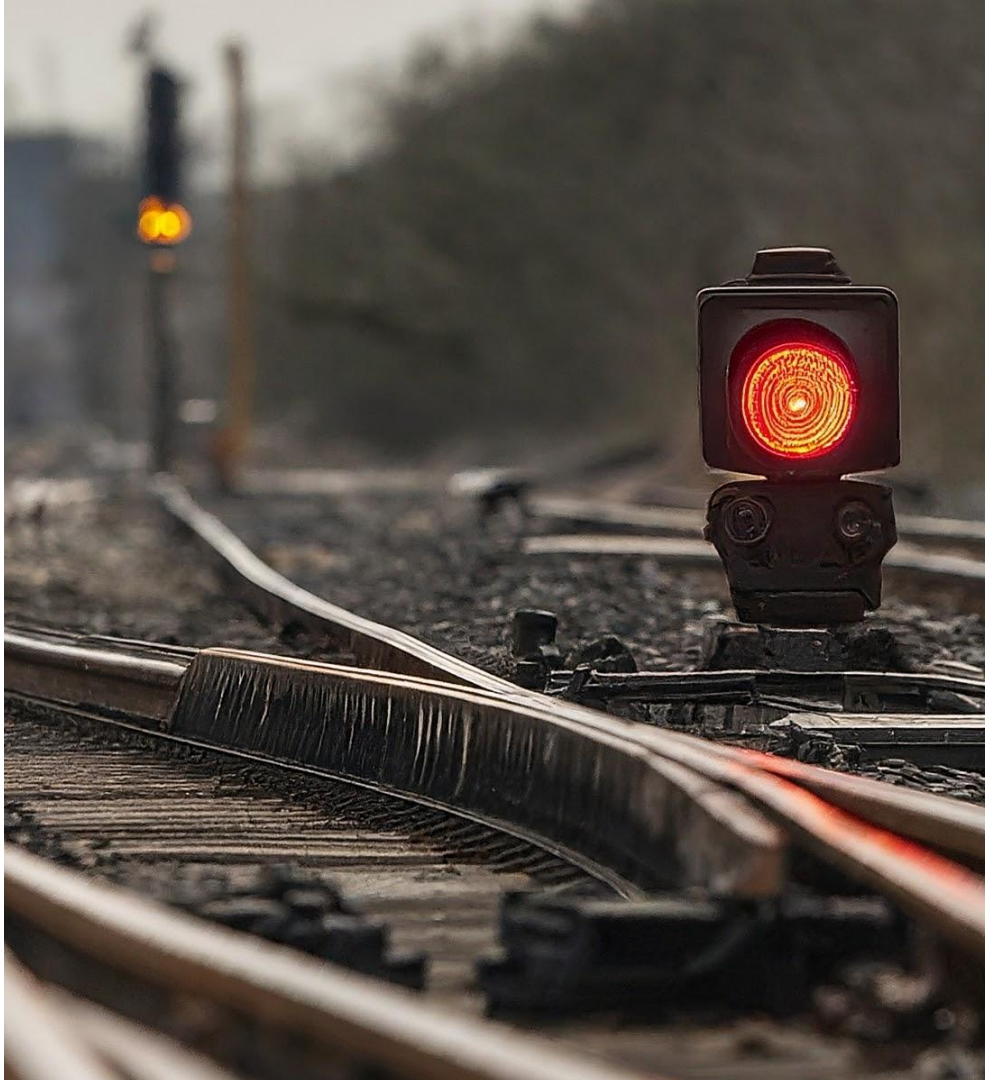
Identificação de Políticas de Validação de Rotas no RPKI

Marcel Mendes
Leonardo Oliveira
Ítalo Cunha
Ethan Katz-Bassett

UFMG
Columbia University



Sequestros de prefixo e vazamento de rotas

renesys

Sequestros de prefixo e vazamento de rotas

The Washington Post
Democracy Dies in Darkness

The Switch

Researchers say U.S. Internet traffic was re-routed through Belarus. That's a problem.

By **Andrea Peterson**
Reporter

November 20, 2013 at 7:38 p.m. EST

The Washington Post

Democracy Dies in Darkness

The Switch

Researchers say U.S. Internet traffic was re-routed through Belarus. That's a problem.

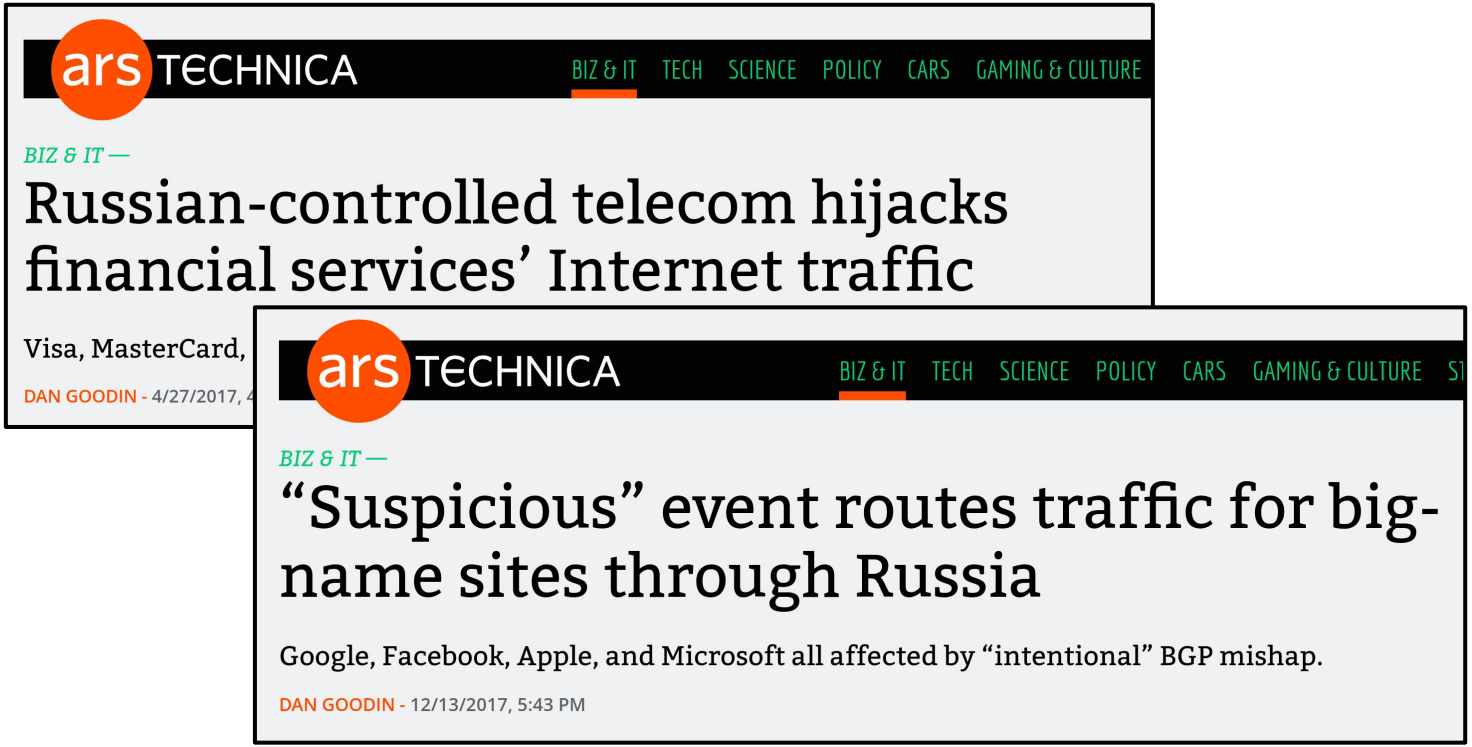
By **Andrea Peterson**

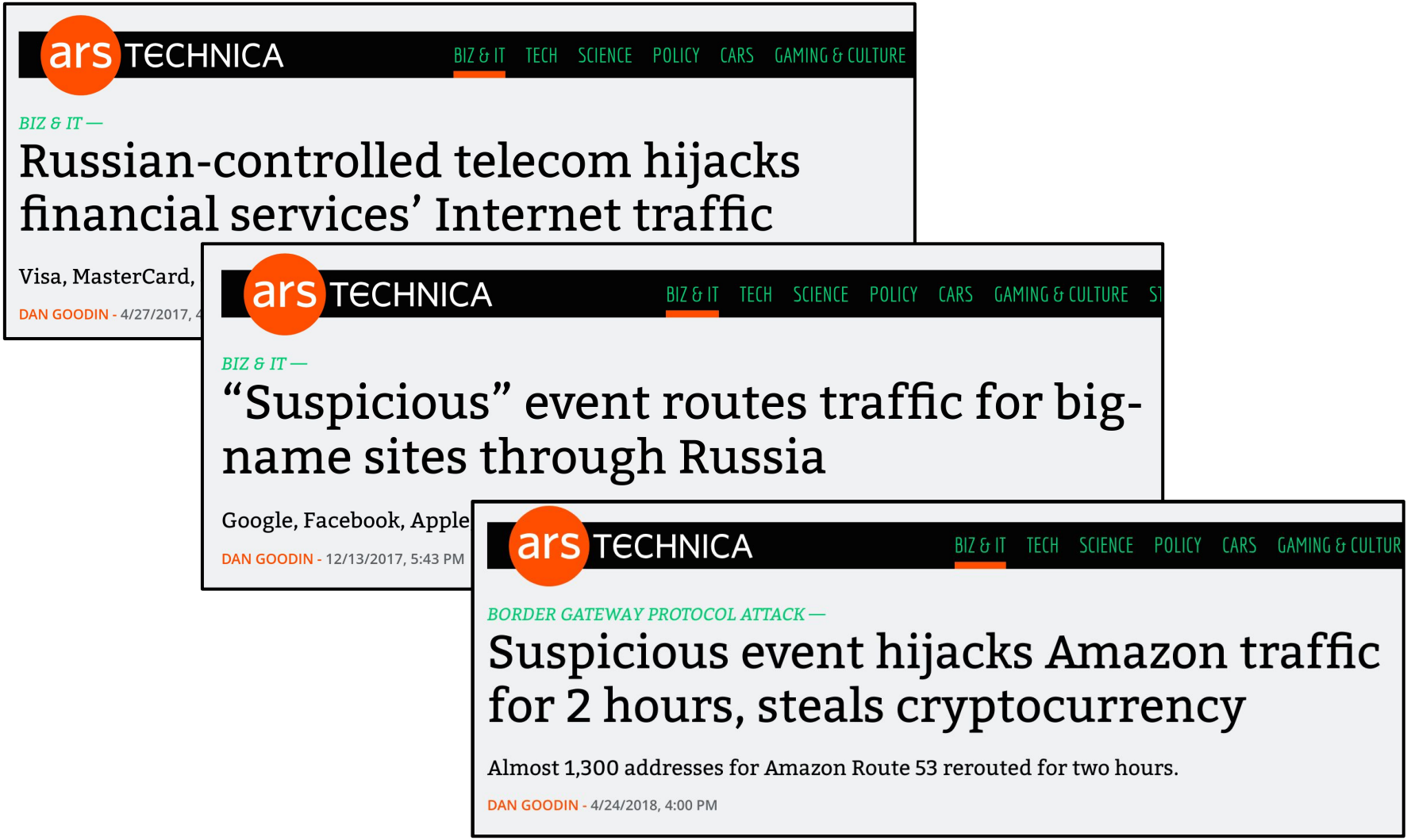
Reporter

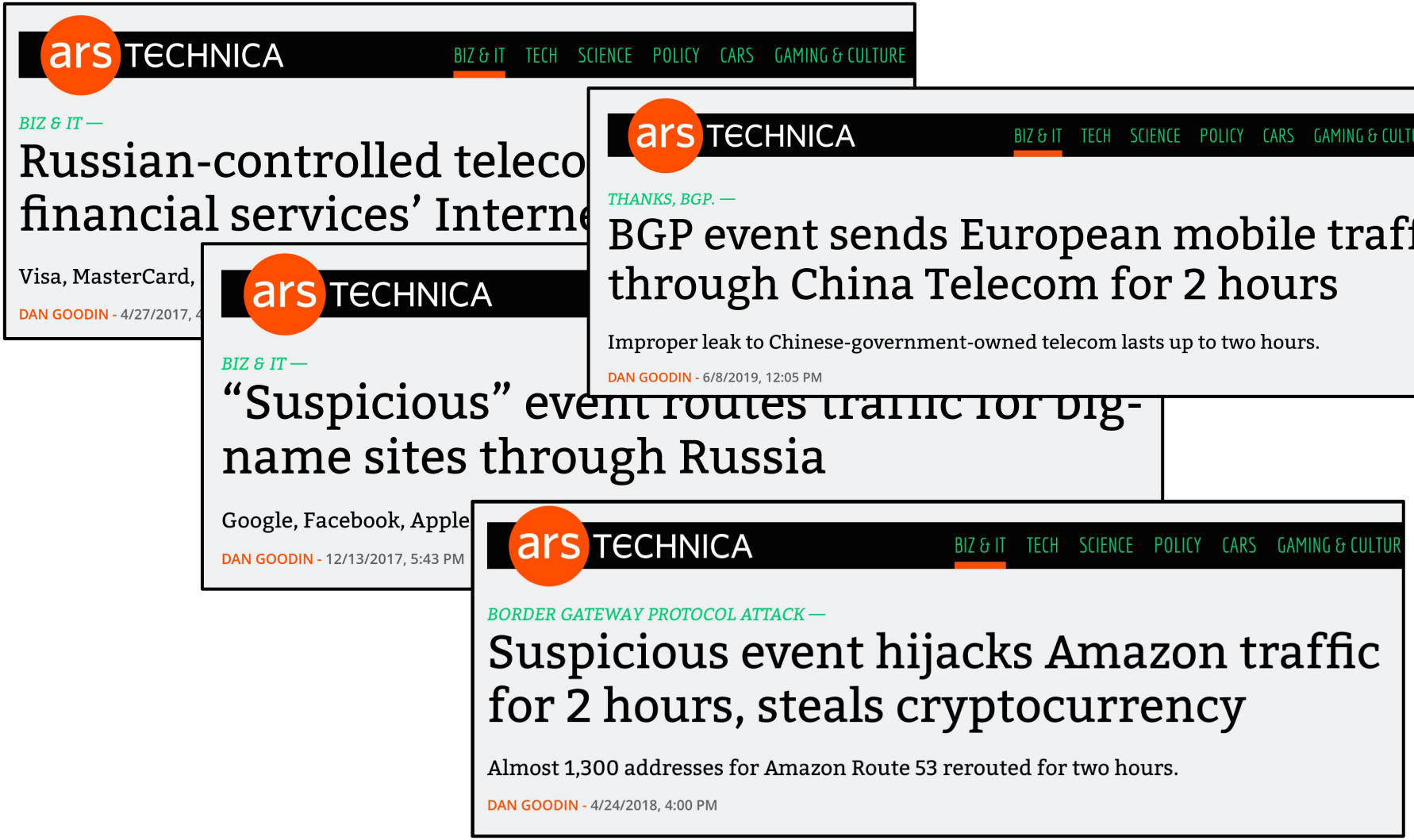
November 20, 2013 at 7:38 p.m. EST

2013


ars TECHNICA
BIZ & IT
TECH
SCIENCE
POLICY
CARS
GAMING & CULTURE
BIZ & IT —
Russian-controlled telecom hijacks financial services' Internet traffic
Visa, MasterCard, and Symantec among dozens affected by "suspicious" BGP mishap.
DAN GOODIN - 4/27/2017, 4:20 PM


ars TECHNICA
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE
BIZ & IT —
Russian-controlled telecom hijacks financial services' Internet traffic
Visa, MasterCard,
DAN GOODIN - 4/27/2017,
ars TECHNICA
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE
BIZ & IT —
"Suspicious" event routes traffic for big-name sites through Russia
Google, Facebook, Apple, and Microsoft all affected by "intentional" BGP mishap.
DAN GOODIN - 12/13/2017, 5:43 PM


ars TECHNICA
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE
BIZ & IT —
Russian-controlled telecom hijacks financial services' Internet traffic
Visa, MasterCard,
DAN GOODIN - 4/27/2017,
ars TECHNICA
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE
BIZ & IT —
"Suspicious" event routes traffic for big-name sites through Russia
Google, Facebook, Apple
DAN GOODIN - 12/13/2017, 5:43 PM
ars TECHNICA
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTUR
BORDER GATEWAY PROTOCOL ATTACK —
Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency
Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.
DAN GOODIN - 4/24/2018, 4:00 PM


ars TECHNICA
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE
BIZ & IT —
Russian-controlled teleco
financial services' Interne
Visa, MasterCard,
DAN GOODIN - 4/27/2017,
ars TECHNICA
BIZ & IT —
"Suspicious" event routes traffic for big-
name sites through Russia
Google, Facebook, Apple
DAN GOODIN - 12/13/2017, 5:43 PM
ars TECHNICA
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTUR
BORDER GATEWAY PROTOCOL ATTACK —
Suspicious event hijacks Amazon traffic for 2 hours, steals cryptocurrency
Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.
DAN GOODIN - 4/24/2018, 4:00 PM
ars TECHNICA
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STC
THANKS, BGP. —
BGP event sends European mobile traffic through China Telecom for 2 hours
Improper leak to Chinese-government-owned telecom lasts up to two hours.
DAN GOODIN - 6/8/2019, 12:05 PM

