SECURING THE INTERNET – VALIDATING ROUTING WITH RPKI

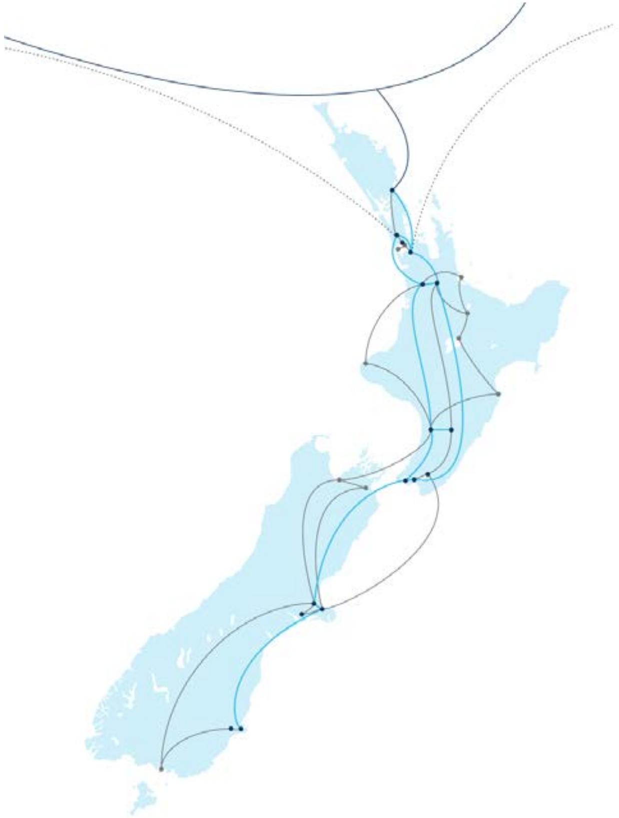
AARON MURRIHY
aaron.murrihy@reannz.co.nz

REANNZ

ABOUT US

REANNZ

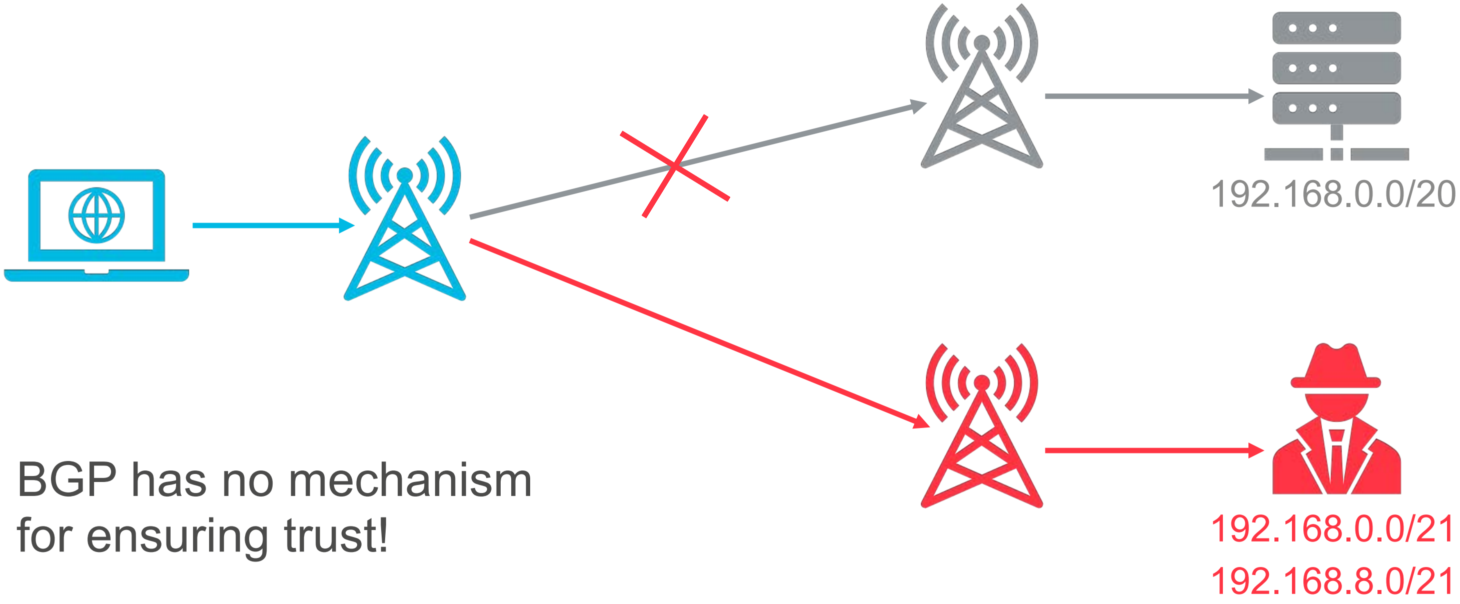
- New Zealand's NREN
- Engineering team of 7
- AS38022
- Peering points in 3 countries
  - NZ, Australia, US
- 100G backbone



