Spoofer

2º Ano – LEI – Redes de Computadores

Tiago Matos Guedes a97369
Tiago André Leça Carneiro a93207
Diogo Afonso Costa Gonçalves a101919
Grupo 9

Introdução

1. O que é o spoofing?
2. Tipos de Spoofing
3. Motivação e Contextualização
4. Objetivos
5. Soluções para Prevenção
6. Nova Solução Proposta
7. Arquitetura
8. Resultados
9. Estado Atual e Próximos Passos
10. Conclusão

O que é o spoofing?

Definição:

O conceito consiste no atacante ganhar a tua confiança fazendo-te acreditar que as suas comunicações são legítimas.

Exemplos:

Fingir utilizar um email oficial do PayPal para requisitar informações pessoais da vítima – **Email Spoofing.**

SMTP : Simple Mail Transfer Protocol
Devido a não ter autenticação, se o servidor não estiver bem configurado pode levar a casos como o exemplo anterior.

Tipos de Spoofing

DNS Spoofing:

Manipulação de consultas **DNS** para redirecionar utilizadores para sites falsos.

Email Spoofing:

Falsificação do atacante de e-mails para aplicar golpes ou **phishing**.

GPS Spoofing:

Manipulação de sinais GPS para iludir o dispositivo de navegação.

Soluções para prevenção

Source Address Validation(SAV)

O SAV é o standard que discarda pacotes com IP's de origem spoofed. A falta de SAV causa distributed denial-of-service (DDoS)

Outbound SAV

Filtragem na entrada da rede do cliente, fazendo com que os routers bloqueiem pacotes que chegam com **IP** de origem spoofed.

Inbound SAV

A filtragem é feita fora da rede do cliente na ponte que faz conexão com o fornecedor, aplicando o mesmo bloqueio que o método anterior.

RPF

É verificado na tabela de **rooting** se o **IP** de origem do pacote recebido é alcançável através do mesmo caminho de onde o pacote veio.
Strict : é verificado se o caminho é exatamente o mesmo
Feasible : aceita também pacotes de **IP**'s que tenham rotas alternativas válidas.

Como saber onde aplicar?

Este novo estudo propõe uma nova forma de detetar redes sem filtragem SAV, usando **loops** em **traceroute.**

Motivação e Contextualização

IP Spoofing: Vulnerabilidade explorada há mais de 25 anos.

Usos Maliciosos: Ataques de redireccionamento, amplificação e anonimato.

Solução (SAV - Source Address Validation): Filtragem de pacotes com IPs falsificados.

Desafios na Adoção : Custo para quem implementa.

Benefícios distribuídos para toda a Internet.

Proposta do Estudo : Identificar redes sem SAV.

Uso de loops em **traceroute** para detetar falhas no SAV em provedores de trânsito.

Objetivos

- Demonstrar a viabilidade da implementação de listas de controle de acesso (**ACLs**) de entrada estáticas nos provedores, dado que os endereços **IP** dos clientes raramente mudam.
- Desenvolver um algoritmo escalável para inferir a ausência de filtragem de entrada a partir de padrões específicos observados em **traceroutes**.
- Validar a precisão do algoritmo por meio de comparação com informações de operadores de rede.
- Analisar a eficácia do método em escala global na Internet.
- Criar um site público que exibe redes que permitem **spoofing**, oferecendo dados acionáveis para que operadores implementem filtragem.

Exemplo dos loops

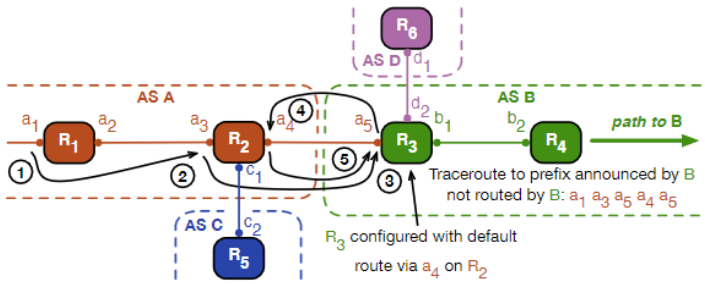


Fig. 3: A simple loop between AS A and its customer B implying absence of filtering by A at R_2. R_2 should discard packet 4 because it arrives with a source address outside of B's network, rather than send it back to B (5).

