Ataques DNS

Grupo: Thiago Saytson, Tiago Borzino e Alan Peterson

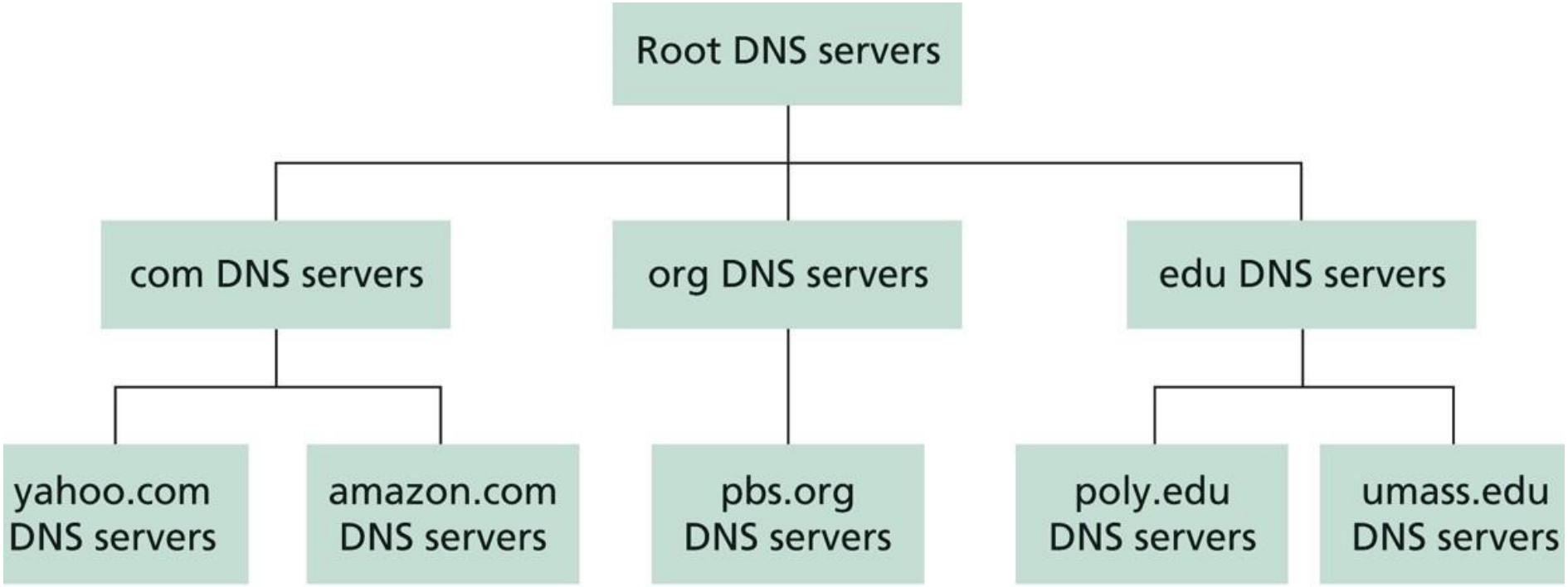
DNS

- DNS é um acrônimo para Domain Name System. É uma peça fundamental no uso da Internet, pois as interfaces de rede trabalham com endereços IP, uma vez que estes possuem tamanhos fixos de 4 bytes, e como é muito mais fácil guardarmos nomes em vez de conjuntos de números, o DNS é o protocolo que faz a correspondência entre nomes de domínios e endereços IP. Seus pacotes tem como protocolo de transporte o UDP e sua camada na pilha TCP/IP é a de Aplicação.

DNS

- O sistema funciona de forma hierárquica e distribuída, possibilitando que seja escalável e que funcione de forma contínua ainda que alguns servidores fiquem indisponíveis. Essa é a principal razão para que nenhum servidor DNS possua registros de recursos (RRs) de todos os domínios da Internet. Caso um servidor não possua resposta para uma requisição, ele retorna o endereço IP de um servidor do nível hierárquico superior.

Hierarquia do DNS



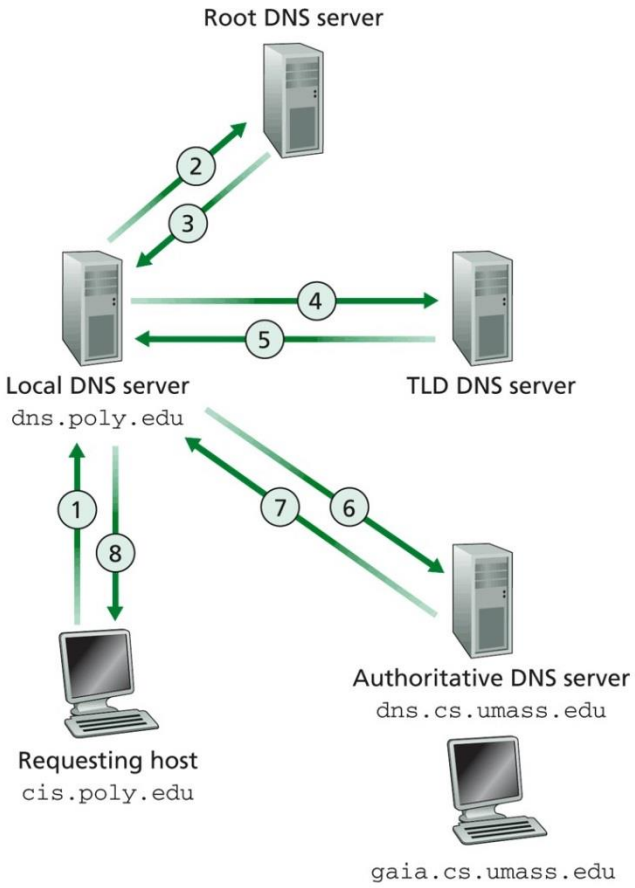
KUROSE, J.F.; ROSS, K.W. REDES DE COMPUTADORES E A INTERNET: UMA ABORDAGEM TOP-DOWN 6A. ED. SÃO PAULO, 2013.

