Network Working Group
Internet-Draft
Intended status: Informational
Expires: June 20, 2014

S. Bortzmeyer
AFNIC

December 17, 2013

Possible solutions to DNS privacy issues
draft-bortzmeyer-dnsop-privacy-sol-00

Abstract

This document describes some possible solutions to the DNS privacy issues described in [I-D.bortzmeyer-dnsop-dns-privacy].

Discussions of the document should currently take place on the dnsop mailing list [dnsop].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on June 20, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction and background

The problem statement is exposed in [I-D.bortzmeyer-dnsop-dns-privacy]. The terminology here is also defined in this companion document.

2. Possible technical solutions

We mention here only the solutions that could be deployed in the current Internet. Disruptive solutions, like replacing the DNS with a completely new resolution protocol, are interesting but are kept for a future work. Remember that the focus of this document is on describing the threats, not in detailing solutions. This section is therefore non-normative and is NOT a technical specification of solutions. For the same reason, there are not yet actual recommendations in this document.

Raising seriously the bar against the eavesdropper will require SEVERAL actions. Not one is decisive by itself but, together, they can have an effect. The most important suggested here are:

qname minimization,

encryption of DNS traffic,

padding (sending random queries from time to time).

We detail some of these actions later, classified by the kind of observer (on the wire, in a server, etc). Some actions will help

against several kinds of observers. For instance, padding, sending gratuitous queries from time to time (queries where you're not interested in the replies, just to disturb the analysis), is useful against all sorts of observers. It is a costly technique, because it increases the traffic on the network but it seriously blurs the picture for the observer.

2.1. On the wire

2.1.1. Reducing the attack surface

See Section 2.2.1 since the solution described there apply against on-the-wire eavesdropping as well as against observation by the resolver.

2.1.2. Encrypting the DNS traffic

To really defeat an eavesdropper, there is only one solution: encryption. But, from the end user point of view, even if you check that your communication between your stub resolver and the resolver is encrypted, you have no way to ensure that the communication between the resolver and the autoritative name servers will be. There are two different cases, communication between the stub resolver and the resolver (no caching but only two parties so solutions which rely on an agreement may work) and communication between the resolver and the authoritative servers (less data because of caching, but many parties involved, so any solution has to scale well). Encrypting the "last mile", between the user's stub resolver and the resolver may be sufficient since the biggest danger for privacy is between the stub resolver and the resolver, because there is no caching involved there.

The only encryption mechanism available for DNS which is today an IETF standard is IPsec in ESP mode. Its deployment in the wide Internet is very limited, for reasons which are out of scope here. Still, it may be a solution for "the last mile" and, indeed, many VPN solutions use it this way, encrypting the whole traffic, including DNS to the safe resolver. In the IETF standards, a possible alternative could be DTLS [RFC6347]. It enjoyed very little actual deployment and its interaction with the DNS has never been considered, studied or of course implemented. There are also non standard encryption techniques like DNScrypt [dnscrypt] for the stub resolver <-> resolver communication or DNScurve [dnscurve] for the resolver <-> authoritative server communication. It seems today that the possibility of massive encryption of DNS traffic is very remote.

A last "pervasive encryption" solution for the DNS could be the promising [I-D.wijngaards-dnsop-confidentialdns].

Another solution would be to use more TCP for the queries, together with TLS [RFC5246]. DNS can run over TCP and it provides a good way to leverage the software and experience of the TLS world. There have been discussions to use more TCP for the DNS, in light of reflection attacks (based on the spoofing of the source IP address, which is much more difficult with TCP). For instance, a stub resolver could open a TCP connection with the resolver at startup and keep it open to send queries and receive responses. The server would of course be free to tear down these connections at will (when it is under stress, for instance) and the client could reestablish them when necessary. Remember that TLS sessions can survive TCP connections so there is no need to restart the TLS negociation each time. This DNS-over-TLS-over-TCP is already implemented in the Unbound resolver. It is safe only if pipelining multiple questions over the same channel. Name compression should also be disabled, or CRIME-style [crime] attacks can apply.

Encryption alone does not guarantee perfect privacy, because of the available metadata. For instance, the size of questions and responses, even encrypted, provide hints about what queries have been sent. (DNScrypt uses random-length padding, and a 64 bytes block size, to limit this risk, but this raises other issues, for instance during amplification attacks. Other security protocols use similar techniques, for instance ESPv3.) Observing the periodicity of encrypted questions/responses also discloses the TTL, which is yet another hint about the queries. Non-cached responses are disclosing the RTT between the resolver and authoritative servers. This is a very useful indication to guess where authoritative servers are located. Web pages are made of many resources, leading to multiple requests, whose number and timing fingerprint which web site is being browsed. So, observing encrypted traffic is not enough to recover any plaintext queries, but is enough to answer the question "is one of my employees browsing Facebook?". Finally, attackers can perform a denial-of-service attack on possible targets, check if this makes a difference on the encrypted traffic they observe, and infer what a query was.

2.2. In the servers

2.2.1. In the resolvers

It does not seem there is a possible solution against a leaky resolver. A resolver has to see the entire DNS traffic in clear.

The best approach to limit the problem is to have local resolvers whose caching will limit the leak. Local networks should have a local caching resolver (even if it forwards the unanswered questions to a forwarder) and individual laptops can have their very own resolver, too.

