DNS man-in-the-middle at the Krasnapolsky hotel in Amsterdam

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

First publication of this article on 11 June 2013

https://www.bortzmeyer.org/dns-swisscom.html

Hotel networks are famous for their brokenness. It seems their network managers are fond of always finding some new and clever ways to break things. The famous Krasnapolsky hotel in Amsterdam, home of many RIPE meetings, decided to attack the DNS.

I discovered the problem during a CENTR meeting. The DNSSEC-validating resolver on my laptop did not work (SERVFAIL for every query). But dig apparently did. Checking with tcpdump :

```
10:47:24.578004 IP (tos 0x0, ttl 64, id 36388, offset 0, flags [none], proto UDP (17), length 56)
    192.168.48.71.38053 > 192.58.128.30.53: [udp sum ok] 17756% [1au] NS? . ar: . OPT UDPsize=4096 OK (28)
10:47:25.567816 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 269)
    192.58.128.30.53 > 192.168.48.71.38053: [udp sum ok] 17756 FormErr q: NS? . 13/0/0  [2d1h59m18s] NS j.root-s
```

The first packet is a priming request from the resolver, trying to check the list of the root name servers. The replies is complete (full list of these servers) but with an abnormal status : FormErr (Format Error). From RFC 1035 [1], it means "The name server was unable to interpret the query".

But if I try with dig ? Here, I request the DNSKEY of the root, from the server K.root-servers.net, with the EDNS options a real resolver would use :

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc1035.txt

```
% dig +bufsize=4096 +dnssec @193.0.14.129 DNSKEY .

; <<>> DiG 9.8.1-P1 <<>> +bufsize=4096 +dnssec @193.0.14.129 DNSKEY .
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41313
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;. IN DNSKEY

;; ANSWER SECTION:
. 30672 IN DNSKEY 256 3 8 AwEAAc5byZvwmHUlCQt7WSeAr3OZ2ao4x0Yj/3UcbtFzQ0T67N7CpYmN qFmfvXxksS1/E+mtT0axFVDji
...
```

Everything goes fine, it seems. No, there are three problems. I let you check, I will explain later. But, first, why do I get a `NOERROR` from dig and a `FORMERR` when it's done by the resolver? That's because dig sets the RD bit in the request (again, from the RFC : "Recursion Desired - this bit may be set in a query and is copied into the response. If RD is set, it directs the name server to pursue the query recursively. Recursive query support is optional."). Typical resolvers, unlike stub resolvers like dig, do not set this bit. Let's try with `+norec` which will disable this bit :

```
% dig +bufsize=4096 +dnssec +norec @193.0.14.129 DNSKEY .

; <<>> DiG 9.8.1-P1 <<>> +bufsize=4096 +dnssec +norec @193.0.14.129 DNSKEY .
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: FORMERR, id: 7135
;; flags: qr ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;. IN DNSKEY

;; ANSWER SECTION:
. 158539 IN DNSKEY 256 3 8 AwEAAc5byZvwmHUlCQt7WSeAr3OZ2ao4x0Yj/3UcbtFzQ0T67N7CpYmN qFmfvXxksS1/E+mtT0axFVDj
...
```

OK, this is consistent : dig and my local resolver gets the same result, a Format Error. The network provider (Swisscom) did that to prevent people from running their own resolvers (or may be simply out of incompetence).

Do note the brokenness is not in the DHCP-provided resolver (which is almost always broken in hotel and airport networks). I queried directly the root name server. So, it's a real man-in-the-middle. As in China, the network intercepts the request (or the response) and rewrites it.

Anything else? I said there were three problems in the reply with the RD bit set. Did you find them? One is conspicuous : the DNSSEC signatures were stripped from the reply, preventing any local validation (the only safe way to do DNSSEC validation). The second is more subtle : the reply should have the AA bit set (from the RFC : "Authoritative Answer - this bit is valid in responses, and specifies that the responding name server is an authority for the domain name in question section.") since I queried directly a root name server. But it has not. Yet another information erased from the reply. And the third

was noticed in this paper by Sebastian Castro : "RA [Recursion Available] is bit set when you are talking to a non-recursive server".

Of course, this sort of man-in-the-middle is very common. What's ironic here is that it takes place at the Krasnapolsky, which is an important place of the Internet in Europe. And that it happens in the Netherlands, which was the first country in the world to protect network neutrality by the law, law which is here blatantly violated.

So, it seems the only solution to have a proper DNS service on your laptop when travelling is to tunnel everything through some VPN.