UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
INSTITUTO DE INFORMÁTICA
CURSO DE GRADUAÇÃO EM CIÊNCIA DA COMPUTAÇÃO

Bruno Rafael Lorensi

Análise da Implantação do RPKI no Brasil

Porto Alegre
2020

Bruno Rafael Lorensi

Análise da Implantação do RPKI no Brasil

Trabalho de conclusão de curso de graduação apresentado ao Instituto de Informática da Universidade Federal do Rio Grande do Sul como requisito para a obtenção do título de Bacharel em Ciência da Computação.

Orientador: Lisandro Zambenedetti Granville
Co-orientador: Leandro Márcio Bertholdo

Porto Alegre

2020

AGRADECIMENTO

Agradeço a todos que acreditaram em mim e de alguma forma tornaram possível à conclusão deste trabalho.

Aos meus pais, Silmar Lorensi e Suzeth Lorensi, por todo o apoio recebido e por acreditar nessa conquista desde o início da graduação. Obrigado por todos os incentivos e conselhos durante esta trajetória tão importante para mim.

À minha namorada, Tamara Freitas dos Santos Fernandes, pela paciência e incentivo dado para a conclusão deste trabalho. Por entender que nem sempre eu poderia estar disponível, muito obrigado.

Ao meu orientador, Lisandro Zambenedetti Granville, por não ter desistido de mim, mesmo depois das outras duas tentativas de conclusão. Obrigado por sempre me apoiar e orientar de forma excepcional para concluir esta etapa tão importante da minha vida.

Ao meu co-orientador, Leandro Márcio Bertholdo, por toda ajuda dada a este trabalho.

Aos meus colegas do PoP-RS, pela compreensão de não poder me dedicar como deveria às atividades e sempre me apoiarem. Em especial ao César Loureiro por sempre me incentivar a concluir este trabalho e pelas dicas dadas.

Sem elas seria quase impossível a conclusão deste trabalho, muito obrigado.

LISTA DE ABREVIATURAS E SIGLAS

AS – Sistema Autônomo (Autonomous System)

ASN – Número de Sistema Autônomo (Autonomous System Number)

BGP – Border Gateway Protocol

BCOP – Curso de Boas Práticas para Sistemas Autônomos

CA – Autoridade Certificadora (Certificate Authority)

CAIDA – Center of Applied Internet Data Analysis

CNPJ – Cadastro Nacional da Pessoal Jurídica

FEBRABAN – Federação Brasileira de Bancos

FIB – Base de Informação de Encaminhamento (Forwarding Information Base)

IANA – Internet Assigned Numbers Authority

IP – Internet Protocol

ISP – Internet Service Provider

IX – Internet Exchange

LIR – Registro de Internet Local (Local Internet Registry)

NIC.br – Núcleo de Informação e Coordenação do Ponto BR

NIR – Registro de Internet Nacional (National Internet Registry)

PKI – Infraestrutura de Chaves Públicas (Public Key Infrastructure)

PTT – Ponto de Troca de Tráfego

RFC – Request for Comments

RIPE – Réseaux IP Européens Network Coordination Center

RIR – Registro Regional de Internet (Regional Internet Registry)

RNP – Rede Nacional de Ensino e Pesquisa

ROA – Registro de Autoridade de Origem (Route Origin Authorization)

RPSL – Routing Police Specification Language

RTR – Router to Router Protocol

RPKI – Resource Public Key Infrastructure

LISTA DE FIGURAS

Figura 1.1 - Tamanho da Tabela BGP 8
Figura 1.2 - Frequência Sequestro de Prefixo 10
Figura 2.1 - Topologia da Internet 13
Figura 2.2 - Organização de Registro de Recursos 14
Figura 2.3 - Tráfego sem PTT 16
Figura 2.4 - Tráfego com PTT 16
Figura 2.5 - Utilização de rota mais específica 18
Figura 2.6 - Tráfego Normal para YouTube 19
Figura 2.7 - Pakistan Telecom aparece da tabela de rotas 19
Figura 2.8 - Tráfego do Youtube Redirecionado 20
Figura 2.9 - Estrutura IRR 22
Figura 2.10- Exemplo de Entrada IRR 22
Figura 2.11 - Cadeia de Confiança do RPKI 25
Figura 2.12 - Modelo Hospedado 27
Figura 2.13 - Modelo Delegado 28
Figura 2.14 - Validação RPKI 29
Figura 4.1 - Adesão por Prefixo 36
Figura 4.2 - Adesão por IP 37
Figura 4.3 - Adesão por ASN 37
Figura 4.4 - Cobertura RPKI por Tipo de AS 38
Figura 4.5 - Cobertura RPKI por ASN Acadêmico 40
Figura 4.6 - Cobertura RPKI por Prefixo Acadêmico 40
Figura 4.7- Relação Cobertura RPKI vs Cursos NIC.br 41

LISTA DE TABELAS

Tabela 1 - Exemplo de ROA sem Max-Lenght 26
Tabela 2 - Exemplo de ROA com Max-Lenght 26
Tabela 3 - Exemplo de Análise 35

SUMÁRIO

AGRADECIMENTO **3**
LISTA DE ABREVIATURAS E SIGLAS **4**
LISTA DE FIGURAS **5**
LISTA DE TABELAS **6**
RESUMO **9**
ABSTRACT **10**
1 INTRODUÇÃO **8**
2 FUNDAMENTAÇÃO TEÓRICA **12**
2.1 Revisão Bibliográfica **12**
2.2 Recursos de Internet **12**
2.2.1 IANA e RIR 14
2.3 Border Gateway Protocol **15**
2.4 Ponto de Troca de Tráfego **15**
2.5 Prefix Hijacking - Sequestro de Prefixos **17**
2.6 Soluções para Sequestro de Prefixo **20**
2.6.1 Internet Routing Registry 21
2.6.2 Resource Public Key Infrastructure 24
3 ACOMPANHAMENTO DA IMPLANTAÇÃO DO RPKI NO BRASIL **31**
3.1 Metodologia **31**
3.2 Coleta e Análise Dos Dados **32**
3.3 Dados de RPKI **32**
3.4 Dados do BGP **33**
3.5 Dados dos RIRs **33**
3.6 Dados dos IRRs **34**
3.7 Padronização dos Dados **34**
3.8 Análise dos Dados **35**
4 ANÁLISE DA IMPLANTAÇÃO DO RPKI NO BRASIL **36**
4.1 Crescimento da Adesão **36**
4.2 Adoção Por Segmento **38**
4.2.1 Por Tipo de ASN 38
4.2.2 Adoção do Setor Financeiro 39

4.2.3 Adoção pelas Redes de Educação e Pesquisa 39
4.3 Investigando o crescimento da adoção do RPKI no Brasil 41
5 CONCLUSÃO 43
REFERÊNCIAS 45

RESUMO

Sequestro de prefixos é um problema que enfrentamos atualmente na internet que pode levar a indisponibilidade de um ASN ou roubo de informações. Existem diversas ferramentas para se proteger desse tipo de ataque, sendo o RPKI o mais promissor, onde é criado certificados digitais para autorizar um ASN a anunciar determinado prefixo e o Brasil está adotando esta solução. Neste trabalho de conclusão analisamos o crescimento da implantação do RPKI neste primeiro ano de adoção no Brasil. Também correlacionamos informações que mostram que os treinamentos para utilização dessa ferramenta têm impulsionado significativamente para o crescimento da adoção do RPKI.

Palavras-chave: RPKI. BGP. Roteamento. Segurança de Rede. Sequestro de Prefixo.

ABSTRACT

Prefix hijacking is a problem we currently face on the internet that can lead to the DoS attack or steal information. There are several tools to protect against this type of attack, the RPKI being the most promising, where digital certificates are created to authorize an ASN to announce a certain prefix, and Brazil is adopting this solution. In this work we analyze the growth of the implementation of RPKI in this first year of adoption in Brazil. We also correlated information that shows that training to use this tool has significantly boosted the growth in the adoption of RPKI.

Keywords: RPKI. BGP. Routing. Network Security. Prefix Hijack.

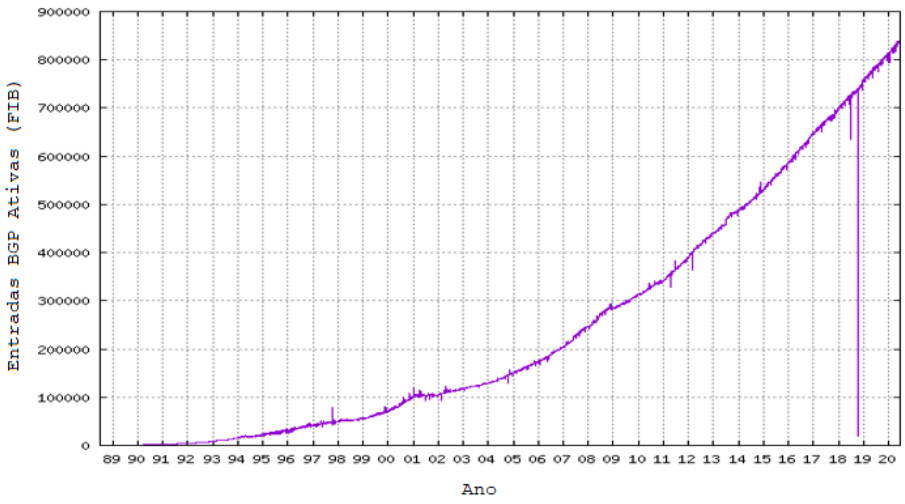
1 INTRODUÇÃO

Nos primórdios da Internet, onde o acesso à rede era limitado apenas às instituições de pesquisa, o roteamento era configurado estaticamente e de forma manual. Com o crescimento da Internet esse modo de operação ficou impraticável e foi necessária a adoção de protocolos de roteamento dinâmicos. Os protocolos dinâmicos permitem que as tabelas de roteamento sejam atualizadas de forma automática (Comer, 1998).

Dentre as classes de protocolos dinâmicos existem dois tipos, os protocolos intradomínio e interdomínio. Enquanto os protocolos intradomínio são utilizados para transportar informação dentro de cada instituição participante da Internet, os protocolos interdomínio são utilizados para que redes de diferentes domínios administrativos se conectem de forma independente à Internet.

Atualmente, o protocolo mais utilizado para comunicação entre diferentes domínios de roteamento é o BGP-4 (Y. Rekhter, 1995). Esse protocolo é responsável pela troca de informações de roteamento entre as diversas redes que compõe a Internet – ou seja, entre os diversos Sistemas Autônomos (*AS – Autonomous System*) que se conectam a Internet. Cada AS possui uma identificação (ASN – *Autonomous System Number*) e um espaço de endereçamento único (prefixo IP) que obedecem a uma mesma política de roteamento (RFC 1930). Conforme será visto na seção 2.2, as redes são endereçadas através de um conjunto de prefixos administrados sob uma mesma política de roteamento.

Figura 1.1 - Tamanho da Tabela BGP



(Fonte: https://www.cidr-report.org/as2.0/

Cada novo prefixo IP de cada participante gera uma entrada no que é conhecido como "Tabela de roteamento BGP". A Figura 1.1 apresenta um gráfico de crescimento da tabela

BGP ao longo do tempo. O eixo Y apresenta o número de entradas válidas da tabela BGP, enquanto o eixo X apresenta o decorrer do tempo durante os anos, de 1989 até o ano de 2020. Como pode ser observado, a tabela BGP apresenta um comportamento histórico de crescimento exponencial, o que influencia, entre outros fatores, no aumento na complexidade de administração do roteamento na Internet. O BGP-4 se tornou assim, um componente crítico na estrutura de roteamento da Internet.

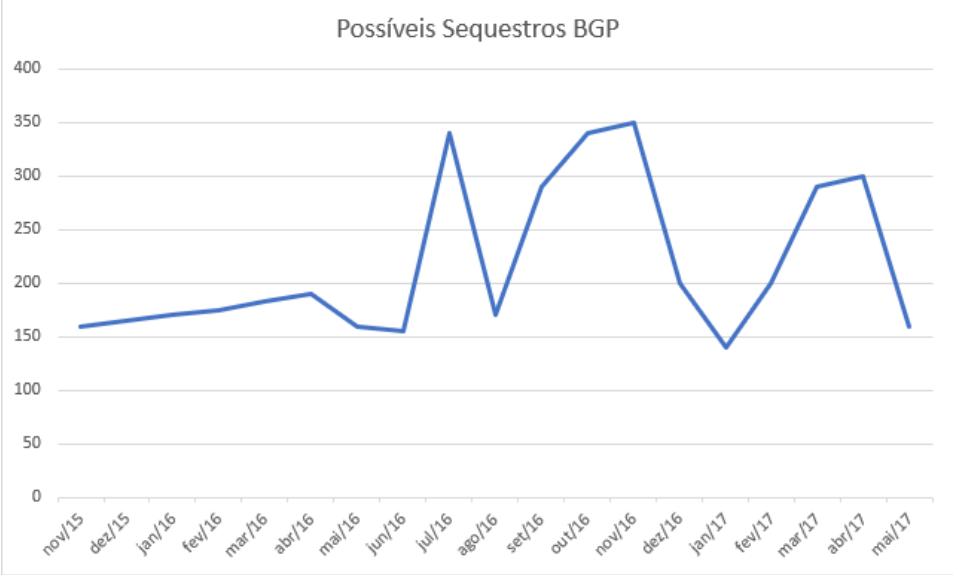
Junto com esse crescimento da tabela BGP, vieram os problemas envolvendo autenticidade e legitimidade dos anúncios BGP (S. Kent, 2000), (Bu, 2002). Como o protocolo BGP não possui mecanismos de autenticação forte para validar qual prefixo pertence a qual ASN, pode ocorrer um problema que é o sequestro de prefixos. No sequestro de prefixos um atacante anuncia o prefixo da vítima na tabela de roteamento global resultando no desvio de boa parte do tráfego da Internet para a rede do atacante. Esse tipo de vulnerabilidade pode ser resultante por diversos fatores, tais como: má configuração do equipamento, *bugs* nas aplicações, ou até mesmo ações maliciosas, onde o atacante pode, por exemplo, utilizar o desvio de fluxo para um possível roubo de informação ou como um ataque de negação de serviço conta a rede (ASN) da vítima (Hu & Mao, 2007).

