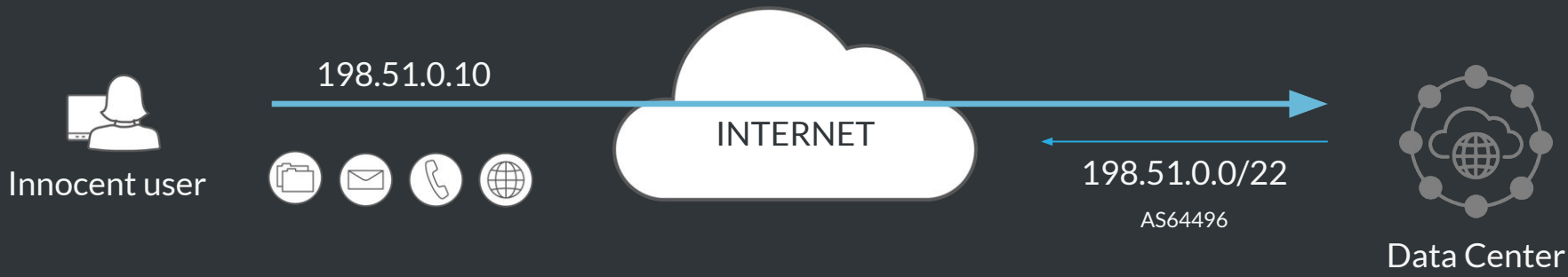
DisNOG 1

Routing Security and RPKI

Melchior Aelmans, Juniper Networks

The Perfect world



Prefix filters, IRR filtering, Peer lock, etc. are all In place?

- Prefix filters
- Peer lock
- “Bignetworks” filter
- Bogon ASN filtering
- Bogon Prefix filtering
- Filter long ASN path
- Filter small prefixes
- IRR filtering

The Perfect world…or not (yet)?

I know all my customers and most peers and have filters and strict IRR applied.

However,…

- Prefix filters don’t care about the originating ASN or AS-PATH
- Peer Lock doesn’t cover every network and is arbitrary
- Filtering small prefix outbound is an issue for DDoS mitigation
- Downstream customers might use private ASN
- IRR databases are far from correct, are incomplete or contain outdated data

BGP Hijacking is happening

June 2019 - European telecommunication networks

- Swiss datacenter hosting company accidentally leaked over 70,000 routes from its internal routing table to China Telecom.
- China Telecom re-announced these routes as its own and declared itself as the shortest way to reach the network of the Swiss datacenter operator and other nearby European telecommunication companies and ISPs.
- Incident lasted over two hours. Users suffered slow connections and denial of service to some servers.