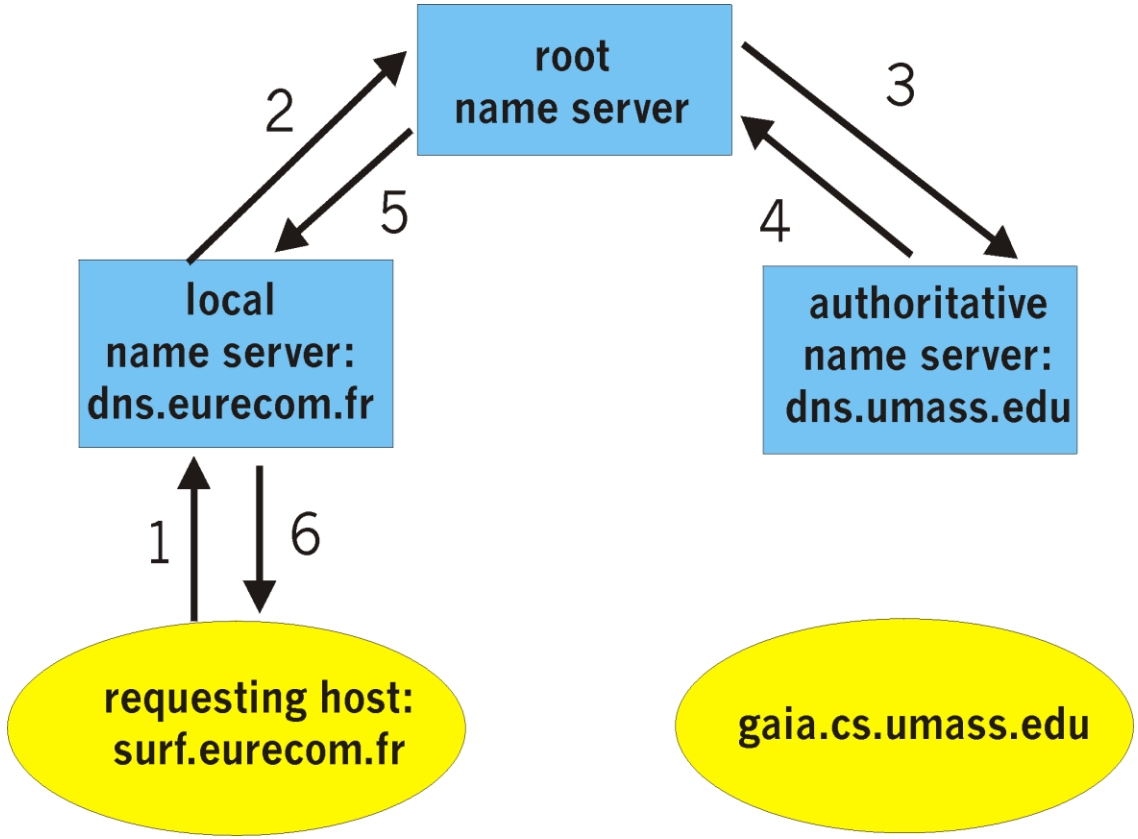
DNS

- A estrutura hierárquica do DNS é a funciona da seguinte forma:

1. Os servidores Root possuem registros dos servidores Top Domain Level.
2. Os servidores TLD, por sua vez, possuem registros dos servidores autoritativos de domínios .com, .br, .edu, .net, e etc.
3. Além destes, existem os servidores DNS locais, normalmente pertencentes a uma ISP (Internet Service Provider). Estes, em geral, fornecem endereços de outros servidores próximos. As consultas aos registros dos servidores DNS podem ser feitas de duas formas: iterativa ou recursiva.

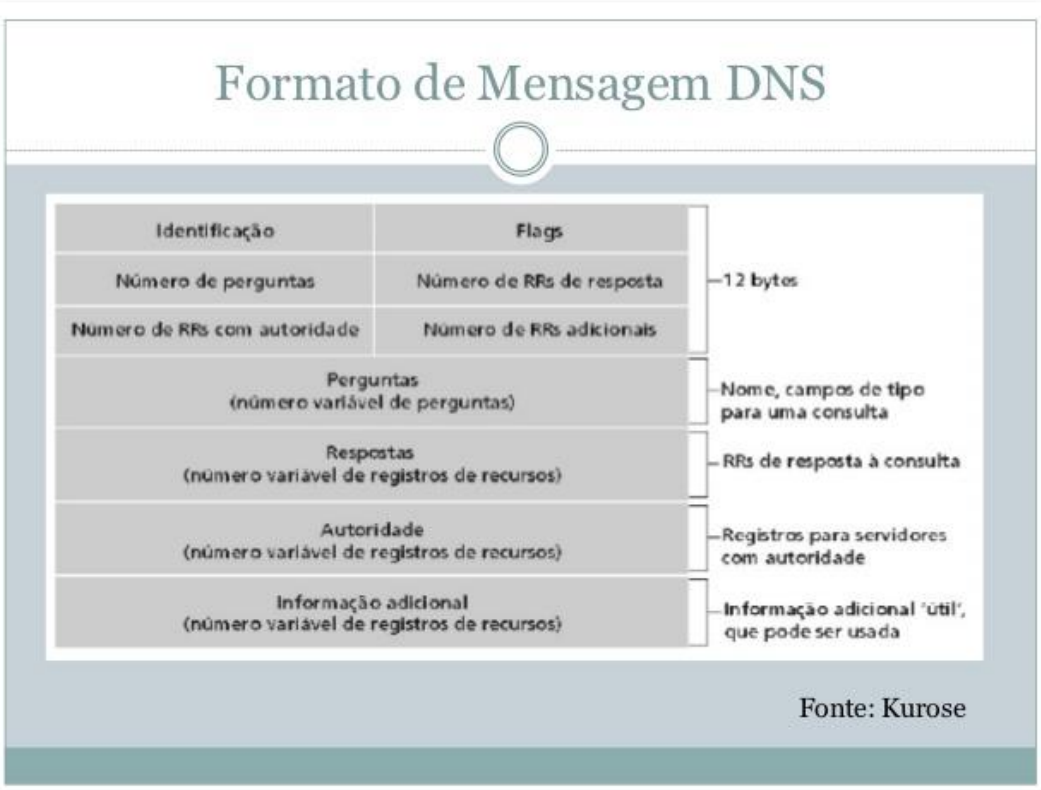
Consultas iterativas e recursivas





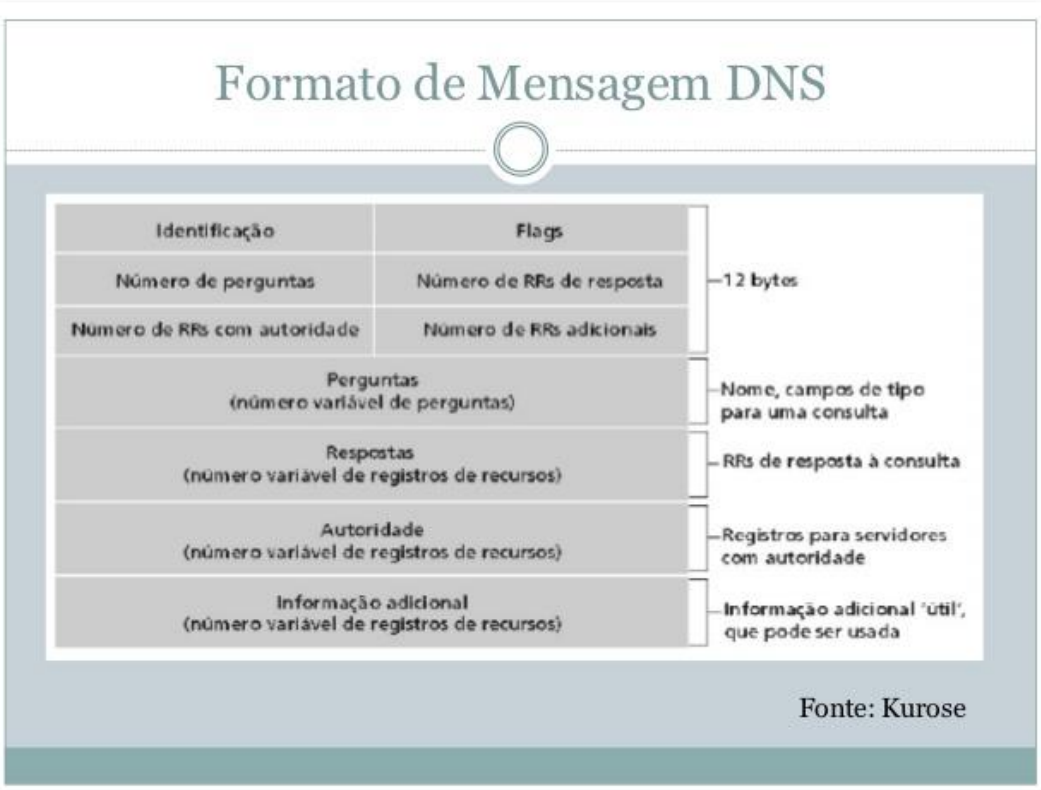
KUROSE, J.F.; ROSS, K.W. REDES DE COMPUTADORES E A INTERNET: UMA ABORDAGEM TOP-DOWN 6A. ED. SÃO PAULO, 2013.