Profiling BGP Serial Hijackers: Capturing Persistent Misbehavior in the Global Routing Table

Cecilia Testart
MIT
ctestart@csail.mit.edu

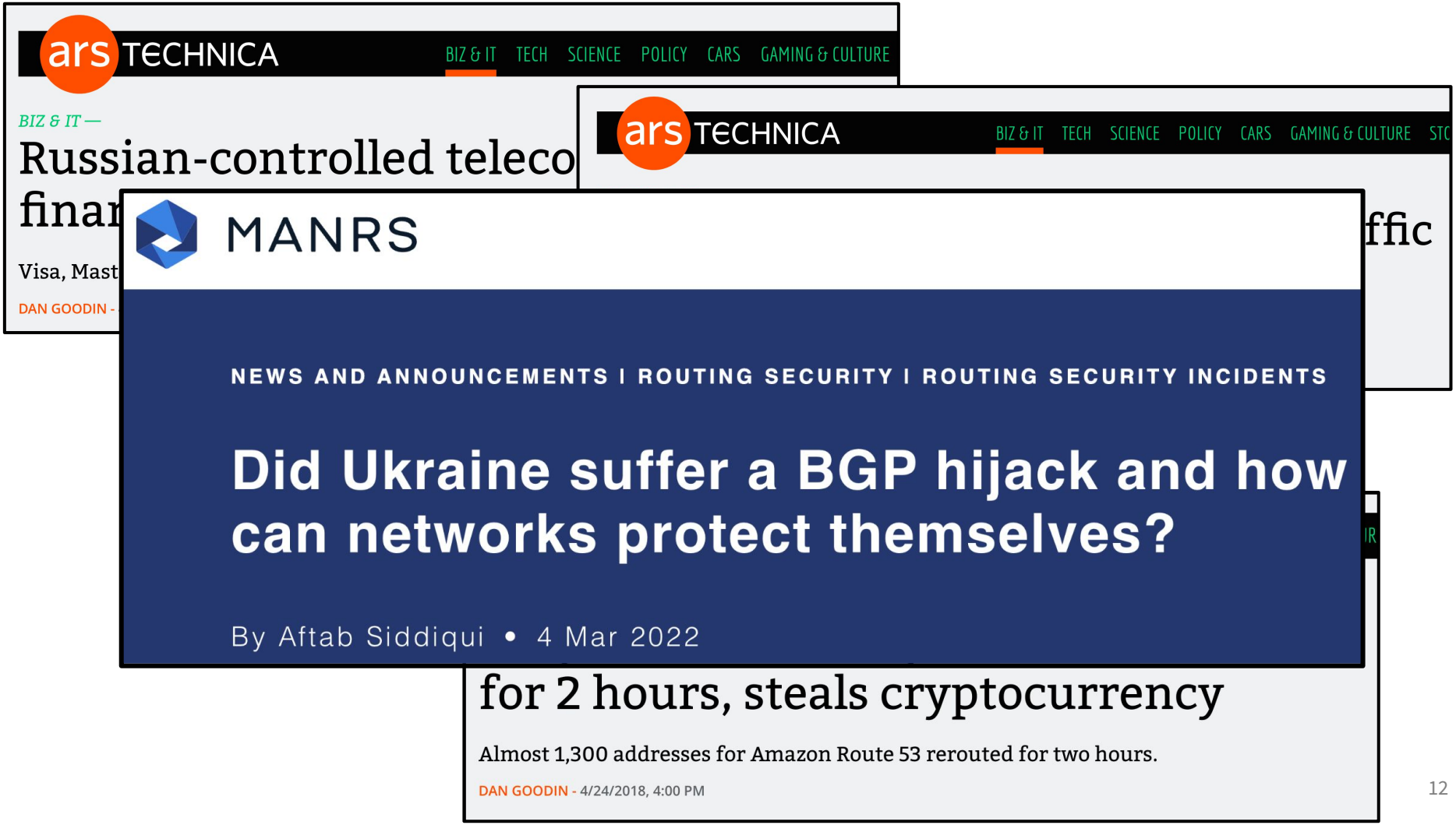
Philipp Richter
MIT
richterp@csail.mit.edu

Alistair King
CAIDA, UC San Diego
alistair@caida.org

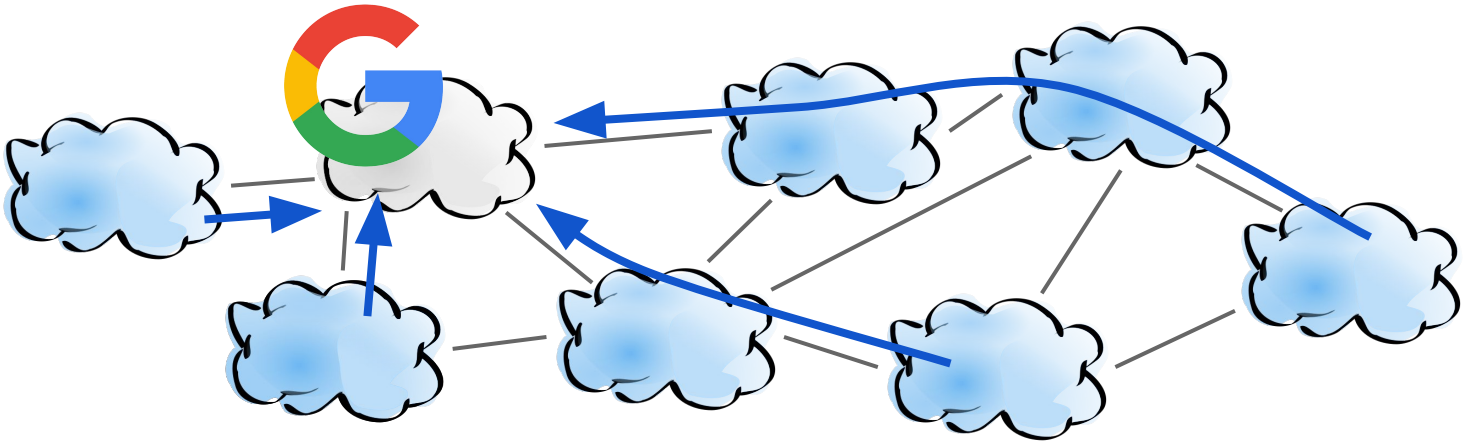
Alberto Dainotti
CAIDA, UC San Diego
alberto@caida.org

David Clark
MIT
ddc@csail.mit.edu

BGP Serial Hijackers

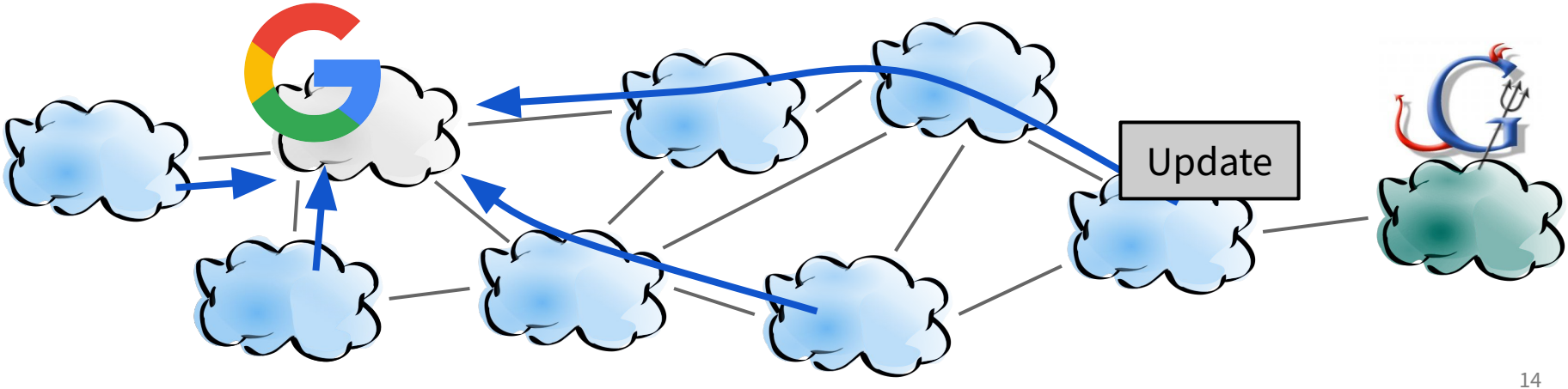

ars TECHNICA
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE
BIZ & IT —
Russian-controlled teleco
finar
Visa, Mast
DAN GOODIN -
ars TECHNICA
BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STC
ffic
MANRS
NEWS AND ANNOUNCEMENTS I ROUTING SECURITY I ROUTING SECURITY INCIDENTS
Did Ukraine suffer a BGP hijack and how can networks protect themselves?
By Aftab Siddiqui • 4 Mar 2022
for 2 hours, steals cryptocurrency
Almost 1,300 addresses for Amazon Route 53 rerouted for two hours.
DAN GOODIN - 4/24/2018, 4:00 PM

Falha fundamental de segurança na Internet



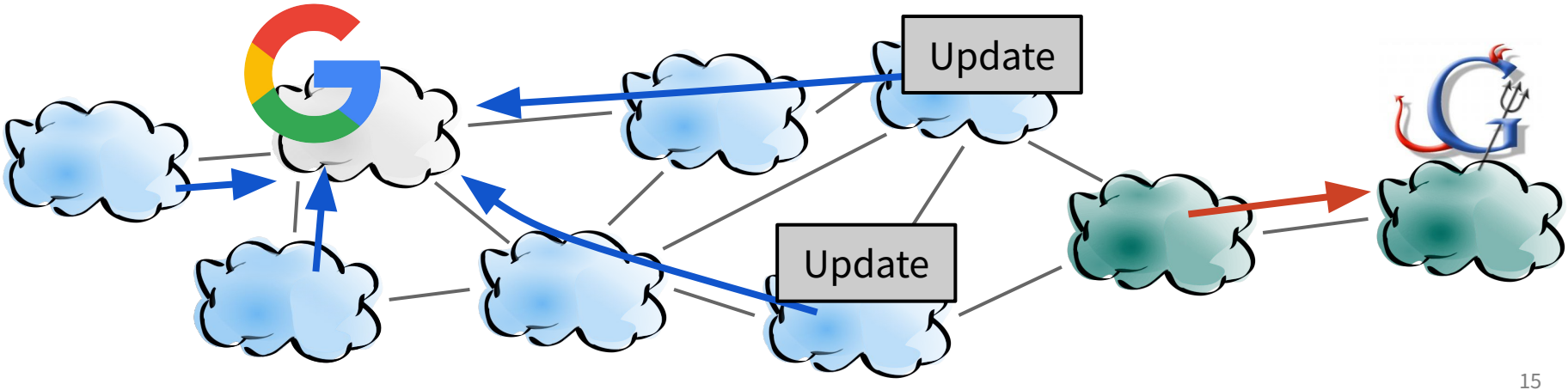
Falha fundamental de segurança na Internet

- Não há autenticação de anúncios



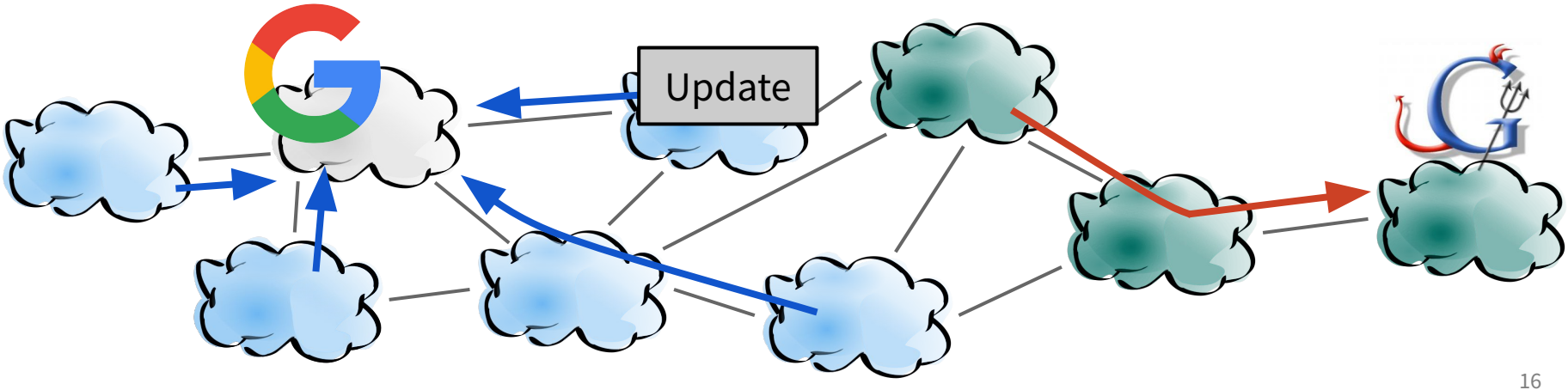
Falha fundamental de segurança na Internet

- Não há autenticação de anúncios
- Impossível diferenciar anúncios ilegítimos



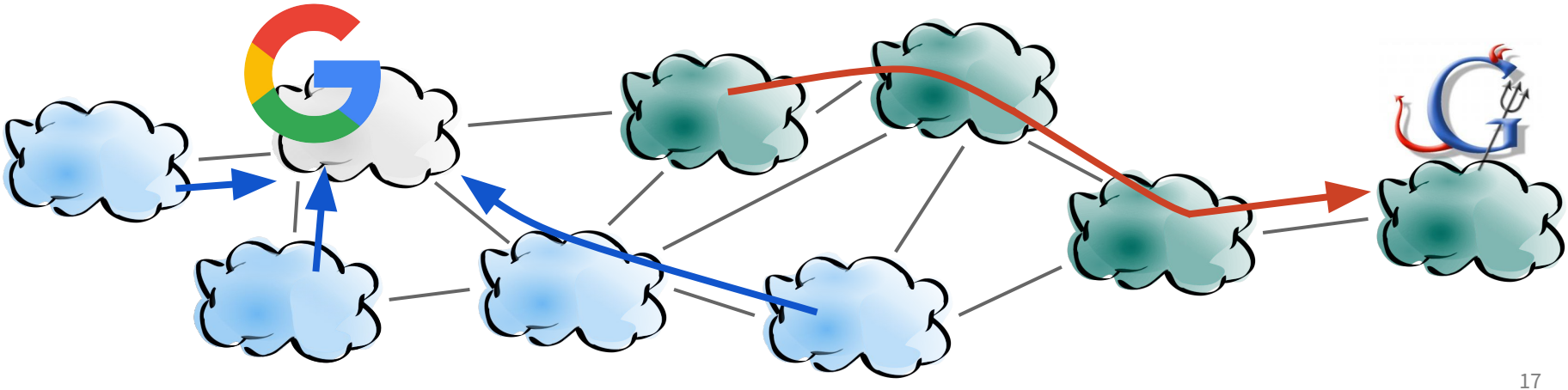
Falha fundamental de segurança na Internet