April 2020 - Akamai, Amazon and Alibaba

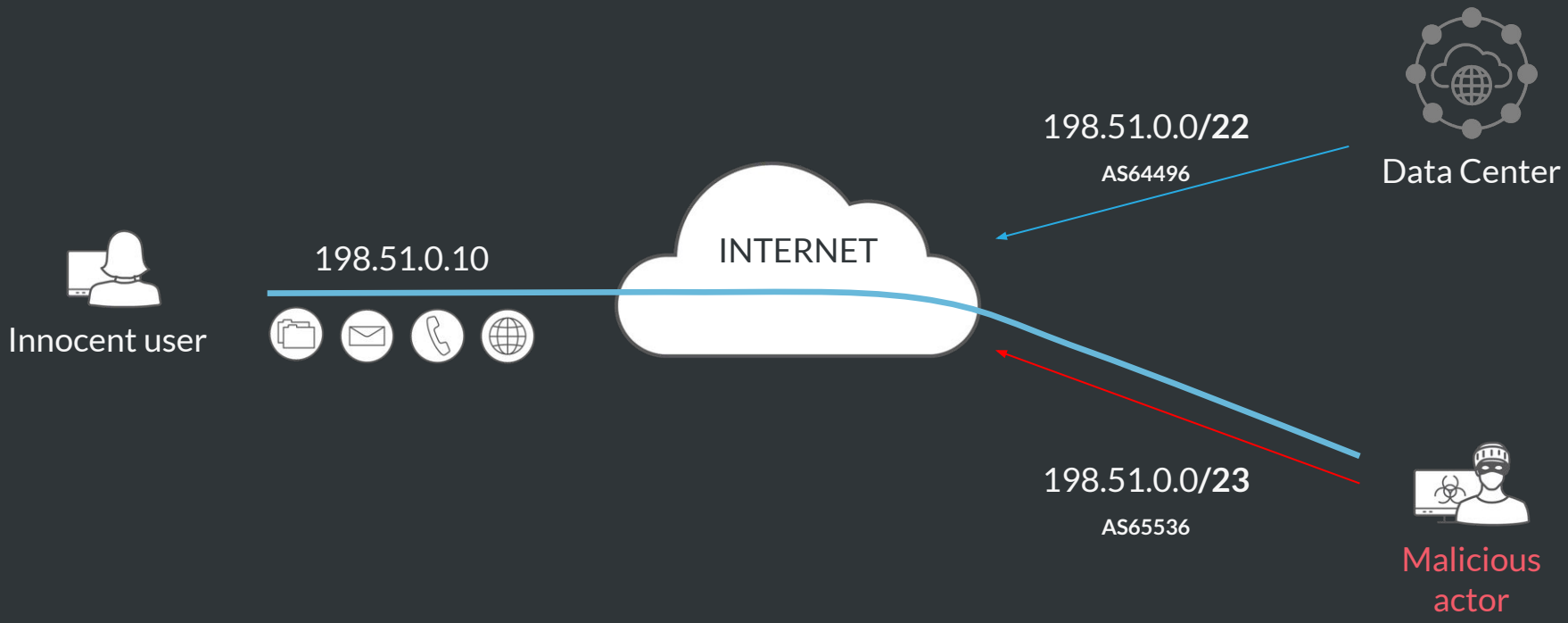
- A massive BGP hijack involving over 8,800 prefixes affected companies such as Akamai, Amazon and Alibaba on April 1, 2020.
- Initiated by a Rostelecom user, the attack caused service disruptions throughout the world.
- Stricter network filtering by Rostelecom could have prevented the attack.

September 2020 - Telstra

- 500 prefixes wrongfully advertised as belonging to Telstra caused lengthy data detours.
- Incident was caused by post verification testing to address an unrelated software bug.

Source: https://www.anapaya.net/blog/border-gateway-protocol-hijacking-examples-and-solutions

What happened to our innocent user?