Os problemas relacionados ao protocolo BGP já causaram interrupções em grande parte da Internet. Em 1997, tivemos o primeiro grande caso registrado. Nesse evento ocorreu o roubo de cerca de 23000 prefixos por parte do ASN 7007 (MAI Network Services em Virginia-USA), impactando na indisponibilidade do acesso à Internet de diversos outros provedores (Bono, 2007). O caso mais famoso de roubo de prefixos ocorreu em 2008 (NCC, 2008), onde a empresa de telecomunicação do Paquistão se apropriou de forma indevida de prefixos do Google. A falha foi causada por um erro de digitação de um administrador de rede e deixou indisponível o YouTube e outros serviços Google por duas horas, gerando grandes transtornos para os usuários e administradores de rede em toda a Internet.

Conforme apresentado na Figura 1.2, podemos verificar que entre novembro de 2015 e maio de 2017 a frequência desses sequestros aumentou consideravelmente, atraindo a atenção da comunidade ao problema. Como solução possível, o foco foi dado aos diferentes métodos de autenticação que se propõem a relacionar determinado AS com os blocos IPv4/IPv6 que são atribuídos a ele. Esses métodos tentam assegurar que os blocos IPv4/IPv6 roteados para um determinado destino sejam anunciados por quem possui o real direito de utilização daquele recurso. No intuito de solucionar esse problema, a comunidade científica propôs várias soluções, tais como RPKI (*Resource Public Key Infrastructure*) (M. Lepinski, 2012) e

BGPSec (*Border Gateway Protocol Security*) (Lepinski & Sriram, 2017). Alguns trabalhos também propõem realizar campanhas para a adoção de filtros de roteamento, considerando a informação já disponibilizada pelos RIRs (*Regional Internet Registers*) ou empresas privadas, utilizando serviços como Whois[1], RaDB[2] e PeeringDB[3] (Siganos & Faloutsos, 2004).

Figura 1.2 - Frequência Sequestro de Prefixo



(fonte: https://www.noction.com/blog/bgp-hijacking)

Algumas dessas soluções já eram adotadas pela comunidade, como RaDB e PeeringDB. Porém, a proposta de uso do IRR (*Internet Routing Registry*) não se demonstrou totalmente confiável, uma vez que as informações são manualmente informadas pelos próprios administradores de redes, e eventuais erros humanos remetem ao mesmo problema original: apropriação de recursos que não lhes pertencem (Siganos & Faloutsos, 2004). Outro problema que dificulta a adoção dessas bases privadas é o custo financeiro, que desincentiva várias redes menores (ASes) de utilizá-las. Em suma, até o presente momento, não existe uma solução definitiva para o problema de autenticação do conjunto AS/Prefixo. Soluções como BGPSec (Goldberg, 2014) são conhecidas por impactares nos recursos computacionais dos roteadores, sendo uma proposta operacionalmente difícil de adotar em uma Internet já funcional, podendo trazer vários efeitos negativo na sua adoção.

Entre as propostas existentes, o uso de certificação digital através do RPKI (*Resource Public Key Infrastructure*) aplicado ao protocolo BGP tem sido adotado. No BGP-RPKI ou,

[1] http://www.whois.net/
[2] https://www.radb.net/
[3] https://www.peeringdb.com/

simplesmente, RPKI, os detentores de recursos criam certificados contendo o ASN (*AS Number*) que tem autorização para o anúncio, o prefixo e o tamanho máximo da máscara de rede que serão divulgados na Internet. A confiabilidade da solução vem do fato de que os próprios *Routing Information Registry (RIR),* responsáveis por atribuir o número de AS e prefixo a uma instituição, fazem a gerência de quem pode criar os Registros de Autoridade do RPKI (*ROA-Route Origin Authorization*). Como os RIRs (Arin, Afrinic, Apnic, Lacnic, RipeNCC) são os responsáveis pela delegação dos recursos a comunidade, eles possuem a autoridade para dizer se um determinado registro de autoridade (ROA) pode ou não ser criado pelo solicitante.

Neste trabalho de conclusão de curso de graduação, é proposto o acompanhamento do primeiro ano de implantação da infraestrutura de RPKI na Internet brasileira. Através da análise dos resultados dos dados coletados, é identificado o progresso dessa implantação nos diferentes segmentos da Internet brasileira, como redes de ensino e pesquisa, setor financeiro, e operadoras de trânsito. Por fim é realizada uma análise de impacto da adoção dessa nova tecnologia em relação ao treinamento do usuário através dos cursos do NIC.br.

Este trabalho possui a seguinte organização: No capítulo 2 é estabelecida a fundamentação teórica. No capítulo 3, são discutidos os detalhes da implementação da análise e coleta dos dados para a realização deste trabalho. No capítulo 4 são apresentados os resultados obtidos por essa análise. Por fim, no capítulo 5 apresentamos as conclusões obtidas a partir de nossos resultados e as contribuições deste trabalho.

2 FUNDAMENTAÇÃO TEÓRICA

2.1 Revisão Bibliográfica

Em 2007, Zhang (Zhang, 2007) já estudava métodos de defesa contra roubo de prefixos e suas limitações de detecção criando prefixos na tabela BGP global pela análise das tabelas de rotas coletadas em diversos servidores espalhados pela Internet.

Lad (M. Lad, 2007) estudou a relação entre a topologia da rede e o impacto no sequestro de prefixos, mostrando que clientes que estão conectados a provedores Tier-1 são mais protegidos contra sequestro de prefixos quanto àqueles que são clientes de provedores de trânsito menores.

O RPKI foi definido na RFC 6480 e, desde então, estudos estão sendo feitos sobre sua implementação e impactos na infraestrutura da Internet. Wahlisch (Wählisch, 2012) estudou maneiras de detectar o sequestro de prefixo e identificar se foi a causa é um erro de configuração, ou um sequestro intencional. Gilad (Gilad, 2017) analisou a utilização do atributo *MaxLength* e seu impacto na segurança quando utilizado de forma muito permissivo a fim de facilitar as alterações de roteamento sem ser necessário recriar o ROA.

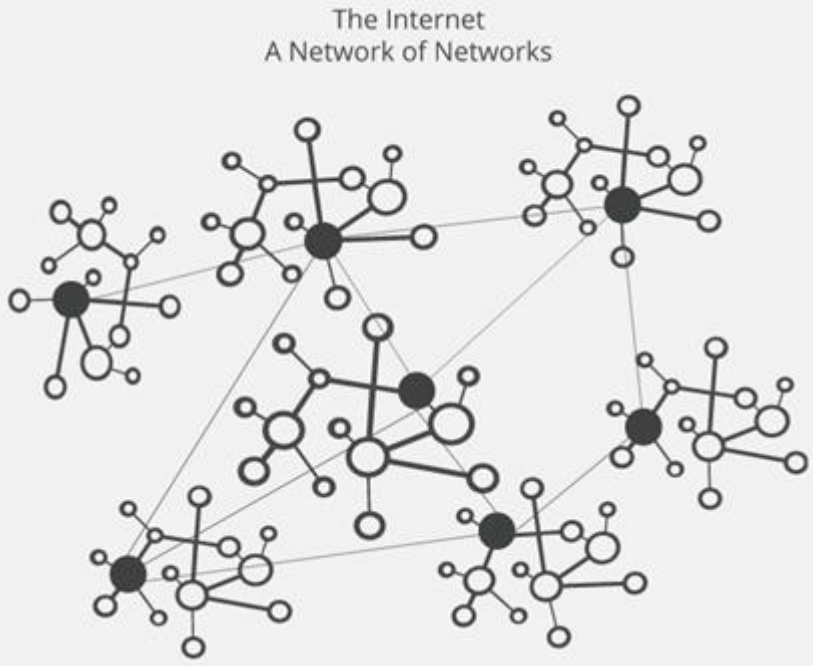
Trabalhos de medição da implementação do RPKI já foram feitos. Iamartino (Iamartino, 2015) fez uma análise dos ROAs criados nas bases de dados dos RIR e apresentou estatísticas de criação de ROAs, como a quantificação dos ROAs por RIR, quantidade de prefixos que estão cobertos pelo RPKI e o motivo da validação de um prefixo ser inválida.

Chung (Chung, 2019) fez um estudo mais completo da implementação do RPKI, analisando oito anos de dados. Esses dados incluíram todos os ROAs criados em todos os RIRs, contabilizaram o seu impacto na tabela BGP global e procuraram identificar casos de erros na configuração do RPKI por parte dos usuários.

2.2 Recursos de Internet

Conforme exemplificado na Figura 2.1, a Internet é composta por centenas de milhares de redes conhecidas como Sistemas Autônomos (AS). Um Sistema Autônomo é um conjunto de redes e endereços IPs sob uma mesma administração e política de roteamento. Cada AS possui um identificador de 16 ou 32 bits conhecido como ASN *(Autonomous Systems Number)* (Comer, 1998).

Figura 2.1 - Topologia da Internet



(Fonte: https://www.cloudflare.com/learning/security/glossary/what-is-bgp/)

Cada AS possui blocos de endereços IPs aos quais utilizarão para identificar os equipamentos de rede do AS. Esses endereços IPs são utilizados para rotear os diversos destinos da Internet. O IP é o principal protocolo da Internet; são identificadores de tamanho fixo (32 bits para IPv4 e 128 bits para IPv6) e são utilizados para localizar, através de uma identificação única, cada dispositivo conectado à Internet. Os endereços IPs são divididos em duas partes: alguns bits são utilizados para identificar a rede e o restante para identificar o *host*. Esses números de bits são variáveis, permitindo a criação de redes maiores ou menores. As máscaras de redes são utilizadas para verificar se um *host* está presente eu uma sub-rede local ou em uma rede remota (Comer, 1998).

O conjunto formado por um endereço de rede e uma máscara de rede determina um prefixo. Tais prefixos podem ser divididos em prefixos menores, também chamados de “prefixos mais específicos”. Os endereços IPs são divididos em blocos a fim de suprir as necessidades de rede dos ASes. Essa divisão é controlada por organizações que supervisionam e controlam a alocação de recursos da Internet como os endereços IPs e número de sistemas autônomos.

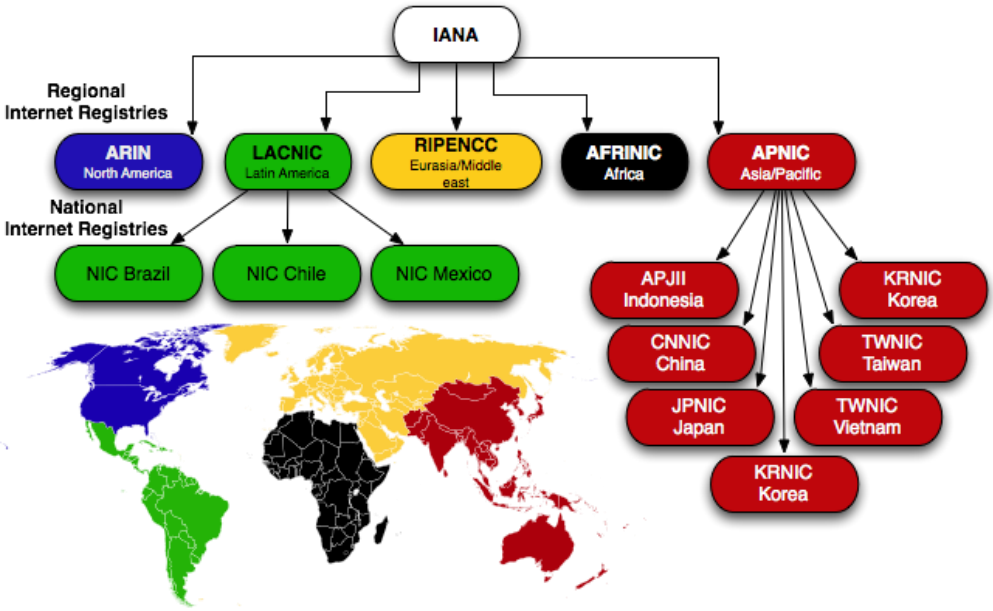
2.2.1 IANA e RIR

Os endereços IPs e ASN devem ser únicos na Internet e, para isso, existe uma organização mundial que controla a distribuição de diversos recursos da Internet, o IANA (*Internet Assigned Numbers Authority*) (IANA, 1988). Esses recursos são os endereços IPs (tanto IPv4 quanto IPv6), número de sistemas autônomos, domínios de Internet, entre outros identificadores utilizados na Internet (Carpenter, Baker, & Roberts, 2000).

O IANA delega os recursos de Internet para os RIR (*Regional Internet Registry*) e cada RIR distribui os recursos de números da Internet alocados a ele para operadores de rede em sua região, de acordo com a alocação e atribuição de políticas definidas por sua própria comunidade regional. Essas políticas regionais são desenvolvidas utilizando os processos de desenvolvimento de regras com base em consenso de indivíduo acessível e ascendente dos RIRs (ICANN, 2018).

Conforme mostra a Figura 2.2, o IANA distribui os recursos através de um sistema hierárquico onde existem atualmente 5 RIRs, um para cada região geográfica.

Figura 2.2 - Organização de Registro de Recursos



(fonte: caida.org)

Alguns RIRs delegam seus recursos a registros nacionais conhecidos como NIR (*National Internet Registry*). O NIC.br é um exemplo de NIR que atua no Brasil, sendo responsável pela alocação de recursos para todo os provedores de Internet, bancos, universidades e quaisquer instituições do território brasileiro que solicitem algum recurso da Internet (Nic.br, 2020).

2.3 Border Gateway Protocol

O protocolo BGP (*Border Gateway Protocol*) é a "cola" que mantem as diferentes partes da Internet unidas e permite a interconexão universal (Comer, 1998). O BGP é utilizado para interconectar diferentes ASes presentes na Internet, e para informar aos outros ASes vizinhos quais são os seus prefixos. O BGP está atualmente na versão 4.