- Não há autenticação de anúncios
- Impossível diferenciar anúncios ilegítimos



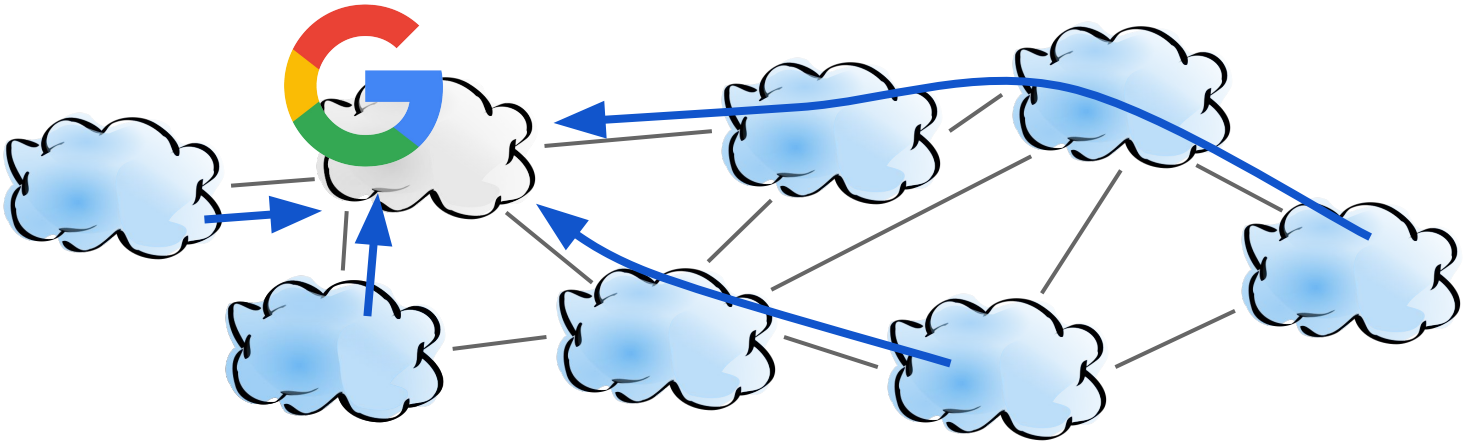
Falha fundamental de segurança na Internet

- Não há autenticação de anúncios
- Impossível diferenciar anúncios ilegítimos



RPKI permite a autenticação de origens

- Operador especifica qual rede pode anunciar uma rota



RPKI permite a autenticação de origens

At least one VRP Matches the Route Prefix

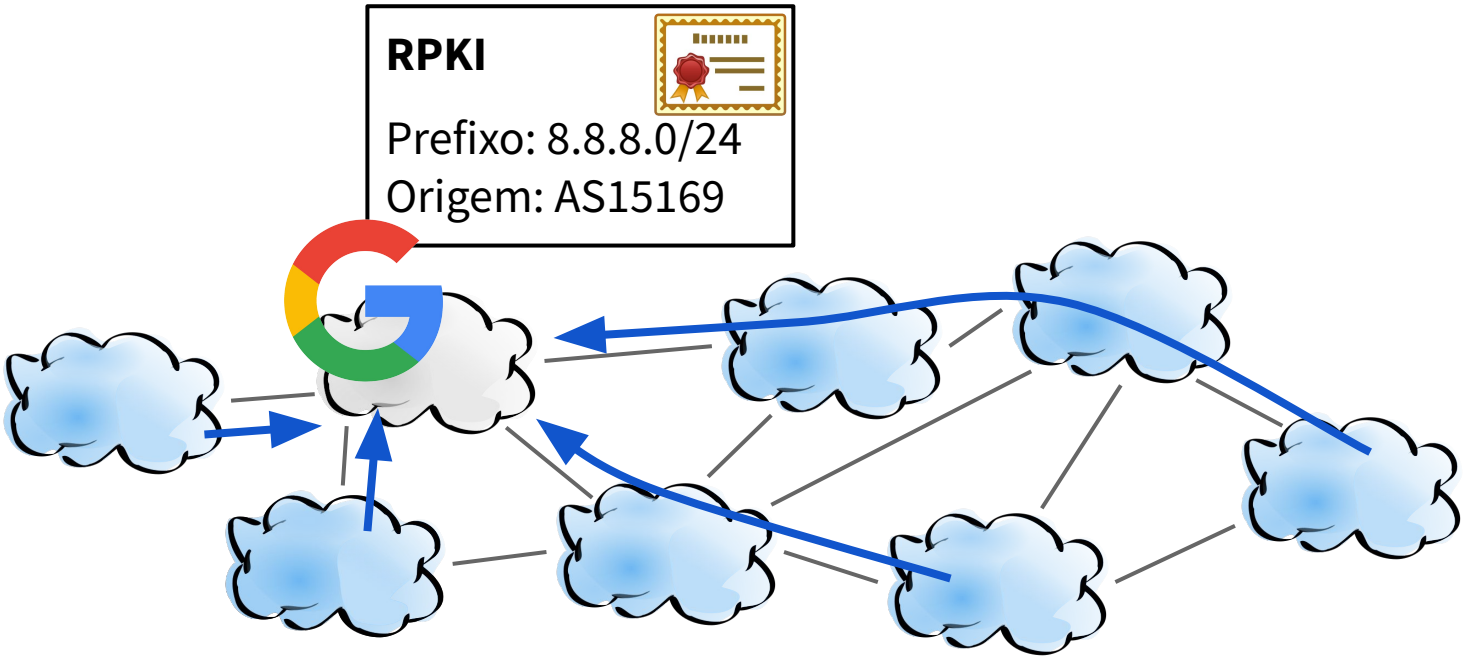
Matched VRPs

Prefix	Max Length	ASN
8.8.8.0/24	24	AS15169

rota

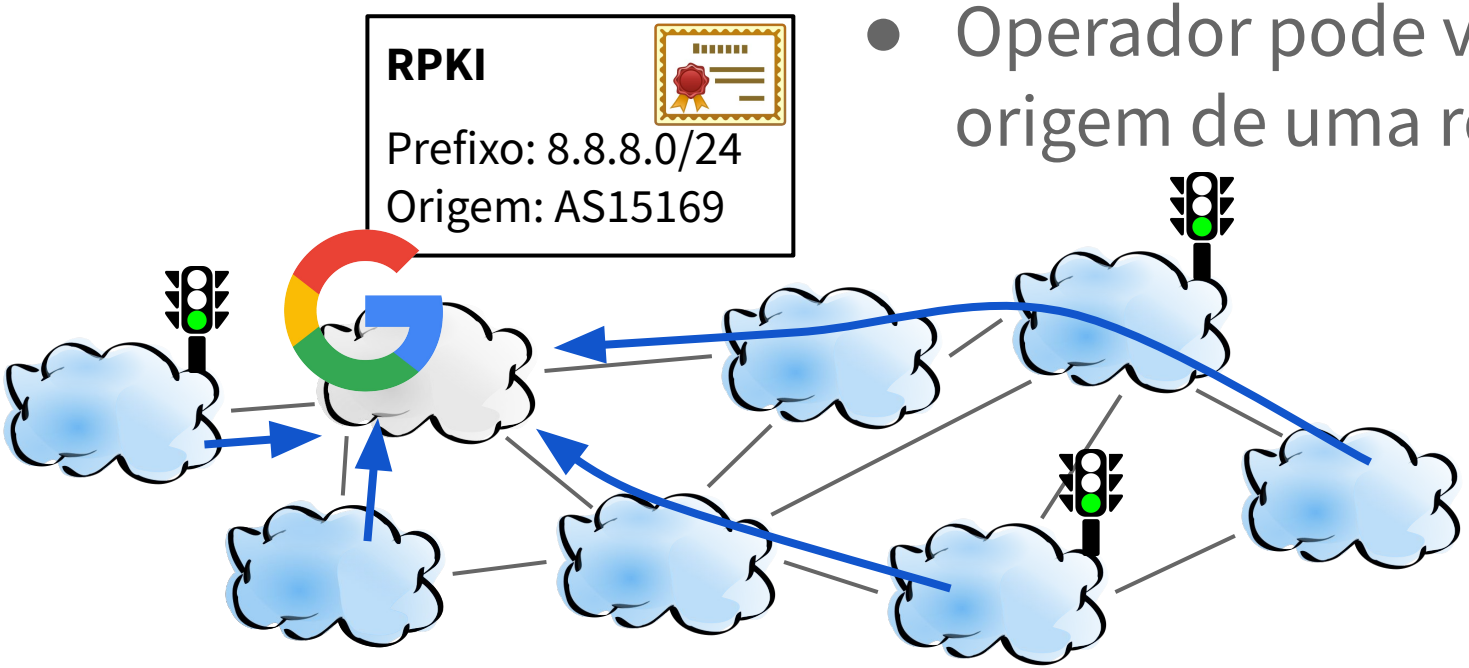
RPKI permite a autenticação de origens

- Operador especifica qual rede pode anunciar uma rota



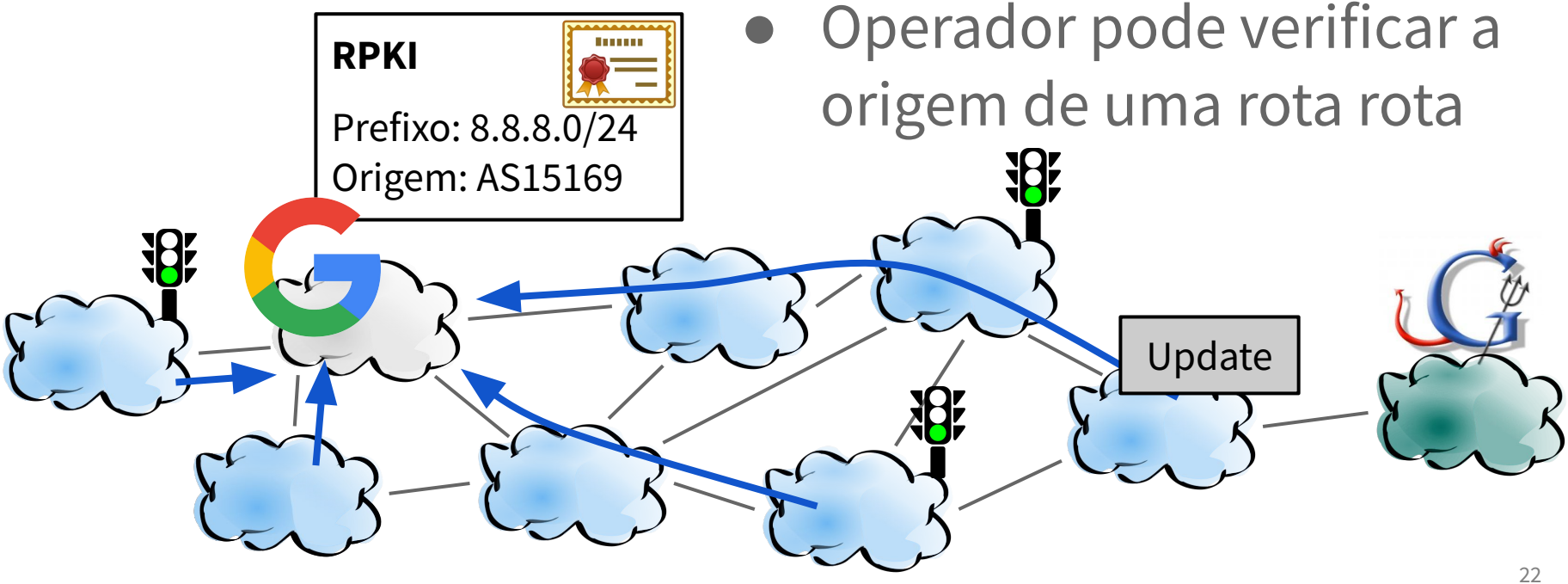
RPKI permite a autenticação de origens

- Operador especifica qual rede pode anunciar uma rota
- Operador pode verificar a origem de uma rota rota



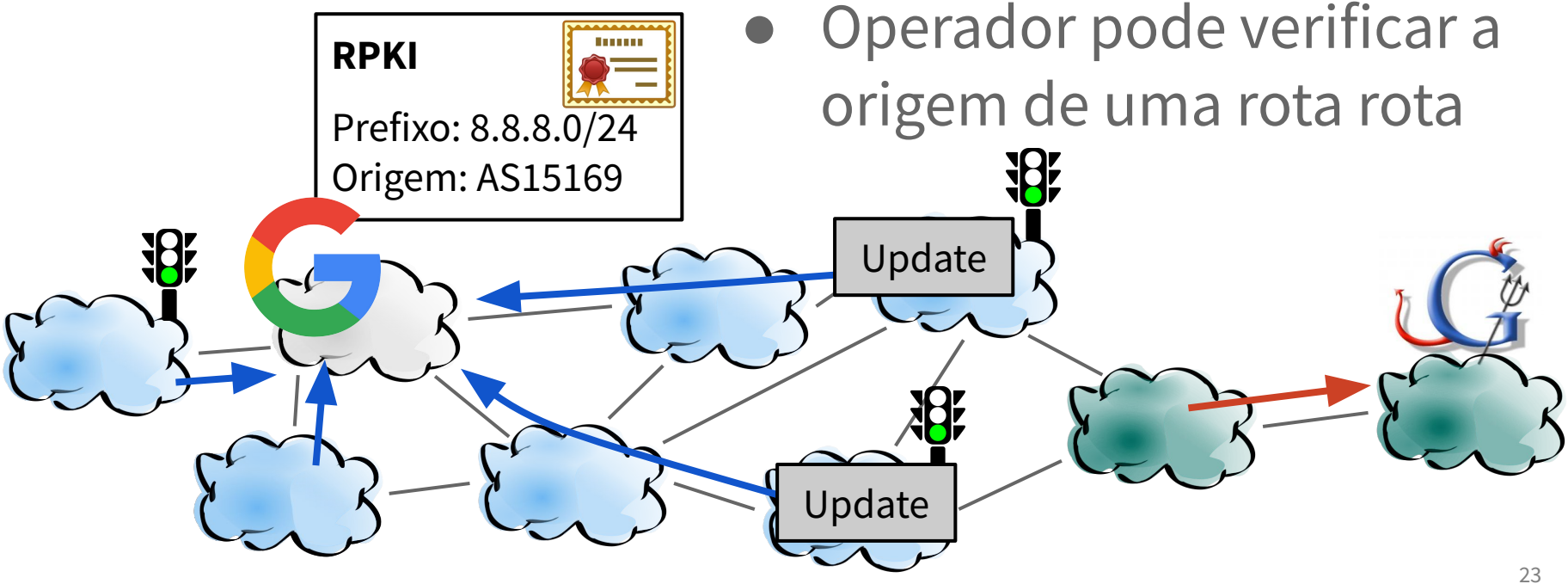
RPKI permite a autenticação de origens

- Operador especifica qual rede pode anunciar uma rota
- Operador pode verificar a origem de uma rota rota