So now what? Origin Validation using Resource Public Key Infrastructure

Photo by Markus Spiske on Unsplash

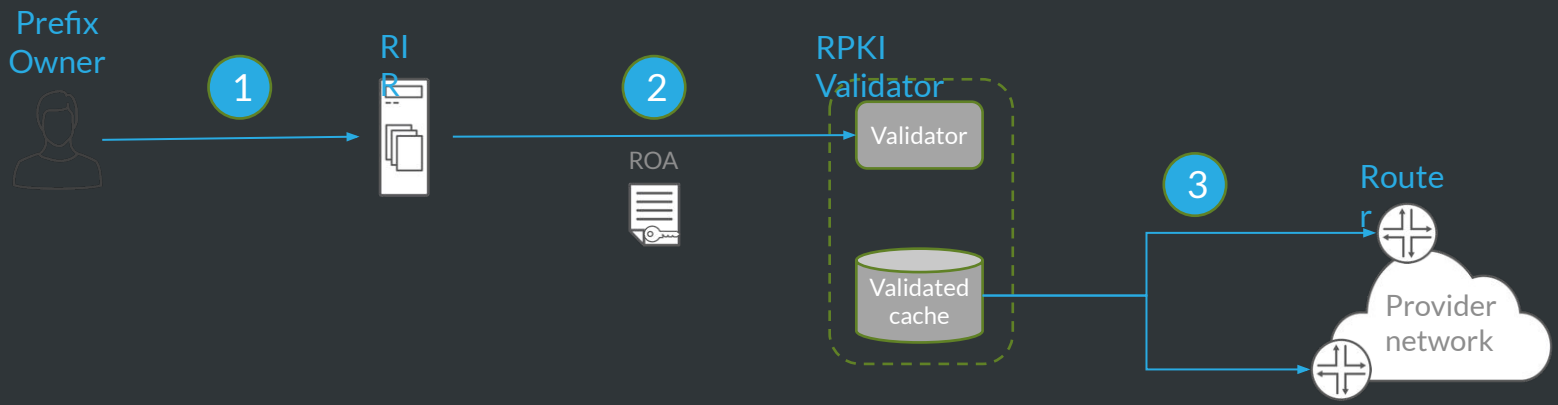
Origin Validation using RPKI

Resource Public Key Infrastructure (RPKI) is a method of cryptographic signing records that associate a prefix with an originating AS number.

All the five RIRs (AFRINIC, APNIC, ARIN, LACNIC & RIPE) provide a method for members to take a prefix/ASN pair and sign those with a Route Origin Authorization (ROA) record.

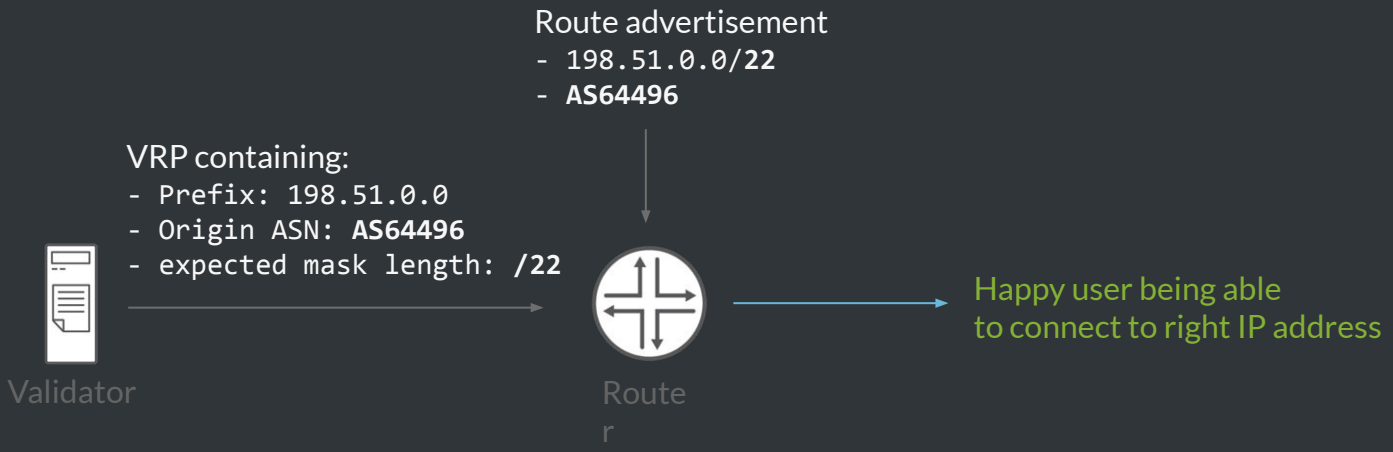
The ROA can then be used by operators to validate route advertisements. They can be sure a route advertisement is intended by the legitimate owner.