As mensagens DNS



KUROSE, J.F.; ROSS, K.W. REDES DE COMPUTADORES E A INTERNET: UMA ABORDAGEM TOP-DOWN 6A. ED. SÃO PAULO, 2013.

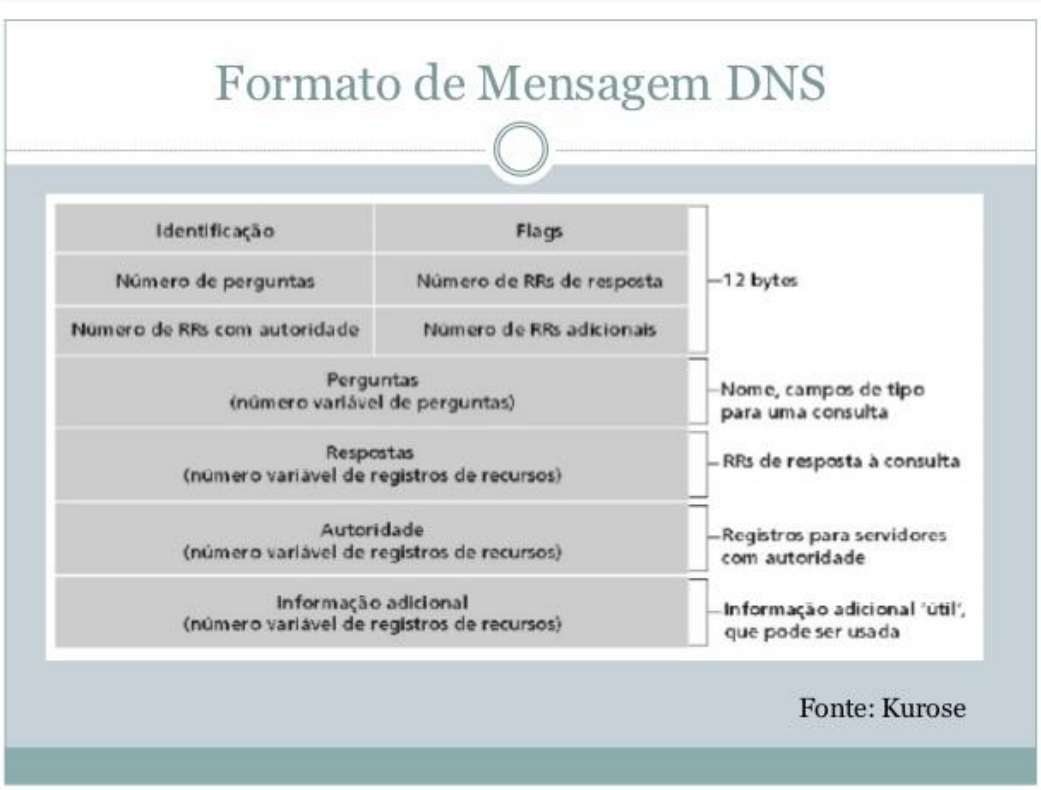
DNS



O campo "indetificação" é um número de 16 bits que identifica a consulta. Esse número é copiado para a mensagem de resposta, permitindo combinar respostas recebidas com consultas enviadas.

DNS

No campo de flags existem:
Flag de Consulta
0 = consulta
1 = resposta.
Flag de autoridade
1 = respostas de servidores autoritativos.

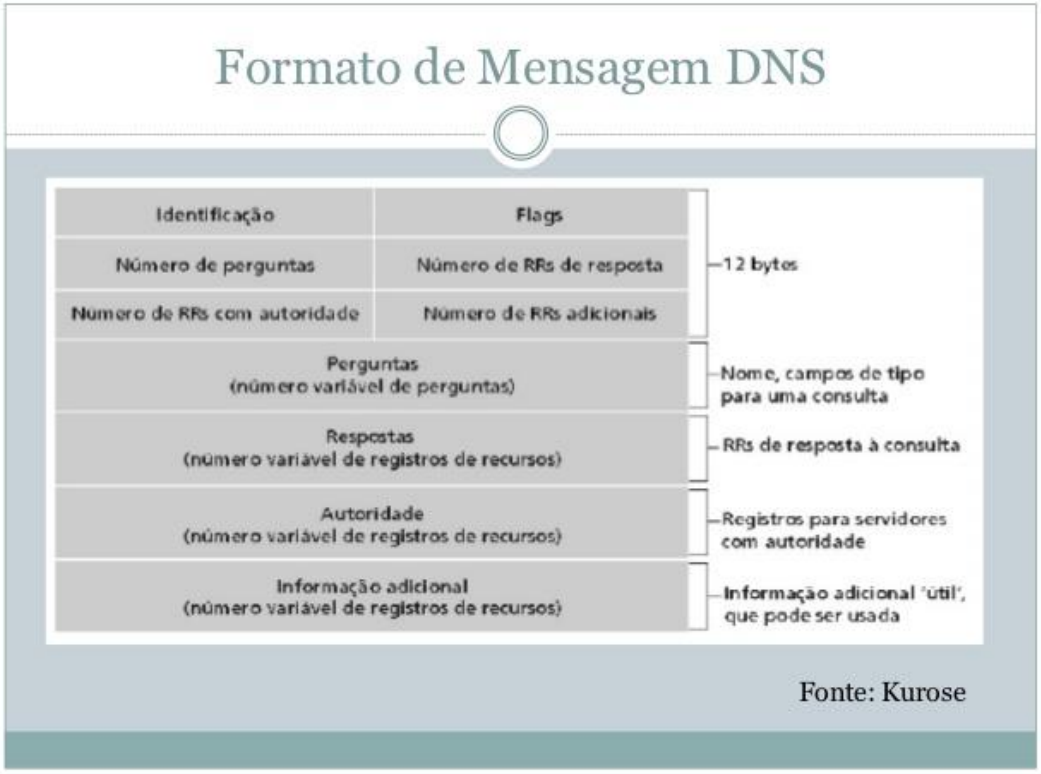


Flag de recursão
1 = cliente (hospedeiro ou servidor DNS) deseja que um servidor DNS atue de forma recursiva. Igualmente, um campo de recursão disponível está presente na resposta.