A comunicação entre os ASes se dá pelo compartilhamento de informação de roteamento entre os roteadores que compõem a rede. Quando um novo roteador se conecta a rede, os roteadores conversam entre si e atualizam suas tabelas de rotas incluindo essa nova rota. O mesmo ocorre se um roteador sai da rede, ou se ocorre qualquer alteração na alcançabilidade de alguma das redes conectada a aquele roteador (Tanenbaum, 2003).

Existem dois tipos de roteamento BGP onde o comportamento e a forma de configuração dos roteadores são diferentes; os roteamentos intradomínio e interdomínio. Quando o roteamento se dá entre roteadores BGP do mesmo AS, diz-se que este é um roteamento intradomínio. Esse tipo de roteamento possui confiança implícita nas rotas que são trocadas entre os roteadores que compõe a rede pelo fato que são configurados pelo mesmo administrador de rede. Quando a comunicação se dá entre diferentes ASes, chama-se de roteamento interdomínio (Quoitin, 2003). Ambos os administradores dos ASes envolvidos trocam informação sobre quais prefixos irão anunciar e, assim, poderão fazer as configurações e filtros necessários. É aqui que começam os problemas de segurança no BGP conforme será visto na seção 2.5.

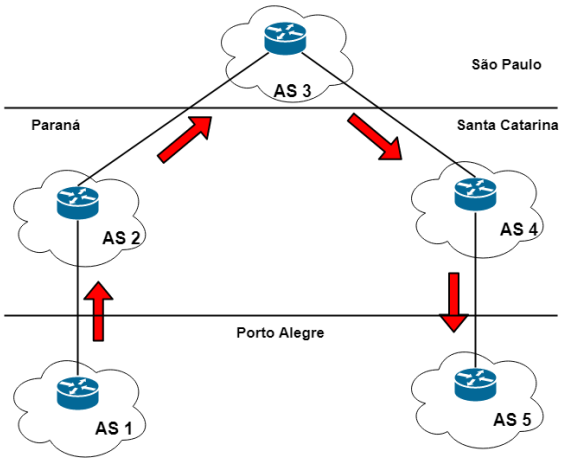
2.4 Ponto de Troca de Tráfego

Dependendo de como os ASes estão interconectados, pode acontecer de um pacote percorrer longos caminhos para chegar até o seu destino, podendo ocorrer que pacotes de ASes de uma mesma região geográfica ter que passar por outra região para chegar ao destino. Na Figura 2.3 podemos ver um exemplo disso. Para que o AS 1, localizado em Porto Alegre, chegue no AS 5, também localizado em Porto Alegre, necessita ir até São Paulo para poder se comunicar. Isso acontece devido os ASes terem diferentes saídas para a Internet e não possuírem uma ligação regional entre si.

Esse tipo de ocorrência causa aumento no número de saltos que os pacotes têm que fazer para chegar ao destino, incrementando, também, a latência e pontos de falhas, além de

tornar a engenharia de tráfego mais complicada, visto que os dados que saem de um AS possuem múltiplos caminhos até o seu destino causando uma descentralização da rede.

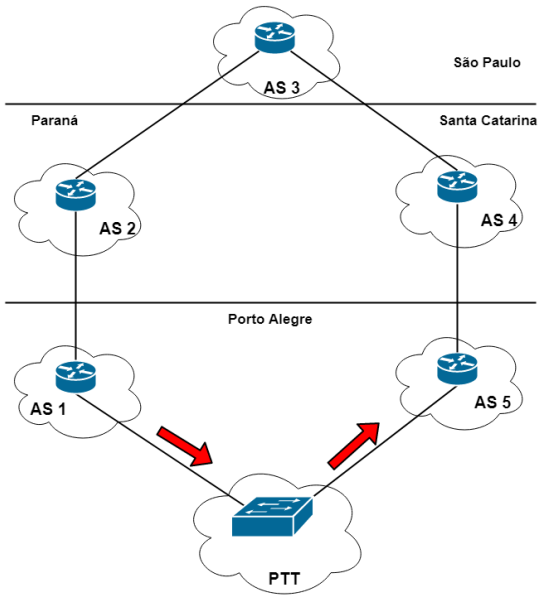
Figura 2.3 - Tráfego sem PTT



(Fonte: Próprio Autor)

Os PTTs (Pontos de Troca de Tráfego) ou IX (*Internet Exchange)* são responsáveis por encurtar esses caminhos, garantindo conexão segura, rápida e confiável para os ASes conectados a ele, além de possibilitar que o tráfego se mantenha local a uma região geográfica (Internet Society, 2020).

Figura 2.4 - Tráfego com PTT



(Fonte: Próprio Autor)

Na Figura 2.4, podemos observar o fluxo do mesmo tráfego do exemplo anterior, mas agora com a estrutura do PTT no meio. Como as rotas via PTT costumam ser melhores do que as rotas via trânsito, o fluxo do tráfego do AS1 para o AS5 irá ir diretamente para o AS5, visto que, do ponto de vista lógico, estão diretamente conectados.

2.5 Prefix Hijacking - Sequestro de Prefixos

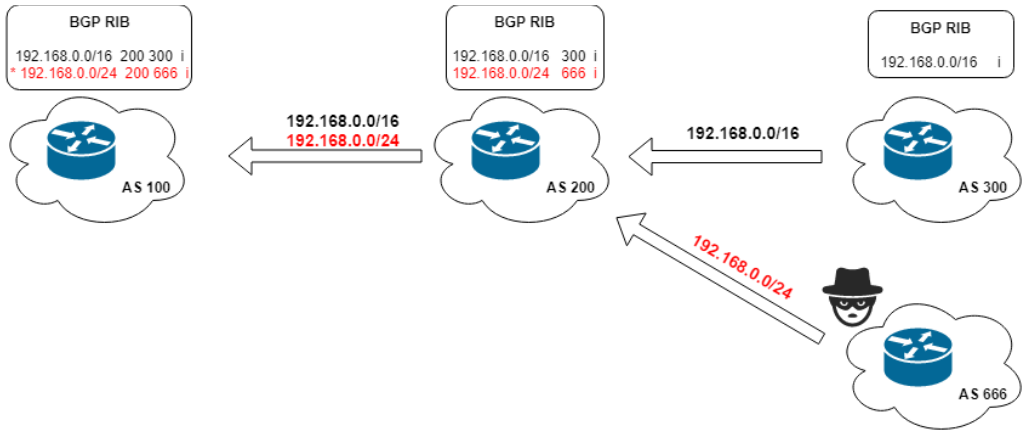
O BGP foi implementado sem nenhum tipo de mecanismo de segurança. Cada AS deve montar seus filtros de forma a remover rotas inválidas recebidas pelos seus *peers* (Butler, 2010). Um erro na configuração desses filtros pode "quebrar" a Internet, causando falhas no roteamento e, consequentemente, *blackholes*[4], caso um AS anuncie um prefixo que não lhe pertença e esse anúncio for propagado para outro AS.

Os roteadores BGP montam suas tabelas de rotas a partir das atualizações recebidas pelos seus vizinhos. Na primeira troca de informações de roteamento, os roteadores enviam toda sua tabela de rotas para seu vizinho e, posteriormente, as rotas são acrescentadas de maneira incremental, realizando troca de mensagens BGP somente quando há alguma rota nova ou uma atualização de uma rota já existente (Y. Rekhter, 1995).

A impossibilidade do BGP em validar a origem do prefixo causa diversos problemas, entre eles o ataque conhecido como sequestro de prefixos. Um caso comum de sequestro de prefixos é quando um atacante realiza o anúncio de um prefixo mais específico de uma rota e, com isso, desvia o tráfego para sua rede, ou, simplesmente, criar um buraco negro para aquela rota tornando-a indisponível (Cho, 2019). Ao receber uma atualização de rota para um prefixo mais específico, o roteador coloca essa rota como prioritária para esse destino, mesmo que o ASN de origem seja diferente do caminho menos específico.

[4] Técnica para descartar tráfego não desejado

Figura 2.5 - Utilização de rota mais específica



(Fonte: Próprio Autor)

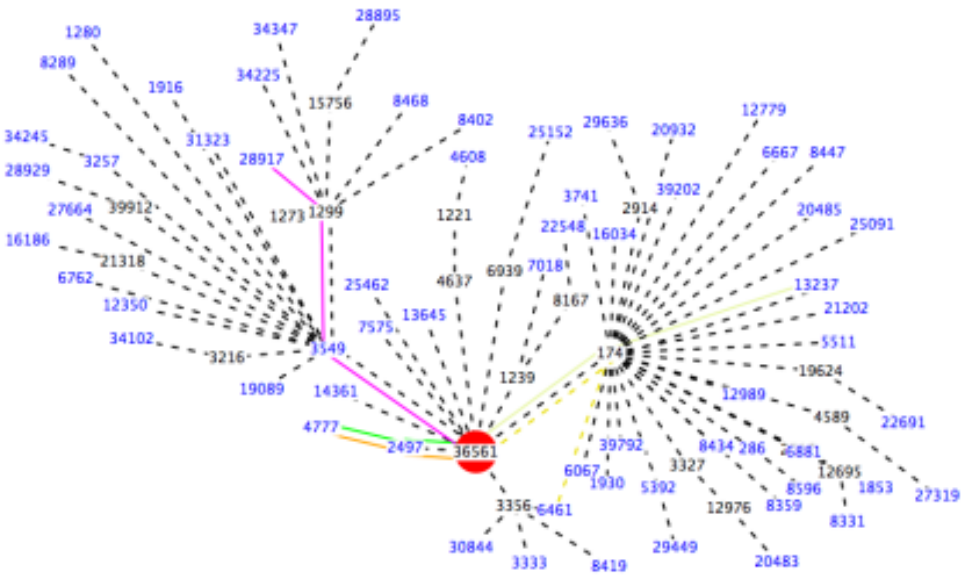
Como exemplo, temos a Figura 2.5, onde o ASN 100 recebe um anúncio da rede 192.168.0.0/16, pertencente ao ASN 300, através de sua conexão com o ASN 200. Porém, o ASN 666 está anunciando o bloco 192.168.0.0/24, uma fração do bloco do ASN 300, para o ASN 200. Visto que o BGP-4 não possui métodos de verificação de origem, o ASN 200 repassa esse anúncio inválido para o ASN 100 que, por sua vez, adiciona esse anúncio em sua tabela de rotas devido ao fato de ser mais específico, mesmo que o ASN esteja incorreto.

Isso faz com que parte do tráfego destinado do ASN 100 para o ASN 300 seja desviado para o ASN 666, fazendo com que os serviços do ASN 300 que se encontram na rede 192.168.0.0/24 se tornem indisponíveis ou, no pior dos casos, utilizados para roubo de informações.

Como mencionado anteriormente, o caso mais famoso de sequestro de prefixo foi em 2008, quando a Pakistan Telecom (ASN 17557) anunciou, sem autorização, o prefixo 208.65.153.0/24, e esse se propagou para o resto da Internet resultando no redirecionamento de todo o tráfego destinado ao YouTube para a rede da Pakistan Telecom.

Inicialmente, o YouTube anunciava o prefixo 208.65.152.0/22, responsável pela plataforma de *streaming*, e tudo fluía corretamente como podemos ver na Figura 2.6, que mostra o fluxo de tráfego das conexões do YouTube (AS36561) todas convergindo para ele.

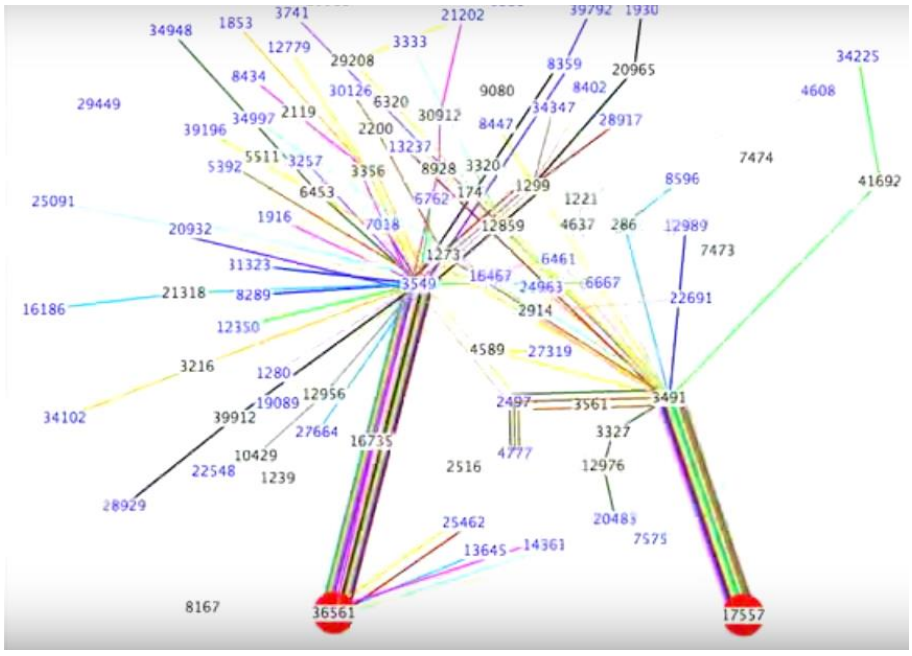
Figura 2.6 - Tráfego Normal para YouTube



(Fonte: https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study)

Porém, a Pakistan Telecom começou a anunciar o prefixo 208.65.153.0/24 e, sendo mais específico que o prefixo /22, os roteadores da Internet começaram a adicionar em suas tabelas de rota esse prefixo. Na Figura 2.7 podemos observar que o ASN 17557 da Pakistan Telecom começa a aparecer com o prefixo anunciado.

