RANGER

Pesquisando segurança em roteamento interdomínio na internet

EQUIPE

Coordenadores no Brasil:
Ítalo Fernando Scotá Cunha
Universidade Federal de Minas Gerais
cunha@dcc.ufmg.br

Ronaldo Alves Ferreira
Universidade Federal de Mato Grosso do Sul
raf@facom.ufms.br

Coordenador nos Estados Unidos:
Ethan Katz-Bassett
Columbia University
ethan@ee.columbia.edu

Pesquisadores:
Cristine Hoepers
CERT.br

Dorgival Olavo Guedes Neto
Universidade Federal de Minas Gerais

Klaus Steding-Jessen
CERT.br

Wagner Meira Jr.
Universidade Federal de Minas Gerais

PARCERIAS
CAIDA
FU-Berlin
Princeton University
RIPE

DESCRIÇÃO

Apesar da sociedade depender cada vez mais de serviços na internet, esses permanecem vulneráveis. Ataques são possibilitados por graves vulnerabilidades no projeto base da internet. Duas funcionalidades fundamentais da internet são construir rotas e encaminhar pacotes de dados, e os mecanismos para ambas não possuem autenticação. A falta de autenticação permite atividade maliciosa, como anúncio de rotas sem autorização e subsequente desvio de tráfego (*prefix hijack*), bem como o envio de pacotes com endereço IP de origem falsificado (*source spoofing*). Os recentes desvios de rota de tráfego doméstico norte-americano transitando pela Islândia expõem tráfego para terceiros. Ataques de negação de serviço contra o GitHub usando amplificação de dados para atingir taxas de 1,7 Tb/s mostram que falsificação do endereço IP de origem permite realizar ataques expressivos com capacidade para afetar serviços bem provisionados. Devido a essas vulnerabilidades, **pesquisa em roteamento na internet é essencial para a cibersegurança**.

Infelizmente, pesquisadores não conseguem realizar experimentos de roteamento na internet que sejam ambos realistas e controlados. Em particular, estudos usando simulação ou emulação da internet são limitados pela nossa capacidade de medi-la e modelá-la.

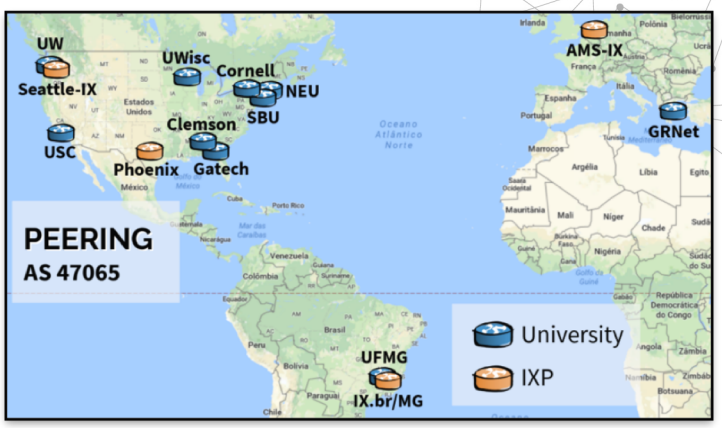
O PEERING é uma plataforma de pesquisa em roteamento interdomínio na internet que permite pesquisadores controlarem uma rede na internet, com roteadores espalhados em quatro continentes e conectados diretamente a centenas de redes reais (como RNP, Google, Facebook, Akamai). O PEERING permite pesquisadores executarem experimentos de roteamento realistas e controlados, mas ainda não suporta várias classes de experimentos relacionados à cibersegurança.

Esse projeto possui três objetivos principais:

(1) Estender a plataforma PEERING para permitir novas classes de pesquisa em roteamento seguro na internet que estão além do alcance de pesquisadores acadêmicos hoje;
(2) Desenvolver técnicas de monitoramento para identificar redes que estão utilizando tecnologias para autenticação de anúncios e evitar sequestros de prefixos; e
(3) Desenvolver técnicas para identificar redes que permitem o envio de pacotes IP com endereço de origem falsificados.

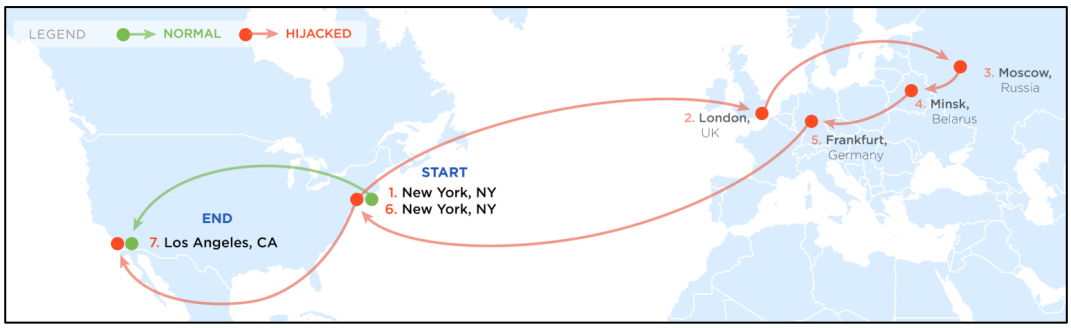
Extensão da plataforma PEERING

Iremos tornar o PEERING mais flexível adicionando funcionalidades e dando suporte a mais classes de experimentos de segurança sem sacrificar desempenho. Em particular, iremos permitir que experimentos executem aplicações nos roteadores da plataforma, permitindo execução de serviços reais.



Monitoramento de adoção de tecnologias de autenticação de rotas (RPKI)

Iremos desenvolver técnicas de medição de redes para desambiguar entres diferentes explicações possíveis para comportamento de redes na internet. Em particular, pretendemos desambiguar se a preferência por uma rota autenticada é devida à autenticação da rota ou simples engenharia de tráfego.



Identificação da fonte de pacotes IP com endereço de origem falsificado

Iremos também propor mecanismos para identificar (conjuntos de) redes vulneráveis ao envio de pacotes com endereços IP de origem falsificados. Para isso, iremos monitorar rotas com grande volume de tráfego malicioso e usar a plataforma PEERING para causar mudanças sistemáticas de roteamento. Pretendemos identificar redes que originam tráfego malicioso observando quais redes aparecem sistematicamente em rotas com grande volume desse tipo de tráfego.