
[

Benchmarking di server e protocolli DNS sicuri

Nicolapio Gagliarde, Alessandro Macaro, Alberto Montefusco

A.A. 2023/2024

]

Abstract

DNS è uno dei protocolli fondamentali di Internet, ma a causa della mancanza di politiche di sicurezza sono nati un insieme di attacchi (sia su larga scala che mirati a determinate vittime) contro la privacy, alla disponibilità e all'integrità dei sistemi. Di conseguenza sono state proposte estensioni e varianti di DNS come DNSSEC per garantire l'autenticazione e l'integrità e DNS-over-TLS e DNS-over-HTTPS per garantire anche la riservatezza. Inoltre per ottenere anche l'affidabilità sono state progettate varianti di DNS basate sui due protocolli di trasporto TCP e QUIC. Tuttavia l'utilizzo di algoritmi crittografici, protocolli di trasporto più sofisticati e protocolli situati nei livelli ISO/OSI superiori al trasporto potrebbero causare un incremento delle latenza di risoluzione delle query DNS, incidendo sull'esperienza di navigazione dell'utente. L'obiettivo di questo lavoro è analizzare le prestazioni dei server DNS Bind9, PowerDNS e Technitium, e di come variano al variare dei protocolli utilizzati. In particolare, ognuno di questi protocolli: DNS-over-UDP, DNS-over-TCP, DNSSEC, DNS-over-TLS e DNS-over-HTTPS è stato testato su ogni server, quindi i dati sono stati analizzati e confrontati considerando uno specifico protocollo su tutti i server e poi uno specifico server per tutti i protocolli. I risultati ottenuti dimostrano che il server più efficiente e più costante nelle risposte in tutti i casi è BIND, inoltre in tutti i test viene riportato l'aumento della latenza media per i protocolli DNSSEC, DNS-over-HTTPS e DNS-over-TLS rispetto DNS-over-UDP e DNS-over-TCP. Inoltre si evince che all'aumentare del numero di richieste si ha un aumento minimo della latenza media in tutti i casi, tranne con DNS-over-TCP eseguito su Technitium, siccome in questo caso l'aumentare del numero di richieste implica una diminuzione della latenza media rispetto DNS-over-UDP. Riguardo Technitium risulta anche che con DNSSEC i primi tre dataset mostrano una latenza media inferiore rispetto DNS-over-UDP. Un altro risultato particolare è dovuto PowerDNS con DNS-over-TCP che presenta una latenza media inferiore rispetto DNS-over-UDP, questo fenomeno avviene anche in Technitium. Infine anche considerando le latenze massime ottenute, tali latenze risultano comunque in linea con i tempi di risposta riportati nei lavori correlati.