WTR
WORKSHOP
DE TECNOLOGIAS DE REDES DO POP-BA

14 A 18 DE SETEMBRO DE 2020

Tendências na área de segurança de redes

Italo Valcy <idasilva@fiu.edu>

PoP-BA
Ponto de Presença da RNP na Bahia

RNP 30 anos
ORGANIZAÇÃO SOCIAL DO MCTI

Incidentes de roteamento

MANRS Home About Programmes MANRS Ambassadors Resources Observatory Blog JOIN

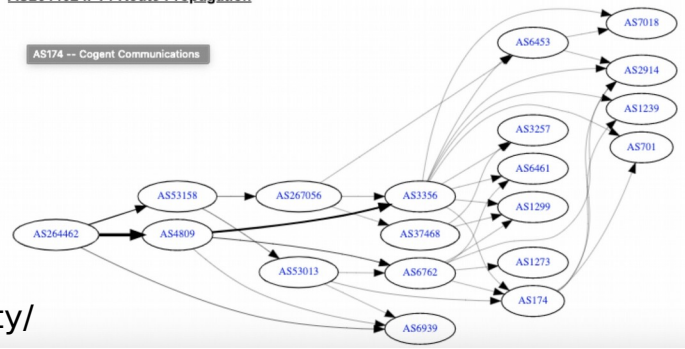
Big route leak shows need for routing security

July 22, 2020 by Aftab Siddiqui Leave a Comment

Yesterday saw another significant routing incident in the global BGP routing system, once again highlighting why it's important for network operators to be implementing good routing security practices.

The following pictures should give you an understanding of what we're going to be discussing:

AS264462 IPv4 Route Propagation



Search this website

Recent Posts

- What is BGP prefix hijacking? (Part 1)
- How to Secure Routing in the IXP Route Servers Infrastructure
- A Look at Route Origin Authorizations Deployment at DNS Registries
- Knowledge Sharing and Meaningful Conversation at InterCommunity 2020: Securing Global Routing
- Another BGP Incident Impacts TWC, Rogers, Charter and Others

https://www.manrs.org/2020/07/big-route-leak-shows-need-for-routing-security/

Incidentes de roteamento

- Excesso de confiança nos protocolos, em particular no BGP
- Má configuração
  - Não intencional
  - Bugs de software
- Maliciosa
  - Concorrência
  - Contestando espaço não utilizado
- Ataques dirigidos
  - Redirecionamento de tráfego
  - Espionagem ou modificação de tráfego

MANRS – boas maneiras na Internet!

- *Mutually Agreed Norms for Routing Security* (MANRS)
- Propõem um conjunto de boas práticas de segurança de roteamento
- Quatro princípios básicos e conhecidos de longa data:
  - Prefix filtering (prevenir propagação de informaçõe roteamento inválidas)
  - Anti-spoofing
  - Coordenação e comunicação
  - Validação global (IRR/RPKI)

Anti-spoofing

https://www.rnp.br/arquivos/

https://bcp.nic.br/antispoofin

Anti-spoofing

- Uso de filtros baseados em ACL
- Uso de RPF (Reverse Path Forwarding check)
  - Modo strict / loose

Top Ten Spoofer Test Results (for the last year)

by Country	Client IP blocks	Spoofing IP blocks
bra (Brazil)	2862	535 (18.7%)
ind (India)	1578	381 (24.1%)
usa (United States)	4505	238 (5.3%)
egy (Egypt)	179	63 (35.2%)
arg (Argentina)	191	62 (32.5%)
rus (Russian Federation)	301	41 (13.6%)
tha (Thailand)	405	36 (8.9%)
aus (Australia)	602	35 (5.8%)
pak (Pakistan)	163	35 (21.5%)
can (Canada)	449	34 (7.6%)

https://spoofer.caida.org/summary.php

RPKI

https://www.rnp.br/noticias/rnp-entra-para-o-projeto-rpki-de-seguranca-de-redes-mundial

