to Improve Transaction Identity

# dnsop-cookies



## dnsop-cookies

### **POWERDNS**

INTERNET-DRAFT Intended Status: Proposed Standard

Donald Eastlake Huawei Mark Andrews ISC August 1, 2015

Expires: January 31, 2016

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.

### DNSSEC

### **POWERDNS**

1



Total number of DNSSEC delegations in the .NL zone: 2438506



### DNSSEC



### Questions?



### **Questions?**





### **Questions?**

### **POWERDNS**





peter.van.dijk@powerdns.com

# Privacy and Security in the DNS

Peter van Dijk Senior Engineer