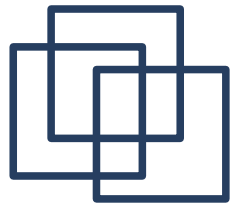


DNS (in)Security : DK*'s DNS Vulnerability

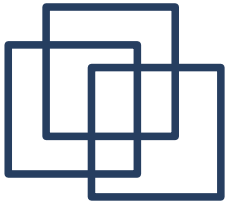
Tedi Heriyanto

19 Agustus 2008

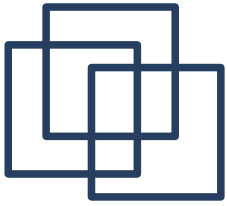


Agenda

- ✓ Pengenalan DNS
 - Apa itu DNS?
 - Sejarah DNS
 - Daftar Istilah dalam DNS
 - Cara Kerja DNS
 - Struktur Paket DNS
- ✓ Keamanan DNS
 - DNS Cache Poisoning
 - Solusi untuk DNS Cache Poisoning
 - DK's DNS Vuln.
- ✓ Diskusi

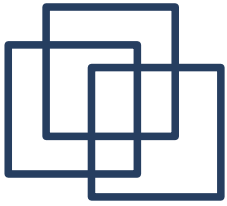


Pengenalan DNS



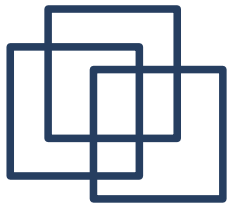
Apa Itu DNS ?

- ♦ Sebuah sistem terdistribusi, hierarkis dan replicated yang menyediakan layanan :
 - ♦ Translasi nama \leftrightarrow alamat IP
 - ♦ Informasi penanganan email
 - ♦ Load balancing
- ♦ DNS dapat menggunakan protokol UDP/TCP
- ♦ Komponen utama DNS :
 - ♦ **domain** yang didefinisikan oleh **resource record**
 - ♦ **name server**
 - ♦ **resolver**



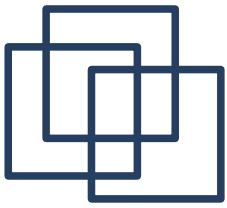
Sejarah DNS

- ♦ Bermula dari ARPANET
- ♦ Semua site yang terhubung dengan ARPANET memelihara file bernama "HOSTS.TXT" yang berisi pemetaan alamat IP dengan nama host.
- ♦ Tahun 1974, Stanford Network Information System menjadi pusat informasi semua host.
- ♦ Tahun 1983, rencana mengenai DNS



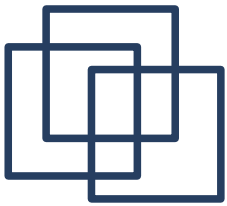
Daftar Istilah dalam DNS

- ♦ Nameserver : server yang menjawab pertanyaan DNS
- ♦ Authoritative Nameserver : server yang berisi informasi aktual mengenai domain
- ♦ Resolving name server : server yang bekerja mencari informasi IP atas hostname
- ♦ Root name server : name server tertinggi dalam hierarki
- ♦ Zona : kumpulan nama host dan IP
- ♦ Resource Record : jenis sumber daya dalam DNS
- ♦ Delegation : ketika name server tidak mengetahui sebuah zona, tetapi mengacu pada name server yang mengetahuinya