[GTER] RPKI no Registro.br

Frederico A C Neves fneves at registro.br
Thu Dec 12 16:35:39 -03 2019

- Previous message (by thread): [GTER] Recarga de Celular e solução para comprovantes
- Next message (by thread): [GTER] RPKI no Registro.br
- **Messages sorted by:** [date] [thread] [subject] [author]

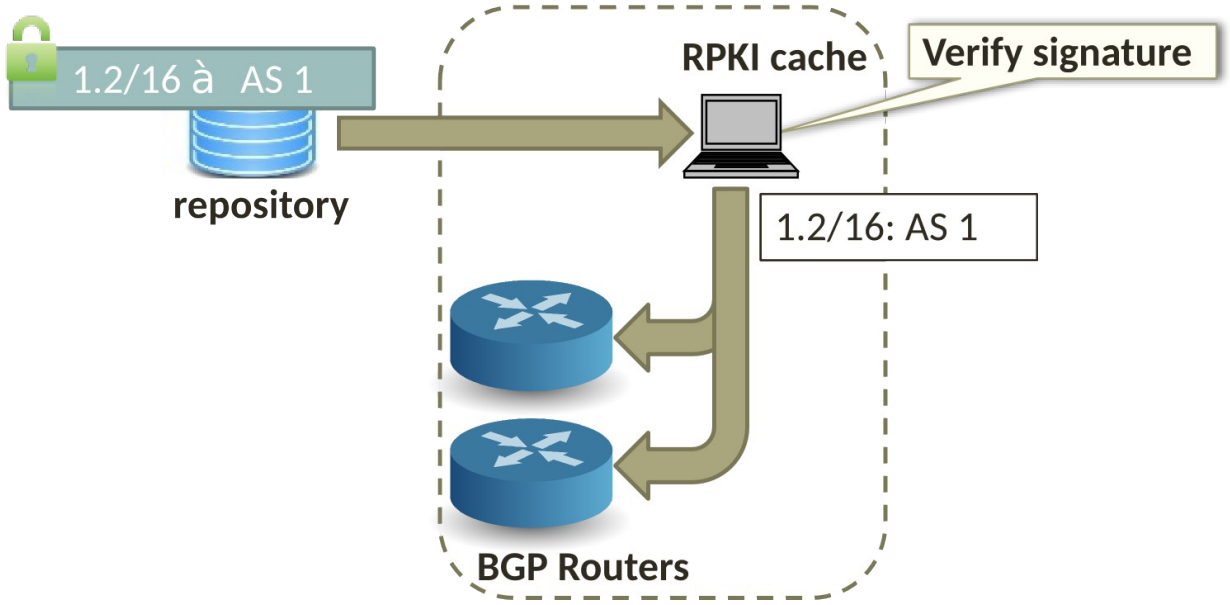
```
Prezados,

O serviço RPKI conforme apresentado no GTER48 [1], já encontra-se
disponível para uso.
```