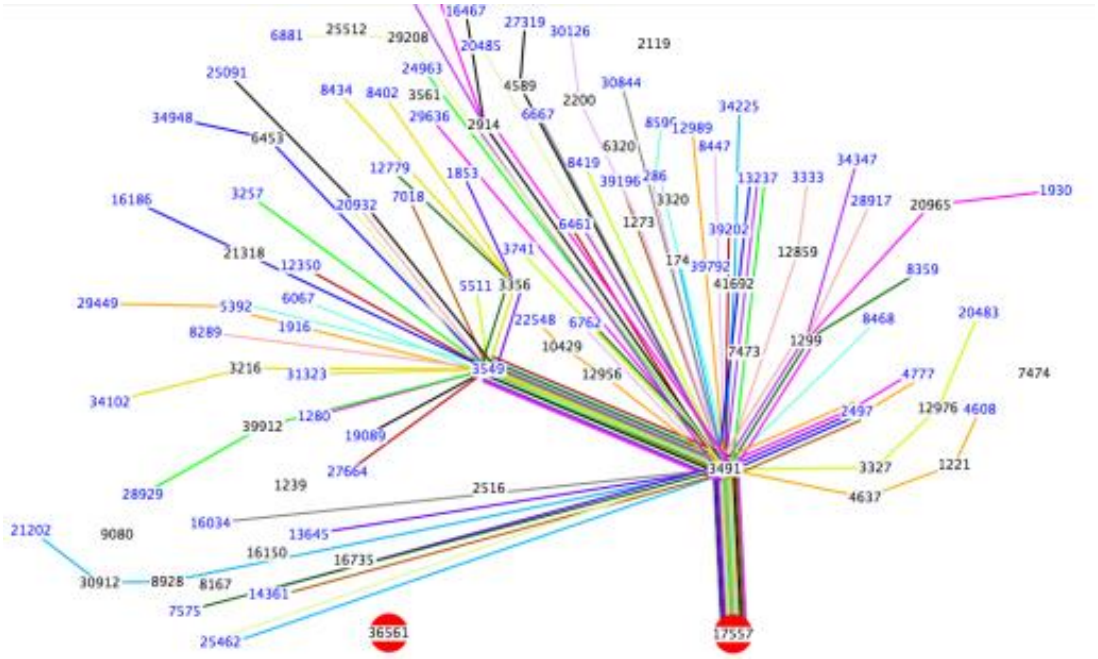
Figura 2.7 - Pakistan Telecom aparece da tabela de rotas



(Fonte: https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study)

Este anúncio mais específico faz com que os roteadores da Internet passem a utilizar a rota anunciada pela Pakistan Telecom como o principal caminho para o YouTube, ocasionando que o serviço de *streaming* fique indisponível. Na Figura 2.8 podemos verificar que o tráfego foi todo redirecionado para a Pakistan Telecom, causando a interrupção do serviço.

Figura 2.8 - Tráfego do Youtube Redirecionado



(Fonte: https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study)

Esse incidente ocorreu porque o provedor de trânsito IP da Pakistan Telecom não descartou este anúncio incorreto. Uma postura esperada de um provedor de trânsito era ter realizado uma verificação da origem dos anúncios recebidos de seus clientes e, assim, ter evitado a propagação desse prefixo para a Internet.

2.6 Soluções para Sequestro de Prefixo

Normalmente, proteções contra sequestro de prefixos são efetuadas nos roteadores por meio de filtros. Dependendo do tipo de conexão que se tem com o vizinho, o filtro pode ser realizado de forma estática. Nesse caso o vizinho informa qual prefixo irá anunciar e o administrador de rede do provedor, e esse implementa os filtros de forma a aceitar somente os prefixos mencionados.

Caso a conexão seja do tipo onde o vizinho envia toda sua tabela de roteamento, como as conexões de trânsito ou *peering*, torna-se inviável fazer esses filtros de forma estática. Além do mais, a criação excessiva de filtros acarreta na utilização de mais espaço em memória do roteador podendo resultar em perda de desempenho (Dharmapurikar, 2003).

A proteção contra o sequestro de prefixo parte do princípio do roteador aceitar somente anúncios onde o ASN de origem tem permissão para fazê-lo e anunciar somente os prefixos alocados para seu ASN. Soluções para este tipo de incidente são baseadas em formas de conhecer a origem do prefixo e onde obter estas informações. Atualmente, duas formas são mais utilizadas para esse tipo de proteção, que são o IRR e o RPKI (M. Ando, 2017), abordados nas próximas seções.

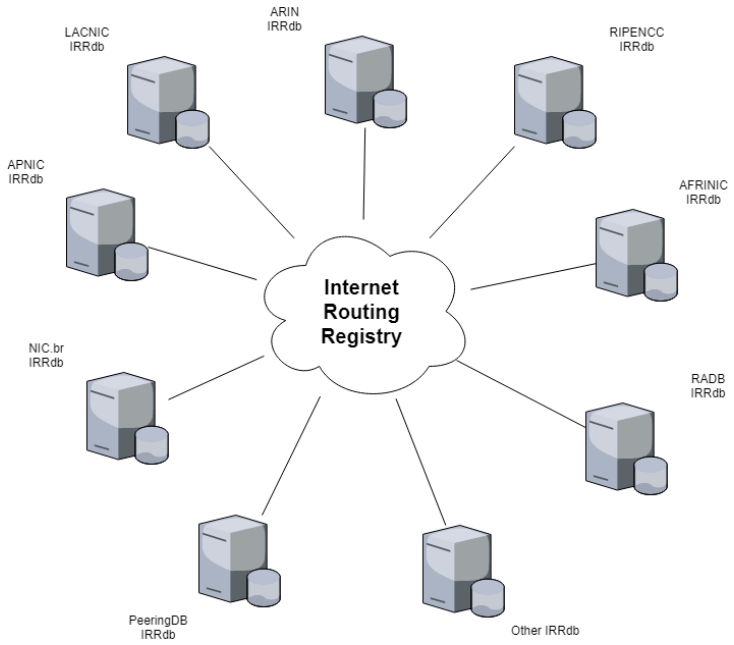
2.6.1 Internet Routing Registry

Como vimos, o BGP não possui mecanismo próprio de validação de origem, devendo aos administradores de redes criarem políticas de filtros para garantir a autenticidade dos dados. Para contornar isso, diversas propostas foram realizadas para minimizar esse problema. Uma dessas soluções foi a criação de uma base de dados para armazenar informações de roteamento chamado *Internet Routing Registry (IRR)* (Khan, 2010).

Estabelecido em 1995, a proposta do IRR é assegurar a estabilidade e consistência do roteamento da Internet disponibilizando informações para os operadores de rede. Essas informações são fornecidas pelos próprios administradores dos ASes (APNIC, 2020).

Na solução proposta pelo IRR, cada AS, ou entidade, pode manter sua própria base de dados IRR, cadastrando em seu banco de dados as informações de roteamento e políticas de seus clientes ou parceiros, e disponibilizando essa informação para terceiros.

Figura 2.9 - Estrutura IRR



(Fonte: Próprio Autor)

Atualmente, todos os RIR possuem suas próprias bases IRR onde disponibilizam informação de todos os recursos alocados a seus membros. Essas bases de dados sincronizam as informações entre si. Algumas bases privadas, como *RADb* e *PeeringDB*, sincronizam suas bases com as dos RIR, mas não espelham esse comportamento quando falam com outras bases privadas. Esse comportamento gera divergência de informações quando consultadas informações sobre um mesmo prefixo em diversas bases de registro de rotas. A Figura 2.9 demonstra como o IRR é formado, agregando informação de várias bases IRR existentes na Internet.

As consultas as bases IRR podem ser feitas através da ferramenta *whois*. A Figura 2.10 mostra o resultado de uma consulta para o prefixo 200.132.0.0/16.

Figura 2.10- Exemplo de Entrada IRR

```
route:      200.132.0.0/16
origin:     AS2716
descr:      Universidade Federal do Rio Grande do Sul
remarks:    Proxy-registered object for customer
remarks:    please direct inquiries to registro@rnp.br
mnt-by:     MAINT-AS1916
changed:    registro@rnp.br 20190930
source:     RADB
```

(Fonte: www.radb.net)

Desde 1999, o IRR se utiliza de uma linguagem padrão chamado *Routing Policy Specification Language (RPSL)* que define os padrões para os provedores de rede especificar suas políticas de roteamento em detalhes (Merit Network Inc., 2018). Essa linguagem define construtores chamados de objetos, que podem ser obrigatórios ou opcionais. Esses objetos podem passar tanto informação de política de roteamento quanto informações administrativas.

Os principais objetos do IRR são:

- Maintaner (`mntner`): Objeto que define que está autorizado a adicionar, remover ou alterar determinados objetos.
- Sistema Autônomo (`aut-num`): Define as informações de um sistema autônomo e suas políticas de roteamento
- Objeto de Rotas (`route/route6`): Objeto contendo informação de um prefixo associando-o a um ASN.

Entretanto, o BGP não possui um mecanismo para publicação ou consulta a essas bases de dados. Elas são utilizadas pelos operadores de rede apenas para confirmar a confiabilidade das informações de roteamento, planejar seu roteamento e implementar filtros. Esses filtros são comumente feitos de forma manual, podendo ser automatizados com utilização de *scripts*. Isso é normalmente realizado pelos administradores de rede, que pesquisam as informações nas bases IRR e criam os filtros com base na resposta.

Embora essas bases possuam um grande esforço da comunidade para mantê-las corretas, elas não são confiáveis devido a diversos problemas. Um deles é que as mantenedoras das bases não possuem autoridade para definir se a entrada cadastrada na base é válida ou não (apenas os RIRs têm esse poder de validação). Isso abre uma falha na segurança, permitindo a um usuário criar uma entrada para qualquer prefixo colocando seu ASN como detentor do prefixo (Kim, 2008). Essa situação nos remete novamente ao problema original: um AS tomando posse de recursos ao qual não possui autorização de uso. Outra falha é relativa à criação de cadastros falsos, onde um participante do IRR tem seus recursos atrelado a prefixo, ou AS, que não lhe pertence. Ambos os casos causam sérios problemas aos gerentes de redes que utilizam dos IRR para estabelecer seus filtros e programar a engenharia de seu tráfego.

Outro fato que impede o IRR de ser utilizado como fator de autenticação na sua implementação atual é o fato de inexistir um sincronismo confiável entre bases IRR, o que frequentemente causa divergência nas respostas obtidas. Normalmente, um administrador de

AS cadastra seus recursos em mais de uma base IRR para conseguir uma melhor visibilidade do seu prefixo. Entretanto, ao longo dos anos, eles somente mantêm atualizada uma delas, levando a uma divergência de informação entre as bases. Isso faz com que as consultas nas bases IRR retornem dados diferentes dependendo em qual base se faz a consulta. Essa situação pode levar a erros de roteamento, caso o administrador utilize uma informação incorreta ou desatualizada para gerar sua engenharia de tráfego.

2.6.2 Resource Public Key Infrastructure

RPKI é uma ferramenta de segurança de roteamento da Internet, definida na RFC 6480. Seu principal objetivo é validar a origem de uma rota vinculando uma faixa de endereços IPs a um ASN (M. Lepinski, 2012). Esse vínculo é utilizado por outros ASes para validar a rota de um determinado prefixo recebido pelos seus vizinhos BGP, a fim de garantir que serão instaladas apenas rotas válidas em sua tabela de roteamento.

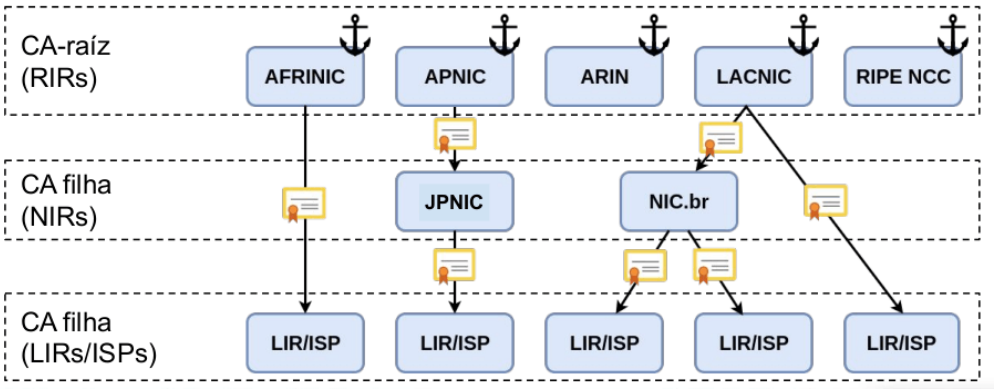
Esse vínculo é feito com uso de certificados digitais X.509 onde uma entidade cria um certificado de autorização de origem informando os recursos alocados a uma determinada organização.

2.6.2.1 Estrutura do RPKI

O RPKI faz utilização de chaves privadas para assinar os certificados criados. Para isso, é necessário estabelecer uma cadeia de confiança ao qual serão gerados os certificados e onde as autoridades certificadoras irão assinar os certificados dos filhos.

O RPKI utiliza a própria hierarquia de distribuição de recursos da Internet para construir sua estrutura de certificados digitais. Como os RIRs possuem a autoridade sobre a distribuição dos recursos, eles possuem sua confiabilidade implícita, formando o topo da cadeia hierárquica de certificação. Cada um dos cinco RIRs opera sua própria Autoridade Certificadora (CA), sendo sua chave privada utilizada para assinar os certificados gerados para as CAs filhas. Logo, os RIRs possuem um certificado auto assinado para todos os recursos alocados sob sua responsabilidade (Chung, 2019).

Figura 2.11 - Cadeia de Confiança do RPKI



(Fonte: NIC.br)

Como podemos observar na Figura 2.11, os RIRs emitem certificados para os recursos alocados a seus NIR/LIR e esses criam certificados para seus LIRs/ISPs, que são os ASes que compõem a Internet. Esses certificados contêm informação dos recursos que o detentor possui e tem autoridade para criar objetos PKI (Public Key Infrastructure). Esses objetos PKI utilizam da extensão descrita na RFC 3779 (C. Lynn, 2004) que permite informar prefixos IP e ASN como recursos do certificado. Com essa estrutura, o AS obtém um certificado digital assinado por sua CA onde é autorizado a criar entradas no banco de dados RPKI relacionando seus prefixos e o AS autorizado a anunciá-lo. Essas entradas são chamadas de ROAs (*Route Origin Authorization*), e são um atestado que um detentor de um conjunto de prefixos autoriza um AS a originar anúncios BGP para um determinado prefixo (M. Lepinski, 2012).