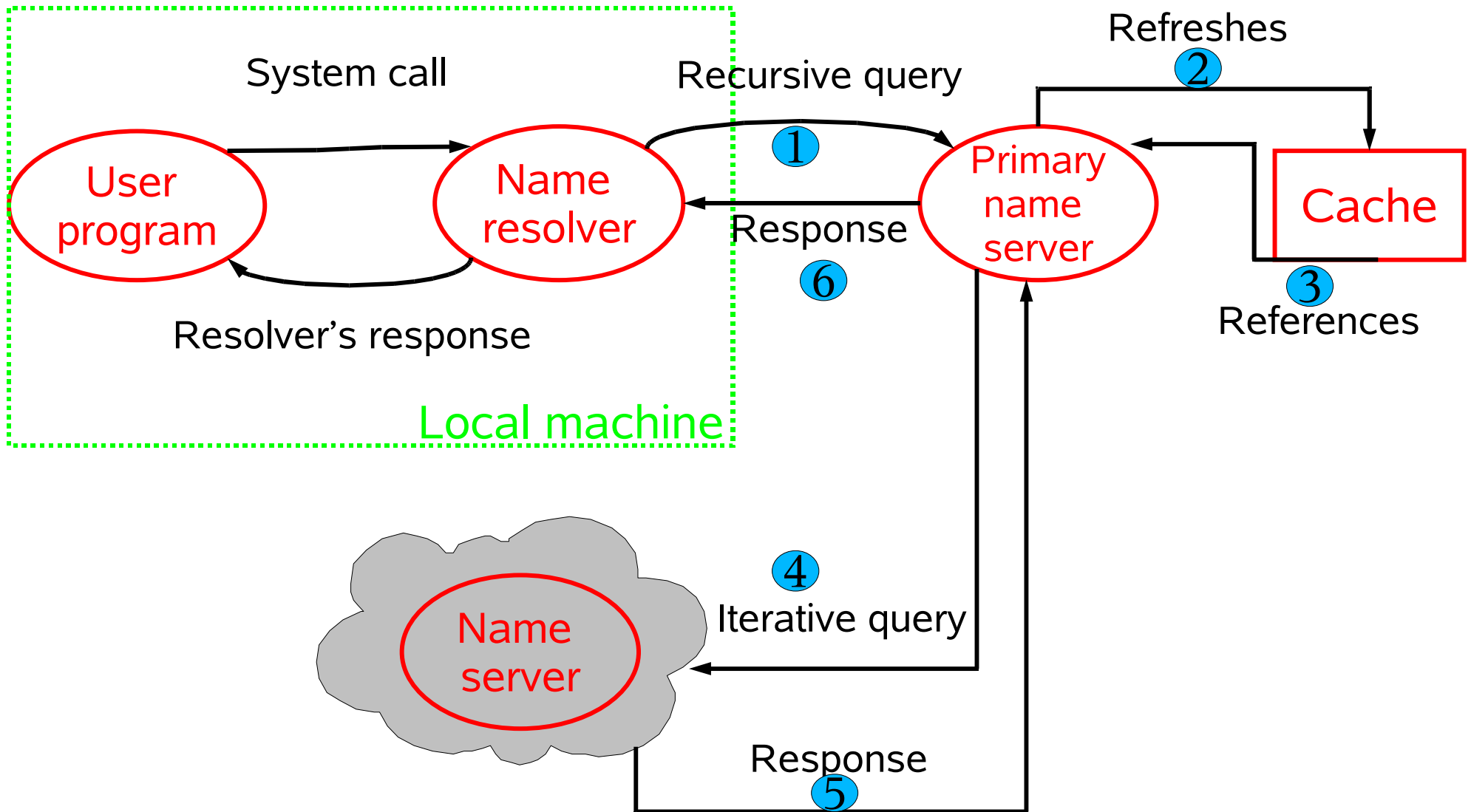


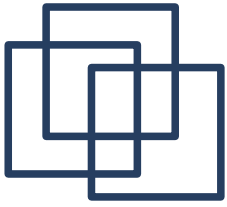
Cara Kerja DNS

- Masukkan nama host (misalnya www.security-1st.net)
- Resolving name server akan memeriksa cachenanya apakah informasi tersebut telah ada
- Jika tidak ada, mereka akan memeriksa root name server yang mengetahui hierarki .net untuk mencari tahu authoritative name server untuk security-1st.net
- Koneksi ke authoritative name server untuk meminta informasi yang diinginkan
- Setelah bertanya ke authoritative name server, resolving name server memberikan balasan berupa :
 - Alamat IP yang benar
 - Pesan kesalahan