Origin validation explained

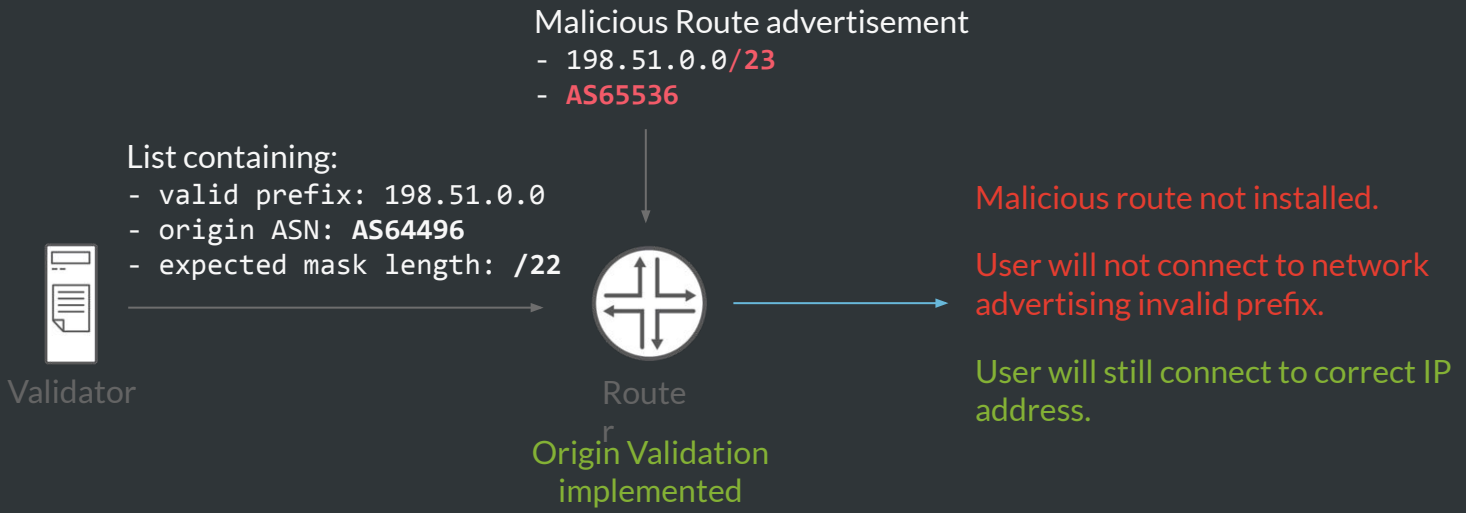


1. The prefix holder creates a (signed) ROA with the RIR
2. The RPKI validator downloads the ROAs, verifies them and builds a database with Validated ROA Payloads (VRPs)
3. RPKI validator sends VRP to border routers that validate the BGP routes