ftp://ftp.registro.br/pub/gter/gter48/03-RPKI-Registro.br

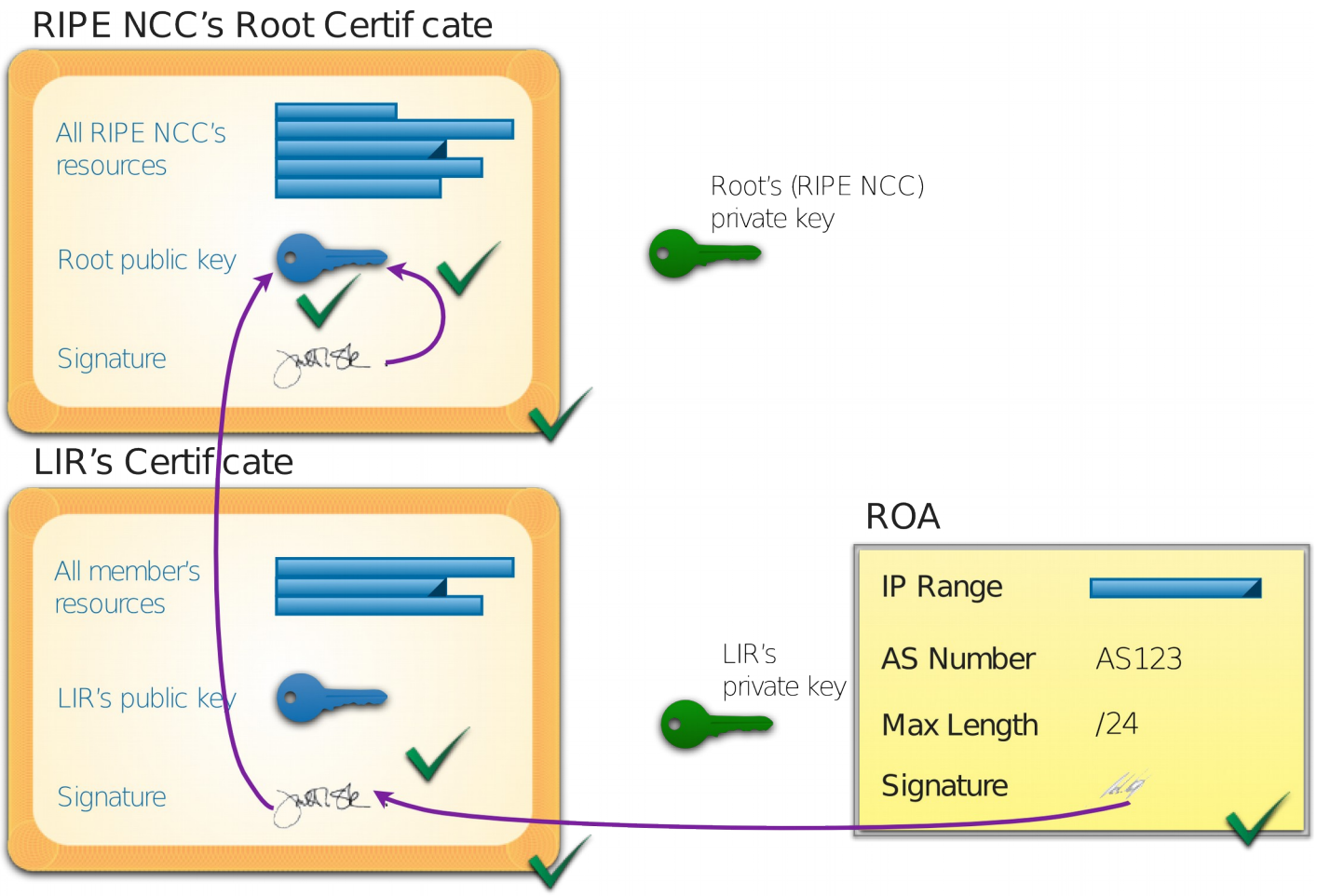
RPKI

- Autenticação da origem
- Protege contra prefix/subprefix hijacking
- Adiciona certificados digitais a recursos de rede, associando-os com seus proprietários
- Route Origin Authorizations (ROAs) + Chain of trust