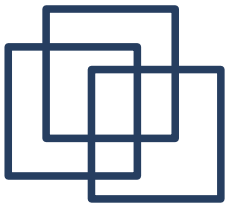
Proses Resolusi Nama



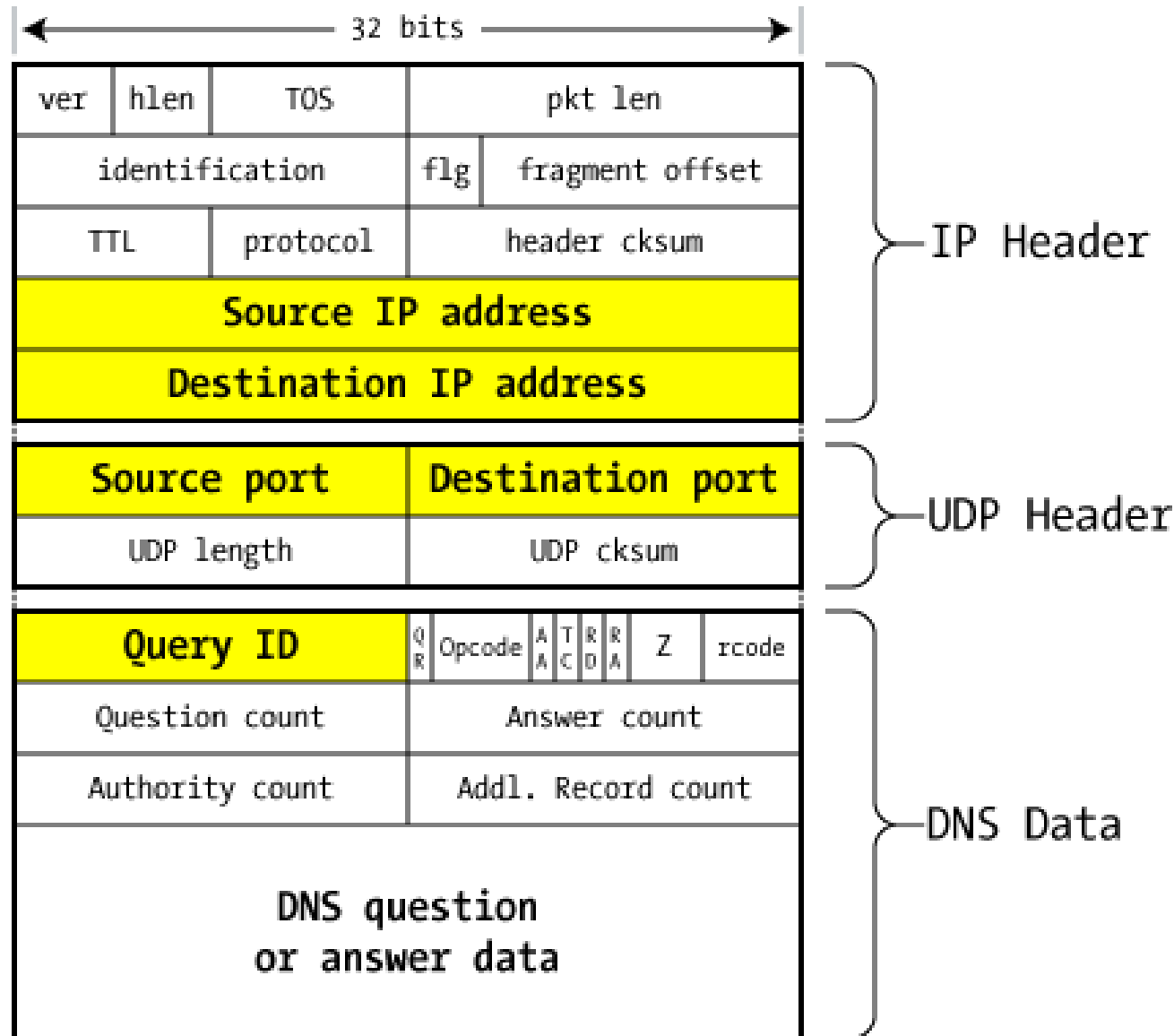


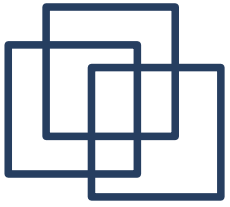
Struktur Paket DNS

- Alamat Sumber dan Tujuan
- Port Sumber dan Tujuan
- Query ID / Transaction ID (TXID)
- QR (Query/Response) → 1:query, 0:respon
- AA (Authoritative Answer) → 1:authoritative, 0:tidak
- TC (Truncated) → 1:jawaban akan dipotong, 0:tidak
- RD (Recursion Desire) → 1:mendukung rekursi, 0:tidak
- rcode → indikasi sukses atau gagal
- Question record count → diisi dengan record yang ingin dicari oleh klien
- TTL → Time to Live



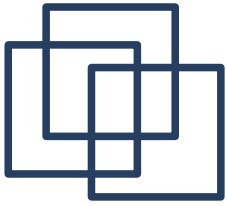
Struktur Paket DNS



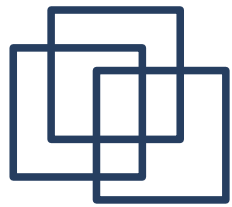


Type Resource Record

- A : Alamat IP
- NS : Nameserver
- MX : Mail Exchanger
- SOA : Start of Authority, menjelaskan beberapa data kunci mengenai zona yang didefinisikan oleh administrator zona.
- CNAME : Canonical Name (Alias)
- TXT : Text yang memberikan data deskriptif tentang domain.