THE PROBLEM

PROBLEM

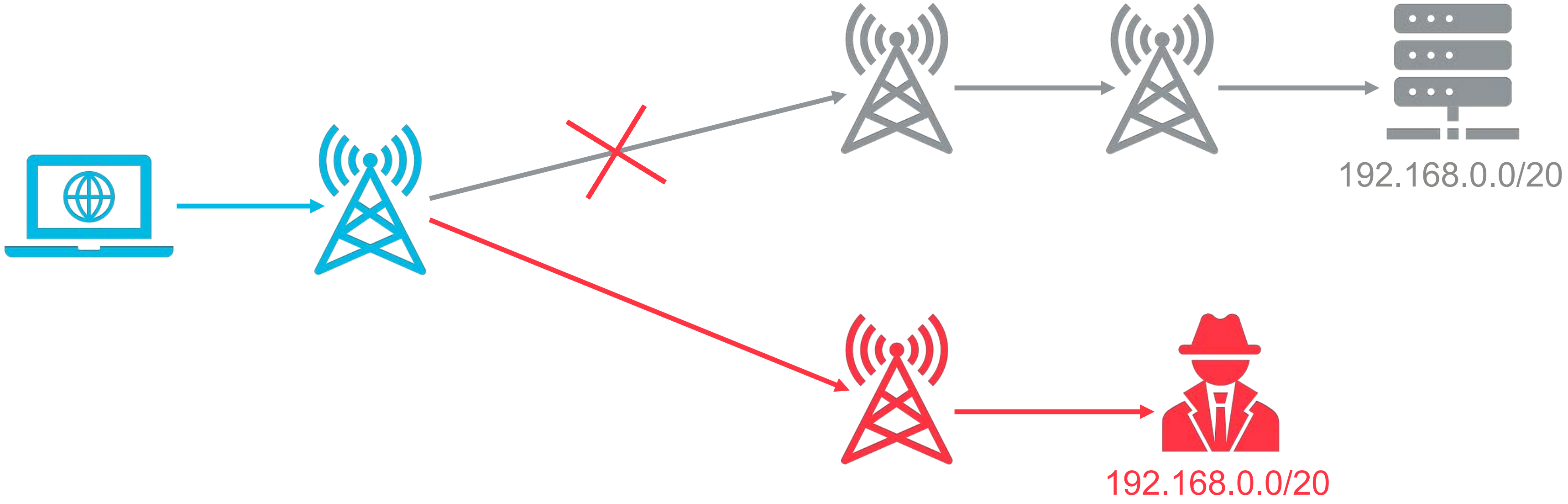
ROUTE HIJACKING



BGP has no mechanism for ensuring trust!

