Cache Poisoning using DNS Transaction ID Prediction

Khi client trong domain sa.com tạo request để phân giải http://www.microsoft.com thì xảy ra:

1. Client sẽ liên hệ với DNS server được cấu hình của nó và hỏi địa chỉ này http://www.microsoft.com để được phân giải. Truy vấn này sẽ chứa thông tin của UDP nguồn của client, IP address và DNS transaction ID

2. Server DNS của client vì không có thẩm quyền với http://www.microsoft.com domain nên sẽ gửi truy vấn đệ quy qua Internet root DNS server liên hệ với máy chủ DNS của Microsoft và nhận trả lời truy vấn.

3. Truy vấn thành công sẽ gửi lại cho client và thông tin sẽ được cache bởi cả sa.com name server và client.

Những điều quan trọng :

- Trong step 3, client sẽ chỉ chấp nhận thông tin được trả về nếu DNS server sử dụng đúng cổng nguồn và địa chỉ của client cũng như chính xác transaction ID được noted ở step 1. 3 mảnh của thông tin là form duy nhất của xác thực được dùng để chấp nhận DNS replies.

- Thông tin http://www.microsoft.com được trả về được cache lại bởi cả client và server với một time to live nhất định. Nếu client khác hỏi ns1.sa.com để phân giải http://www.microsoft.com trong TTL thì nameserver sẽ trả về thông tin từ cache của nó và mà không cần hỏi ns1.microsoft.com

- TransactionID dùng để phân biệt giữa client và name server , name server với name server là khác nhau.