The 2017 roundtable of AFNIC's Scientific Board

AFNIC

For seven years now, AFNIC (Association Française pour le Nommage Internet en Coopération), the manager of the domain *.fr*, has organized the *Journées du Conseil scientifique de l'AFNIC (JCSA)*. This roundtable of the organization's Scientific Board is the occasion for reviewing the advances made in the research on, and standardization of, the protocols used by the Internet, in particular by the Domain Name System. This DNS mainly serves to link the names of devices and the addresses used by them on the Internet. As the Internet's cornerstone, it masks a technical device with an IP address (*e.g.*, 192.134.5.24) for easier manipulation by human beings (*e.g.*, afnic.fr).[1]

Over the years, the functions of the DNS have been expanded, for example, to: distributing the load of the most visited websites, managing encryption keys and registering other identifications than the names of devices. The DNS architecture is constantly evolving both to improve the handling of the growing number of queries and to reinforce the security of this critical service so as to reduce the impact of attacks, protect privacy better and add new features by using the robust infrastructure already in use.

Close to academic circles and standardization organizations, the members of the Scientific Board help AFNIC to consider and reconsider the means for accomplishing its assignments. They emit an opinion on the general orientation of R&D, of trends in technology and of Internet governance. In previous years, the board drew attention to: the Internet of things, alternative architectures, metrology, and resilience. On 6 July, it focused on the management of privacy.

Since the DNS was invented in the 1980s, the successive DNS queries that lead to resolving a name have never been encrypted and can be passed up to root servers. The intermediate servers that limit the number of queries being passed usually mask the user's identity; but the information might leak out of the DNS. For a firm, this could lead to a breach of confidential business information (*e.g.*, the list of customers). These problems can become more serious if the names to be resolved contain sensitive information. For example, the interception of identifications obtained by scanning *qr*-codes might lead to divulging a manufacturing process.

The *JCSA* reviewed the approaches developed by the Internet Engineering Task Force (IETF, the international organization that standardizes Internet protocols) to reduce the protocol's vulnerability in relation to the management of privacy. Two improvements were proposed.

- ● The first is based on the hierarchical nature of domain names. When a user tries to resolve a name such as *qrcode.ident.exemple.fr*, the query is sent to a resolver (a server located in a firm, at a service-provider or an "open" DNS resolver of the sort provided by Google or Cisco). The resolver is going to pass a query to the root DNS servers to locate the servers that manage the domain *.fr*. It then queries these servers to locate *exemple.fr*, etc., till obtaining the full response to the query. In the original approach, the full query is passed to these various servers. But with the so-called "minimization of queries" extensions for the management of privacy, only the part of interest to each server will be sent to it: the root will receive only the query about *.fr* (instead of *qrcode.ident.exemple.fr*).

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France).

● The second improvement has to do with encrypting queries between the machine and the resolver. The main change is the switch from the UDP to the TCP protocol in order to be able to use TLS, a protocol also used for the security of exchanges on the Web. The *JCSA* discussed this improvement along with its implications in terms of changing protocols and behaviors.

The *JCSA*'s morning sessions are usually devoted to tutorials. Sara Dickinson (Sinodun) and Willem Toorop (NLnet Labs) demonstrated the software getDNS and its programming interfaces (including the extensions for managing privacy). Maxence Tury (Agence Nationale de la Sécurité des Systèmes d'Information, ANSSI) presented the TLS protocol and, using interactive examples with the software Scapy on virtual machines, explained how certificates can be used to encrypt messages.

The afternoon session was devoted to lectures on various forms of technology. Sarah Dickinson detailed the work of the IETF on managing privacy for the DNS; and Alexander Mayrhofer (registre nic.at) presented the first studies on the dimensioning of the servers that use TLS. It turns out that the proposed changes will have little impact on the performance of the DNS. Marck To (EfficientIP) demonstrated how data can be captured from a site using the DNS, and described the methods to protect against such an attack. The last presentation at the roundtable by Bruno Rasle (AFCDP) was more general: the coming application of the EU''s General Data Protection Regulation (GDPR) and its impact on the design of Internet services.

The lectures presented at this roundtable (videos and slides) are found at:
https://www.afnic.fr/fr/l-afnic-en-bref/actualites/actualites-generales/10660/show/jcsa17-retour-sur-l-edition-2017-de-la-journee-du-conseil-scientifique-de-l-afnic.html