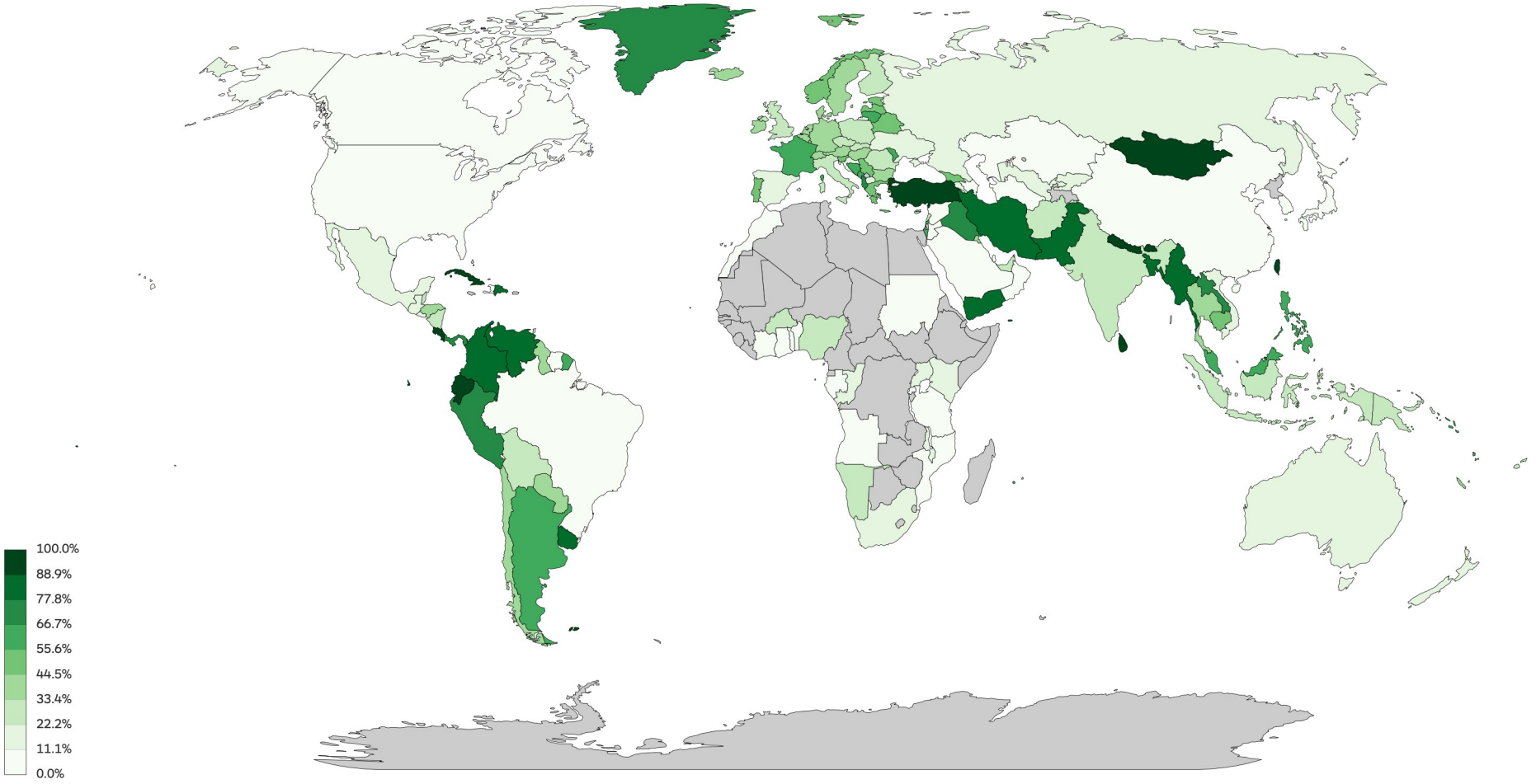
Fonte: Jumpstarting, Avichai, SIGCOMM

RPKI



Fonte: bgp-operations-and-security (RIPE)