No cabeçalho há também quatro campos que indicam o número de ocorrências dos quatro tipos de seção de dados seguintes.

DNS

Os RRs são da forma:
(Type, Name, Value, TTL)
Type A:
(Domínio, IP)
Endereços web
Type MX:
(Domínio, IP)
Servidores de e-mail.
Type NS:
(Domínio, IP)
Servidores autoritativos



Type CNAME:
(Apelido, Nome canônico)
Pedidos para nomes canônicos de domínios.
Por exemplo:
(foo.com, relay1.bar.foo.com, CNAME)

Type define o tipo de consulta que será feita ao servidor, Name corresponde ao domínio, Value ao respectivo endereço IP e, TTL, o tempo que o registro será mantido no cache do servidor.

DNS

- Para que os registros entrem no banco de dados do DNS é preciso registrar o nome de domínio com uma das entidades registradoras credenciadas pela Internet Corporation for Assigned Names and Numbers (ICANN), que verificarão a exclusividade do nome.

Random Subdomain Attacks

- Random subdomain attack é um tipo de ataque que tem como vítima principal os servidores que suportam requisições DNS recursivas.
- Ele se baseia em enviar perguntas com nomes de domínio gerados de forma pseudo-aleatória, de modo que os servidores DNS não possam responder e enviem as requisições para as hierarquias superiores, inundando a rede com tais mensagens.

Random Subdomain Attacks

- Para que seja eficiente, na grande maioria dos casos trata-se de um ataque distribuído que tem como fonte endereços IP de grandes botnets.
- Como se trata de requisições DNS aparentemente comuns, em geral é difícil identificar que se trata de um ataque em vez de mensagens legítimas.
- Além disso, muitas empresas utilizam nomes de domínio randômicos como “domínios descartáveis”.

Exemplo de domínios descartáveis

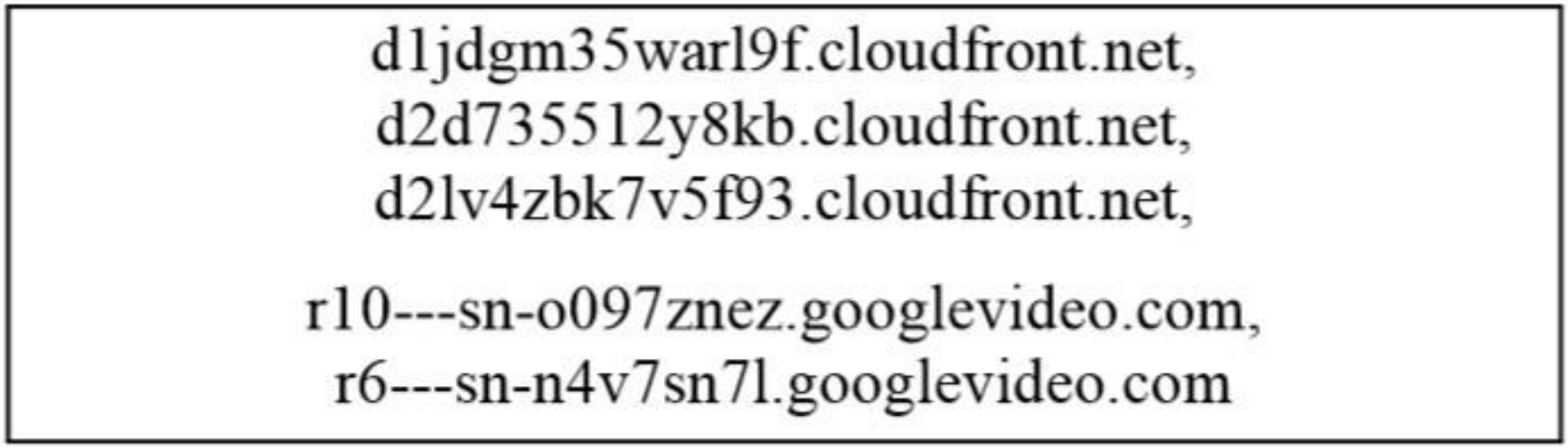


Figure 2 Disposable Domain Name Example

Seo, Y. Mitigating Random Subdomain DDoS Attacks from IoT Devices at Recursive DNS Servers, Conference Paper, December 2018