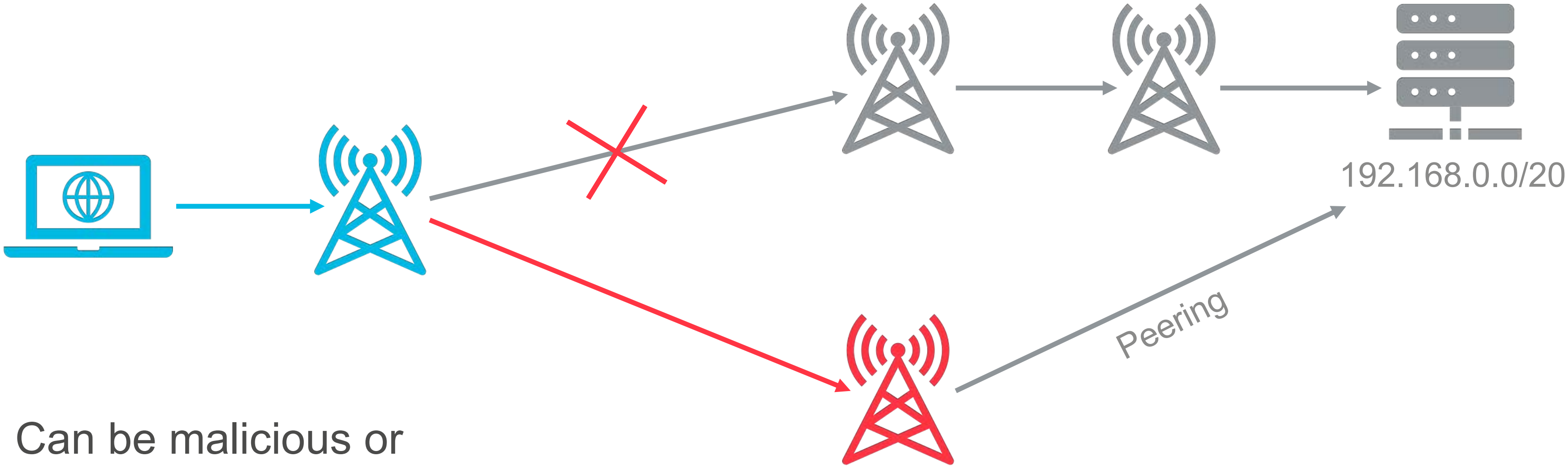
PROBLEM

ROUTE HIJACKING



PROBLEM

ROUTE HIJACKING



Can be malicious or accidental

MITIGATIONS

- Route filters based on IRR information
  - Which registry?
  - What about transit providers?
  - Still no mechanism for ensuring trust
- Or…