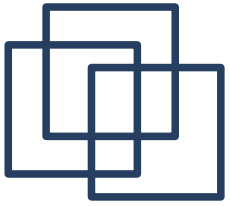


Keamanan DNS



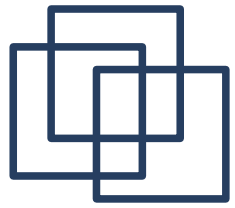
Mengapa Keamanan DNS Penting?

- ♦ Digunakan secara luas oleh aplikasi Internet :
 - ♦ Internet banking
 - ♦ Email
 - ♦ DNS block-list
- ♦ Permasalahan keamanan DNS :
 - ♦ Name server dapat dengan mudah di-*spoof* dan rentan terhadap beragam tipe serangan (DoS, buffer overrun, replay, dsb.)
 - ♦ Zona transfer
 - ♦ DNS Cache poisoning



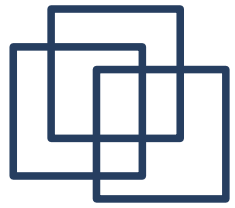
DNS Cache Poisoning

- ♦ Adalah sebuah teknik serangan yang memungkinkan penyerang memasukkan informasi DNS palsu ke dalam cache sebuah caching nameserver.
- ♦ Skenario :
 - ♦ Mengalihkan alamat IP Internet banking
 - ♦ Mengalihkan alamat search engine ke site berisi virus/malware
 - ♦ Dan lain-lain (hanya dibatasi oleh imajinasi penyerang... :D)



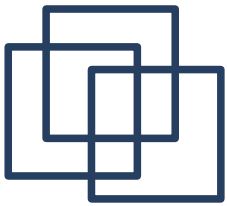
Syarat Respon Paket Yg Diharapkan

- Tiba pada port UDP yang sama dengan port pengiriman.
- Bagian Question cocok dengan Question yang ada dalam query yang *pending*.
- ID Query cocok dengan query yang *pending*.
- Bagian Authority dan Additional berisikan nama yang berada dalam domain yang sama dengan yang ada di dalam Question (Bailiwick Checking).