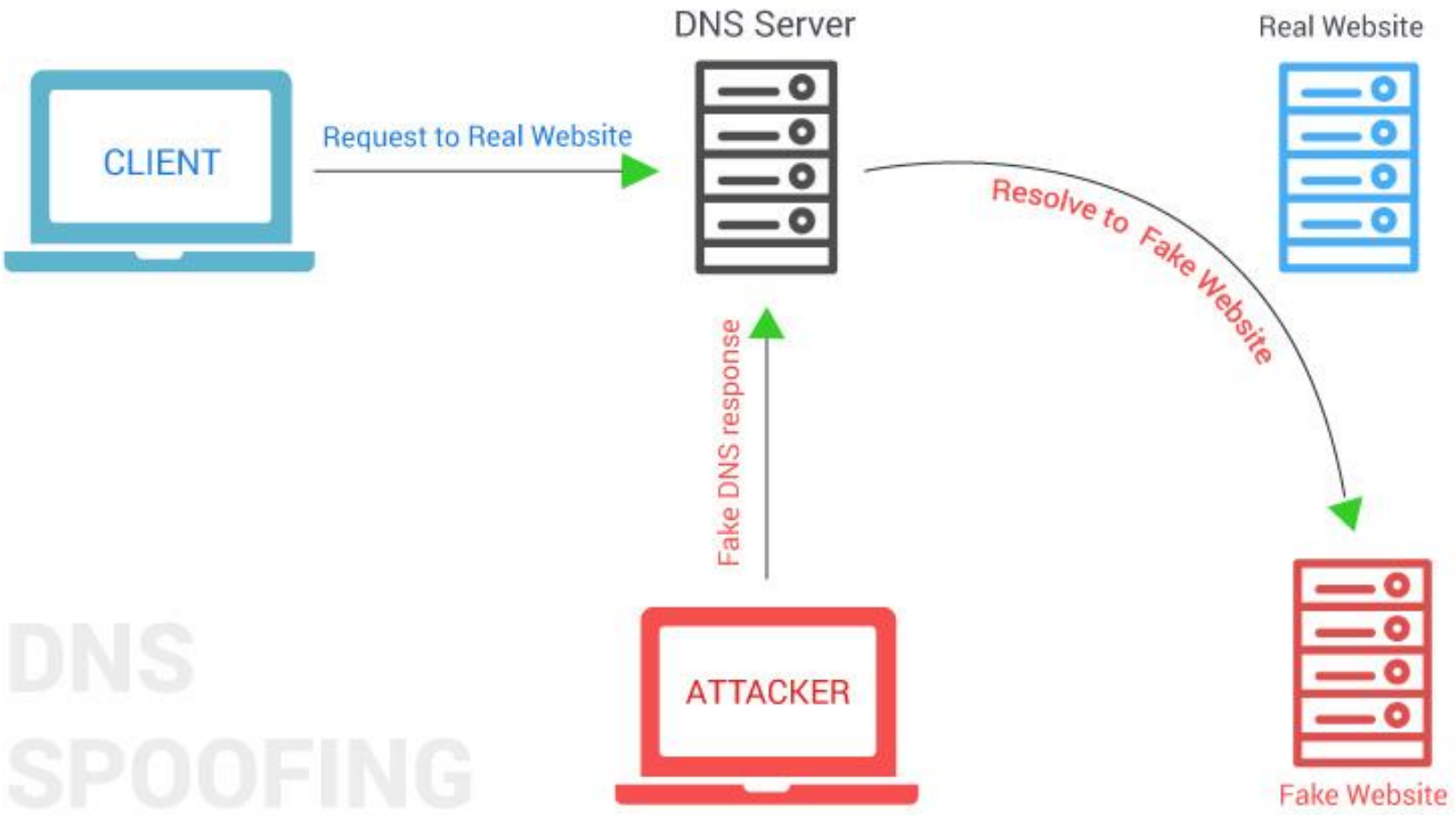
Random Subdomain Attacks

- Método proposto de defesa:
- Criar uma lista branca de quais domínios utilizam quais diferentes subdomínios e armazenar seus prefixos. Com essa lista identificar requisições maliciosas com subdomínios gerados de forma pseudo-aleatória.

Spoofing

- O DNS Spoofing é a alteração do campo ‘Value’ em uma resposta a uma requisição. Para o caso de um servidor DNS, o ataque se torna bem sucedido quando o servidor armazena em seu cache o IP falso.
- Uma das verificações feitas para validar uma resposta é a do campo ID no cabeçalho da resposta, a única exigida na RFC 1035.

Spoofing


DNS Server
Real Website
CLIENT
Request to Real Website
Resolve to Fake Website
Fake DNS response
ATTACKER
Fake Website
DNS
SPOOFING

Spoofing

- Softwares como o DNS Server da Microsoft verificam apenas se a ID da resposta é a mesma que a da pergunta. O Berkley Internet Name Domain (BIND), no intuito de aumentar a segurança, verifica outros campos como IP e porta UDP da resposta recebida.
- Como a ID tem 16 bits, teoricamente é possível realizar um ataque de força bruta variando as IDs de 1 a 65535 e enviando essa mesma quantidade de pacotes.

Spoofing

- Como o cache do servidor que aceita a resposta falsa fica “envenenado” por um tempo considerável, há várias consequências desse tipo de ataque, que serão abordadas em “Cache Poisoning”.

Spoofing

- Método proposto de defesa:
- Um método de defesa é guardar uma lista de respostas para uma determinada requisição por um intervalo de tempo. Enquanto outra resposta não for recebida o servidor pode armazenar a primeira resposta em seu cache ou não. Assim que outra resposta chega com o mesmo ID, são verificadas as outras informações. Se o *Value* de alguma das respostas subsequentes for diferente, é identificado o ataque e as devidas medidas são tomadas, como remover a resposta do cache e relatar o ocorrido à administração da rede. As respostas que tiverem o mesmo *Value* são consideradas como uma única resposta.

Spoofing

- Método proposto de defesa:
- O tempo estimado para análise das respostas DNS é baseado nas estatísticas de performance do DNS mostradas pelo MIT Laboratory for Computer Science e pelo Kore Advance Institute of Science and Technology (KAIST). Essas estatísticas mostram que o tempo médio para resolução de um nome é de 97 ms, sendo assim, um tempo 5000<T<=9999 ms estipulado para análise de detecção de um ataque é suficiente.

Spoofing

- Método proposto de defesa:
- Outro método de defesa é utilizar o DNSSEC, nome dado às extensões de segurança que estão sendo propostas para o protocolo DNS, definido pela RFC 2035.
- A principal característica desse modelo é prover autenticação da origem dos dados e verificar a integridade desses dados utilizando criptografia de chave pública.