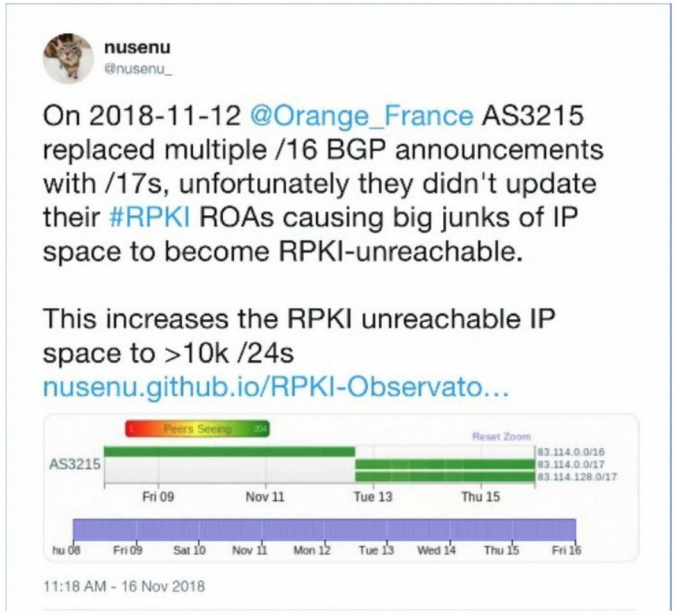
RPKI



https://www.nlnetlabs.nl/projects/rpki/rpki-analytics/

RPKI - Desafios

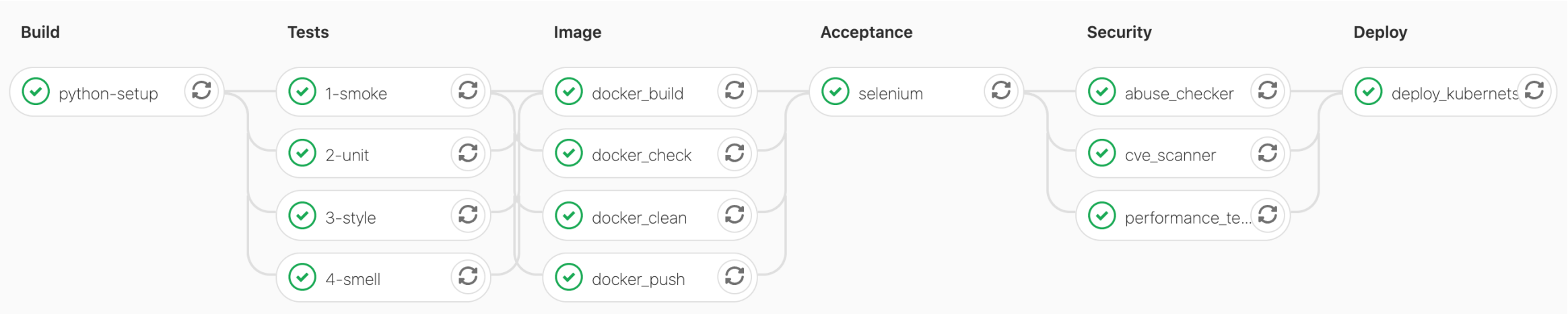
- Capacitação
  - https://tutoriais.semanainfrabr.nic.br/files/apresentacao/arquivo/803/RPKI.pdf
- Operação
  - Modo delegado do NIC.br
  - Manutenção dos ROAs
  - O que fazer com rotas inválidas?
  - Termos do ARIN (Relying Party Agreement)
- RPKI – proteção de origem, e o caminho



Automação e orquestração da rede

- Redução no uso da CLI e aumento do uso de ferramentas de orquestração ou soluções baseadas em Netconf, gNNI, gNOI, etc
  - Automação
  - Sistematização
  - Documentação
  - Controle de versão
  - Teste
  - Reuso
- CI/CD, Pipeline

Exemplo de pipeline



tps://www.youtube.com/linuxtips

Desafios

- Mudança no *mindset* do operador de rede
- Conhecer as APIs, ferramentas e interfaces de gerencia
- Aproximação com a área de Dev

Outras tendências

- Uso de Machine Learning/IA para investigação de incidentes e caça às ameaças (Threat Hunting)
- Scan de vulnerabilidade, honeypot, ferramentas de auditoria automática de aplicações web
- Análise de logs, visualização e curvas de tendencia (Grafana, Graylog, ELK)

WTR

WORKSHOP

DE TECNOLOGIAS DE REDES DO POP-BA

14 A 18 DE SETEMBRO DE 2020

PoP-BA Ponto de Presença da RNP na Bahia

RNP 30 anos ORGANIZAÇÃO SOCIAL DO MCTI

MINISTÉRIO DO TURISMO

MINISTÉRIO DA DEFESA

MINISTÉRIO DA SAÚDE

MINISTÉRIO DA EDUCAÇÃO

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES

PÁTRIA AMADA BRASIL GOVERNO FEDERAL