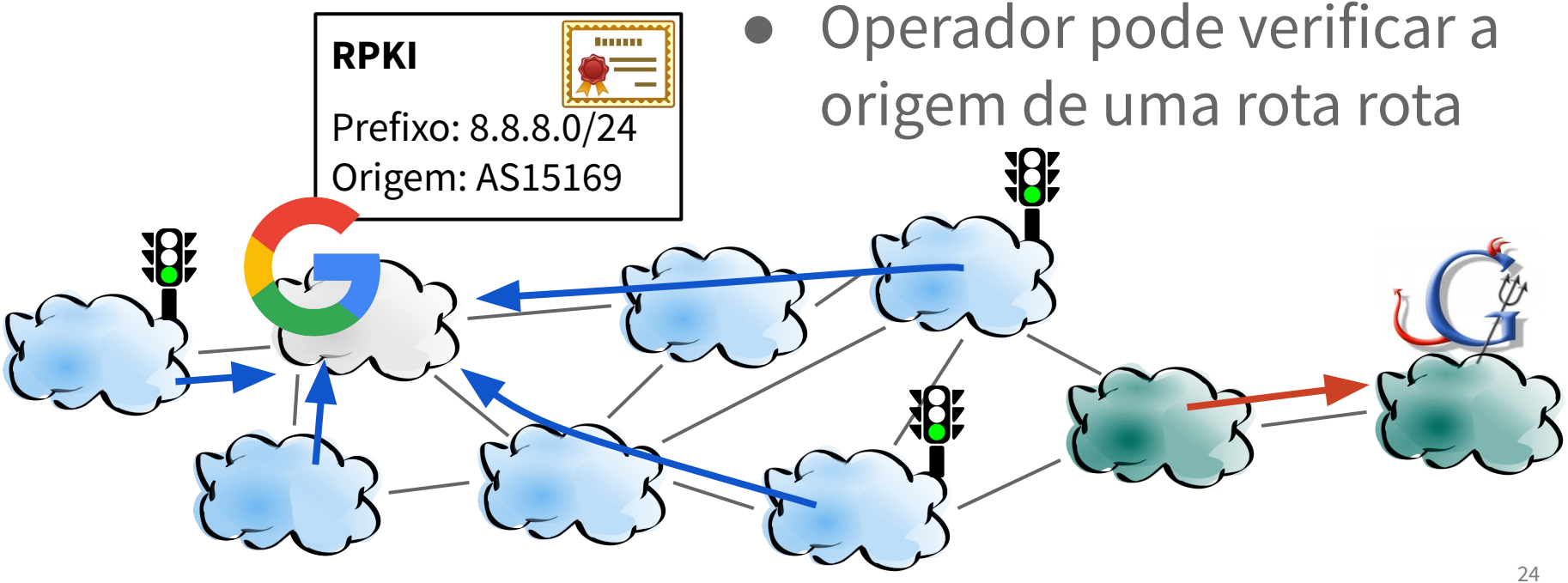
RPKI permite a autenticação de origens

- Operador especifica qual rede pode anunciar uma rota
- Operador pode verificar a origem de uma rota rota

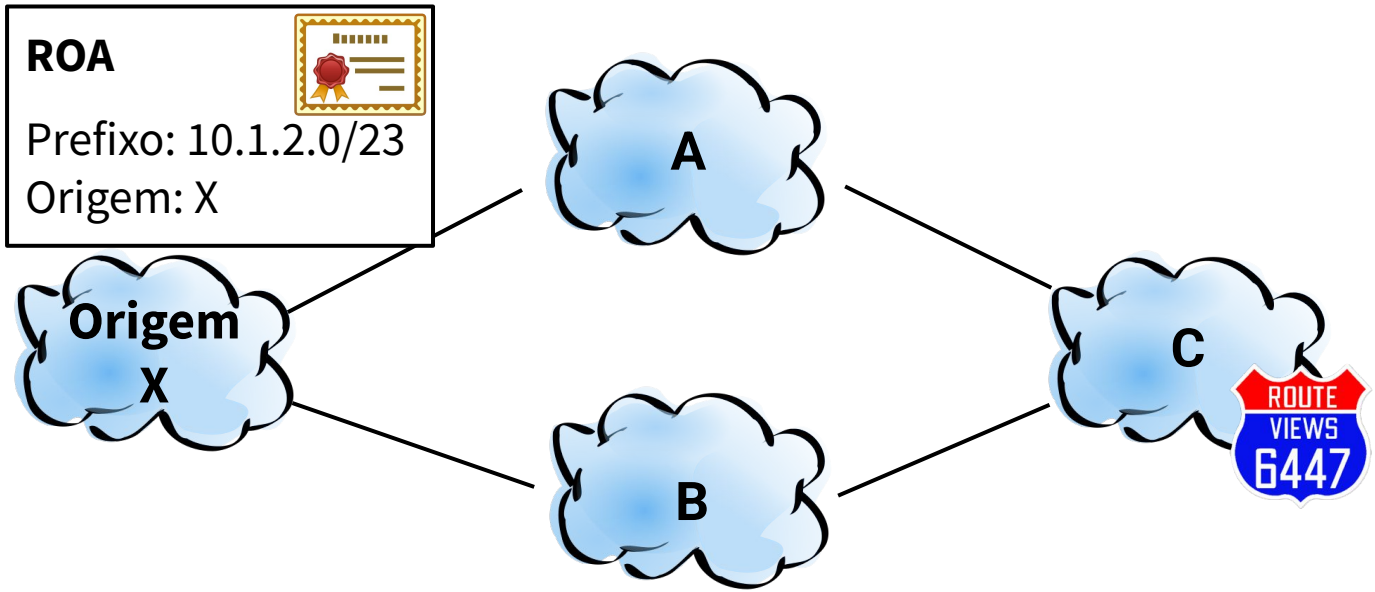


RPKI permite a autenticação de origens

- Operador especifica qual rede pode anunciar uma rota
- Operador pode verificar a origem de uma rota rota

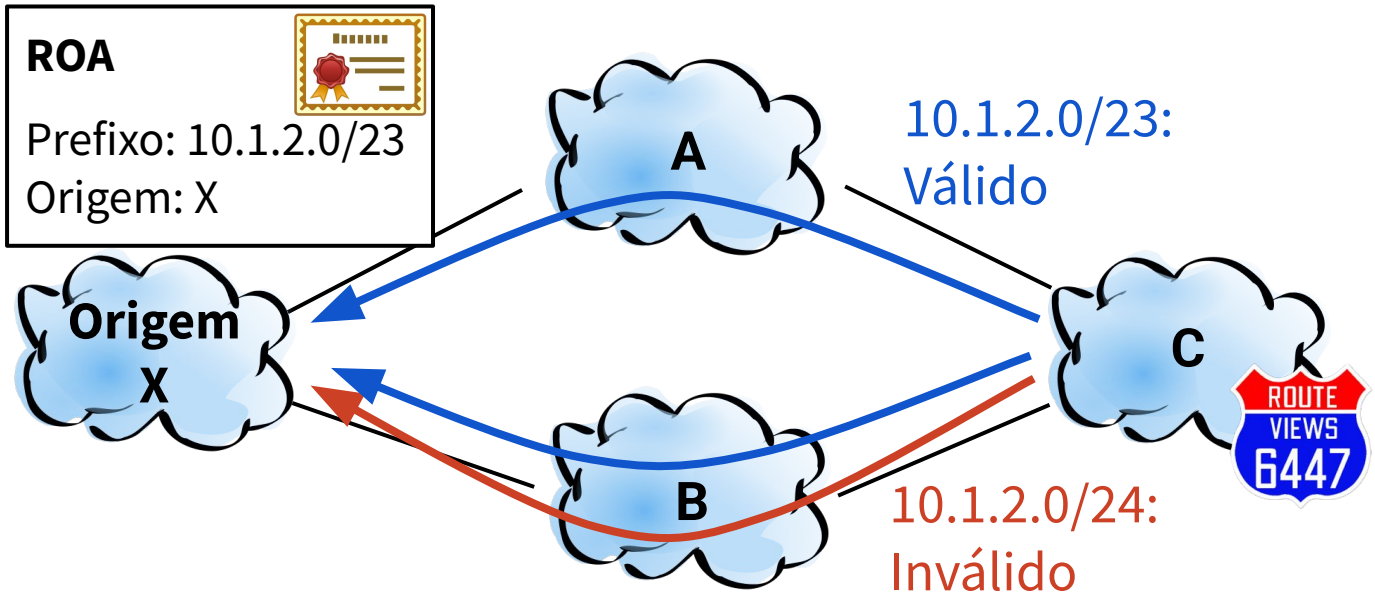


Técnicas prévias de inferência



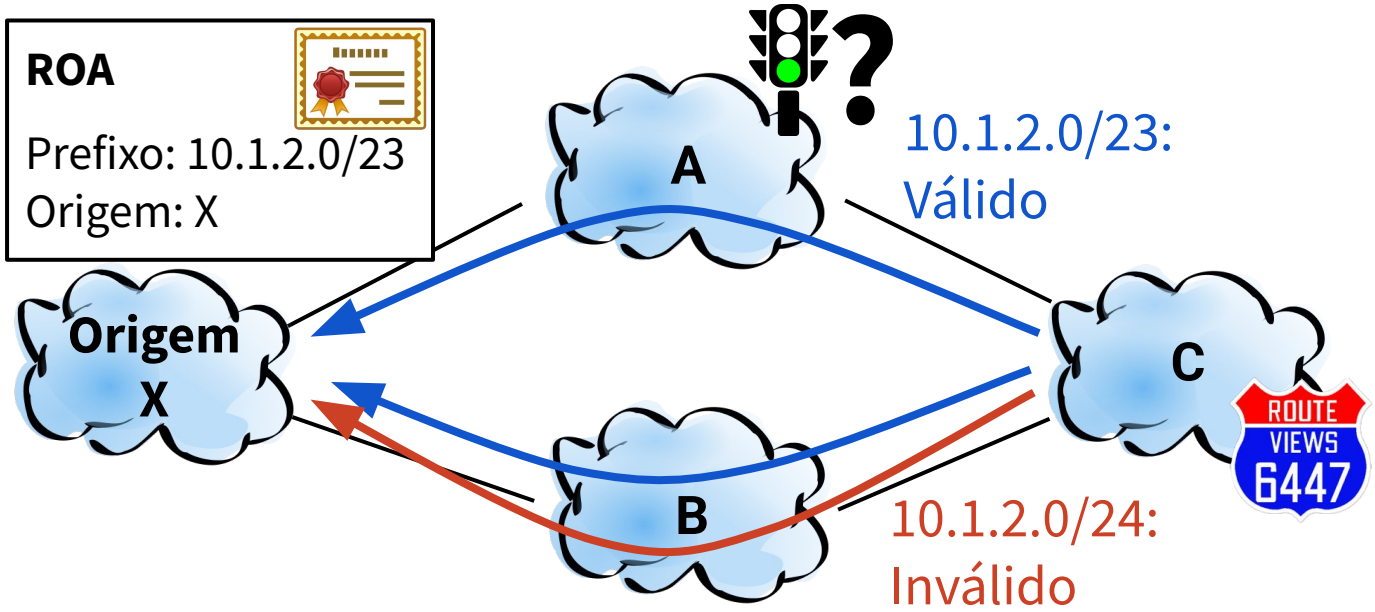
Trabalhos anteriores utilizam dados de coletores BGP para inferir redes que implantam validação de rotas

Técnicas prévias de inferência



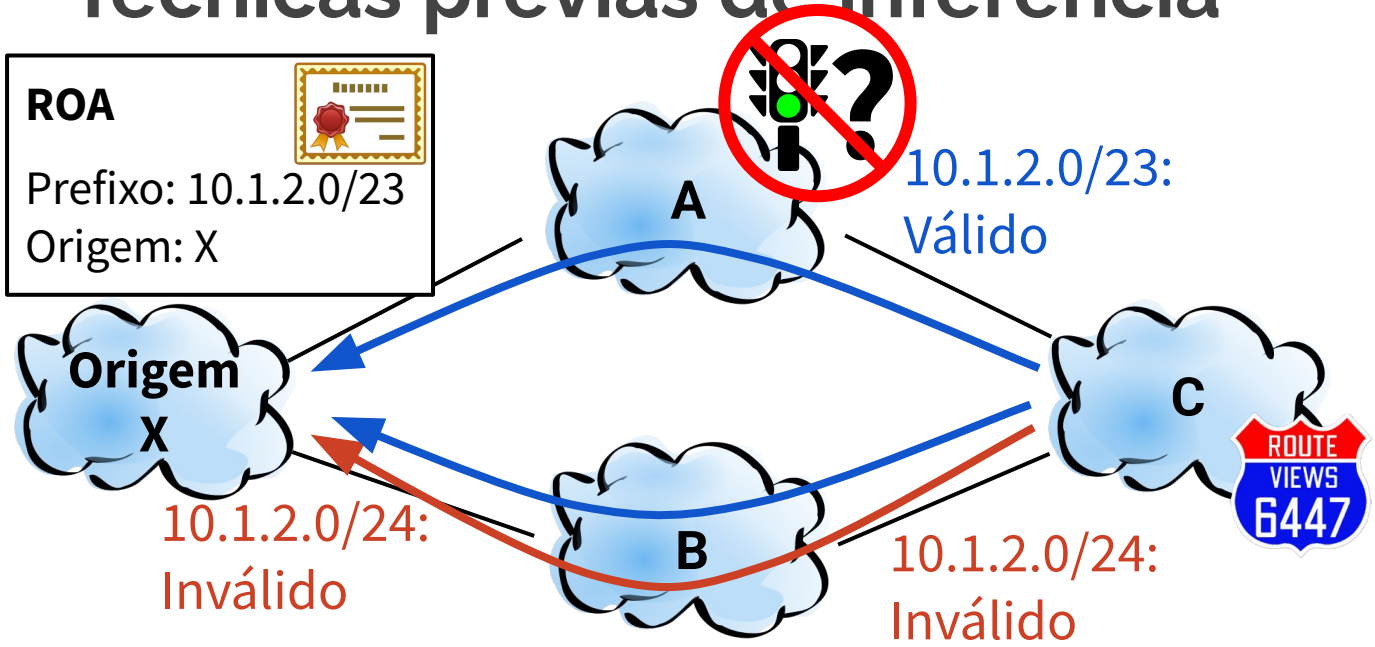
1. Comparar rotas válidas e inválidas recebidas da mesma origem

Técnicas prévias de inferência



1. Comparar rotas válidas e inválidas recebidas da mesma origem
2. Inferir como potenciais validadores redes que não escolhem rotas inválidas

Técnicas prévias de inferência



1. Comparar rotas válidas e inválidas recebidas da mesma origem
2. Inferir como potenciais validadores redes que não escolhem rotas inválidas
3. Diversos fatores podem levar a erros de inferência

Dois desafios levam a ambiguidades

Controle limitado: sem informações sobre políticas de roteamento

Dois desafios levam a ambiguidades

Controle limitado: sem informações sobre políticas de roteamento

Falta de visibilidade: nem todas as redes publicam suas rotas

Inferindo validação de rotas

Flexibilização da política de redes na Internet

- Ignora RPKI 
- Prefere Válida 
- Descarta Inválida 

Inferindo validação de rotas

Anúncios:

Anúncios de dois prefixos com configurações distintas

- Anúncios de dois pontos de presença (PoPs): malicioso e legítimo
- Prefixo 1: **Inválido** do PoP malicioso
- Prefixo 2: **Inválido** do PoP malicioso
  & **válido** do PoP legítimo

Inferindo validação de rotas

Anúncios:

Caso 1:

Inferindo validação de rotas

Anúncios:

Caso 1:

Inferindo validação de rotas

Anúncios:

Caso 1:

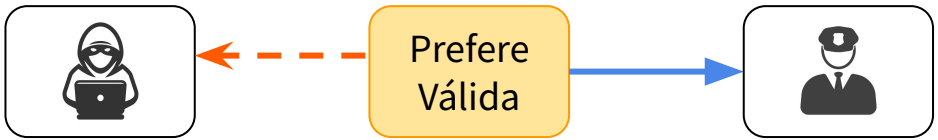
Caso 2:

Inferindo validação de rotas

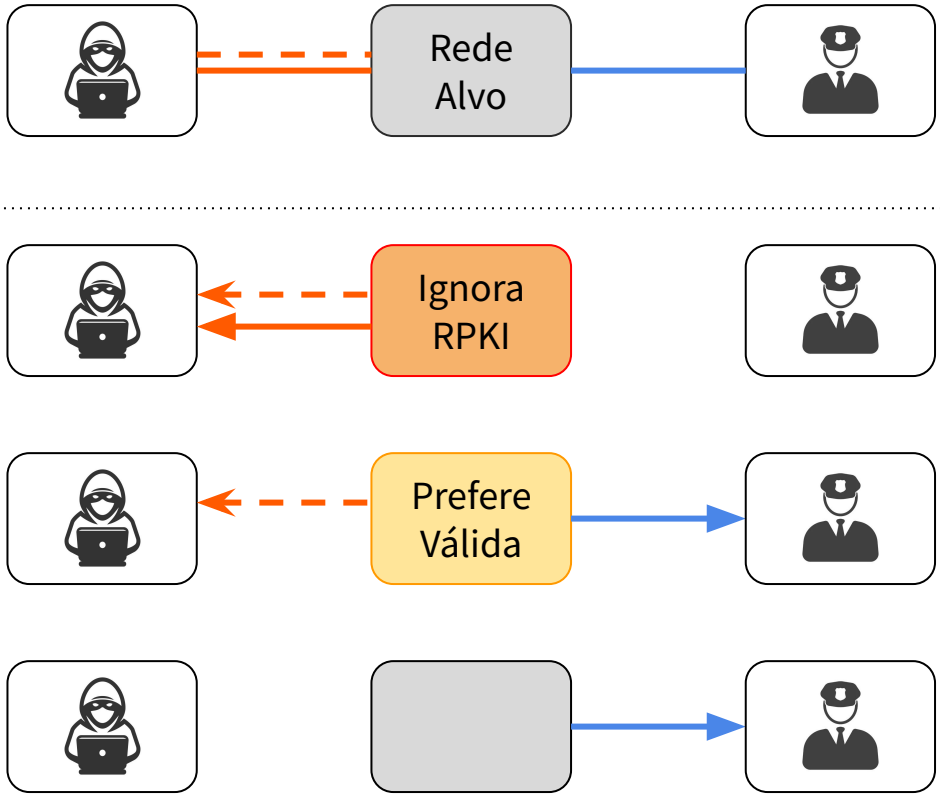
Anúncios:

Caso 1:

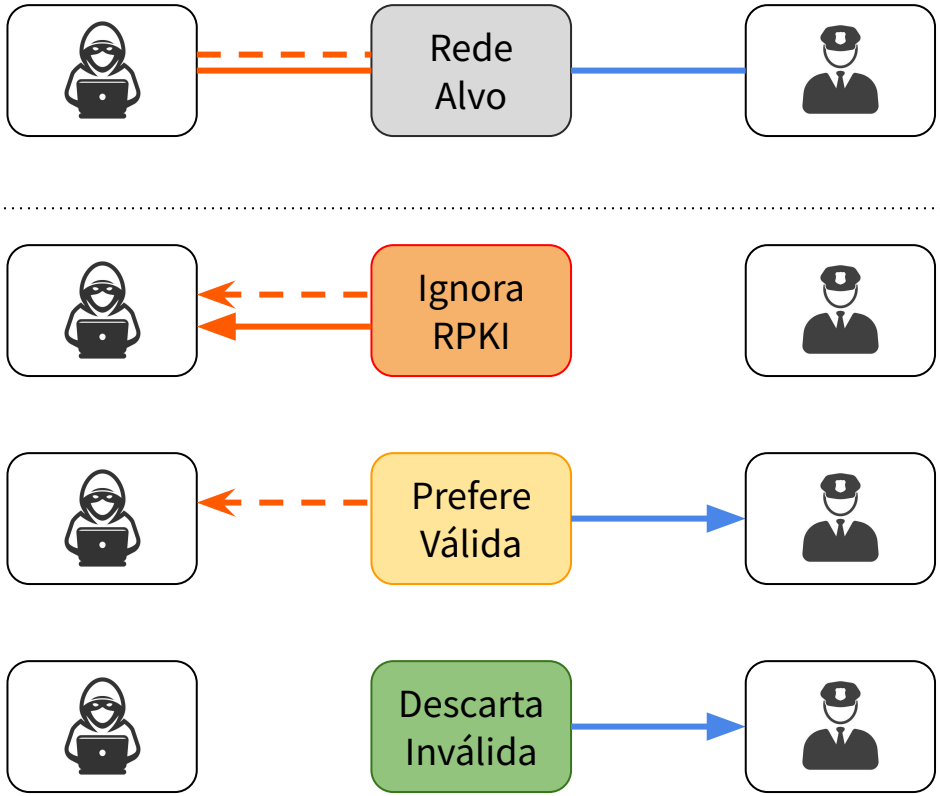
Caso 2:



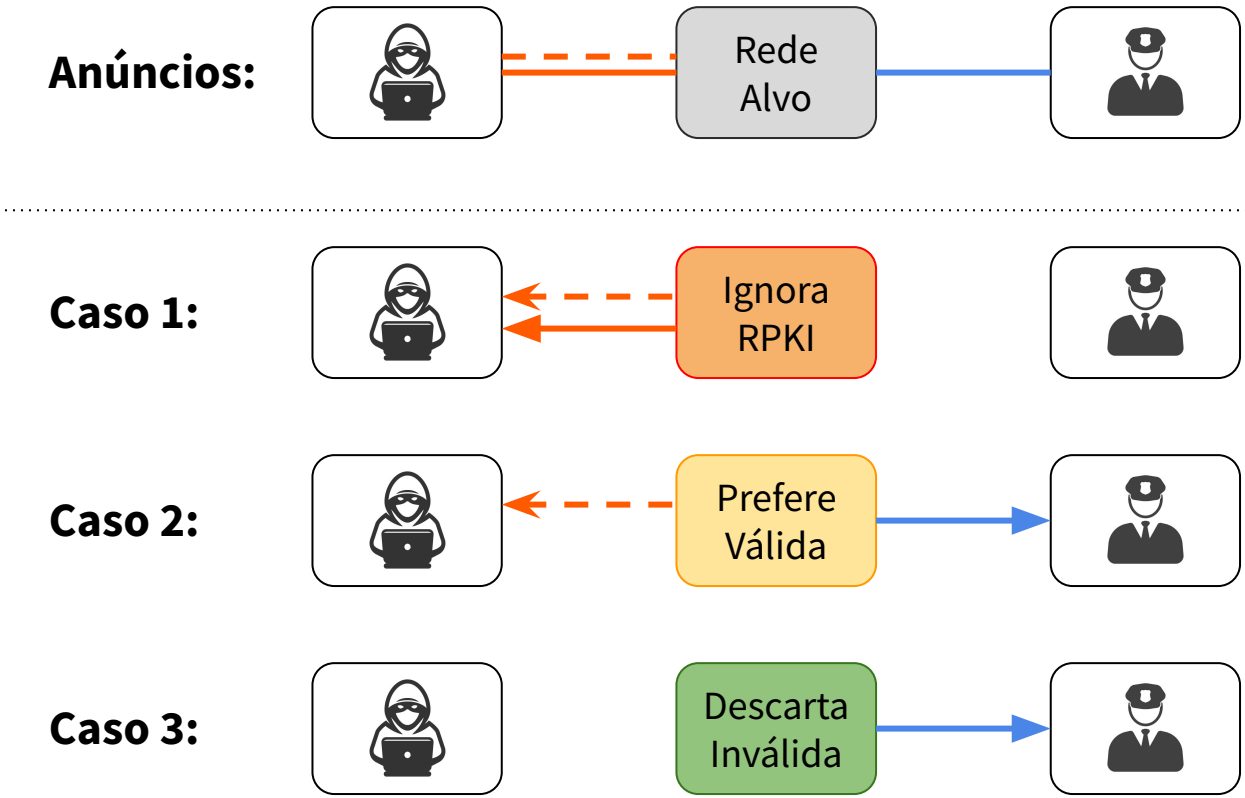
Inferindo validação de rotas



Inferindo validação de rotas



Inferindo validação de rotas



Desafios:

- Nenhum controle das rotas disponíveis
- Falta de visibilidade

Nestes casos:

- Controle das rotas via conexão direta
- Visibilidade total

Inferindo validação de rotas

Anúncios:

Inferindo validação de rotas

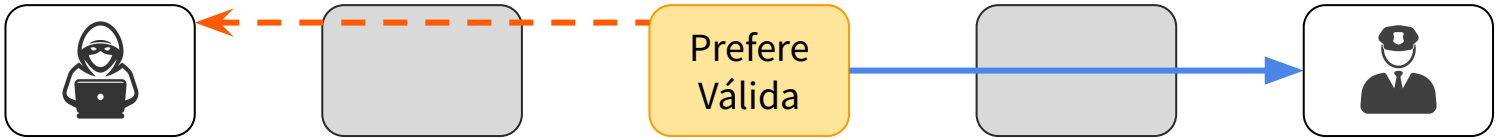
Anúncios:

Caso 2A:

Inferindo validação de rotas

Anúncios:

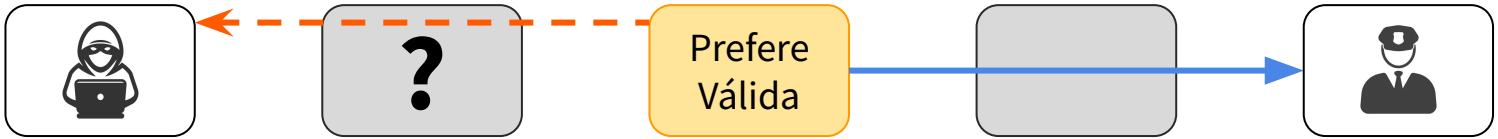
Caso 2A:



Inferindo validação de rotas

Anúncios:

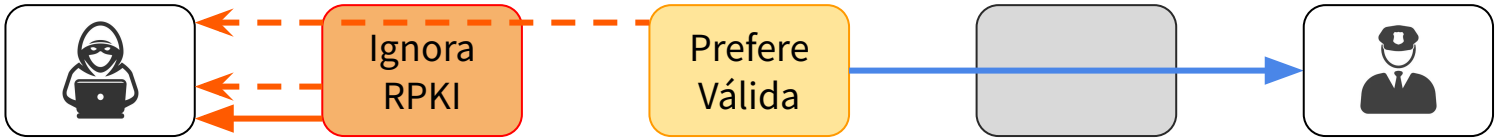
Caso 2A:



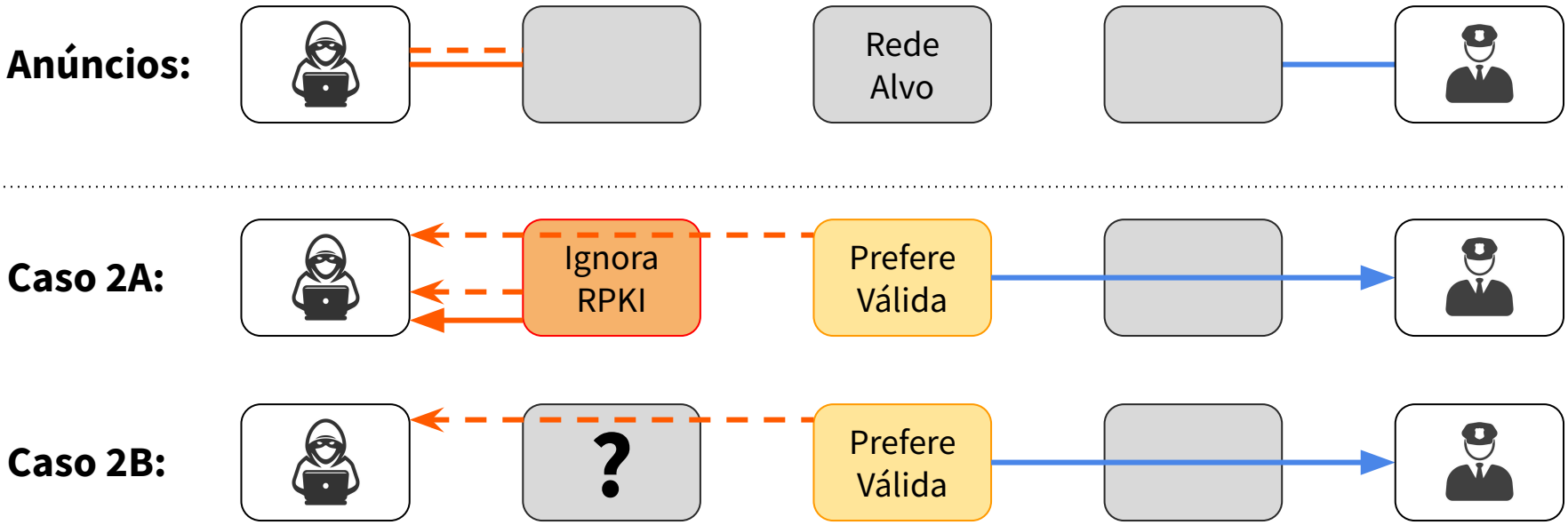
Inferindo validação de rotas

Anúncios:

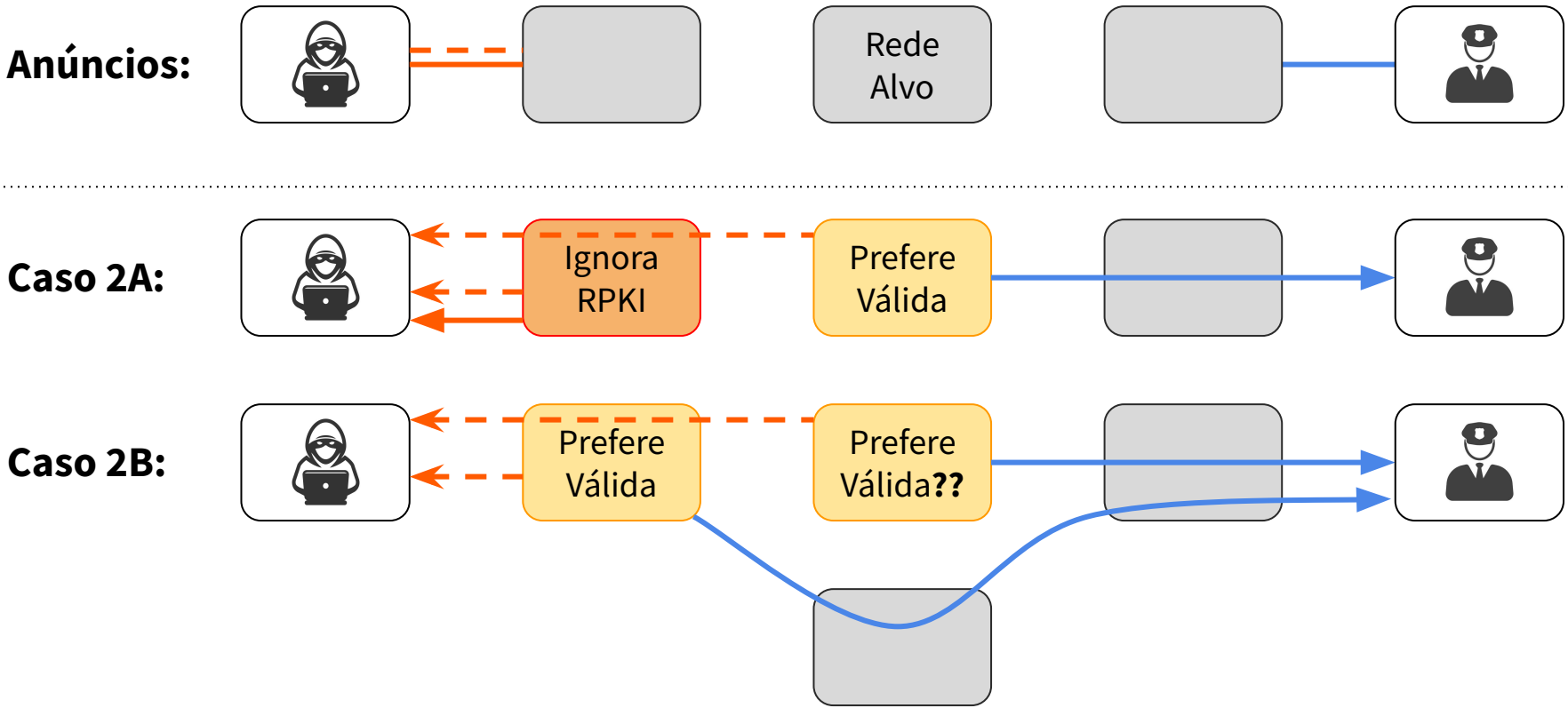
Caso 2A:



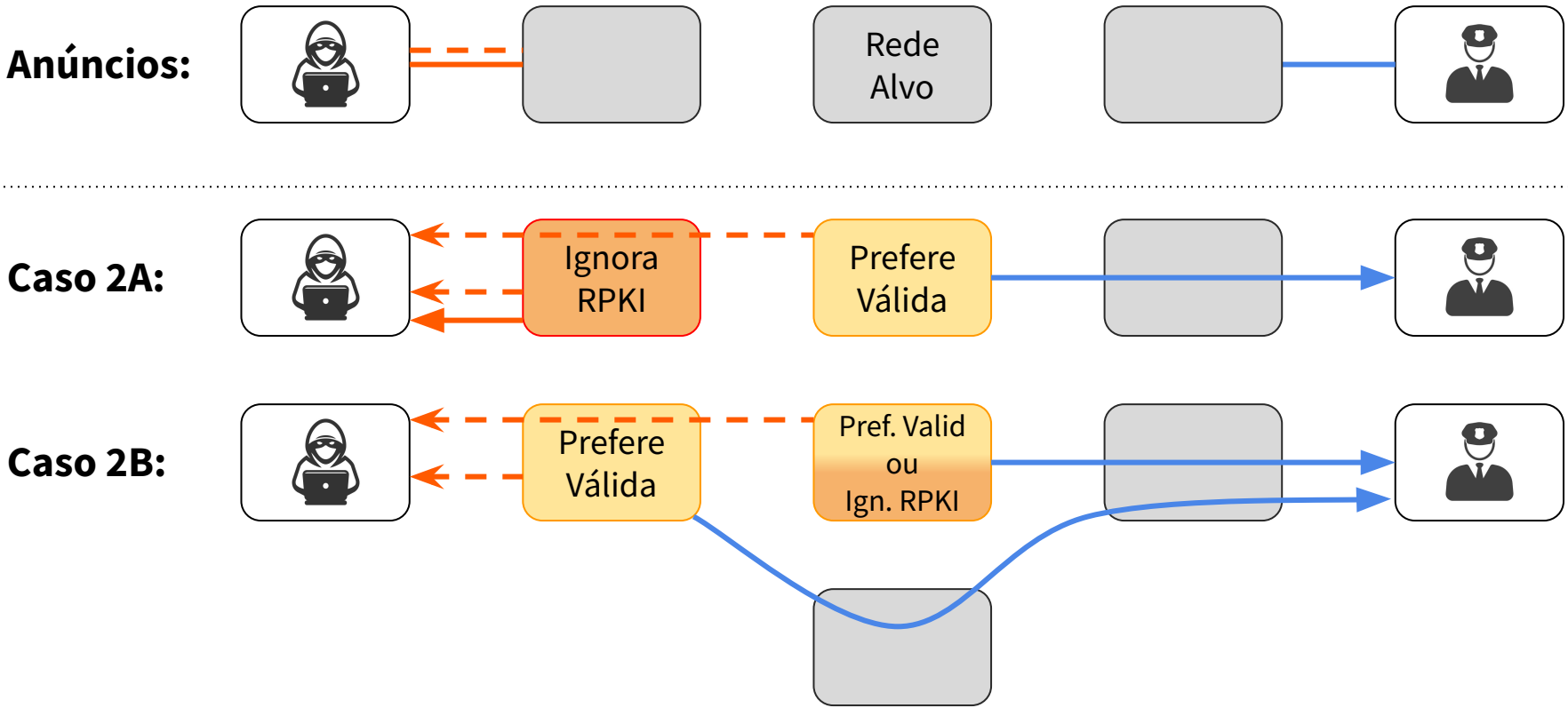
Inferindo validação de rotas



Inferindo validação de rotas



Inferindo validação de rotas



Lidando com ambiguidades

Controle limitado: sem informações sobre políticas de roteamento

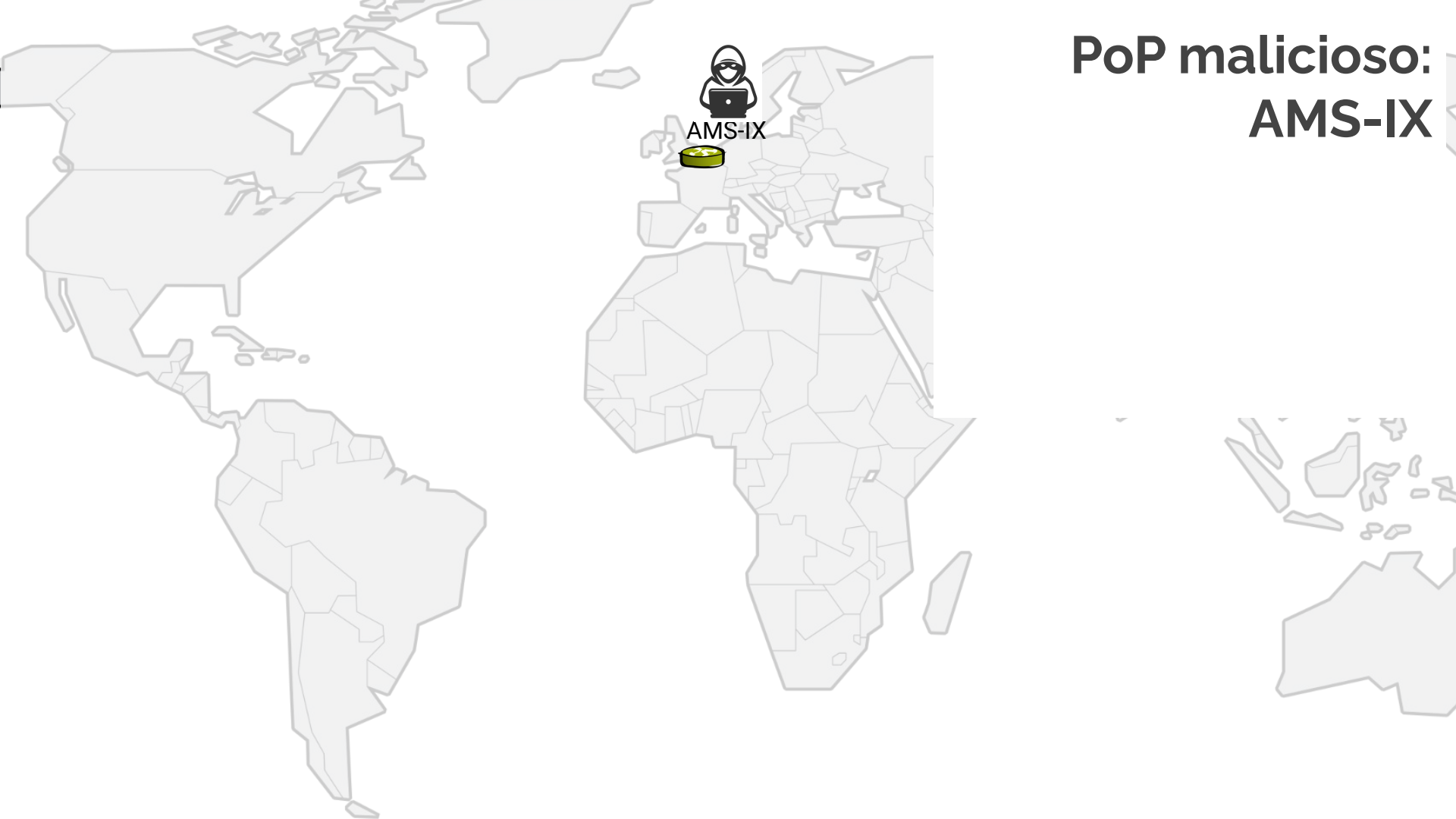
- Inferência gradual utilizando busca em largura no grafo de conectividade
  - Propagação de inferências e ambiguidades

Falta de visibilidade: nem todas as redes publicam suas rotas

- Inferir rotas disponíveis

Experimentos reais na plataforma PEERING

PoP malicioso: AMS-IX



PoP malicioso: AMS-IX

4 PoPs legítimos escolhidos aleatoriamente

Resultados

Inferência	Redes
Total	**506**

- Aumento da cobertura das inferências

Resultados

Inferência	Redes	
Descarta inválida	41	8,10%
Ignora ROA	33	6,52%
Prefere válida	7	1,38%
Total	**506**	

- Aumento da cobertura das inferências
- Quantidade significativa de redes utilizam política “prefere válida”
- Inferência exata é desafiadora
  - Depende de PoPs bem localizados para realização de anúncios

Resultados

Inferência	Redes	
Descarta inválida	41	8,10%
Ignora ROA	33	6,52%
Prefere válida	7	1,38%
Pref. válida ou ignora ROA	36	7,11%
Pref. válida ou vizinho	5	0,99%
Total	**506**	

- Aumento da cobertura das inferências
- Quantidade significativa de redes utilizam política “prefere válida”
- Inferência exata é desafiadora
  - Depende de PoPs bem localizados para realização de anúncios
- Ambiguidade permite estender inferências para mais redes

Resultados

Inferência	Redes	
Descarta inválida	41	8,10%
Ignora ROA	33	6,52%
Prefere válida	7	1,38%
Pref. válida ou ignora ROA	36	7,11%
Pref. válida ou vizinho	5	0,99%
Protegido	280	55,34%
Oculto	104	20,55%
Total	**506**	

- Aumento da cobertura das inferências
- Quantidade significativa de redes utilizam política “prefere válida”
- Inferência exata é desafiadora
  - Depende de PoPs bem localizados para realização de anúncios
- Ambiguidade permite estender inferências para mais redes

Resultados

Inferência	Redes	
Descarta inválida	41	8,10%
Ignora ROA	33	6,52%
Prefere válida	7	1,38%
Pref. válida ou ignora ROA	36	7,11%
Pref. válida ou vizinho	5	0,99%
Protegido	280	55,34%
Oculto	104	20,55%
Total	**506**	

- Aumento da cobertura das inferências
- Quantidade significativa de redes utilizam política “prefere válida”
- Inferência exata é desafiadora
  - Depende de PoPs bem localizados para realização de anúncios
- Ambiguidade permite estender inferências para mais redes
- Inferências são consistentes entre diferentes experimentos
- As duas fases do algoritmo são essenciais para evitar erros

Conclusões

Novo algoritmo para inferência de validação de rotas

- Maior cobertura e precisão que trabalhos anteriores
- Capaz de identificar redes que utilizam a política “prefere válida”

Dados públicos

- Nossos resultados estão disponíveis para *download* e podem ser visualizados via uma interface Web

Resultados indicam aumento da adoção do RPKI por operadores

- Melhoria da segurança do roteamento na Internet

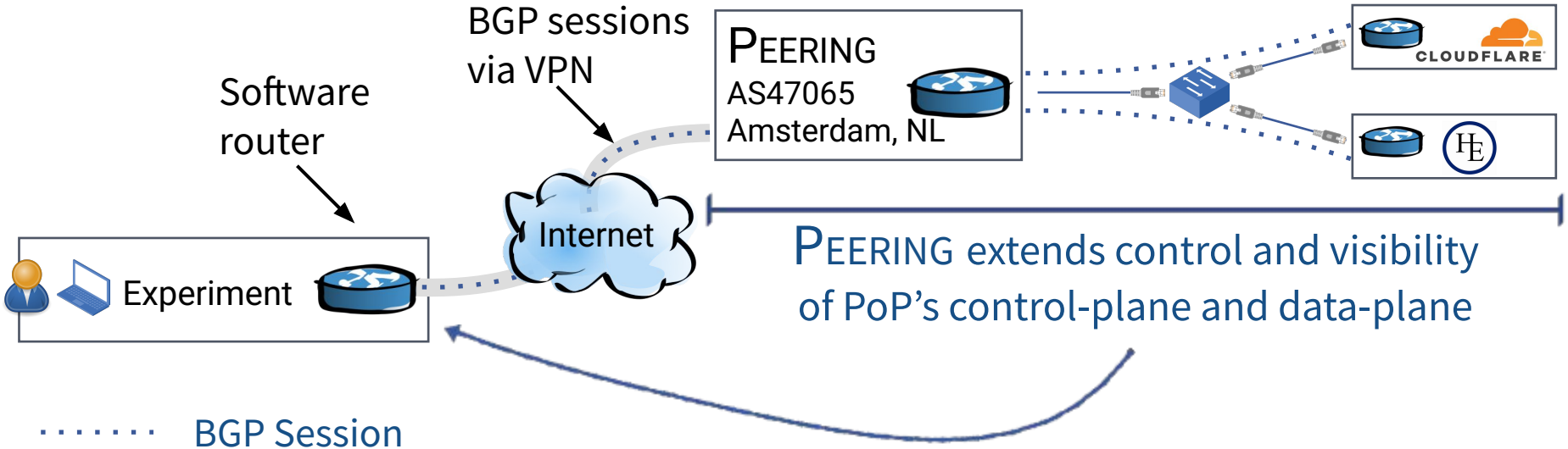
Identificação de Políticas de Validação de Rotas no RPKI

Marcel Mendes
Leonardo Oliveira
Ítalo Cunha (cunha@dcc.ufmg.br)
Ethan Katz-Bassett

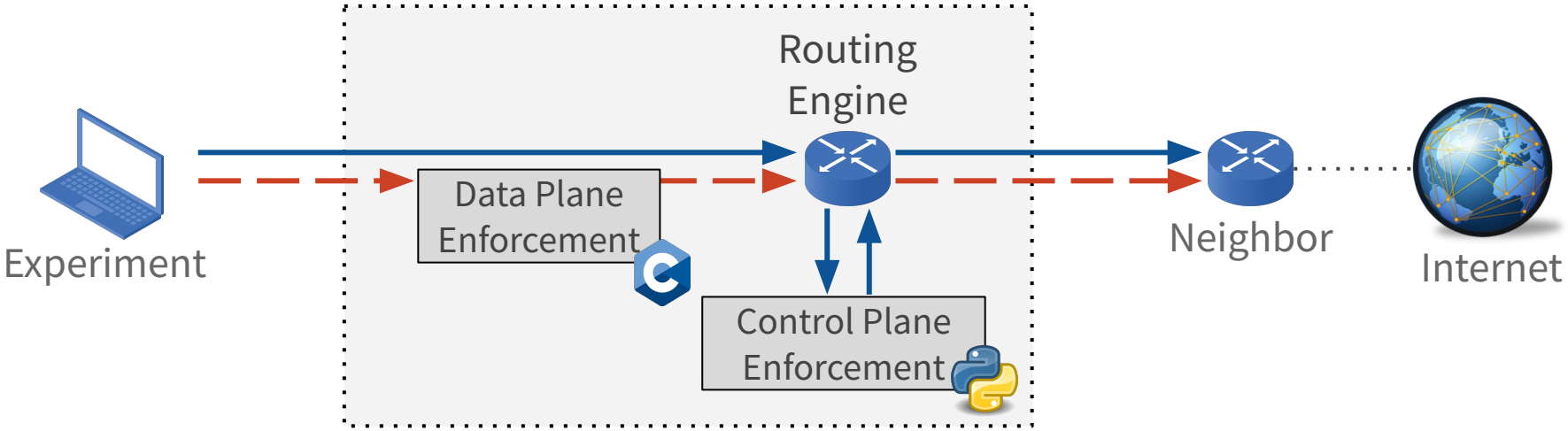
UFMG

Columbia University

Connecting to PEERING PoPs



PEERING's Security Framework



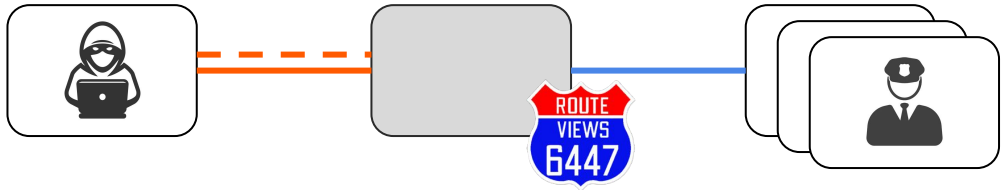
Enforcement engines programmed
in general-purpose languages

Control Plane

Data Plane

Inferindo validação de rotas

Anúncios:

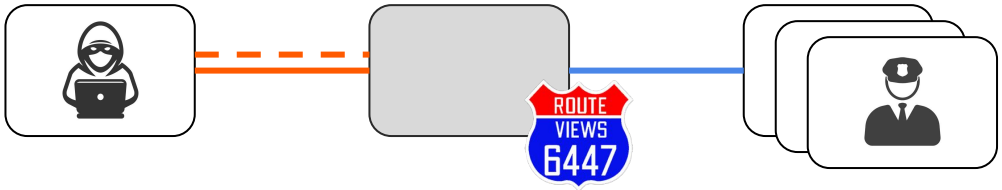


Anúncios de dois prefixos com configurações distintas

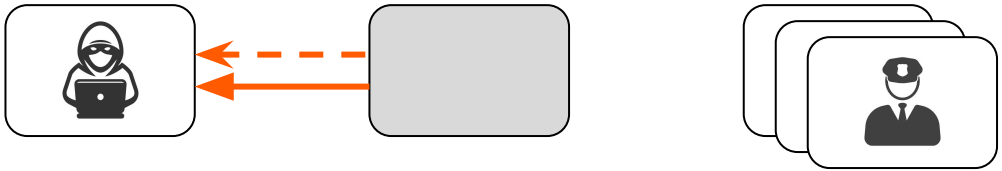
- Anúncios de dois pontos de presença (PoPs): malicioso e legítimo
- Prefixo 1: **Inválido** do PoP malicioso
- Prefixo 2: **Inválido** curto do PoP malicioso
  & **válido** longo do PoP legítimo

Inferindo validação de rotas

Anúncios:

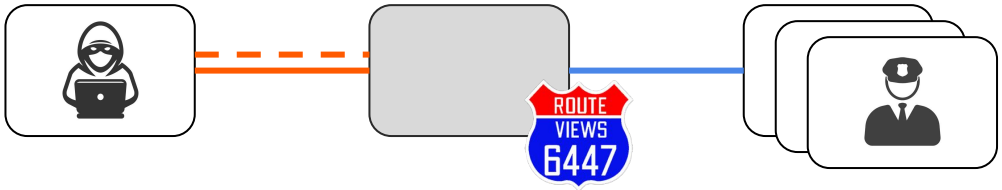


Caso 1:

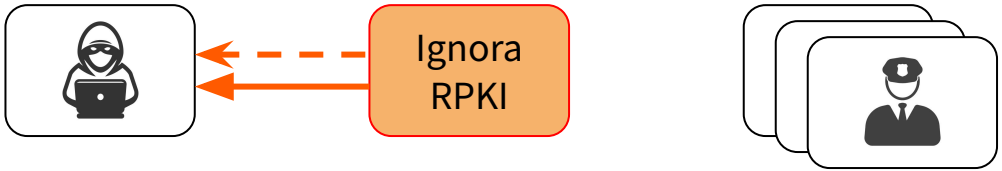


Inferindo validação de rotas

Anúncios:

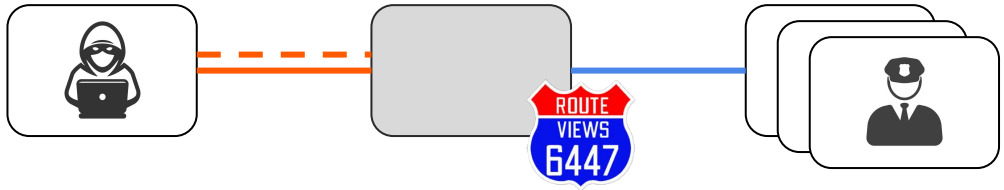


Caso 1:

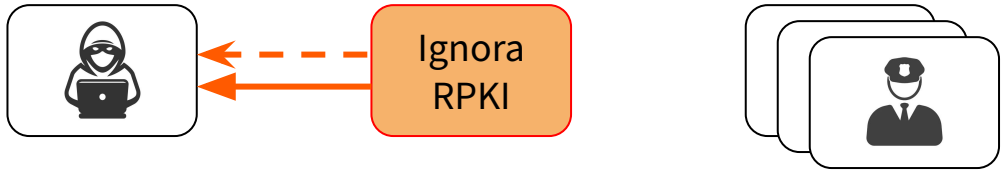


Inferindo validação de rotas

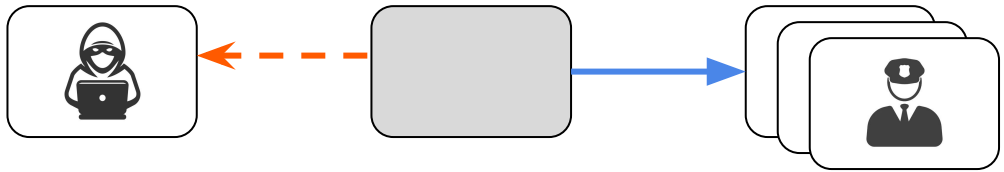
Anúncios:



Caso 1:

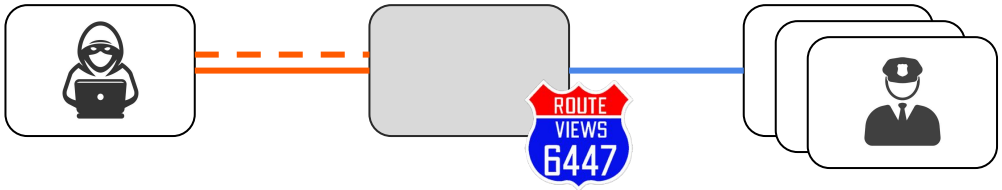


Caso 2:

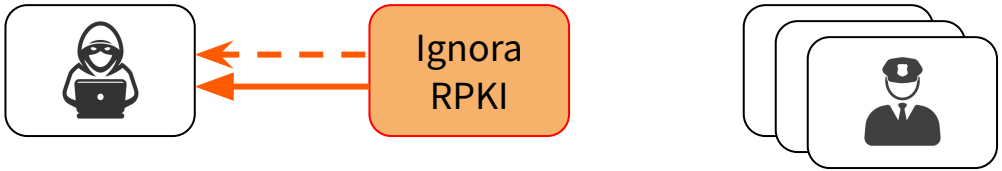


Inferindo validação de rotas

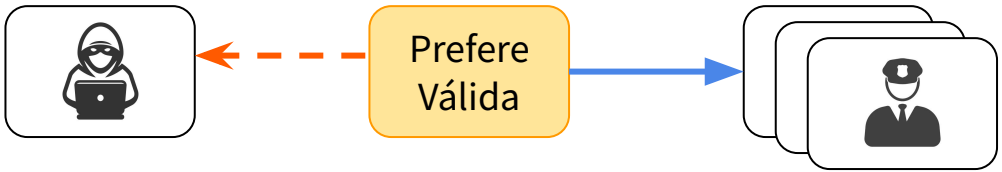
Anúncios:



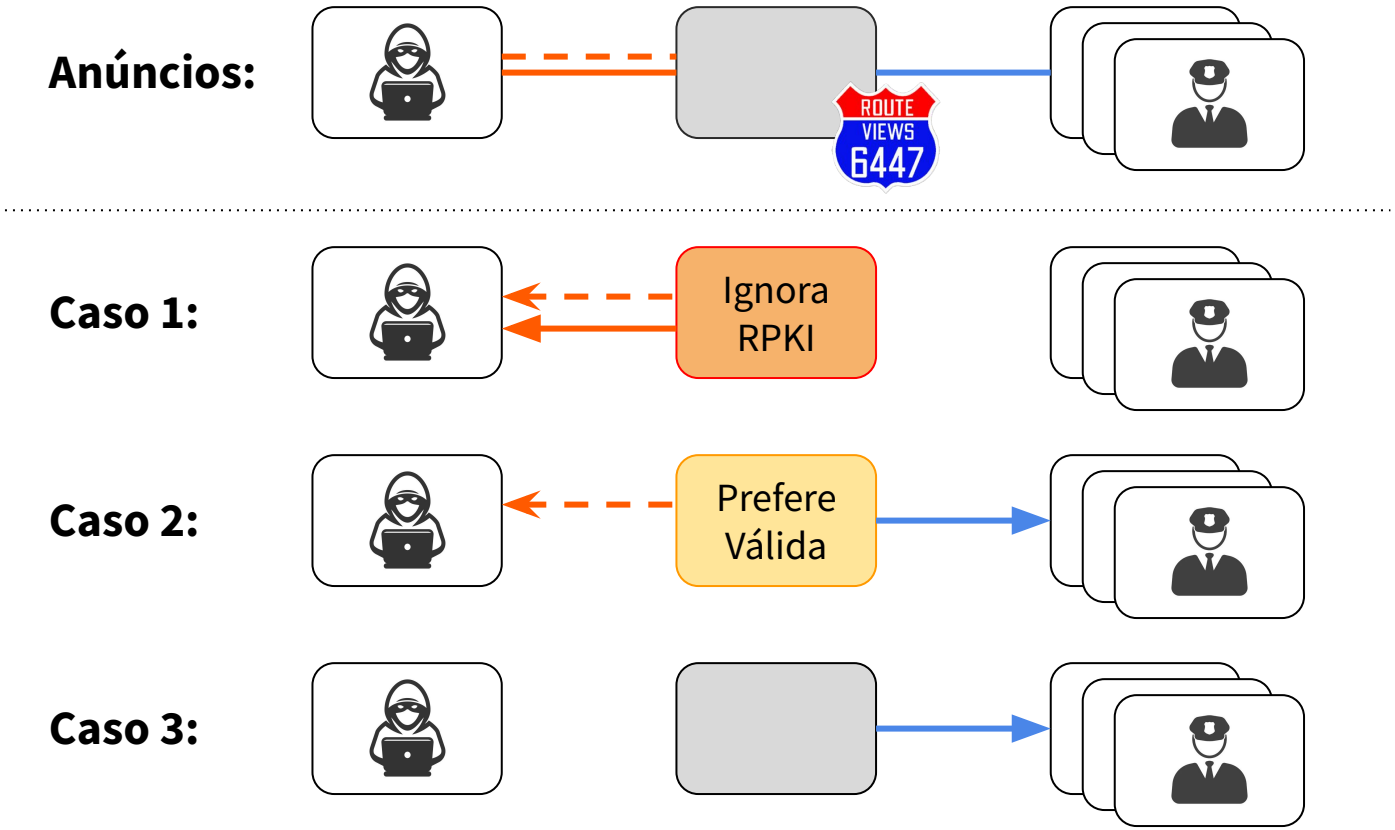
Caso 1:



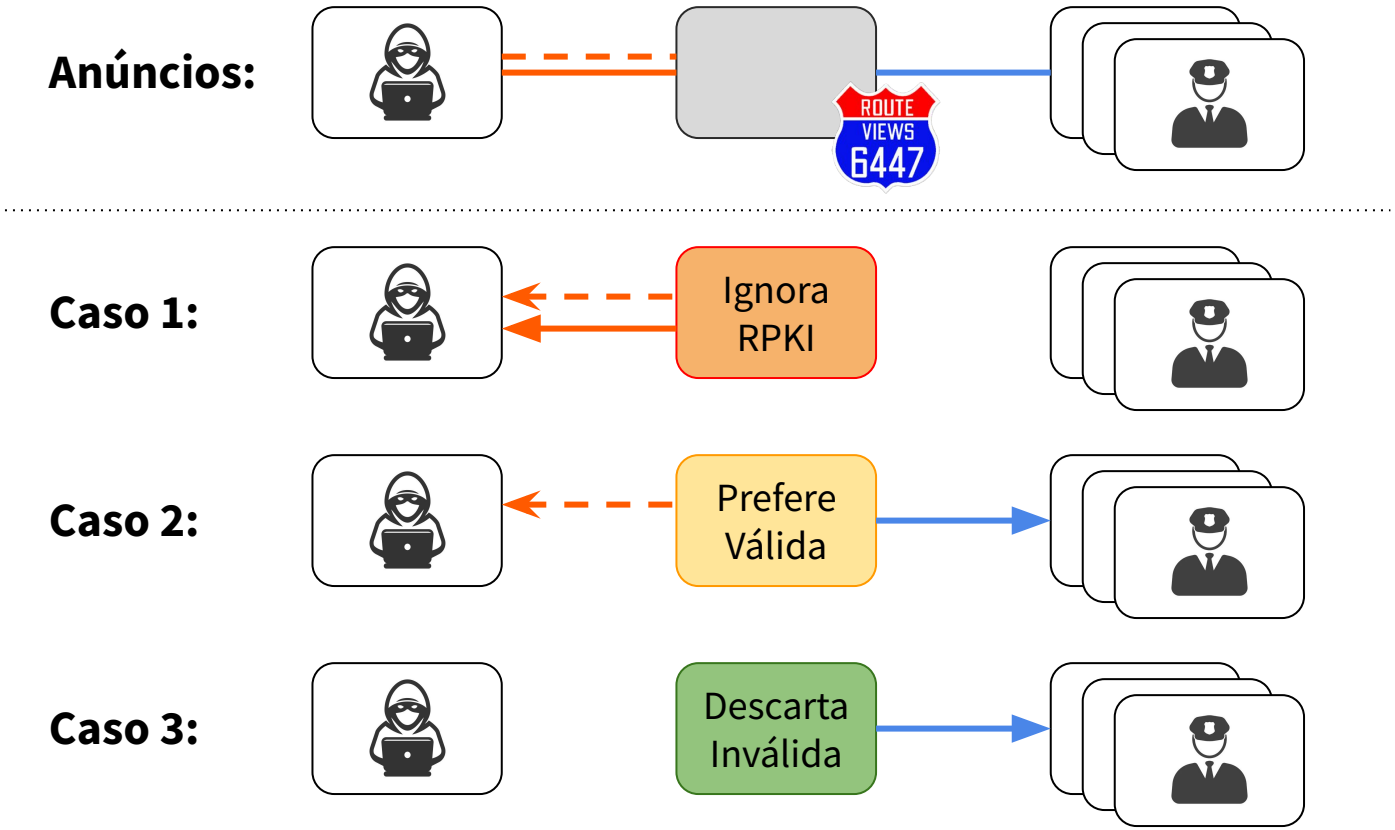
Caso 2:



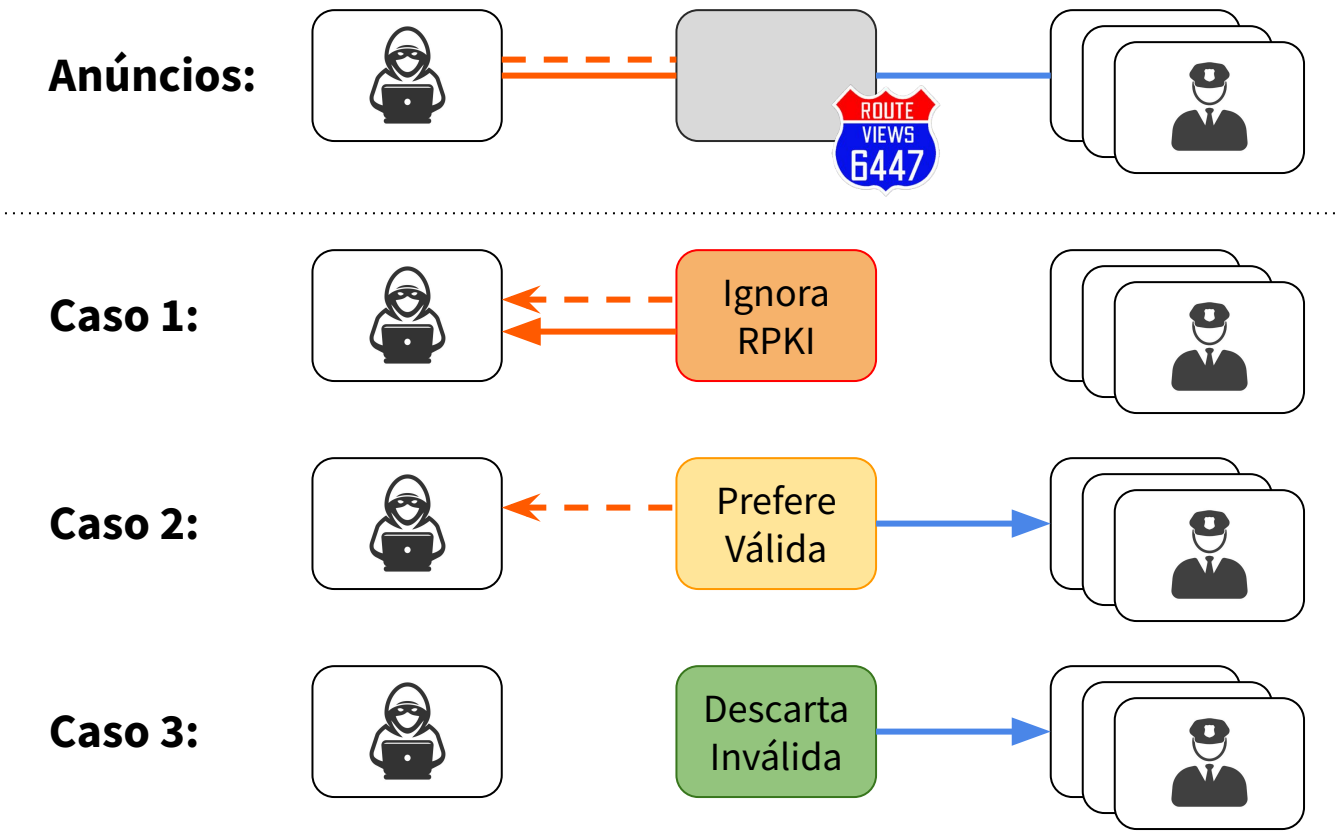
Inferindo validação de rotas



Inferindo validação de rotas



Inferindo validação de rotas



Desafios:

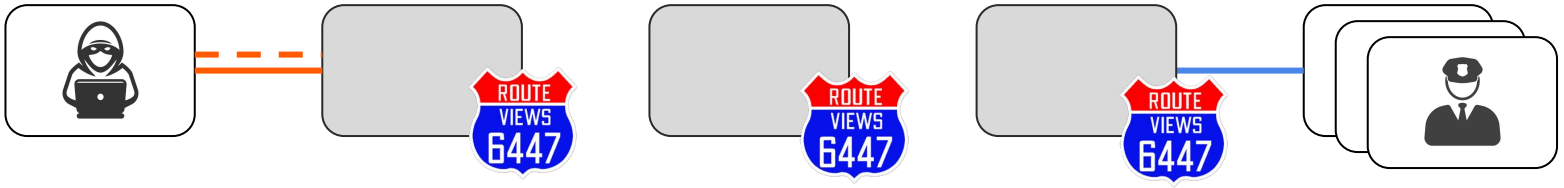
- Falta de visibilidade
- Controle limitado

Estes cenários:

- Visibilidade da rota
- Controle do anúncio

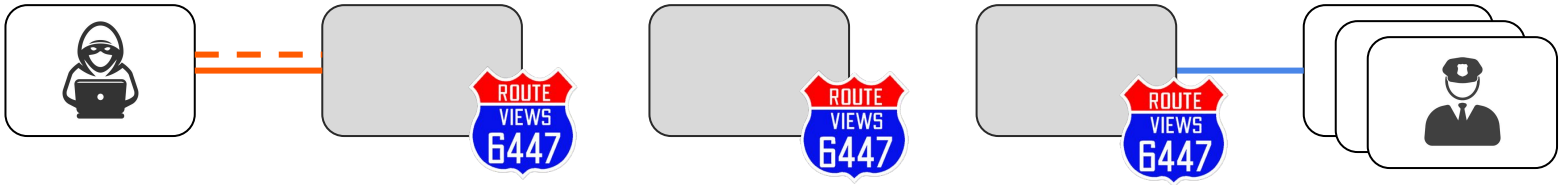
Inferindo validação de rotas

Anúncios:

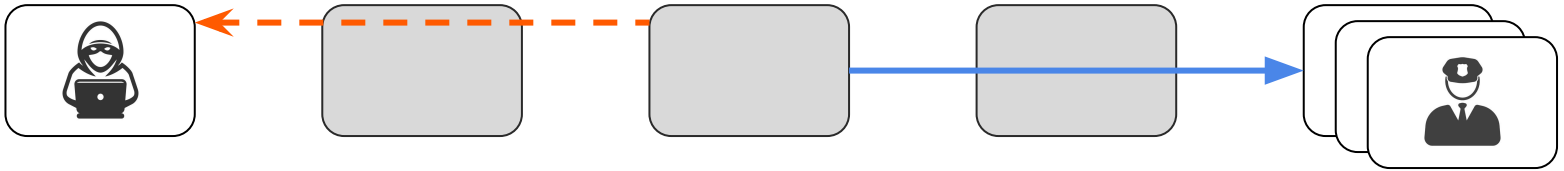


Inferindo validação de rotas

Anúncios:

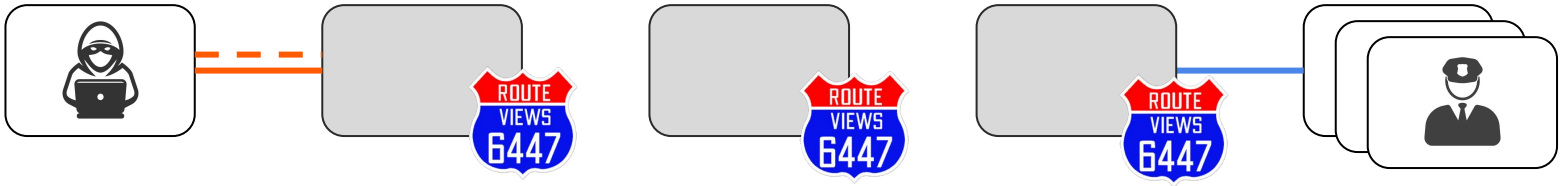


Caso 2A:

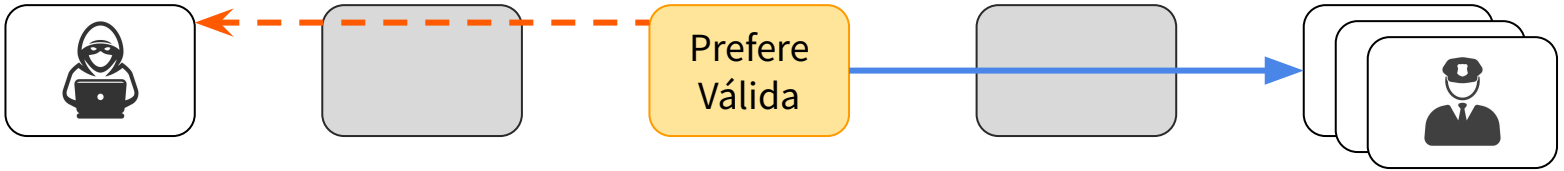


Inferindo validação de rotas

Anúncios:

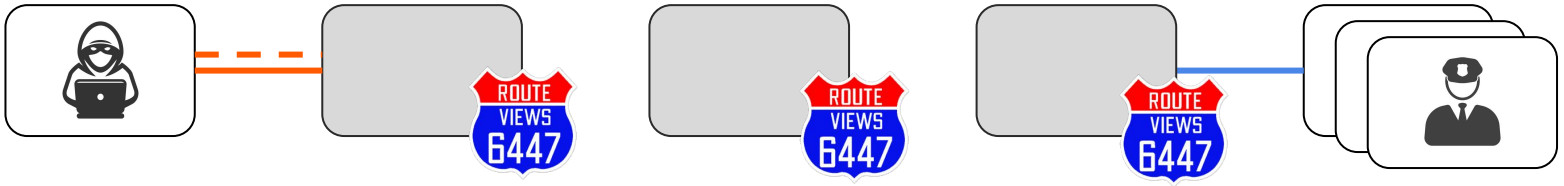


Caso 2A:

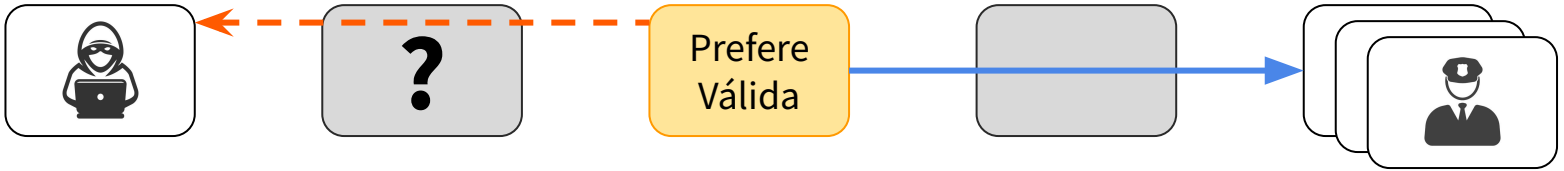


Inferindo validação de rotas

Anúncios:

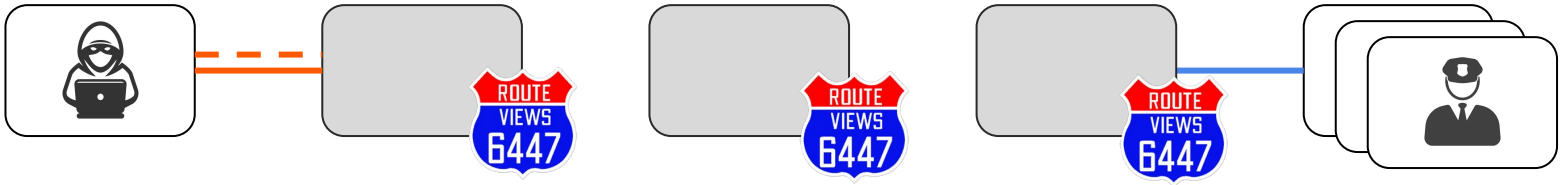


Caso 2A:

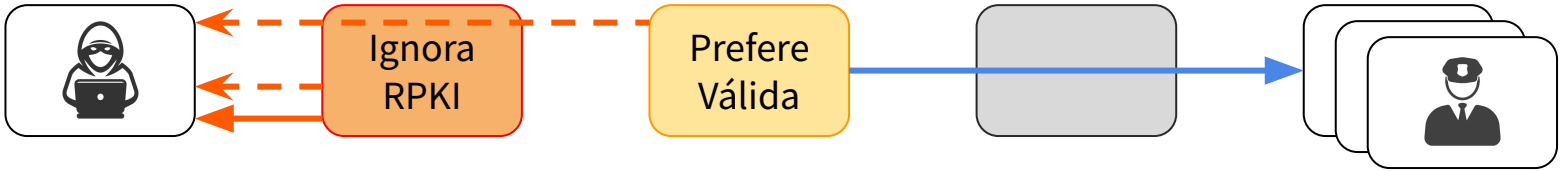


Inferindo validação de rotas

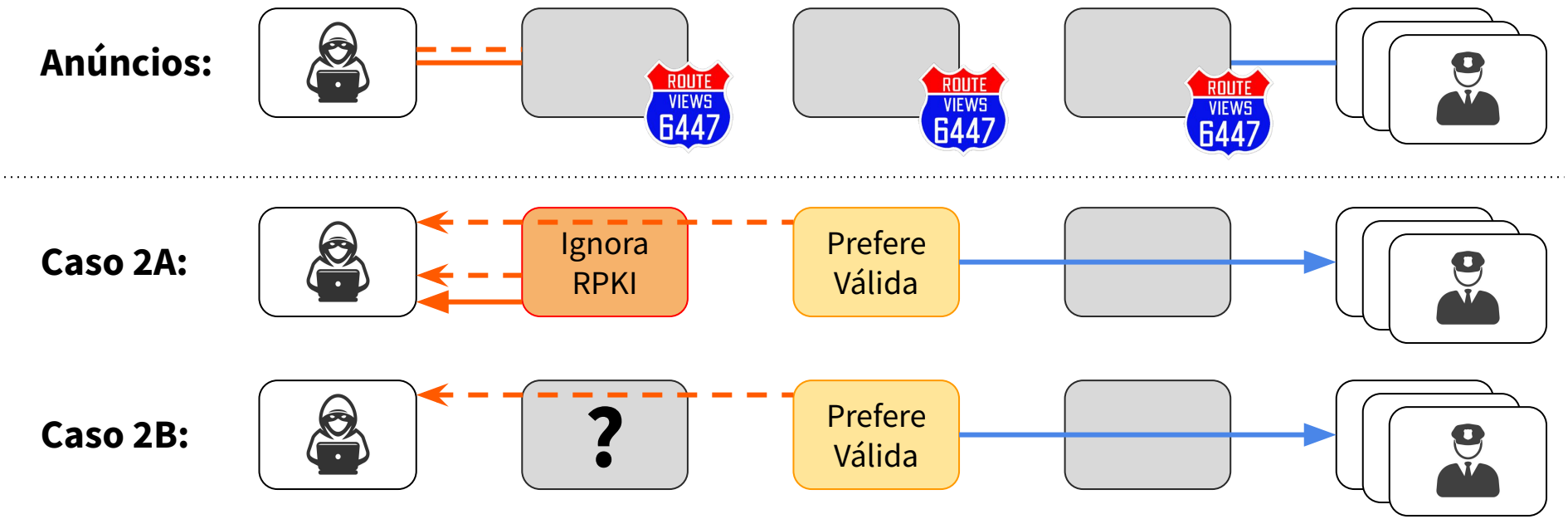
Anúncios:



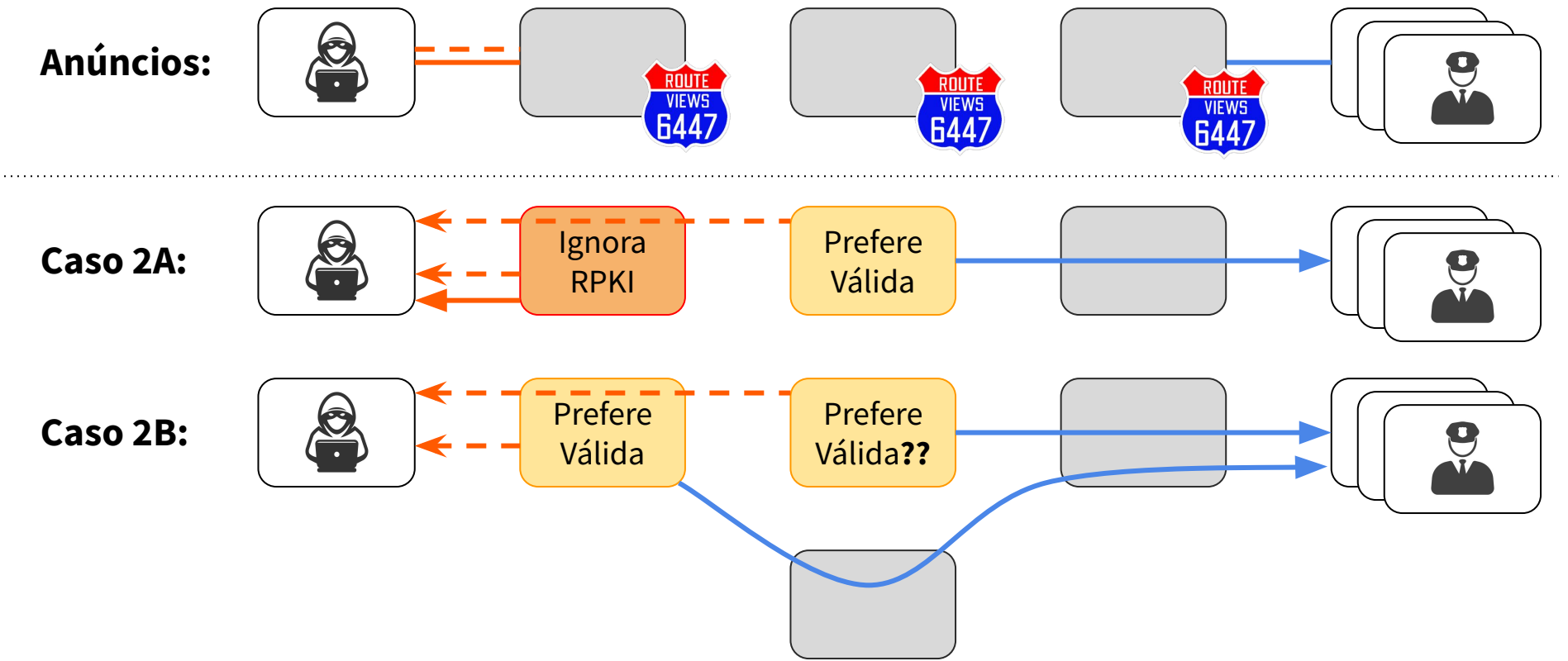
Caso 2A:



Inferindo validação de rotas



Inferindo validação de rotas



Inferindo validação de rotas