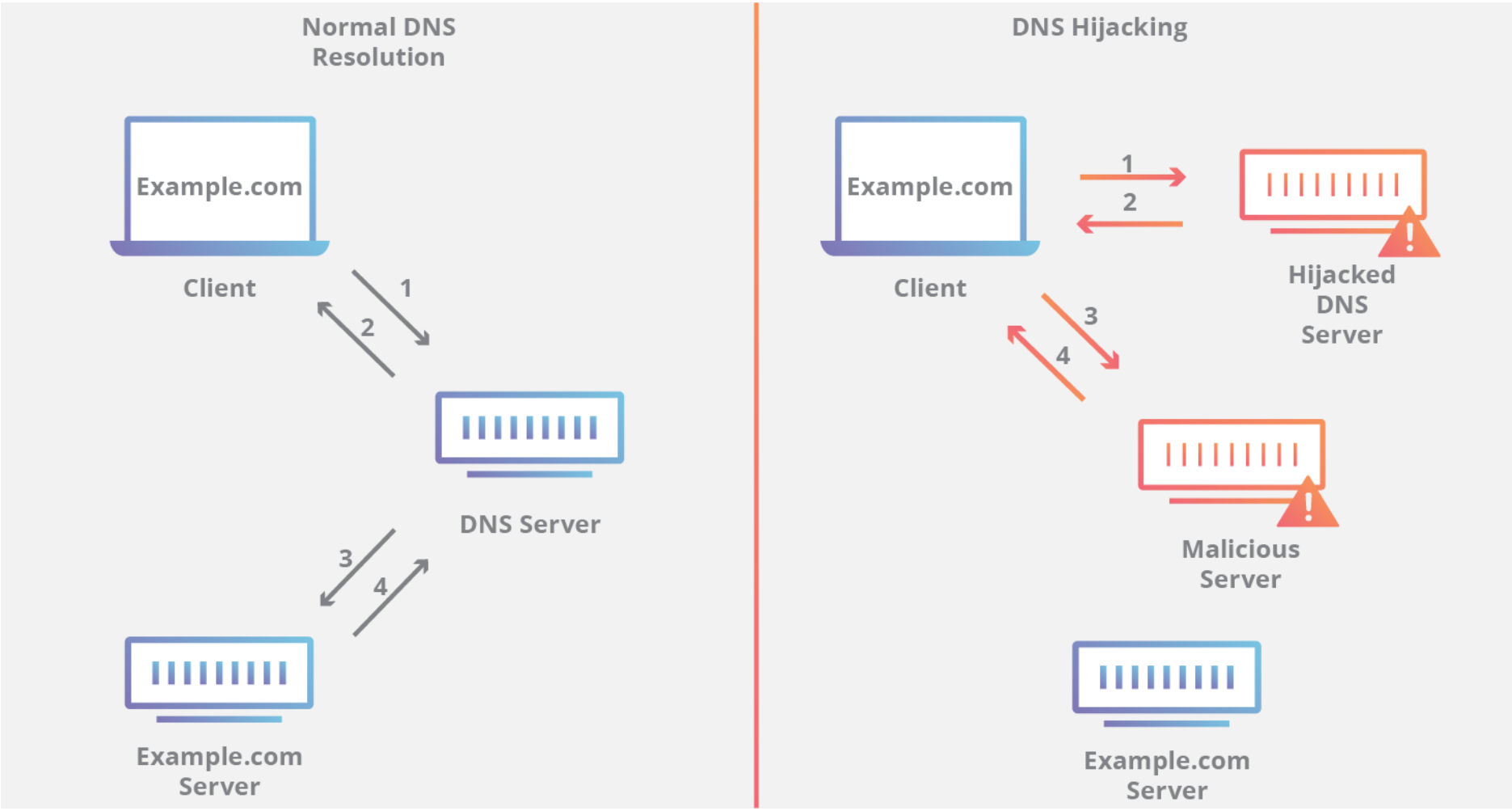
Spoofing

- Método proposto de defesa:
- No entanto o custo de processamento para validação de assinaturas digitais é demasiadamente elevado. Esse custo depende do algoritmo utilizado.
- Com DSA-512 é possível assinar aproximadamente 135 domínios/segundo em um PC de 500 Mhz utilizando FreeBSD e com RSA-1024 a taxa cai para 17 domínios/segundo. Para efeito de comparação um Root Server recebe em torno de 1.8 milhão de requisições por minuto.

Hijacking

- O roubo de domínio de DNS é a alteração de RRs em respostas às requisições das vítimas. Pode ser realizado em tempo real, como no normalmente acontece no DNS Spoofing, ou injetando RR falso na zonefile (tipo de arquivo utilizado, por exemplo, pelo BIND) do servidor DNS. O ‘Cache Poisoning’ também pode ser utilizado para roubo de domínio.
- O DNS hijacking também é utilizado para censura e vigilância, roubo de crendenciais e outros.

Hijacking


Normal DNS Resolution
Example.com
Client
1
2
DNS Server
3
4
Example.com Server
DNS Hijacking
Example.com
Client
1
2
Hijacked DNS Server
3
4
Malicious Server
Example.com Server

Hijacking

- Em 15 de Março de 2014 o servidor DNS do Goole, 8.8.8.8/32, foi sequestrado e teve seu tráfego redirecionado para divisões da Venezuela e Brasil de uma empresa de telecomunicações britânicas, devido a uma vulnerabilidade no Border Gateway Protocol (BGP) utilizado por grandes corporações.

Hijacking

- Método proposto de defesa:
- Como na maioria dos casos o Hijacking é feito através de spoofing ou cache poisoning, os mesmos métodos propostos nesses casos continuam válidos.

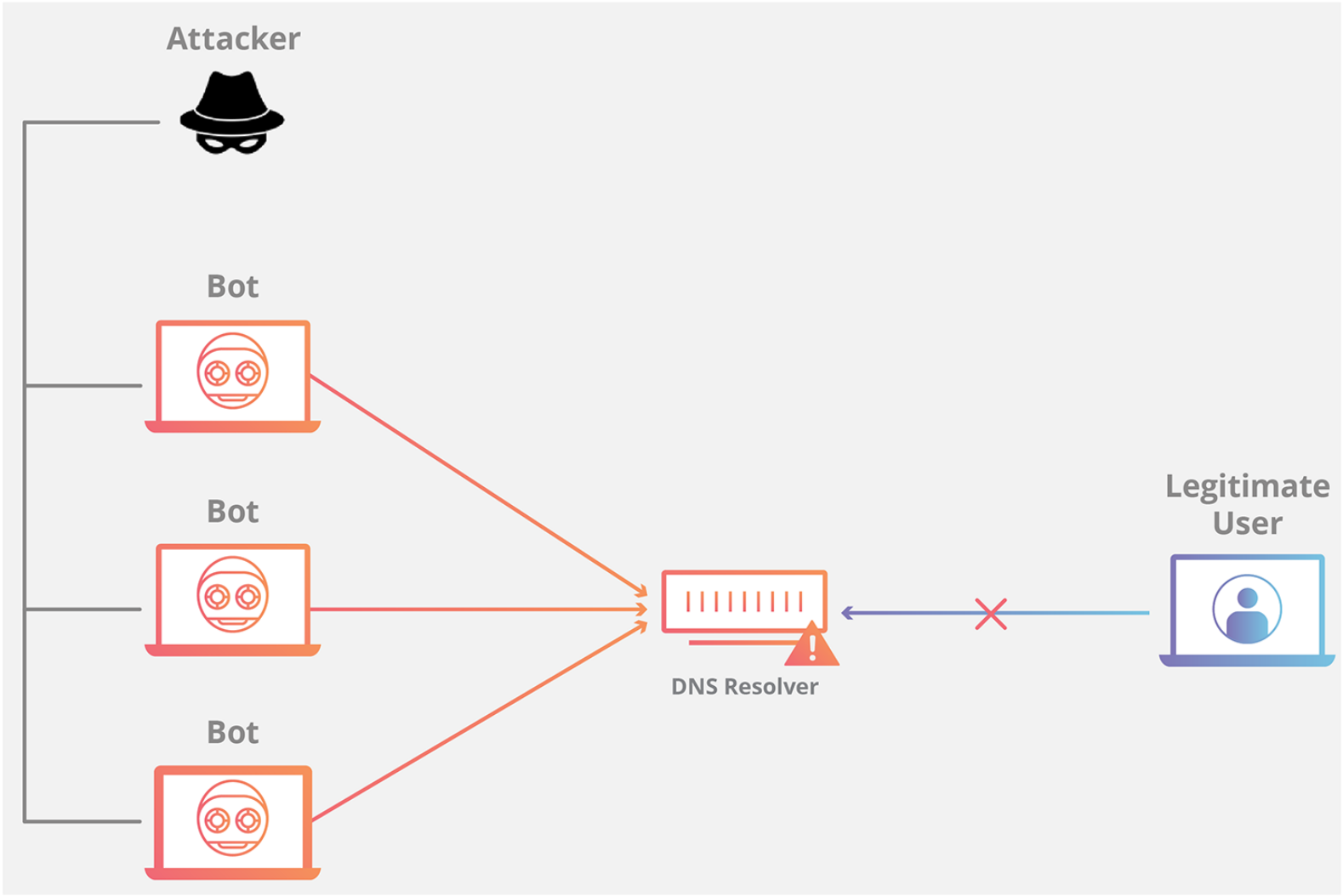
Flood Attack

- Os flood attacks ao DNS tem como objetivo inundar a largura de banda dos servidores DNS, tornando-os inoperantes para requisições legítimas, isto é, um ataque de negação de serviço (DoS).

Flood Attack

- Como o número de dispositivos IoT também vem aumentando consideravelmente, enquanto, por outro lado, o mesmo não ocorre com seus mecanismos de segurança (IDS, Firewall, etc.), estes têm se tornado o principal alvo de ataques botnets, realizando ‘distributed DoS’ (DDoS).

Flood Attack



Flood Attack

- O relatório de ameaças de Março de 2018 do McAfee labs apontou os ataques DDoS como o terceiro maior na lista de ataques à segurança da rede, e crescem a cada ano.
- Ainda, de acordo com a pesquisa do Kaspersky Labs, um em cada três empreendimentos sofreu um ataque DDoS em 2017
- E pelo relatório anual de segurança de 2016 da CISCO, 91.3% dos malware "reconhecidamente malignos" usam DNS para se proliferar.