Perfect world routing

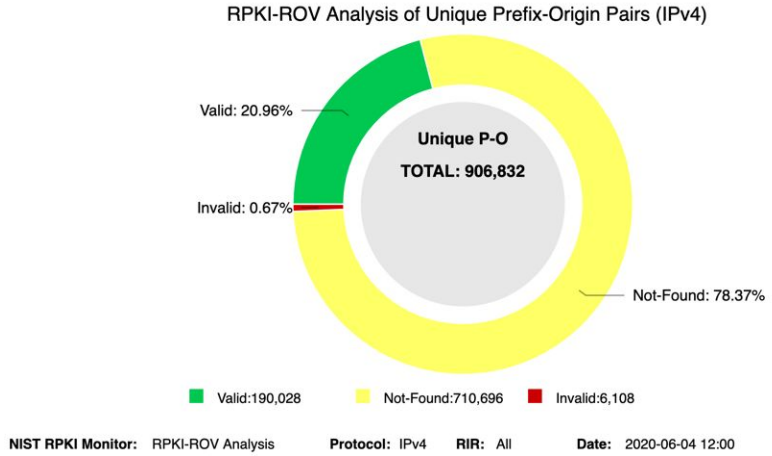


Mitigating a BGP Route Hijack

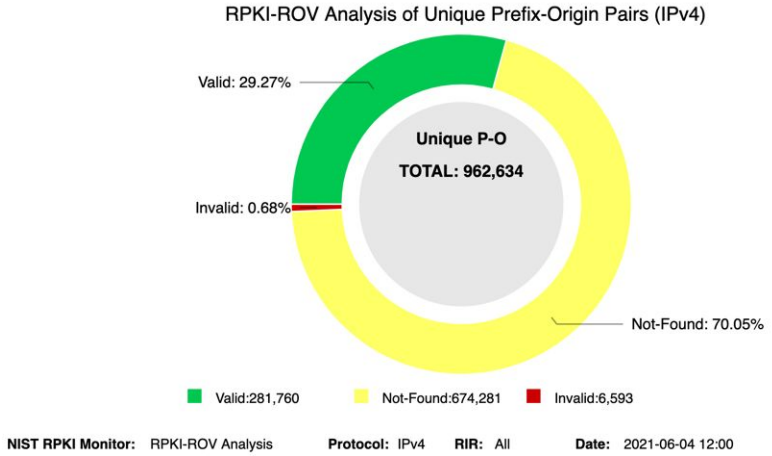


But…only if the world was perfect

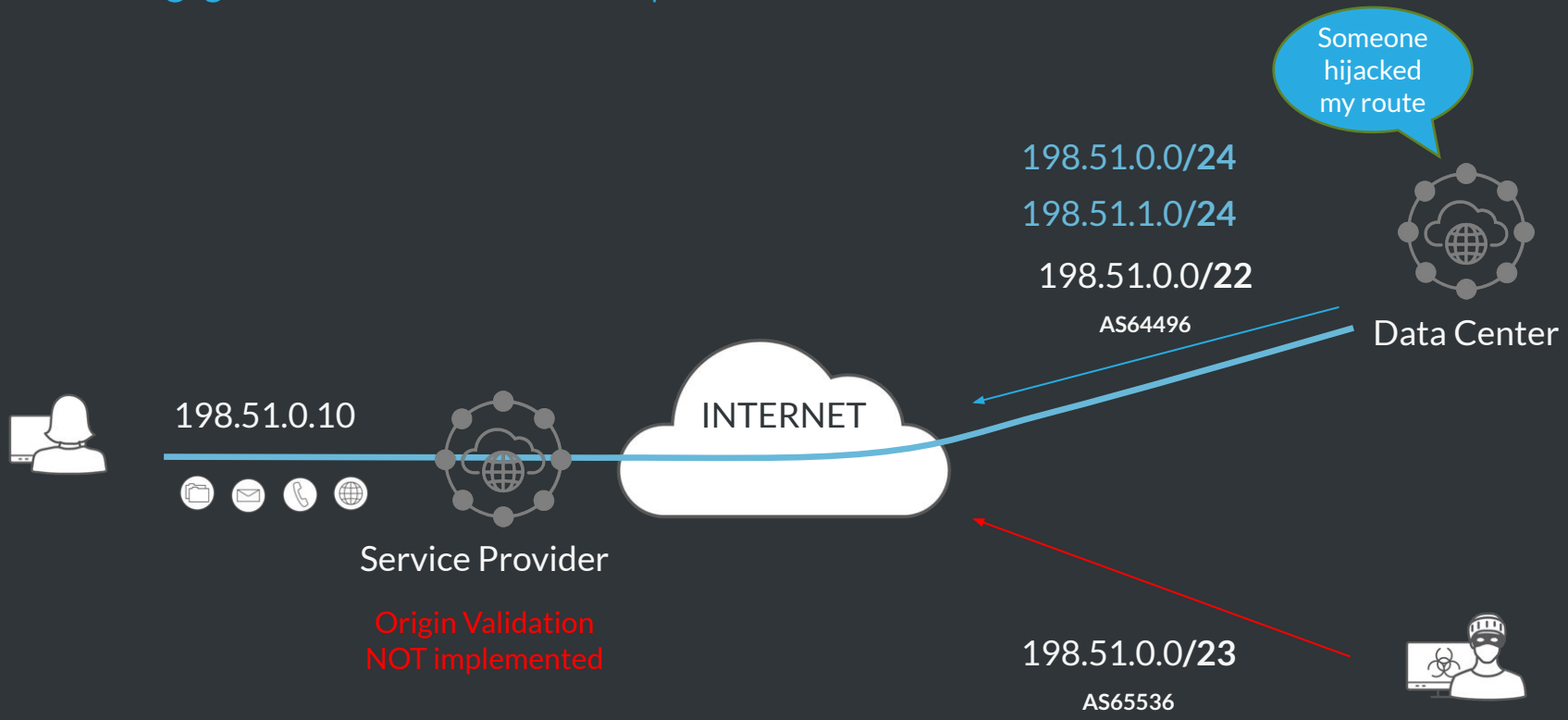
June 2020
(Valid: ~21%)