Conforme descrito na RFC 6482 (Lepinski, Kent, & Kong, 2012), as principais informações contidas em um ROA são o ASN, prefixo e tamanho máximo (*max-length*) que esse prefixo pode ser subdividido. O campo ASN informa o número do Sistema Autônomo que estará autorizado a originar os prefixos listados no ROA até seu tamanho máximo.

A criação do ROA está vinculada apenas ao prefixo listado no certificado e não ao ASN. Isso leva a possibilidade detentor de um prefixo há poder autorizar múltiplos ASes a originar o seu prefixo e não apenas seu próprio ASN (NLnet Labs, 2020).

O atributo *max-lenght* permite que o AS origine anúncios BGP mais específicos que o prefixo original contido no ROA até o tamanho máximo estipulado. Por exemplo, caso o ASN 2716 queira dividir seu prefixo 200.132.0.0/16 em prefixos /20, para permitir alguma engenharia de tráfego, não precisará criar 16 ROAs contendo cada subprefixo do /16, conforme o ROA da Tabela 1.

Tabela 1 - Exemplo de ROA sem Max-Lenght

ROA 200.132.0.0/16

Prefixo	ASN
200.132.0.0/20	2716
...	
200.132.240.0/20	2716

(Fonte: Próprio Autor)

Para evitar essa divisão desnecessária, podemos utilizar do recurso *max-lenght* para especificar o quanto o prefixo pode ser subdividido:

Tabela 2 - Exemplo de ROA com Max-Lenght

ROA 200.132.0.0/16

Prefixo	Max-Lenght	ASN
200.132.0.0/16	/20	2716

(Fonte: Próprio Autor)

Na Tabela 2, foi criado um ROA que autoriza o ASN 2716 a originar rotas para o prefixo 200.132.0.0/16 e para rotas dos subprefixos desse bloco com tamanhos entre /16 e /20, não permitindo, por exemplo, que o ASN 2716 origine anúncios para o prefixo /24.

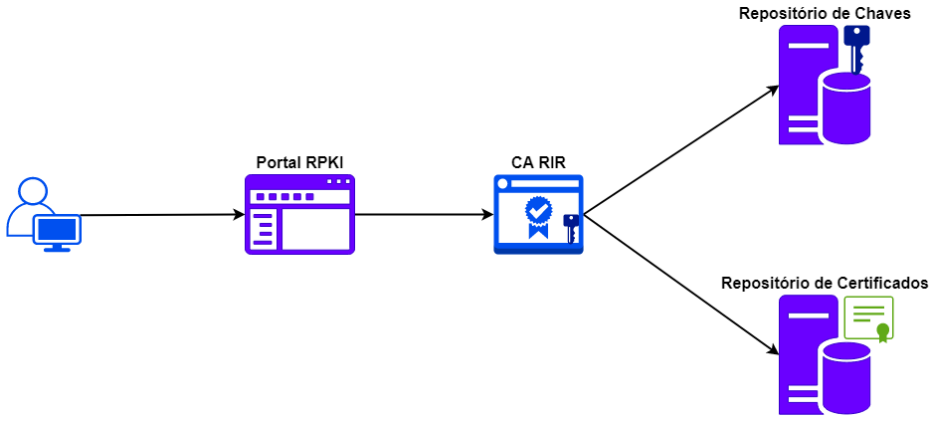
Para a criação dos ROAs existe dois modelos que os ASes podem adotar: o modelo hospedado e modelo delegado. Vistos a seguir.

2.6.2.2 O Modelo Hospedado

O modelo hospedado é o método mais simples de se criar os ROAs e gerir os certificados, pois toda a implementação dos softwares necessários para a criação é feita pelos RIR/NIR ao qual o AS é membro. Esse modelo foi adotado pelos RIR para diminuir as dificuldades da adoção do RPKI, não sendo necessária a criação de CAs dentro da infraestrutura do AS.

Conforme podemos ver na Figura 2.12, para criar o ROA, o AS entra no portal RPKI do RIR ao qual é membro, e faz as requisições de chaves e certificados de recurso que ficam armazenados de forma segura nos servidores do RIR. O AS não precisa se preocupar em gerir os certificados, tendo apenas a responsabilidade de criar e atualizar os ROAs (NLnet Labs, 2020).

Figura 2.12 - Modelo Hospedado



(Fonte: Próprio Autor)

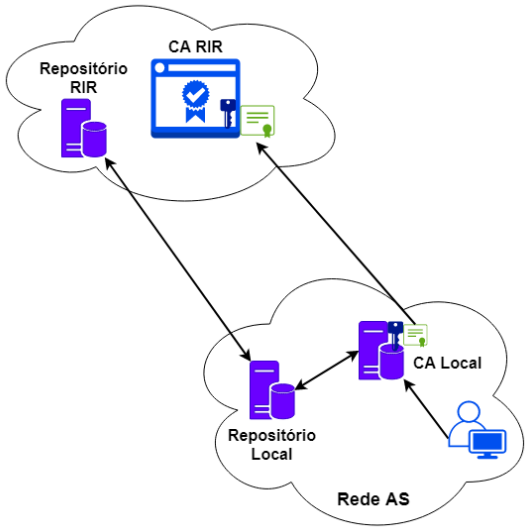
O modelo hospedado facilita a operação do RPKI para os pequenos provedores que fazem parte de apenas um RIR, e cujos anúncios de prefixos são realizados somente pelo seu próprio ASN. Para os grandes provedores, que possuem muitos ASNs em diferentes RIRs, esse modelo acrescenta uma complexidade desnecessária podendo induzir ao erro, visto que deverá entrar no portal de cada RIR para gerir e criar seus certificados.

O uso do modelo hospedado possui dois limitadores: Primeiro, caso o provedor delegue algum prefixo para um cliente, toda a alteração de ROAs que o cliente necessite terá de ser feito pelo dono do recurso, inviabilizando a operação direta pelo atual detentor do bloco. Esse fator é especialmente limitante em tempos de escassez de prefixos IPv4, onde operações como empréstimo e aluguel de IPv4 já são práticas de mercado. Segundo, caso o AS necessite criar, ou alterar, um ROA, e o portal do RIR estiver indisponível, poderá ocorrer do AS publicar o prefixo na tabela de roteamento e esse se tornar inválido devido a não alteração do ROA. Alterações no roteamento do AS ficariam dependentes do portal BGP-RPKI do RIR.

2.6.2.3 Modelo Delegado

Conforme dito anteriormente, o modelo hospedado dificulta a operação caso o provedor possua mais de um ASN em diferentes RIRs, visto que deve entrar no portal do RIR ao qual o prefixo pertence para a criação dos certificados. O modelo delegado resolve esse problema, pois toda a criação e manutenção dos certificados são feitas dentro da própria rede do AS e em um único local, independente do RIR ao qual o prefixo foi alocado.

Figura 2.13 - Modelo Delegado



(Fonte: Próprio autor)

A Figura 2.13 mostra o funcionamento do modelo delegado. O AS terá em sua infraestrutura um servidor que irá executar um software que vai cuidar da criação e manutenção dos certificados. Esses certificados são submetidos ao RIR ao qual faz parte que irá assinar esses certificados, validando que o AS tem a permissão de criar os certificados para seus respectivos recursos alocados pelo RIR. Com os certificados assinados, o AS pode criar os ROAs para seus prefixos e publicá-los em um repositório. Esse repositório é o local onde ficarão armazenados todos os recursos criados pelo AS, e pode estar dentro da própria estrutura do AS, ou utilizar repositórios de terceiro como, por exemplo, dos próprios RIRs.

O modelo delegado requer que o provedor mantenha sua própria infraestrutura de certificados, gerenciando e armazenando dentro de sua estrutura e, caso opte por utilizar um repositório próprio, o AS deverá mantê-lo sempre disponível para que outros AS possam consultar seus certificados (NLnet Labs, 2020). Caso este servidor se torne indisponível, seus ROAs não serão vistos pelos outros ASes tornando seus prefixos desconhecidos nas bases RPKI.

Uma vez que o próprio provedor é uma CA, esse pode delegar recursos para seus clientes e assinar seus certificados. Nesse modelo não é necessária a intervenção do provedor para a criação ou alteração dos ROAs para os prefixos que foram alocados a seus clientes (Hoffmann, 2019). O provedor pode fornecer um portal para que seus clientes façam as

alterações dos ROAs (como no modelo hospedado) ou os clientes podem criar suas próprias CAs onde o provedor irá assinar os certificados criados.

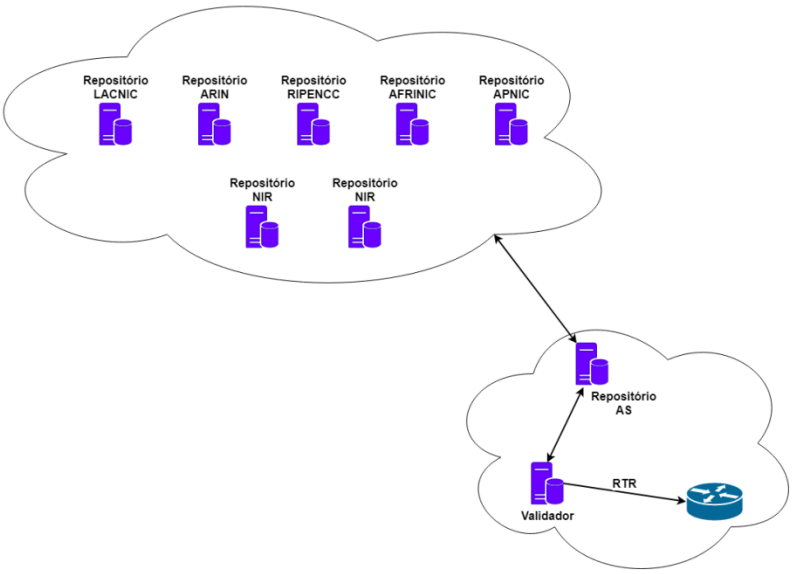
Esse foi o modelo ao qual o RPKI foi projetado para trabalhar, onde se tem as CAs raiz no topo da árvore hierárquica e as CAs filhas abaixo, criando e gerenciando os próprios certificados de recursos alocados a elas e assinado pelos CAs pais. Isso torna a estrutura mais segura, pois as chaves privadas serão armazenadas dentro das próprias CAs e não em estrutura de terceiros.

Embora seja uma forma de operação que necessite de um maior conhecimento dos operadores de redes, pois toda a instalação e gerência dos softwares são feitas por eles, esse modelo oferece uma maior segurança e flexibilidade na operação do RPKI, deixando toda a operação local ao AS, ou a seus clientes.

2.6.2.4 Validação dos Dados RPKI e Protocolo RTR

O processo de validação dos dados RPKI é o ponto fundamental da estrutura do BGP-RPKI. Para cada rota recebida, necessitamos comparar o prefixo e o ASN que está originando esse prefixo com os ROAs presentes na base de dados do RPKI.

Figura 2.14 - Validação RPKI



(Fonte: Próprio Autor)

A Figura 2.14 mostra o processo de validação das rotas utilizando o RPKI. Periodicamente, uma cópia de todos os ROAs é armazenada no repositório local do AS

utilizando o protocolo *rsync*[5]. Esses ROAs são sincronizados com as CAs confiáveis previamente configuradas. Após, um software validador utiliza esses dados do repositório local e faz a validação de todos os ROAs, verificando suas assinaturas e descartando os objetos assinados de forma incorreta. Com todos os dados corretos, o validador envia ao roteador RPKI, utilizando o protocolo RTR (R. Bush, 2013). Esses dados são armazenados na memória do roteador e, então, feito a comparação das informações presentes nos ROAs com a tabela de roteamento do roteador. Essa comparação pode retornar três resultados:

- **ROA Desconhecido**: Não foi encontrado um ROA para um determinado prefixo.
- **Válido**: Foi encontrado um ROA que bate com o ASN origem e o prefixo exato ou máximo estipulado.
- **Inválido**: Foi encontrado um ROA, porém possui divergências com o anúncio BGP encontrado na tabela de rotas:
    - ASN origem correto, porém prefixo máximo incorreto.
    - Prefixo máximo correto, porém, ASN de origem incorreto.

Com base nesses resultados, o operador de rede pode efetuar filtros para manipular esses anúncios BGP com base na validação RPKI.

[5] https://rsync.samba.org/

3 ACOMPANHAMENTO DA IMPLANTAÇÃO DO RPKI NO BRASIL

No Brasil, o BGP-RPKI começou a ser implementado de forma tardia em relação ao restante da Internet. Por se tratar de um NIR, a implementação do RPKI dependia da iniciativa do NIC.br que, apenas em dezembro de 2019, lançou a plataforma de cadastro. A adoção de RPKI por parte dos RIRs já tinha sido iniciada em 2012. Neste capítulo será explicado o processo de coleta de dados que foi utilizado para obter os dados necessários para o acompanhamento do processo de adoção do RPKI no Brasil.

3.1 Metodologia

Para acompanharmos a evolução da adoção do RPKI no Brasil foi necessário realizar a coleta de um conjunto de dados obtidos a partir de várias fontes de informação. Primeiramente, precisávamos observar a situação dos prefixos em um ambiente de produção, e para isso, decidimos por utilizar a tabela de roteamento do *Internet Exchange – IX* - de São Paulo, uma vez que é o maior IX do Brasil e que sua tabela de rotas possui informação sobre cerca de 82% dos ASes brasileiros (NIC.br, 2020), demonstrando-se um ótimo ponto de observação da Internet brasileira.

Em um segundo momento precisávamos validar os dados divulgados pelos ASes na Internet e compará-los com as diversas bases existentes. Para validarmos os prefixos anunciados no IX de São Paulo, utilizamos os dados publicados pelos diversos RIRs. Os dados foram obtidos diretamente dos sites do AFRINIC, ARIN, APNIC, LACNIC e RIPE.

Posteriormente, instalamos o software Routinator[6] para verificação dos prefixos e ASes com assinatura RPKI. Os dados de RPKI foram coletados diariamente, e um website foi criado para disponibilizar seus resultados de maneira gráfica. Esses dados nos permitiram acompanhar todos os ROAs criados na base de dados do RPKI possibilitando uma visão do crescimento da adesão ao RPKI por parte das entidades que compõem a internet.