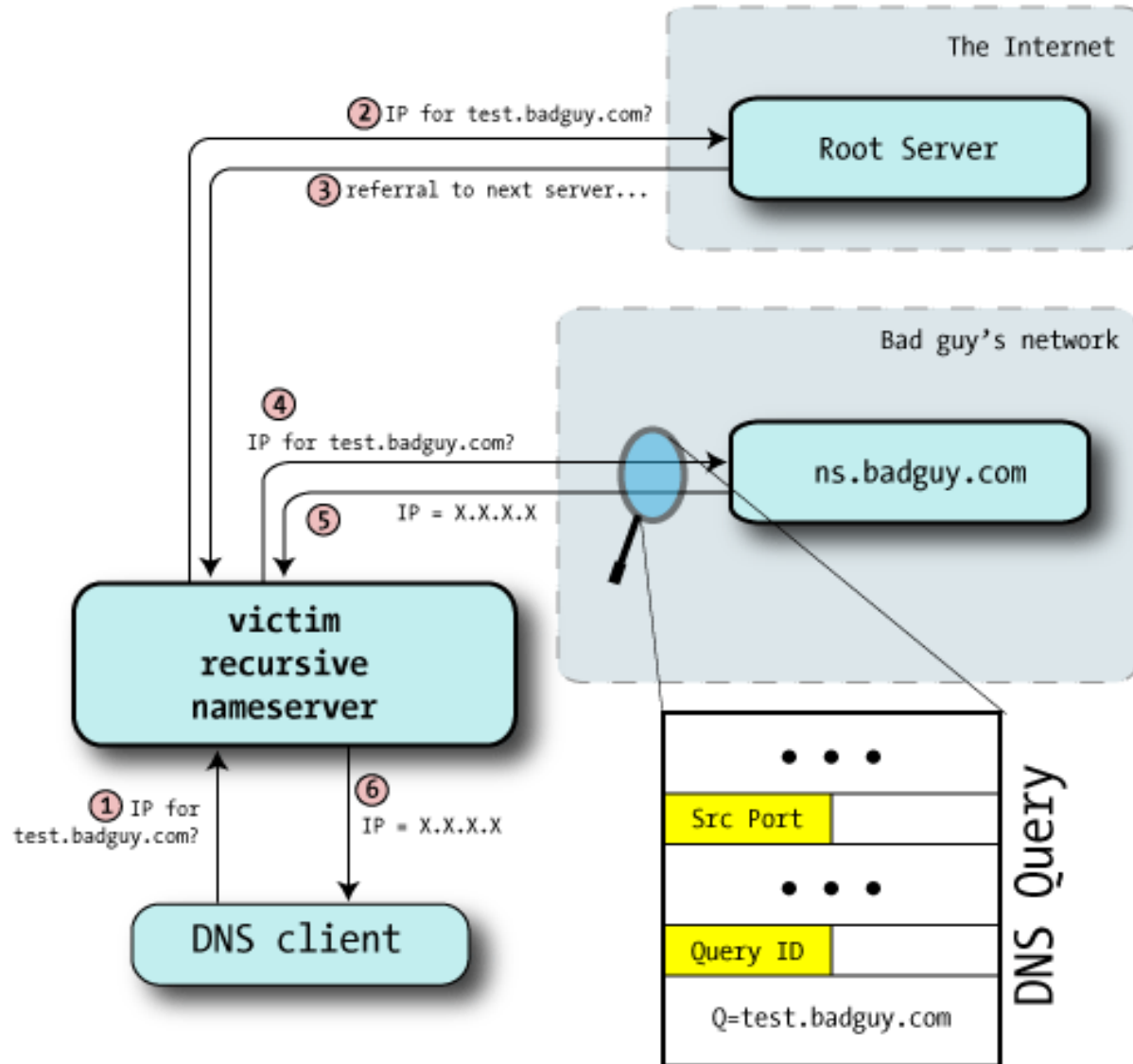


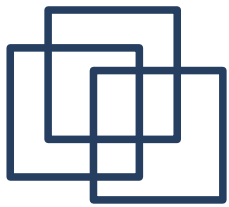
Penyebab DNS Cache Poisoning

- ♦ ID Transaksi/Query DNS yang tidak random (1995)
- ♦ RR Set poisoning (1997) :
 - RR Answer : berisikan jawaban atas pertanyaan yang diajukan
 - RR Authority : memberitahu resolver name server yang diacu untuk memperoleh jawaban
 - RR Additional : berisi informasi tambahan untuk membuat respon lebih efektif, contoh informasi mengenai NS dan alamat IP-nya