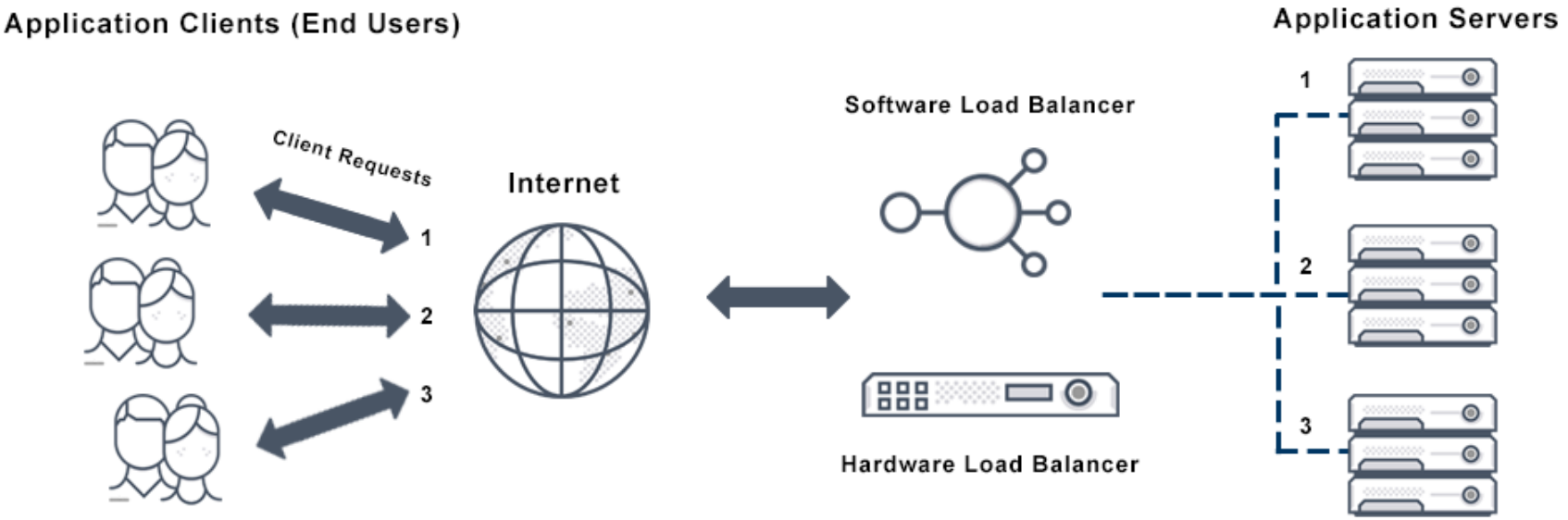
Flood Attack

- Em 2016 houve um DDoS flood attack capaz de derrubar a rede da Dyn, companhia responsável por gerenciar performance de redes e aplicações web seguras, além dos serviços de registro de domínio e e-mail.
- Sites como Twitter, Reddit, Github, Amazon.com, Netflix, Spotify, Runescape, Quora e o próprio site da Dyn ficaram inalcançáveis através de URL, embora a maioria dos sites tenha permanecido acessível via endereço IP de forma manual.

Flood Attack

- Método proposto de defesa:
- Criar uma rede de servidores DNS em topologia circular/hierárquica/backup, de forma que caso um servidor comece a ficar indisponível, o tráfego seja destinado ao próximo, aliviando os recursos do primeiro e assim dificultando a inoperabilidade de toda a rede.

Flood Attack



Cache Poisoning

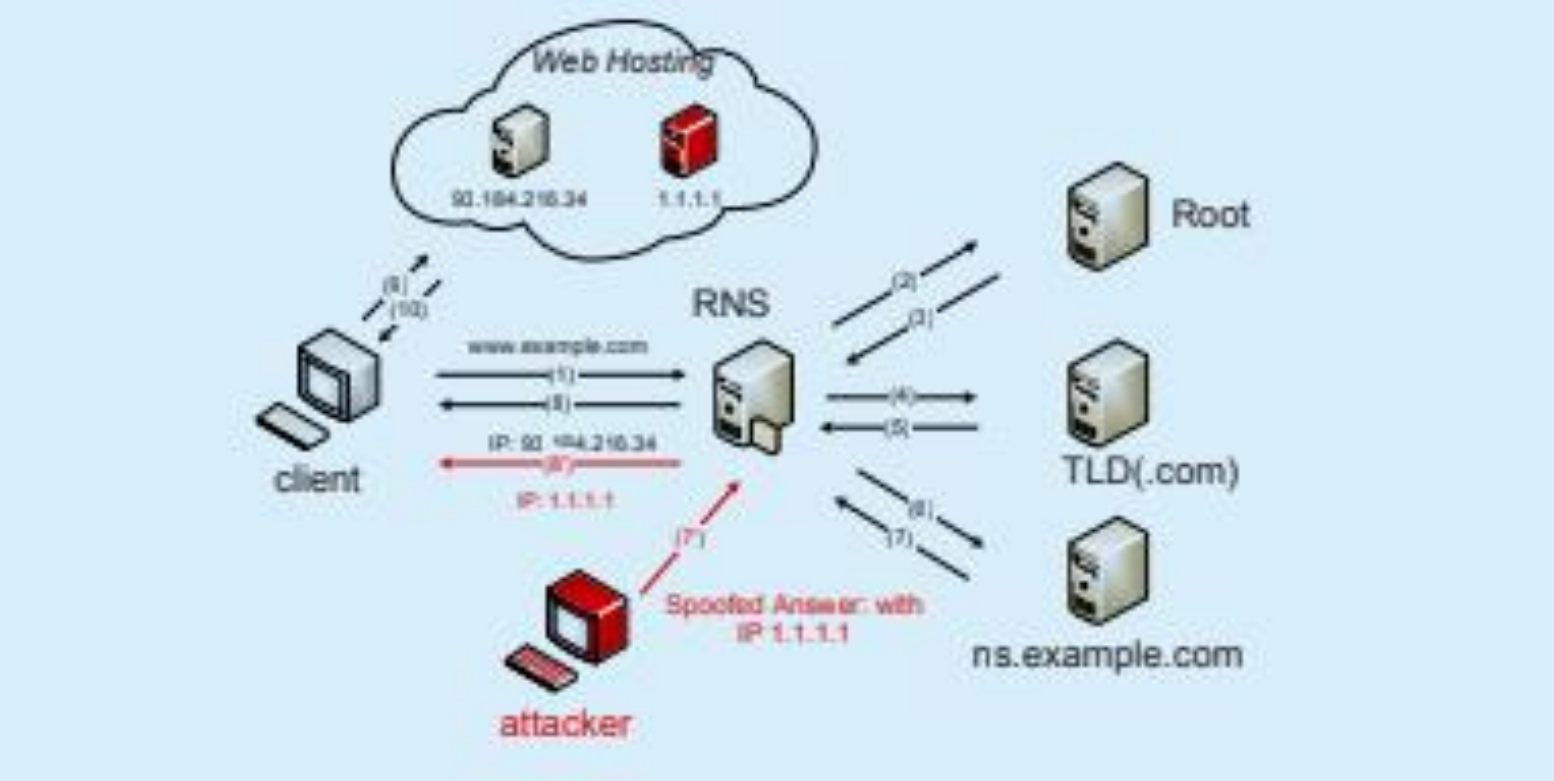
- O Ataque

O envenenamento de cache é um ataque que visa:

- mudar a URL (Localizador uniforme de recursos) de um site;
- roubar informações pessoais e senhas;
- prejudicar economicamente.