Por fim, realizamos a análise destes dados cruzando informações como a classificação de ASes (CAIDA) em provedores de acesso/trânsito, empresas e provedores de conteúdo. Além de várias outras análises descritas em nossos resultados.

[6] https://github.com/NLnetLabs/routinator

3.2 Coleta e Análise Dos Dados

Para este trabalho de conclusão, nós começamos a monitorar a criações dos ROAs desde o início da implementação em novembro de 2019. Inicialmente foi coletada a tabela de roteamento do IX de São Paulo. O início da coleta dos dados se deu desde o dia 11/11/2019 com alguns saltos de dias e, após o dia 18/02/2020, foram feitas coletas diárias da tabela de roteamento.

A coleta de dados compreende dados de RPKI, dados das tabelas de rotas BGP do IX.br, dados de alocação de ASN e prefixo dos RIRs e NIC.br e dados do IRR.

Após a obtenção desses dados, um *parser* na tabela de roteamento foi executado para obter uma tabela contendo o prefixo e o ASN que originou o anúncio no IX de São Paulo. Com essa nova tabela, para cada tupla prefixo-ASN foi verificada sua situação nas bases de registro de todos os IRR, verificando se o prefixo foi designado para o ASN que está originando. Também foi verificado a status RPKI dos prefixos. Ao final, foi criada uma tabela contendo todas essas informações para iniciar a análise. Essa tabela foi disponibilizada em um *site*[7] para que os administradores de ASes do Brasil possam verificar a situação dos seus prefixos no IX de São Paulo.

3.3 Dados de RPKI

Todos os RIRs mantêm repositórios para que seus clientes possam fazer a sincronização dos ROAs para utilização nas validações de rotas. Os dados para uso neste projeto foram retirados do repositório do RIR europeu RIPE NCC, ao qual possui arquivos contendo os ROAs de todos os RIR desde o início da implementação em 2011.

Decidimos não utilizar os arquivos dos ROAs disponíveis pelo NIC.br devido a falta de padronização de seus arquivos disponibilizados. Contudo, o RIPE NCC mantém os arquivos de todos os ROAS de forma padrão desde os primeiros registros:

```
<URI, ASN,IP Prefix, Max Length, Not Before, Not After>
```

- `URI`: Repositório onde foi coletada a informação
- `ASN`: ASN de Origem
- `IP Prefix`: Prefixo a ser originado

[7] https://rpkibrasil.ufrgs.br

- `Max Length`: Máxima máscara de rede permitida
- `Not Before`: Inicio da validade do ROA
- `Not After`: Fim da validade do ROA

3.4 Dados do BGP

Para verificarmos a utilização do RPKI do IX de São Paulo, necessitávamos de sua tabela de roteamento. Para isso, utilizamos a tabela publica do IX de São Paulo disponível através do serviço de L*ookingGlass*[8] . Diariamente um *script* conecta nesse servidor do IX e armazena a tabela de roteamento completa.

O início da coleta se deu no dia anterior ao anúncio do Registro.br começar a implementar o RPKI no Brasil. Devido a problemas no script, houve falhas na coleta dos anúncios, sendo normalizado no dia 17/02/2020.

Após a coleta, foi realizada uma filtragem nos dados coletados para pegar apenas os prefixos anunciados e o ASN originador.

3.5 Dados dos RIRs

Semelhante ao RPKI, os RIR guardam em seus repositórios arquivos contendo todos seus prefixos e suas atribuições, garantindo que possamos identificar os detentores dos recursos. Infelizmente, essas informações não possuem uma tupla do tipo `<Prefix, ASN>` para podermos fazer a relação correta. Ao contrário disso, possuímos as relações `<opaque-id, prefixo>` e `<opaque-id, ASN>`.

Opaque-id é o identificador de um detentor de recursos, podendo esse ter mais de um ASN ou prefixo associado. Isso faz com que possamos ter falsos positivos, pois nesta base de dados temos apenas a relação de que determinados prefixos podem ser anunciados por determinados ASNs, não sendo possível saber se um ASN específico pode realmente anunciar o prefixo, mesmo estando correto na base do RIR. Podemos mostrar como exemplo a entrada a seguir, do repositório do Lacnic:

```
lacnic|BR|ipv4|143.54.0.0|65536|19900828|assigned|112244
lacnic|BR|ipv4|200.132.0.0|65536|20000215|assigned|112244
lacnic|BR|asn|2716|1|20081128|allocated|112244
lacnic|BR|asn|19200|1|20090601|allocated|112244
```

[8] Ferramenta instalada em um servidor que permite acesso remoto para visualizar informações de roteamento.

O `opaque-id 112244` possui (além de outros) os prefixos 143.54.0.0/16 e 200.132.0.0/16 relacionado a ele, bem como os ASN 2716 e 19200, porém, são ASes antigos criados com o mesmo CNPJ (Cadastro Nacional da Pessoa Jurídica), mas sendo instituições diferentes. Sendo assim, o ASN 2716 poderia anunciar ambos prefixos, porém o prefixo 143.54.0.0/16 pertence ao ASN 19200, construindo um erro de roteamento e roubo de prefixo, embora pela base de dados do RIR esteja correto.

Mesmo que essas bases dos RIR sejam as fontes confiáveis para obter a validação de origem, não podemos utilizá-las devido a falta de relação ASN/Prefixo, uma vez que teríamos a ocorrências de muitos falsos-positivos.

3.6 Dados dos IRRs

Diferentemente do RPKI e dos RIR, as bases IRR não possuem um repositório ao qual podemos acessar para consultas, sendo necessária utilização de APIs ao qual conectamos em um servidor IRR para efetuar consultas.

Essa foi uma dificuldade encontrada na execução do trabalho, devido ao tempo de resposta dos servidores, pois teve de ser feito consultas individuais para cada entrada da tabela de roteamento, demorando cerca de 12 horas para finalizar os 400 mil prefixos da tabela de roteamento do IX de São Paulo. Por este motivo, e por não ser uma base confiável, não efetuamos a comparação dos prefixos com o IRR.

3.7 Padronização dos Dados

Todos os dados utilizados para este trabalho contêm informações que nem sempre são necessárias para a análise e, devido a isso, necessitou-se filtrar os dados obtidos das diversas bases de dados com o intuito de coletar apenas as informações necessárias para a execução das análises:

- BGP Data: Da tabela de roteamento do IX de São Paulo, retiramos apenas o prefixo anunciado e ASN de origem.
- RIR Data: Retirou-se os prefixos, o ASN e o *opaque-id* (para podermos fazer a relação prefixo/ASN

- RPKI Data: Dos dados obtidos dos RIRs, retiramos Prefixo, *Max Length* e RIR de onde foi retirada a informação.

Com os dados normalizados, armazenamos as informações em arquivos, separados pela origem do dado e pela data de quando, a informação foi obtida.

3.8 Análise dos Dados

Após a padronização de todos os dados coletados, comparamos todos os prefixos retirados da tabela BGP do IX de São Paulo. Verificamos, em cada base de dados (RIR, RPKI e Registro.br) correspondente, no dia em que a tabela foi coletada, a validade do anúncio e armazenamos em uma tabela o resultado obtido.

cidr	asn	rir_asn	nicbr_asn	rir_pfx	nicbr_pfx	rir	rir_cc	rir_status	nicbr_status	rpki_status
186.211.197.0/24	20940	[14840 26622]	14840	186.211.128.0/17	186.211.128.0/17	lacnic	BR	Invalid	Invalid	Valid

Tabela 3 - Exemplo de Análise

Na Tabela 3 podemos observar um exemplo dessa análise para um prefixo anunciado na tabela BGP do IX de São Paulo. O prefixo 186.211.197.0/24 é anunciado no IX de São Paulo pelo ASN 20940. Pela base de dados do RIR, esse prefixo faz parte do bloco 186.211.128.0/17 (coluna rir_pfx) e temos os ASNs 14840 e 26622 vinculados no mesmo *opaque-id* que desse prefixo (coluna rir_asn). Isso significa, por essa base de dados, que o prefixo pode ser anunciado por ambos ASNs, tornando inválido o anúncio feito pelo ASN 20940 no IX de São Paulo (resultado da coluna rir_status). Da mesma forma, pela base de dados do Registro.br (coluna nicbr_pfx e nicbr_asn) o ASN que pode anunciar esse prefixo é o ASN 14840, tornando inválido o anúncio no IX de São Paulo, se analisar a base de dados do Registro.br (coluna nicbr_status).

De forma contrária, no RPKI, o detentor do recurso pode criar ROAs liberando outro ASN a anunciar seus prefixos ou subprefixo. Nesse caso, o ASN 14840 criou um ROA permitindo que o ASN 20940 anuncie o subprefixo 186.211.197.0/24 e, nesse caso, temos um anúncio válido como mostra a coluna *rpki_status*.

Essa análise foi feita para todos os prefixos anunciados na tabela do IX de São Paulo e armazenada em arquivos diários com o intuito de analisarmos o crescimento da utilização em um ambiente de produção. Para o crescimento da adoção no Brasil, foi comparada toda a base de dados do Registro.br buscando quais prefixos possui pelo menos um ROA criado para o prefixo ou para um de seus subprefixo.

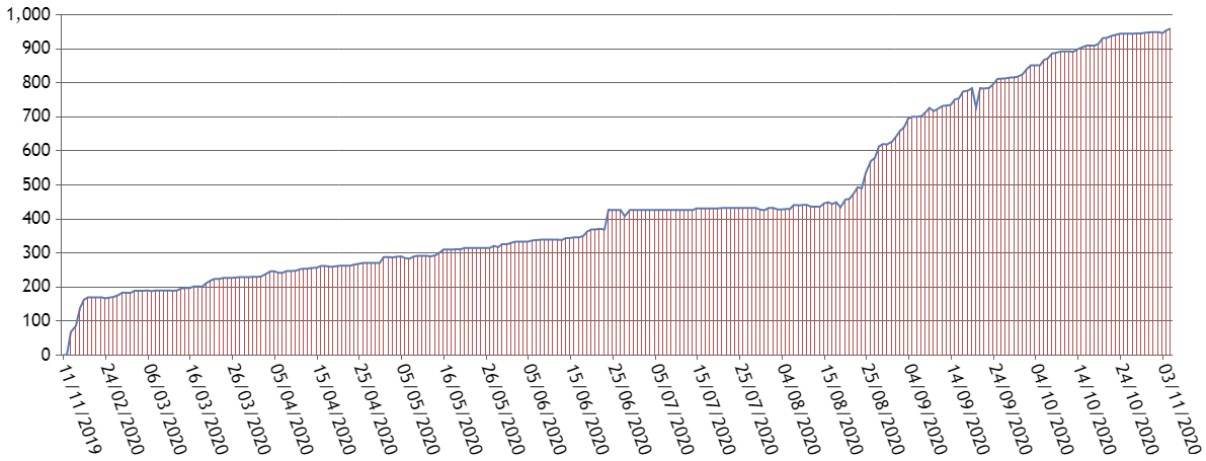
4 ANÁLISE DA IMPLANTAÇÃO DO RPKI NO BRASIL

Neste capítulo apresentamos os resultados obtidos após um ano de observação dos ROAS criados na base de dados do RPKI.

4.1 Crescimento da Adesão

No primeiro ano de implantação do RPKI, a criação de ROAs para os recursos IPs alocados no Brasil e a sua adoção pelas instituições que detêm esses recursos alocados pelo NIC.br ainda é pequena. Do total de prefixos IPv4 alocados ao Brasil, apenas pouco mais de 8% contêm pelo menos um ROA criado na base de dados do RPKI.

Figura 4.1 - Adesão por Prefixo

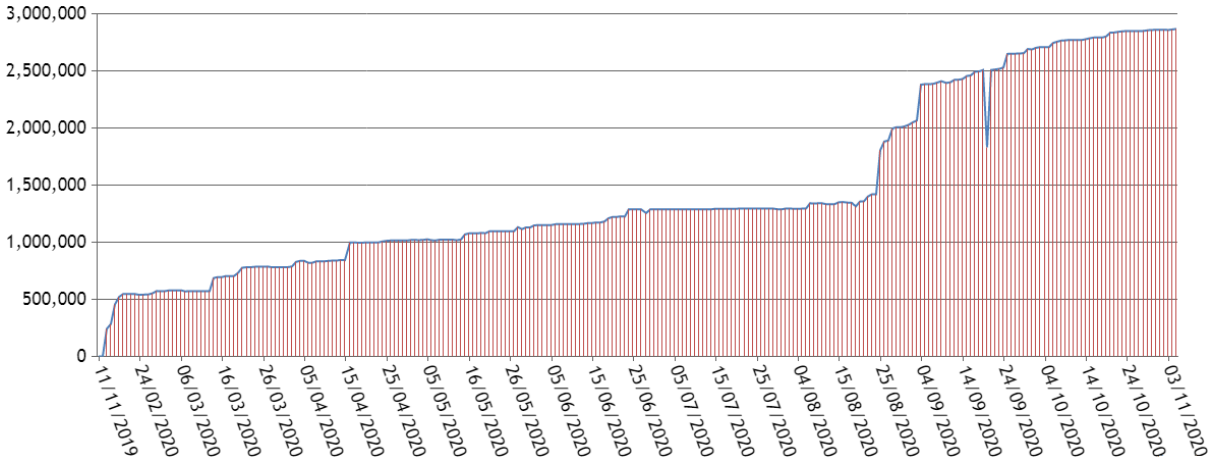


(Fonte: Próprio Autor)

A Figura 4.1, apresenta o crescimento dos prefixos brasileiros cobertos pelo RPKI ao longo do ano. O eixo Y apresenta o número de prefixos com pelo menos um ROA e o eixo X a data correspondente. Esse gráfico se aproxima do que temos na tabela de roteamento BGP, onde estão presentes os prefixos que são utilizados pelos roteadores da Internet para determinar as rotas usadas para a chegada dos pacotes aos destinos. No início de novembro de 2020, cerca de 8% dos prefixos brasileiros estavam cobertos pelo RPKI.