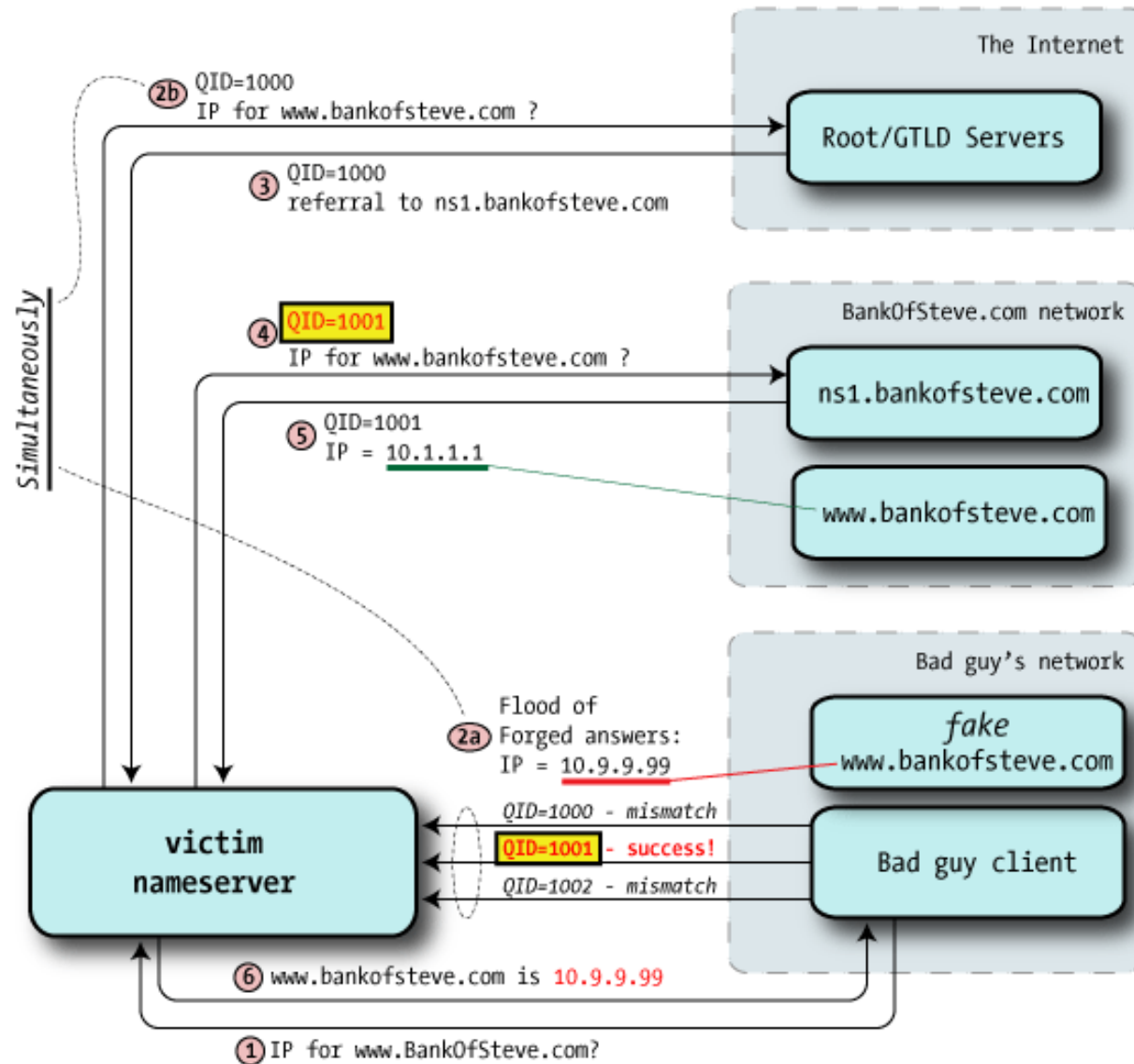


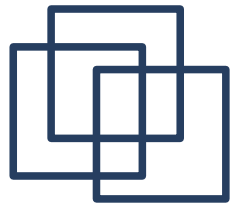
Predict Query ID





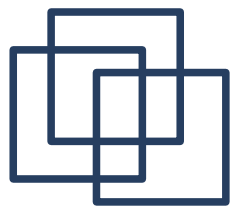
DNS Poisoning





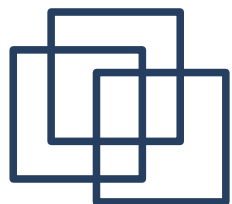
Solusi untuk Serangan Poisoning

1. Randomize Transaction/Query ID
2. Bailiwick Checking
 - ♦ Resolver mengingat bahwa bila mereka bertanya tentang www.korban.com, mereka tidak menyimpan alamat baru untuk www.google.com dalam transaksi yang sama.



DK's DNS Vuln. (2008)

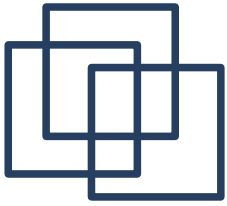
- ♦ Buat klien meminta alamat AAAAA.KORBAN.COM, AAAAB.KORBAN.COM dan seterusnya hingga misalnya CXOPQ. Klien percaya bahwa CXOPQ.KORBAN.COM adalah 6.6.6.0.
 - => menulis javascript yang menambahkan sekumpulan tag image berukuran 0 ke halaman web, yang mengacu pada image yang tidak ada ke setiap domain.
 - ♦ Respon dari penyerang juga berisikan RR Tambahan yang mengarahkan NS.KORBAN.COM ke 6.6.6.0.
 - => Karena CXOPQ dan NS berada dalam domain yang sama, maka BC dapat di-bypass.
- => Kombinasi serangan 1 dan 2



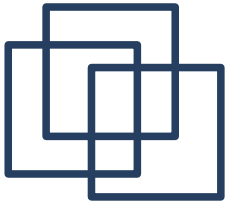
Fix untuk DK's DNS Vuln.

Randomizing source port

=> transaction space $\approx 2^{16} \times 2^{16} = 2^{32}$



DJB* WAS RIGHT



Terima Kasih