Cache Poisoning

O ataque ocorre durante o mapeamento DNS.



Cache Poisoning

- DNSSEC

O DNSSEC foi proposto para combater esse ataque, mas não muito utilizado.

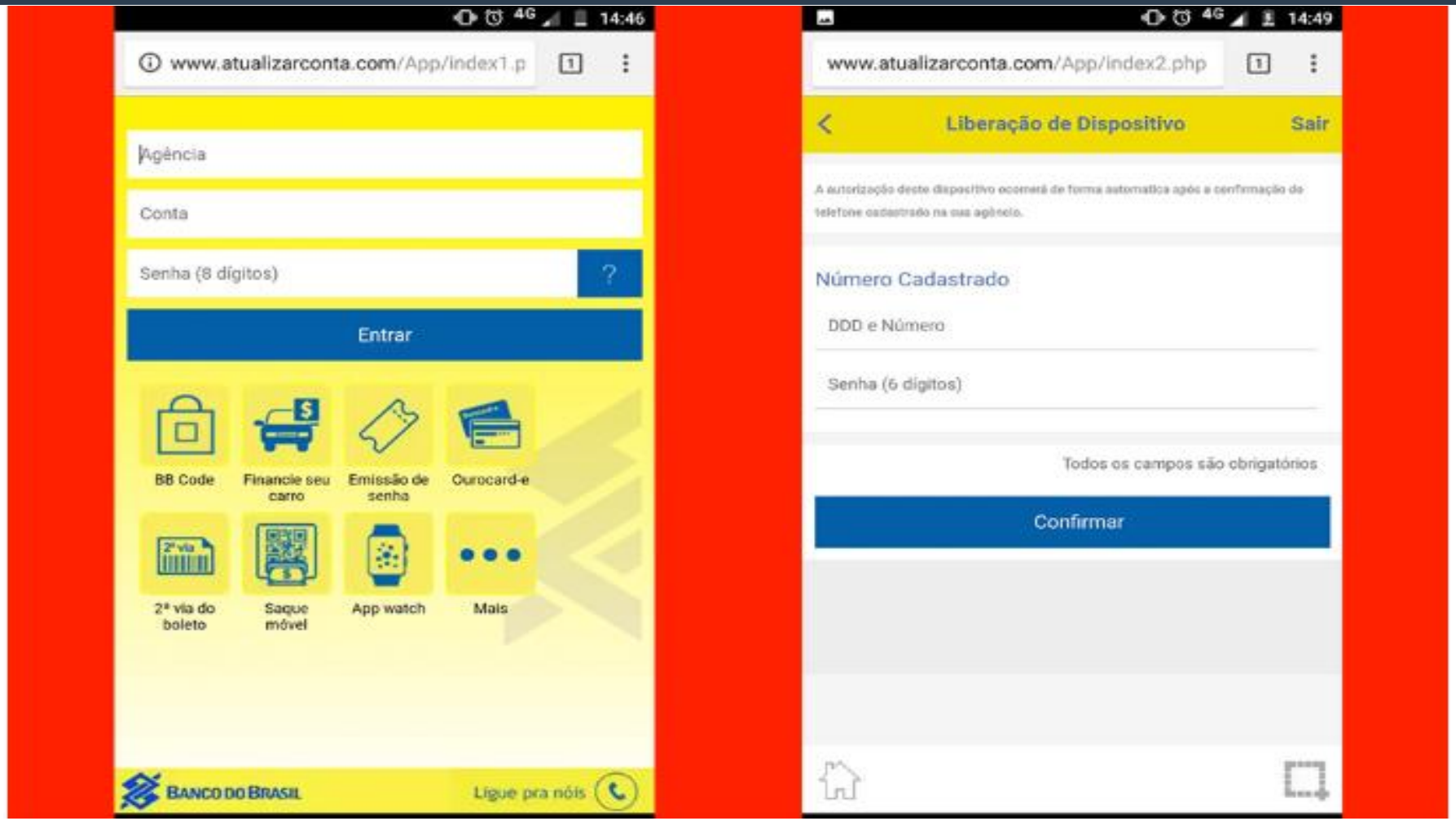
- Método proposto para prevenir o ataque:

Usar vários servidores DNS diferentes para obter respostas referentes à um único pedido e comparar as respostas recebidas para determinar a confiabilidade delas.

- Método proposto para mitigar o impacto:

Recuperar parte do cache do servidor DNS.

Exemplo de site falsificado



Tunneling

- O Ataque

O tunelamento de DNS consiste em esconder dados em pedidos e respostas DNS

Tunneling

- Método proposto de defesa:

Uso de uma rede neural que iria analisar os pacotes e aprender com a informação retirada deles, para poder classificá-los em normais ou maliciosos

Pergunta

- Qual a principal razão para que os servidores DNS não tenham RRs sobre todos os domínios?

Resposta

- Qual a principal razão para que os servidores DNS não tenham RRs sobre todos os domínios?
- R: Para que o sistema seja distribuído, permitindo o funcionamento contínuo, e para que seja escalável nas infraestruturas de redes.

Pergunta

- Qual dos princípios da segurança da informação é quebrado com o ataque de DNS spoofing?

Resposta

- Qual dos princípios da segurança da informação é quebrado com o ataque de DNS spoofing?

R: O princípio de autenticidade, uma vez que a resposta à requisição não foi enviada pelo destino legítimo da requisição.

Pergunta

- Em que parte da atuação do DNS ocorre o envenenamento de cache e como ele é feito?

Resposta

- Em que parte da atuação do DNS ocorre o envenenamento de cache e como ele é feito?

R: O ataque ocorre durante a resolução de nome(mapeamento) DNS. o envenenamento do cache é feito quando um servidor autoritário de DNS feito por um atacante resolve o pedido DNS, dando uma resposta de endereço IP falso de um ou vários sites e o servidor DNS que fez o pedido aceita essa resposta falsa.

Pergunta

- Como seria possível criar um flood attack utilizando as respostas DNS?

Resposta

- Como seria possível criar um flood attack utilizando as respostas DNS?

R: Fazendo um DNS DDoS com um IP de origem falso, direcionando um grande número de respostas DNS para uma determinada rede.

Resposta

- Em que consiste o tunelamento de DNS?

R: O tunelamento de DNS é um mecanismo que tem como premissa esconder informações, que são criptografadas, dentro de pedidos e respostas DNS.

Pergunta

- Qual é a dificuldade em identificar um random subdomain attack?

Pergunta

- Qual é a dificuldade em identificar um random subdomain attack?

R: A dificuldade está em diferenciar as requisições com domínios randômicos das requisições legítimas.