One mechanism to potentially mitigate on the wire attacks between stub resolvers and caching resolvers is to determine if the network location of the caching resolver can be moved closer to the end user's computer (reducing the attack surface). As noted earlier in [I-D.bortzmeyer-dnsop-dns-privacy], if an end user's computer is configured with a caching resolver on the edge of the local network, an attacker would need to gain access to that local network in order to successfully execute an on the wire attack against the stub resolver. On the other hand, if the end user's computer is configured to use a public DNS service as the caching resolver, the attacker needs to simply get in the network path between the end user and the public DNS server and so there is a much greater opportunity for a successful attack. Configuring a caching resolver closer to the end user can also reduce the possibility of on the wire attacks.

2.2.2. In the authoritative name servers

A possible solution would be to minimize the amount of data sent from the resolver. When a resolver receives the query "What is the AAAA record for www.example.com?", it sends to the root (assuming a cold resolver, whose cache is empty) the very same question. Sending "What are the NS records for .com?" would be sufficient (since it will be the answer from the root anyway). To do so would be compatible with the current DNS system and therefore could be deployable, since it is an unilateral change to the resolvers.

To do so, the resolver needs to know the zone cut [RFC2181]. There is not a zone cut at every label boundary. If we take the name www.foo.bar.example, it is possible that there is a zone cut between "foo" and "bar" but not between "bar" and "example". So, assuming the resolver already knows the name servers of .example, when it receives the query "What is the AAAA record of www.foo.bar.example", it does not always know if the request should be sent to the name servers of bar.example or to those of example. [RFC2181] suggests an algorithm to find the zone cut, so resolvers may try it.

Note that DNSSEC-validating resolvers already have access to this information, since they have to find the zone cut (the DNSKEY record set is just below, the DS record set just above).

It can be noted that minimizing the amount of data sent also partially addresses the case of a wire sniffer.

One should note that the behaviour suggested here (minimizing the amount of data sent in qnames) is NOT forbidden by the [RFC1034] (section 5.3.3) or [RFC1035] (section 7.2). Sending the full qname to the authoritative name server is a tradition, not a protocol requirment.

Another note is that the answer to the NS query, unlike the referral sent when the question is a full qname, is in the Answer section, not in the Authoritative section. It has probably no practical consequences.

2.2.3. Rogue servers

Traditional security measures (do not let malware change the system configuration) are of course a must. A protection against rogue servers announced by DHCP could be to have a local resolver, and to always use it, ignoring DHCP.

3. Security considerations

Hey, man, the entire document is about security!

4. Acknowledgments

Thanks to Olaf Kolkman and Francis Dupont for the interesting discussions, specially about qname minimization. Thanks to Mohsen Souissi for proofreading.

5. References

5.1. Normative References

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, November 1987.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, November 1987.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC6973] Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", RFC 6973, July 2013.

[I-D.bortzmeyer-dnsop-dns-privacy]

Bortzmeyer, S., "DNS privacy problem statement", draft-bortzmeyer-dnsop-dns-privacy-00 (work in progress), November 2013.

5.2. Informative References

[RFC2181] Elz, R. and R. Bush, "Clarifications to the DNS Specification", RFC 2181, July 1997.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, March 2005.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5936] Lewis, E. and A. Hoenes, "DNS Zone Transfer Protocol (AXFR)", RFC 5936, June 2010.

[RFC6347] Rescorla, E. and N. Modadugu, "Datagram Transport Layer Security Version 1.2", RFC 6347, January 2012.

[I-D.koch-perpass-dns-confidentiality] Koch, P., "Confidentiality Aspects of DNS Data, Publication, and Resolution", draft-koch-perpass-dns-confidentiality-00 (work in progress), November 2013.

[I-D.vandergaast-edns-client-subnet] Contavalli, C., Gaast, W., Leach, S., and E. Lewis, "Client Subnet in DNS Requests", draft-vandergaast-edns-client-subnet-02 (work in progress), July 2013.

[I-D.wijngaards-dnsop-confidentialdns] Wijngaards, W., "Confidential DNS", draft-wijngaards-dnsop-confidentialdns-00 (work in progress), November 2013.

[dnsop] IETF, , "The dnsop mailing list", October 2013.

[dagon-malware] Dagon, D., "Corrupted DNS Resolution Paths: The Rise of a Malicious Resolution Authority", 2007.

[dns-footprint] Stoner, E., "DNS footprint of malware", October 2010.

[darkreading-dns]

Lemos, R., "Got Malware? Three Signs Revealed In DNS Traffic", May 2013.

[dnschanger] Wikipedia, , "DNSchanger", November 2011.

[dnscrypt] Denis, F., "DNSCrypt", .

[dnscurve] Bernstein, D., "DNScurve", .

[prism] NSA, , "PRISM", 2007.

[crime] Rizzo, J. and T. Dong, "The CRIME attack against TLS", 2012.

[ditl] , "A Day in the Life of the Internet (DITL)", 2002.

[data-protection-directive] , "European directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data", November 1995.

[passive-dns] Weimer, F., "Passive DNS Replication", April 2005.

[tor-leak] , "DNS leaks in Tor", 2013.

Author's Address

Stephane Bortzmeyer
AFNIC
Immeuble International
Saint-Quentin-en-Yvelines 78181
France

Phone: +33 1 39 30 83 46
Email: bortzmeyer+ietf@nic.fr
URI: http://www.afnic.fr/