Il DNS non prevede procedure di autenticazioni preliminari alle richieste di servizio.

Attacco (IP spoofing): propagazione di molteplici domande (ad es. risoluzioni FQDN appartenenti a domini diversi da quelli gestiti dal server locale) ad un server DNS (locale) sovraccaricando il sistema e rendendolo non disponibile per la risoluzione delle query dei legittimi utenti.

Soluzione: configurare ciascuna stazione client con una lista di server DNS alternativi; la presenza di una lista con possibile alternative offre al client la possibilità di tradurre un nome simbolico in indirizzo IP (FQDN) anche quando il server DNS usato per default risulta temporaneamente irraggiungibile.

Attacco (DNS spoofing): un hacker può tentare di inserire informazioni false in un client oppure in un server inviando ***DNS reply false*** (reply relative a query mai effettuate….); in questo modo si possono alterare le informazioni contenute nel database del server DNS e compromettere la raggiungibilità di una singola stazione finale.

L'alterazione di un database di un server DNS (DNS spoofing) può produrre il risultato di un attacco DOS oppure un attacco per redirezione; poiché un server DNS può propagare ad altri server solo informazioni relative alla zona su cui ha autorità, le ripercussioni possono essere amplificate se l'attacco viene condotto a livello di ***zone transfer*** . Un hacker che riesce ad intromettersi in una zone transfer può modificare tutte le informazioni relative ad una zona ed ottenere che queste si diffondano nel resto dell'Internet.

Soluzione (sistemi Trusted): implementazioni di Name Server recenti sono state aggiornate includendo meccanismi per tenere traccia a livello applicativo delle query lanciate e memorizzare soltanto le risposte ad esse relative: inoltre è buona regola accettare richieste di zone transfer solo da e verso server DNS fidati.
In mancanza di sistemi di autenticazione evoluti un server fidato può essere riconosciuto sulla base dell'indirizzo IP che deve essere incluso in una lista di sistemi trusted.