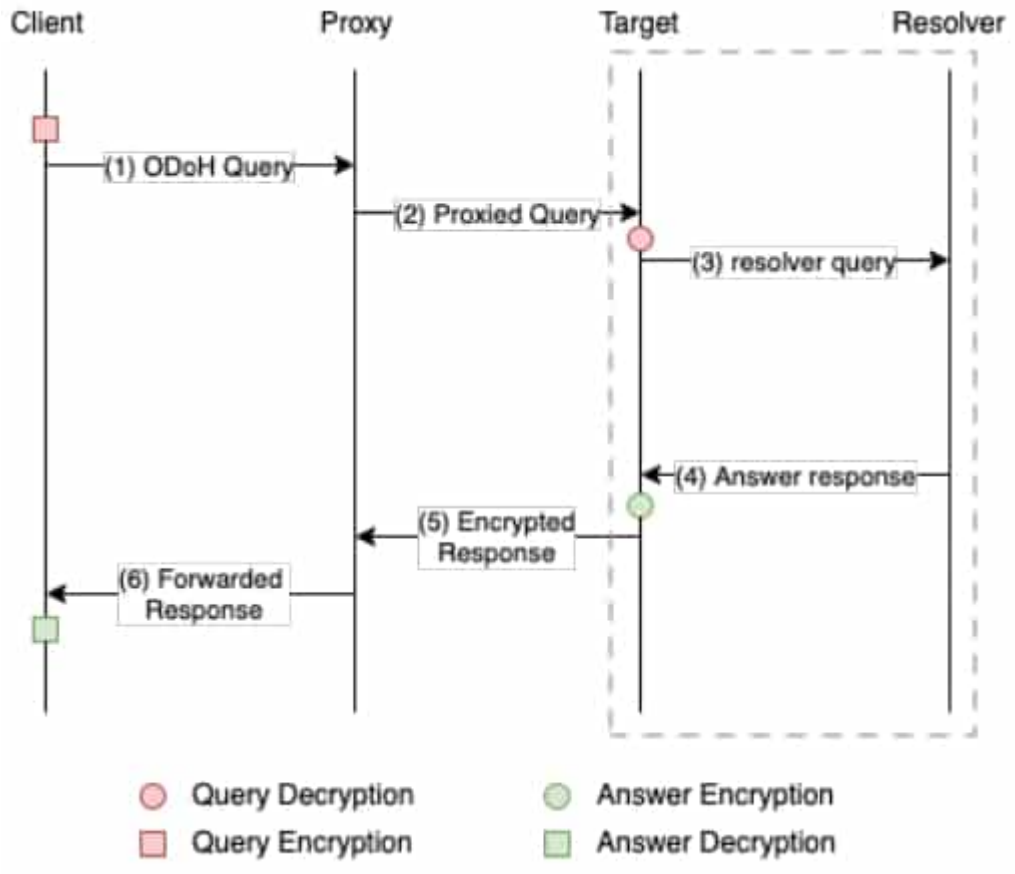
ODoH : Apple et Cloudflare poussent leur implémentation du DNS sécurisé

Voulez-vous tester ODoH ? Apple, Cloudflare et Fastly ont lancé un appel dans ce sens. Et mis des outils à disposition.

Les trois entreprises tentent de standardiser, auprès de l'IETF, leur implémentation de cette extension du protocole DoH (DNS *over* HTTPS).

Le « O » initial signifie « oblivious » ; littéralement, « inconscient ». Il traduit un objectif : qu'aucun serveur n'ait jamais accès de manière simultanée à l'IP d'un client et à sa requête DNS. Cela implique le recours à un proxy*, additionné d'un chiffrement hybride à clés publiques.

Ce chiffrement est indépendant de la couche de transport (TLS/HTTPS). Il est rendu nécessaire par le fait qu'il existe deux connexions distinctes : client-proxy et proxy-serveur. Dans les grandes lignes, le client récupère, par DNSSEC, la clé publique de la cible – qui est généralement le résolveur DNS, pour des raisons de performances – et l'utilise pour chiffrer sa requête. Il y inclut de quoi permettre à la cible de déduire une clé symétrique… et de chiffrer sa réponse.



Le proxy n'est pas censé déchiffrer les requêtes, sauf en l'absence de variables définissant le serveur cible (targethost et targetpath). Côté client, il est recommandé d'utiliser des méthodes HTTP qui évitent la mise en cache (POST plutôt que GET, par exemple).

ODoH : une « confiance technologique »

ODoH se présente comme une alternative « 100 % technologique » au système d'accords de confiance que Mozilla a mis en place. La fondation ne s'associe en l'occurrence qu'avec des partenaires DNS qui prennent des engagements sur la protection des données des utilisateurs.

Des bibliothèques expérimentales en Rust et Go sont disponibles depuis fin octobre. Cloudflare a par ailleurs intégré une cible ODoH dans son DNS récursif. Equinix, PCCW et SURF sont les premiers partenaires pour la fourniture des proxys.

** L'implémentation d'ODoH sur la couche applicative le rend plus « léger » que des solutions de type proxy Tor. Selon les benchmarks que présentent Apple et al., le délai médian de résolution DNS s'élève à 228 ms. Chiffrées, les requêtes pèsent environ quatre fois plus qu'en clair.*

Microbenchmark	Type	P99 **Overhead**
ODoH Encryption	X25519/SHA256	360μs
ODoH Decryption	X25519/SHA256	246μs
ODoH Query	AES-128-GCM	107B
ODoH Answer	AES-128-GCM	16B

Photo d'illustration © chiqui – shutterstock.com