Porém, na teoria, cada *host* que se encontra na Internet possui um endereço IP distinto que o diferencia dos demais *hosts* da Internet. Se analisarmos a cobertura dos endereços IPs cobertos pelo RPKI, podemos concluir que a adoção está bem abaixo para os endereços IPs brasileiros.

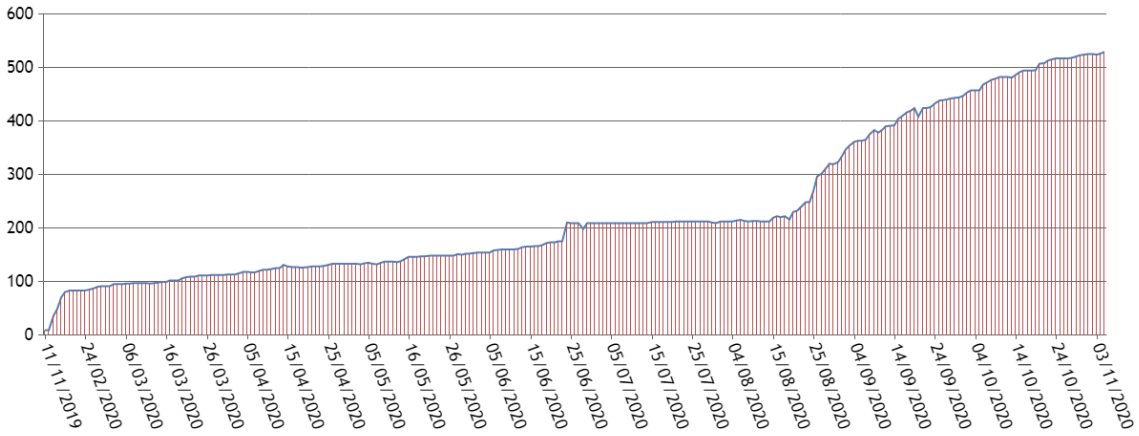
Figura 4.2 - Adesão por IP



(Próprio Autor)

A Figura 4.2 mostra exatamente essa informação: atualmente cerca de 2,8 milhões de IPs estão contidos em algum ROA. Esse valor representa apenas 3,3% dos IPs registrados no Brasil que estão cobertos pela segurança fornecida pelo RPKI, ou seja, cerca de 97% dos endereços IPs ainda não adotaram RPKI e estão suscetíveis a algum problema de segurança de roteamento como sequestro de prefixo.

Figura 4.3 - Adesão por ASN



(Fonte: Próprio Autor)

Conforme podemos observar na Figura 4.3, a quantidade de ASNs (eixo Y) que possuem pelo menos um ROA criado da base de dados ao longo do tempo (eixo X) é de 529 ASes. O que corresponde a uma cobertura do RPKI de aproximadamente 6,2% dos ASN do Brasil. Isso mostra pouca preocupação por parte dos administradores de rede na implementação de um mecanismo de proteção de seus recursos no escopo da Internet. Acreditamos que isso possa ser melhorado com o aumento da divulgação dessa ferramenta

pelos órgãos que controlam a Internet, com, por exemplo, ministrando cursos para capacitar os operadores e mostrar a importância dessa ferramenta. O benefício destes cursos é apresentado na seção 4.3.

Um detalhe interessante que podemos observar na Figura 4.3 é que antes do início da implementação do RPKI por parte do Registro.br, já possuíamos ASNs registrados no Brasil que continham pelo menos um ROA configurado. Isso se dá, possivelmente, porque o ASN possui algum *host* em outro país ao qual se utiliza endereçamento de algum ASN local ao qual configurou um ROA autorizando esse ASN brasileiro a originar rotas para um determinado prefixo.

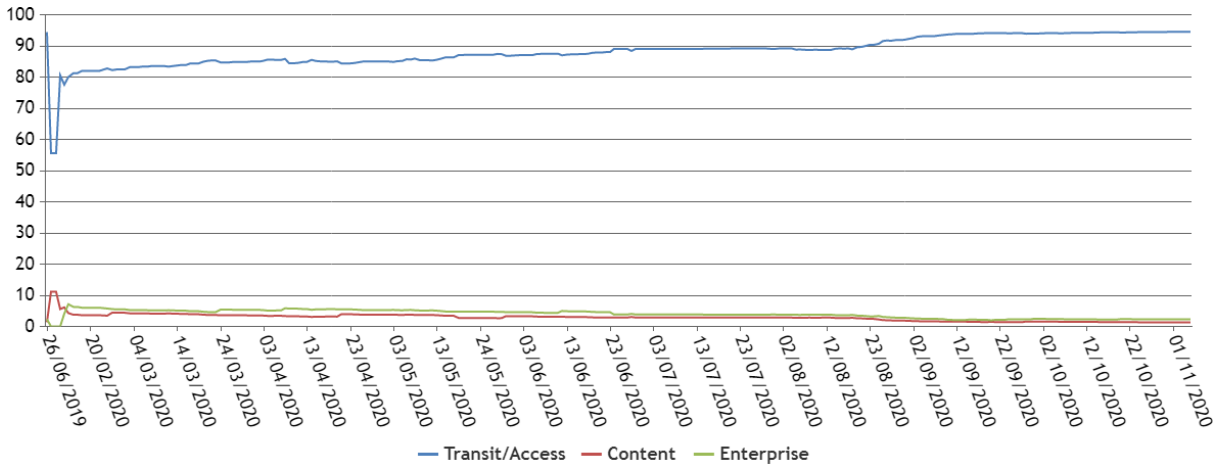
4.2 Adoção Por Segmento

4.2.1 Por Tipo de ASN

Neste estudo, fizemos a análise do crescimento pelo tipo de AS conforme segmentação feita pelo CAIDA (*Center for Applied Internet Data Analysis*) [9] onde dividem os ASes em três tipos:

- Trânsito/Acesso: Provedores que fornecem acesso à Internet para as entidades.
- Conteúdo: Provedores de conteúdo e hospedagem.
- Empresarial: Demais organizações folha da rede de Internet, tais como universidades e empresas que não provêm trânsito ou acesso.

Figura 4.4 - Cobertura RPKI por Tipo de AS



(Fonte: Próprio Autor)

[9] www.caida.org

Na Figura 4.4 podemos observar que, embora os provedores de conteúdo e empresas sejam os principais beneficiários da proteção imposta pelo RPKI, temos os fornecedores de trânsito como os principais responsáveis pelo crescimento da implementação do RPKI nos recursos de Internet do Brasil. O eixo Y mostra a porcentagem de ASN criados por categoria ao longo do tempo (eixo X), e pode-se constatar que as empresas de trânsito representam, atualmente, mais que 90% dos ASes que contém, pelo menos, um ROA associado ao seu ASN na base de dados do RPKI.

4.2.2 Adoção do Setor Financeiro

Os sistemas financeiros presentes na Internet, e que possuem AS, são um dos principais beneficiários da implementação do RPKI, pois são vítimas potenciais para ataques do tipo sequestro de prefixos onde o tráfego é desviado para servidores maliciosos com o intuito de obter dados financeiros das empresas e usuários.

Retiramos da lista da Federação Brasileira de Bancos (FEBRABAN) os bancos que possuem ASN para cruzamento de dados. Verificamos que neste primeiro ano de coletas de dados de roteamento e ROAs analisados, nenhum dos principais bancos do território brasileiro criou certificados para seus recursos, fazendo com que seus prefixos continuem suscetíveis a ataques de sequestro de prefixos.

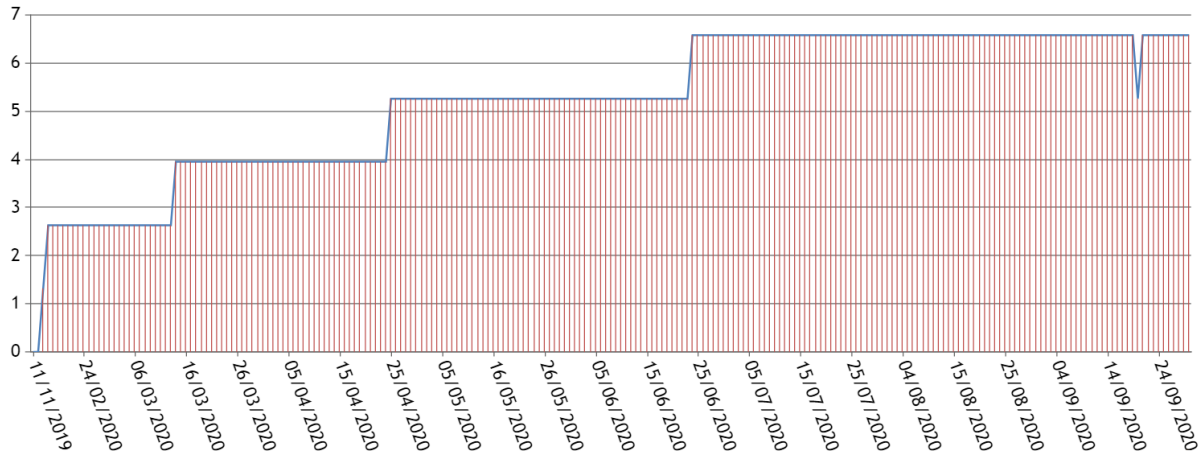
Entendendo-se benéfico ao sistema financeiro a implementação do RPKI, tentamos obter junto aos bancos as dificuldades da não implementação nesse primeiro ano de implantação. Primeiramente, tentamos contato via e-mail para os administradores desses ASes mas, infelizmente, não obtivemos resposta. Para tanto conseguimos o posicionamento informal de dois grandes bancos. Informaram que o processo de RPKI não havia sido incluído no mapa de mudanças para o ano de 2020, mas que a equipe já estava ciente da tecnologia e o pessoal capacitado para a sua adoção.

4.2.3 Adoção pelas Redes de Educação e Pesquisa

As instituições de educação e pesquisa são uma das principais fontes de estudo sobre as diversas ferramentas e protocolos existentes na Internet e, com isso, analisamos a adoção do RPKI por parte destas instituições e ensino. A lista destas instituições acadêmicas foi retirada dos clientes da Rede Nacional de Ensino e Pesquisa (RNP), um provedor de Internet

acadêmico responsável por fornecer Internet para as instituições de ensino e pesquisa em todo o Brasil.

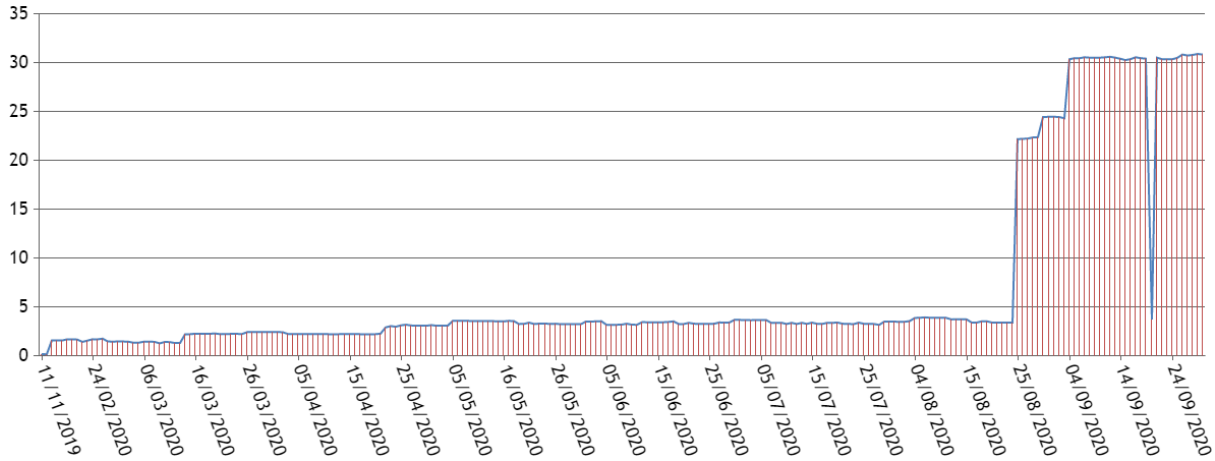
Figura 4.5 - Cobertura RPKI por ASN Acadêmico



(Fonte: Próprio Autor)

Na Figura 4.5 observa-se a porcentagem dos ASN acadêmicos que implementaram o RPKI em seus recursos. Nota-se que pouco mais que 6% dos AS criaram certificados para seus recursos, evidenciando pouco interesse da adoção do RPKI por parte da comunidade acadêmica. Isso, provavelmente, se deve ao fato da tecnologia ainda ser recente, não dando tempo para que essas instituições possam realizar os treinamentos necessários para implantação em seus ASes.

Figura 4.6 - Cobertura RPKI por Prefixo Acadêmico



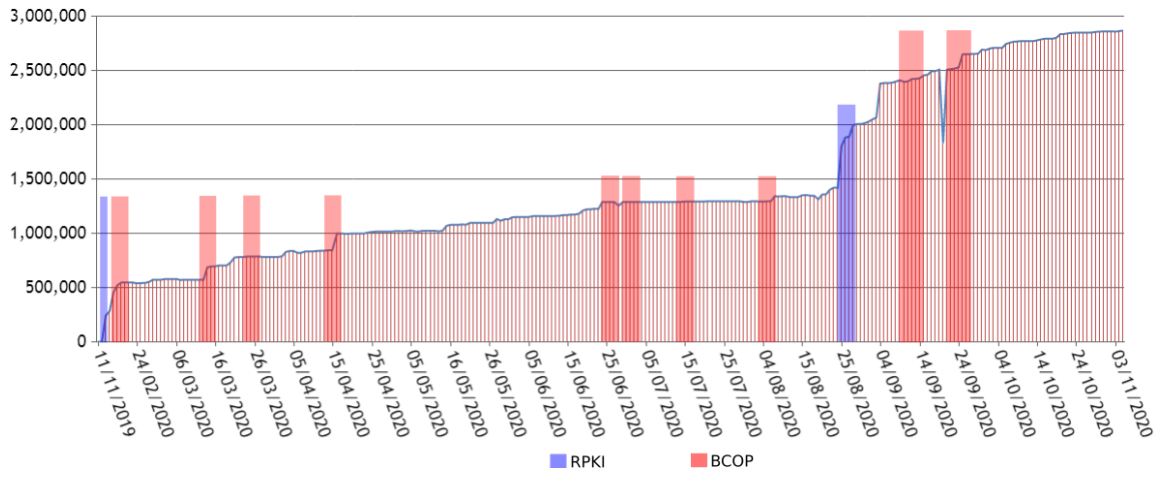
(Fonte Próprio Autor)

Embora a quantidade de ASes acadêmicos com pelo menos um ROA assinado para seu ASN esteja baixo, quando comparamos com o volume de prefixos acadêmicos assinados na estrutura do RPKI, notamos um aumento interessante. Na Figura 4.6, a partir do dia 25 de agosto registramos um crescimento de 5% para 30% dos prefixos acadêmicos assinados. Quando inspecionados em mais detalhes, notamos que todos os novos prefixos assinados eram de um único ASN. O AS1916 da Rede Nacional de Ensino e Pesquisa. Nesse caso registramos um impacto positivo no volume de prefixos assinados considerando a entrada do maior AS acadêmico do Brasil.