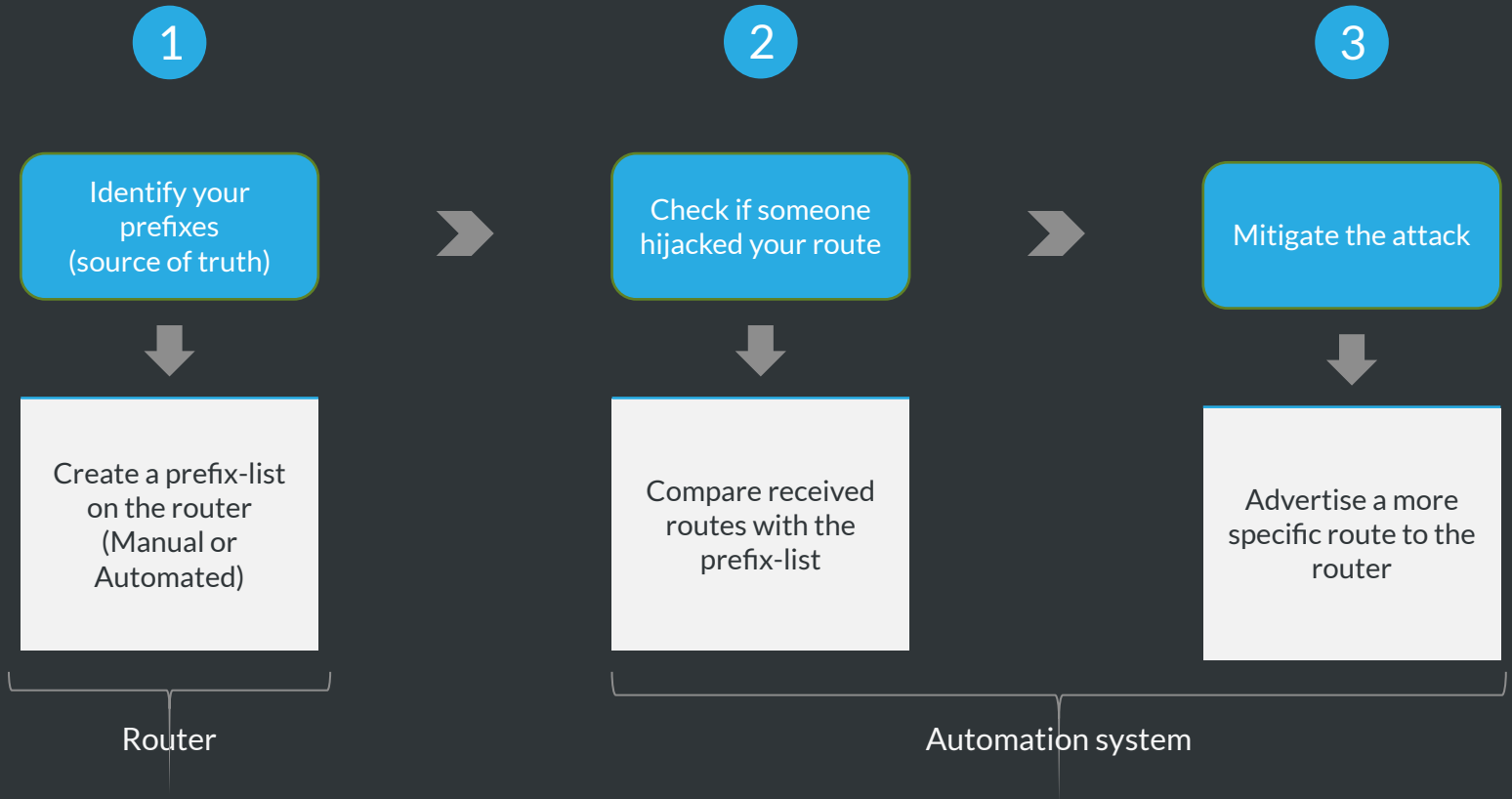
June 2021
(Valid: ~29%)