RPKI

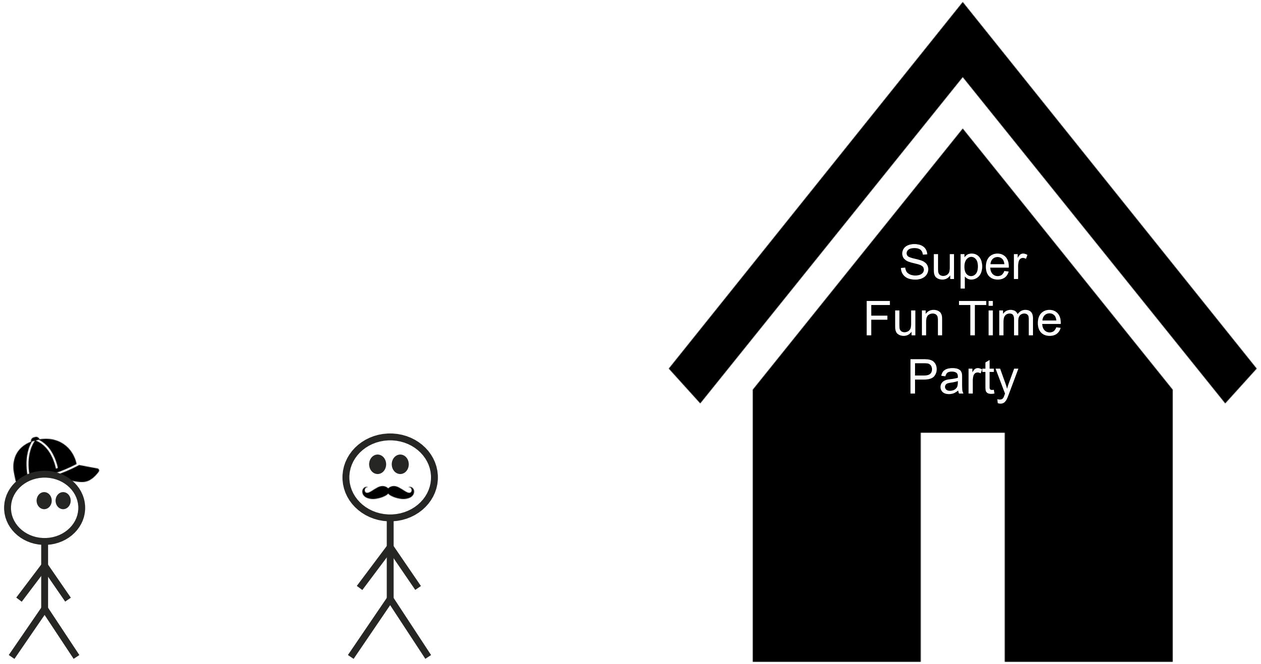
ABOUT RPKI

Resource **P**ublic **K**ey **I**nfrastructure

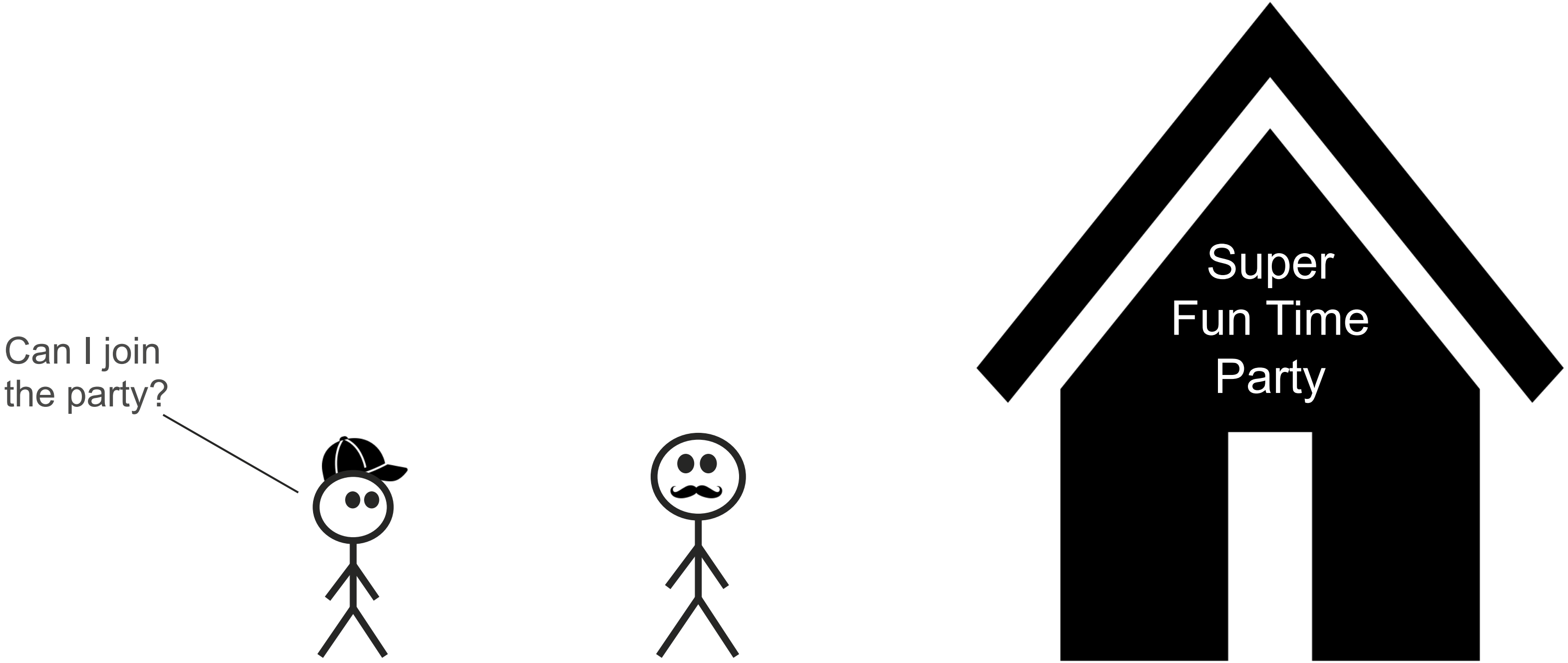
- RFC6480 (and many others)
- Binds route prefix to origin ASN
  - Signed cryptographically
  - Ensures trust (sort of)
- Recommended for MANRS compliance
  - https://www.manrs.org
- Signed prefixes stored (and distributed) by the 5 RIRs

https://blog.cloudflare.com/rpki/

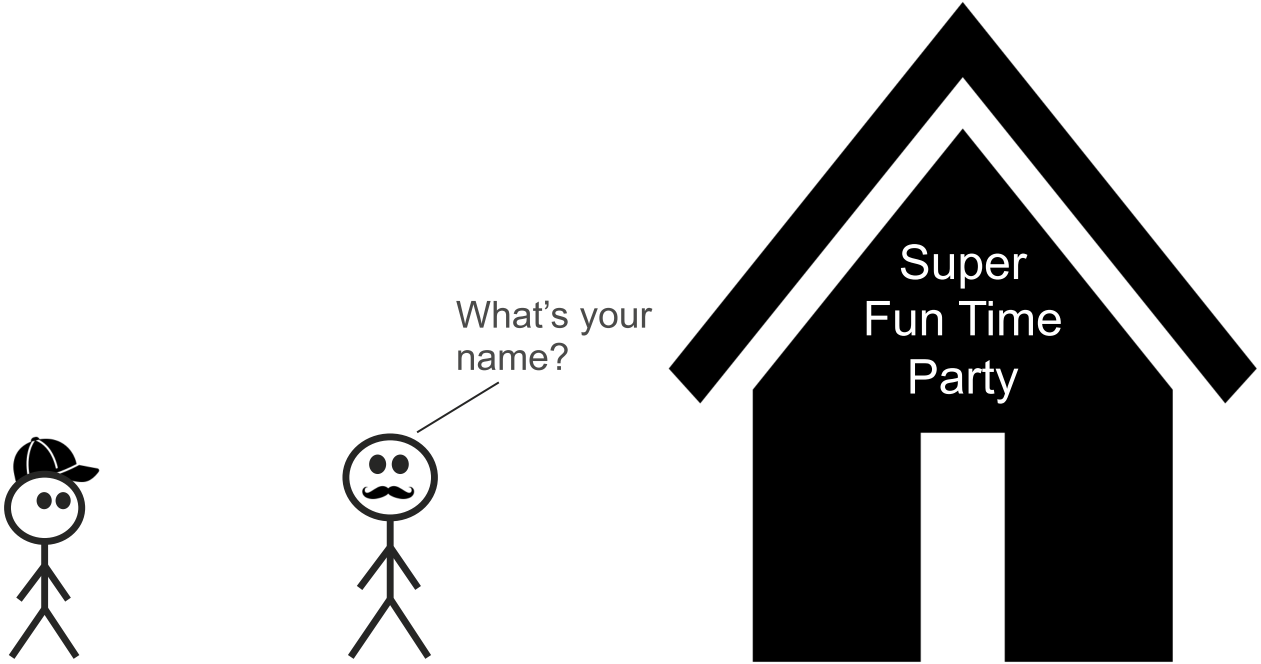
WHAT DOES RPKI PROTECT AGAINST (#1)