4.3 Investigando o crescimento da adoção do RPKI no Brasil

Um dos objetivos deste trabalho é analisar os motivos que levaram os administradores de rede a implementar o RPKI em seus recursos. Para isso, correlacionamos a agenda de cursos do NIC.br disponibilizado em seu site com o gráfico de crescimento da cobertura RPKI dos endereços IPs brasileiros.

Figura 4.7- Relação Cobertura RPKI vs Cursos NIC.br



(Fonte: Próprio Autor)

A Figura 4.7 nos mostra o gráfico do crescimento da cobertura RPKI dos endereços IPs brasileiros onde as barras perpendiculares ao eixo X representam os cursos ministrados pelo NIC.br, onde as barras azuis são cursos exclusivamente sobre RPKI e as barras vermelhas são cursos sobre boas práticas operacionais para sistemas autônomos – BCOP - que tem em seu conteúdo a utilização do RPKI pelos administradores de rede. Na Figura 4.7 podemos observar que, na maioria dos casos, logo após o NIC ministrar um curso, ocorre um

crescimento exponencial da cobertura dos endereços IPs brasileiros, evidenciando que os cursos ministrados pelo NIC estão gerando impactos positivos para o crescimento da cobertura RPKI.

O pico inicial aconteceu após o lançamento da plataforma do Registro.br para a possibilidade de criação de ROAs dos recursos de Internet brasileiro ao qual ocorreu na Semana da Infraestrutura de Internet no Brasil. Nesse evento, foi realizado um curso sobre o RPKI e como criar os certificados de recursos utilizando a plataforma do Registro.br. Esse evento iniciou a largada da criação dos ROAs dos prefixos brasileiros, incentivando os administradores de rede a protegerem seus recursos de Internet com a utilização do RPKI.

No decorrer do ano de 2020, o NIC proporcionou cursos sobre boas práticas operacionais para sistemas autônomos ao qual incluía em seu currículo o protocolo RPKI, incentivando os operadores de rede que participam do curso a implementar o RPKI nos recursos de seus AS. Como observado na Figura 4.7, esses cursos geram resultados positivos para o crescimento cobertura RPKI no Brasil, uma vez que sempre temos um crescimento exponencial no gráfico após a realização. Cursos específicos sobre RPKI corroboram significativamente para o crescimento, como podemos observar o crescimento do dia 25 de agosto, no qual foi dobrado o número de endereços IPs cobertos pelo RPKI. Identificamos que neste momento ocorreu a Semana da Capacitação oferecida pelo CEPTRO/Nic.br onde ocorreu um curso sobre segurança de roteamento utilizando o RPKI, motivando os administradores de redes a criar os certificados para seus recursos. Isto mostra que os administradores de rede saem convencidos da importância de protegerem seus recursos.

5 CONCLUSÃO

Neste trabalho, analisamos os diversos aspectos sobre a adoção do RPKI por parte das instituições brasileiras ligadas à Internet. Verificamos porque ferramentas já utilizadas pela comunidade, como o IRR, não são totalmente confiáveis para validação de prefixos, podendo conter informações incorretas ou desatualizadas. A utilização dessas bases se torna difícil visto a falta de padronização e a forma da disponibilidade das informações, inclusive por parte dos RIRs uma vez que, em suas próprias bases de dados encontramos falsos positivos.

O RPKI veio para suprir essas limitações das ferramentas existentes. É uma ferramenta necessária para garantir a segurança no roteamento dos pacotes pela Internet. Como ponto forte, suas informações são alimentadas apenas por pessoas autorizadas e validadas pela cadeia de certificados digitais onde as raízes são os próprios órgãos que disponibilizam os recursos para as entidades que compõe a Internet.

Após um ano de análise do crescimento da adesão do RPKI pelas entidades brasileiras, podemos notar que a sua adoção ainda é baixa, porém esses valores vêm crescendo à medida que a ferramenta e o conhecimento começam a ser difundidos e os administradores de redes começam a ter confiança para a sua implementação.

Observamos que os provedores de trânsito e de acesso a Internet estão mais avançados na adoção do RPKI, representando cerca de 95% dos registros (ROAs) criados. Complementarmente, notamos que empresas e provedores de conteúdo - as maiores vítimas de roubo de prefixos e, consequentemente, os mais beneficiados - ainda não adotaram a tecnologia no Brasil.

No mesmo âmbito das empresas que mais se beneficiam com o RPKI, estão as instituições financeiras, onde nenhuma ainda fez uso do RPKI. Embora não termos obtido êxito no contato com essas instituições, apenas contato informal com administradores de rede de dois grandes bancos, o motivo informado foi a não inclusão do projeto de RPKI no *roadmap* de 2020. Assim, acreditamos que este seja o motivo da não implementação por parte dos outros bancos.

Como ponto positivo neste estudo, tivemos uma boa adoção por parte da comunidade acadêmica, onde tivemos 31% dos prefixos acadêmicos cobertos pelo RPKI mostrando que esse grupo de ASNs está sempre a favor de novas tecnologias colaborando com a segurança da Internet.

Outro ponto importante do estudo foi a medida de impacto do treinamento sobre a adoção de novas tecnologias, onde verificamos que os cursos específicos de RPKI

ministrados pelo NIC.BR resultaram em um aumento significativo no crescimento da cobertura RPKI dos prefixos brasileiros. Notamos também que outros cursos, não exclusivos de RPKI, mostraram um impacto menor, mas mesmo assim influenciam positivamente a adoção da tecnologia, mostrando que na maioria dos casos, após ou durante os cursos verificamos um aumento nos prefixos cobertos por algum ROA na base de dados do RPKI.

Criar os ROAs para os prefixos é um passo muito importante para a segurança de nossa Internet, porém, como trabalhos futuros, há um ponto fundamental para o funcionamento dessa tecnologia: verificar se os administradores de rede estão utilizando a validação RPKI para manipular os prefixos BGP recebidos. Devemos analisar se os prefixos inválidos estão sendo descartados nas tabelas BGP dos roteadores, não permitindo a utilização de uma rota incorreta para um determinado destino.

As contribuições deste trabalho estão no âmbito de aprendizado desta ferramenta e da conscientização da importância da proteção da validação da origem dos prefixos com a utilização do RPKI. Também, através do portal criado (https://rpkibrasil.ufrgs.br), possibilitamos que os administradores de rede possam pesquisar a situação de seus prefixos na tabela de roteamento do IX de São Paulo e possam tomar as devidas decisões para melhorar a segurança de seus recursos.

REFERÊNCIAS

APNIC. (2020). *The Internet Routing Registry (IRR)*. Retrieved 04 29, 2020, from The Internet Routing Registry (IRR): https://www.apnic.net/manage-ip/apnic-services/routing-registry

Bono, V. J. (2007, Apr 26). *7007 Explanation and Apology on NANOG maillist*. Retrieved from https://archive.nanog.org/mailinglist/mailarchives/old_archive/1997-04/msg00444.html

Bu, T. a. (2002). On characterizing BGP routing table growth. *Global Telecommunications Conference, 2002. GLOBECOM'02. IEEE*, 2185--2189.

Butler, K. a. (2010). A Survey of BGP Security Issues and Solutions. pp. 100 - 122.

C. Lynn, S. K. (2004). RFC 3799 - X.509 Extensions for IP Addresses and AS Identifiers.

Carpenter, B., Baker, F., & Roberts, M. (06 de 2000). *RFC 2860 - Memorandum of Understanding Concerning the Technical.* Acesso em 10 de 11 de 2020, disponível em Memorandum of Understanding Concerning the Technical: https://tools.ietf.org/html/rfc2860

Cho, S. F. (2019). BGP hijacking classification. pp. 25-32.

Chung, T. a.-D. (2019). RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins. pp. 406--419.

Comer, D. E. (1998). *Interligação em rede com TCP/IP: princípios, potocolos e arquitetura.* Rio de Janeiro: Campus.

Dharmapurikar, S. a. (2003). Longest Prefix Matching Using Bloom Filters. *Proceedings of the 2003 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications*, pp. 201–212.

Gilad, Y. S. (2017). MaxLength considered harmful to the RPKI. *13th International Conference on Emerging Networking EXperiments and Technologies*, 101-107.

Goldberg, S. (2014). Why Is It Taking So Long to Secure Internet Routing? Routing Security Incidents Can Still Slip Past Deployed Security Defenses. *Association for Computing Machinery*, pp. 20-33.

Hoffmann, M. (2019). *RPKI Certificate Authority.* Acesso em 05 de 10 de 2020, disponível em NLNetLabs: https://www.nlnetlabs.nl/downloads/presentations/Running-Your-Own-CA-NANOG75.pdf

Hu, X., & Mao, Z. M. (2007). Accurate Real-time Identification of IP Prefix Hijacking. *IEEE Symposium on Security and Privacy*, pp. 3-17.

Iamartino, D. P. (2015). Measuring BGP route origin registration and validation. *16th International Conference on Passive and Active Measurement*, 28-40.

IANA. (1988). Fonte: Internet Assigned Numbers Authority: www.iana.org

ICANN. (2018). *As Funções do IANA.* Fonte: https://www.icann.org/pt/system/files/files/iana-functions-18dec15-pt.pdf

Internet Society. (2020). *Explainer: What is an Internet Exchange Point (IXP).* Acesso em 09 de 10 de 2020, disponível em Internet Society: https://www.internetsociety.org/resources/doc/2020/explainer-what-is-an-internet-exchange-point-ixp/

Khan, A. a. (2010). Public Internet Routing Registries (IRR) Evolution. pp. 55–59.

Kim, E.-y. a. (2008). Secure interdomain routing registry. pp. 304--316.

Lepinski, M., & Sriram, K. (09 de 2017). *RFC 8205 - BGPsec Protocol Specification.* Acesso em 14 de 10 de 2020, disponível em BGPsec Protocol Specification: https://tools.ietf.org/html/rfc8205

Lepinski, M., Kent, S., & Kong, D. (2012). RFC 6482 - A Profile for Route Origin Authorizations (ROAs).

Levy, M. J. (2018). *RPKI - The required cryptographic upgrade to BGP routing.* Acesso em 14 de 09 de 2020, disponível em Blog CloudFlare: https://blog.cloudflare.com/rpki/

M. Ando, M. O. (2017). Simulation Study of BGP Origin Validation Effect against Mis-Origination with Internet Topology. *2017 12th Asia Joint Conference on Information Security* , pp. 75-82.

M. Lad, R. O. (2007). Understanding Resiliency of Internet Topology Against Prefix Hijack Attacks. *37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN'07)*, 368-377.

M. Lepinski, S. K. (2012). RFC6480 - An Infrastructure to Support Secure Internet Routing. Fonte: RFC 6480: https://www.rfc-editor.org/rfc/rfc6480.txt

Merit Network Inc. (2018). *RPSL Reference Guide.* Acesso em 19 de 06 de 2020, disponível em Internet Routing Registry: http://www.irr.net/docs/rpsl.html

NCC, R. (2008). *YouTube Hijacking: A RIPE NCC RIS case study.*

Nic.br. (2020). *Atividades do NIC.br*. Fonte: https://nic.br/atividades/

NIC.br. (18 de 11 de 2020). *Live "Panorama, infraestrutura e uso dos PTTs nos últimos meses: desafios surgidos e superados".* Acesso em 08 de 12 de 2020, disponível em Intrarede NIC.br: https://intrarede.nic.br/files/apresentacao/arquivo/967/galvao-rezende-v2-n.pdf

NLnet Labs. (2020). *RPKI Technology.* Acesso em 08 de 07 de 2020, disponível em RPKI Documentation: https://rpki.readthedocs.io/en/latest/rpki/securing-bgp.html

Quoitin, B. (2003). Interdomain traffic engineering with BGP. *IEEE Communications Magazine*, pp. 122-128.

R. Bush, R. A. (2013). *RFC 6810 - The Resource Public Key Infrastructure (RPKI) to Router Protocol.* Fonte: https://tools.ietf.org/html/rfc6810

RFC 2622 - Routing Policy Specification Language (RPSL). (06 de 1999). Acesso em 19 de 06 de 2020, disponível em https://tools.ietf.org/html/rfc2622

S. Kent, C. L. (2000). Secure Border Gateway Protocol (S-BGP). *IEEE Journal on Selected Areas in Communications*, 582-592.

Siganos, G., & Faloutsos, M. (2004). Analyzing BGP policies: methodology and tool. *IEEE INFOCOM 2004*, pp. 1640-1651.

Tanenbaum, A. S. (2003). *Computer Networks.*

Wählisch, M. M. (2012). Towards detecting BGP route hijacking. *Sigcomm 2012*, 103–104.

Y. Rekhter, T. L. (1995). *RFC 1771 - A Border Gateway Protocol 4 (BGP4)*. Fonte: https://tools.ietf.org/html/rfc1771

Zhang, Z. a. (2007). Practical Defenses Against BGP Prefix Hijacking. *Proceedings of the 2007 ACM CoNEXT conference*, pp. 1--12.