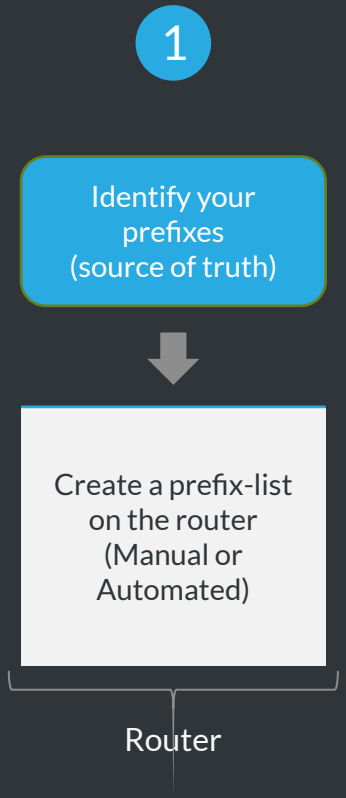
Protecting your network in an imperfect world



3 steps to detect & mitigate route hijacks with Automation

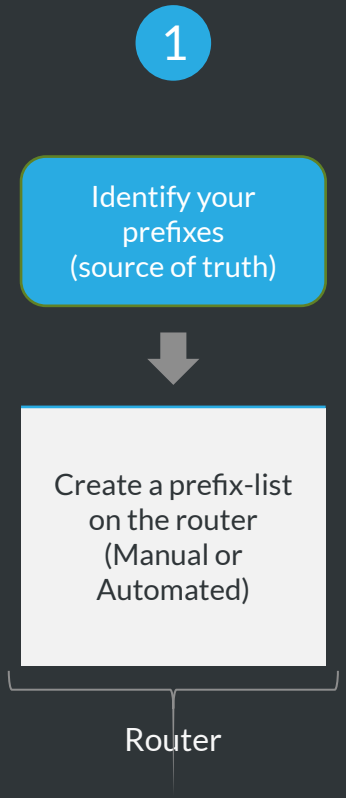


3 steps to detect & mitigate route hijacks with Automation




```
policy-options {
    prefix-list AS64496-prefixes {
        198.51.0.0/22;
    }
}
```

3 steps to detect & mitigate route hijacks with Automation




```
policy-options {
    policy-statement hijack-check {
        term invalid-myprefixes {
            from {
                protocol bgp;
                prefix-list-filter AS64496-prefixes
orlonger;
            }
            then {
                community add HIJACKED;
                reject;
            }
        }
    }
    community HIJACKED members 64496:666;
    community MITIGATED members 64496:2222;
    community MYCUSTOMERS members 64496:9999;
    community MYROUTES members 64496:1000;
}
```

```
protocols {
    bgp {
        group ebgp {
            type external;
            import hijack-check;
            family inet {
                unicast;
            }
            export [ EXPORT-PEER deny-all ];
            neighbor 17.8.2.2 {
                peer-as 200;
            }
            neighbor 17.8.3.2 {
                peer-as 300;
            }
        }
    }
}
```

3 steps to detect & mitigate route hijacks with Automation

2

Check if someone hijacked your route

Compare received routes with the prefix-list

Automation system

```
root@isp-r1> show route community 64496:666 all

inet.0: 781928 destinations, 2345613 routes (781922 active, 0 holddown, 781864
hidden)
+ = Active Route, - = Last Active, * = Both

198.51.0.0/23          [BGP ] 00:01:17, localpref 100
                       AS path: 200 65535 I, validation-state: unverified
                     > to 17.8.2.2 via ge-0/0/2.0
```

Someone hijacked my route

Automation system
(for example Paragon Insights)