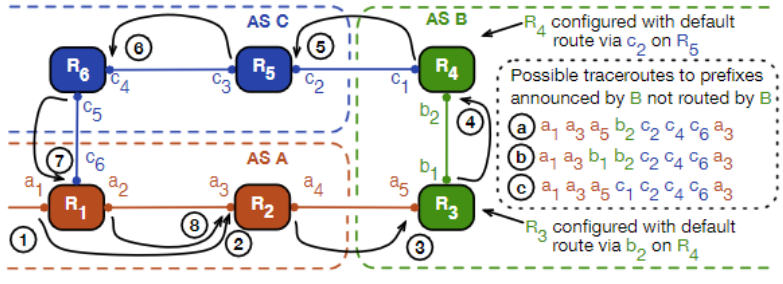


Fig. 4: A two-provider loop between ASes A and C and their customer B implying absence of filtering by C at R_5. R_5 should discard packet 5 because it arrives with a source address outside of B, rather than forward the packet to R_6.

Arquitetura

- Coletar **traceroutes** através de um conjunto de **vantage points (VP)** globais.
- Identificação de fornecedores de trânsito e suas conexões com clientes.
- Aplicação de heurísticas para determinar **loops** que indicam falta de filtragem.
- Validação dos resultados com operadores de rede.

Resultados

Foram encontrados **2.500 loops** únicos em **703 fornecedores e 1.780 redes clientes**.

O método identificou novos casos que os projetos **Spoofer** e **Open Resolver** não detetaram.

95% de precisão ao validar com operadores de redes.

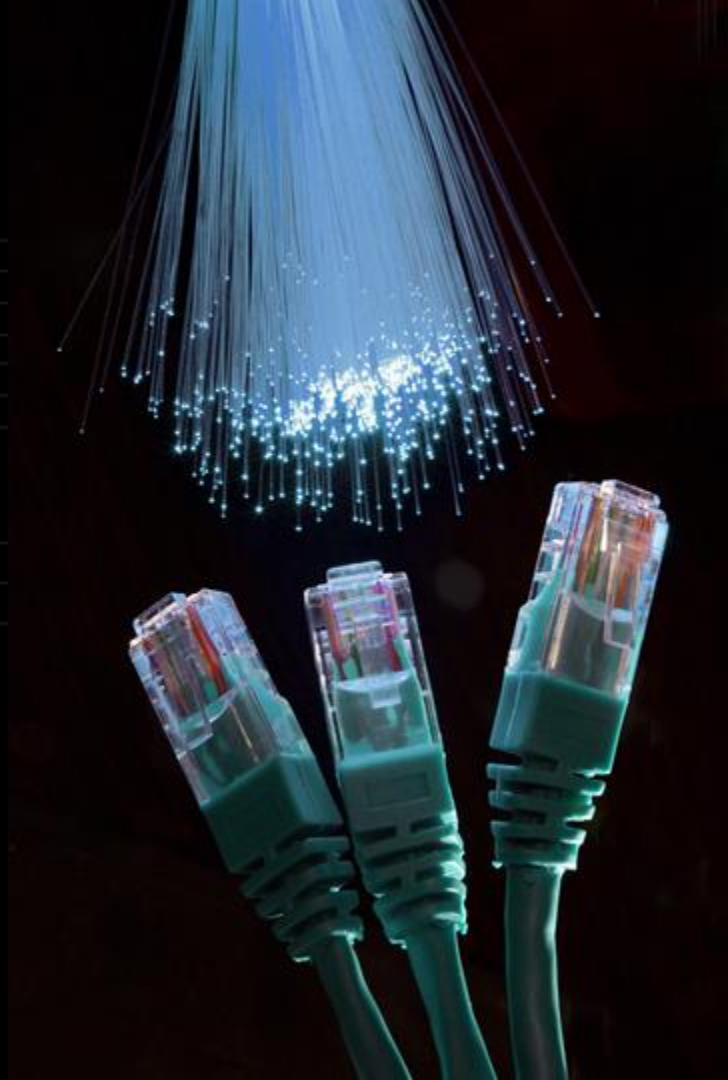
A maioria das redes clientes com vulnerabilidades possui prefixos pequenos (≤ /20), o que sugere que não têm infraestrutura robusta para implementar filtragem.

Estado Atual e Próximos Passos

Estado Atual:
- Resultados disponíveis publicamente em um site.
- Permite que operadores de rede verifiquem a implementação de **ingress filtering**.

Melhorias Propostas:
- Aprimorar a deteção de fronteiras entre provedores e clientes.
- Distinguir **loops** temporários de falhas reais no **SAV**.

Próximos Passos:
- Avaliar se a exposição pública de redes inseguras incentiva correções.
- Estudar estratégias para impulsionar a adoção do **SAV**:
  - Pressão da comunidade.
  - Regulamentação e normas.



Conclusão

O estudo propõe um novo método para detetar redes vulneráveis a **IP spoofing** usando **loops em traceroute**. Essa abordagem melhora a visibilidade do problema e é um passo importante na luta contra **ataques cibernéticos**.

FIM

Alguma dúvida ou questão sobre
o estudo e a
luta contra o **spoofing**?"