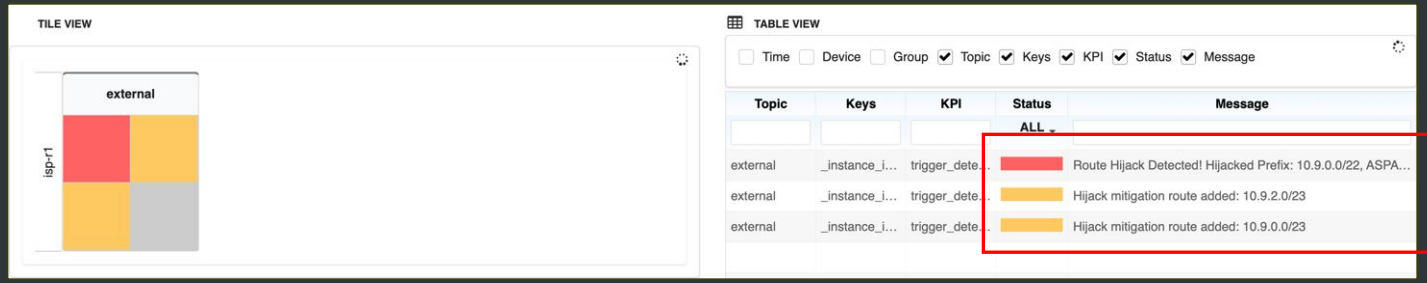
3 steps to detect & mitigate route hijacks with Automation

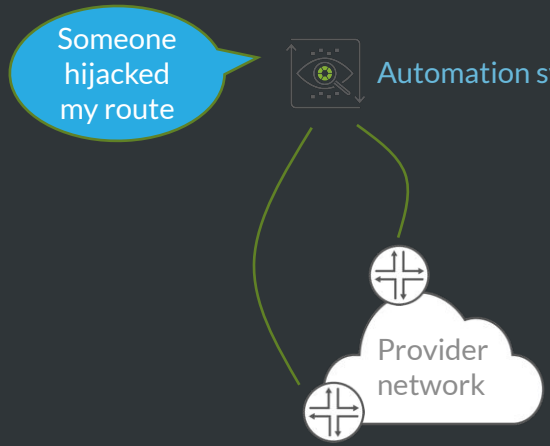
2

Check if someone hijacked your route

Compare received routes with the prefix-list

Automation system





3 steps to detect & mitigate route hijacks with Automation

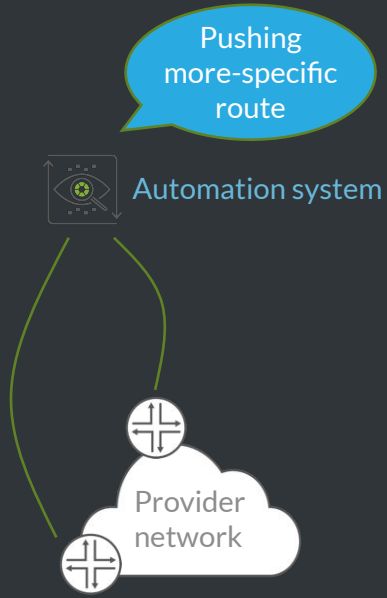
3

Mitigate the attack

Advertise a more specific route to the router

Automation system

```
root@isp-r1# show groups __automation_routeHijack__
routing-options {
    static {
        route 198.51.0.0/24 {
            discard;
            no-install;
            community 64496:2222;
        }
        route 198.51.1.0/24 {
            discard;
            no-install;
            community 64496:2222;
        }
    }
}
```



Ready? Call to action!

To Do:

- Sign your Prefixes (create ROAs)
- Setup a Validator
- Configure your routers
- Support work in IETF and the RIRs

Start now: make the internet more reliable and secure!

So, are we safe now?

Unfortunately not…we still need another parachute.

Or in other words, we can now perform Origin Validation for IP prefixes but spoofing the originating ASN is still possible.

More work is to be done…

There is work in IETF addressing this problem:

https://datatracker.ietf.org/doc/draft-azimov-sidrops-aspa-profile/

...and...

https://datatracker.ietf.org/doc/draft-ietf-grow-rpki-as-cones/

Questions?

Or sent me an email:
maelmans@juniper.net

Or look for Melchior Aelmans on:
Twitter & LinkedIn

Start now: make the internet more reliable and secure!