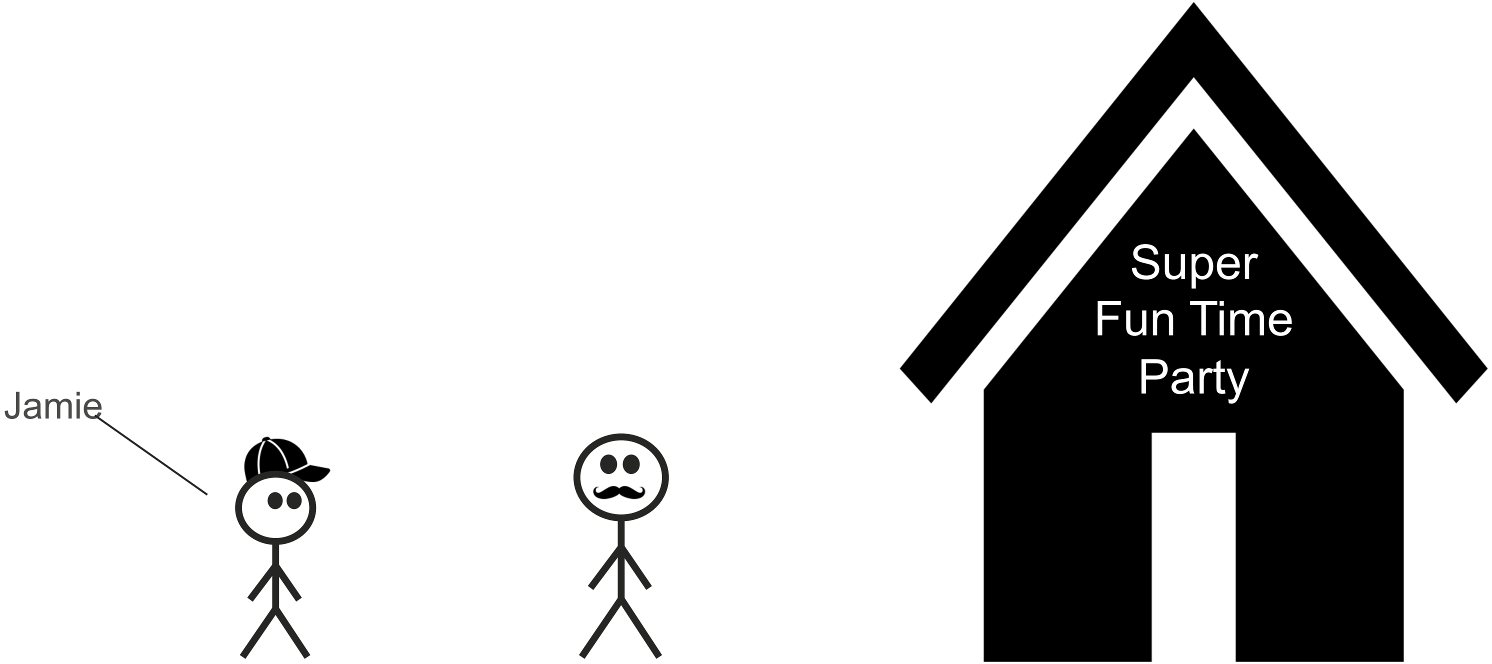
WHAT DOES RPKI PROTECT AGAINST (#1)



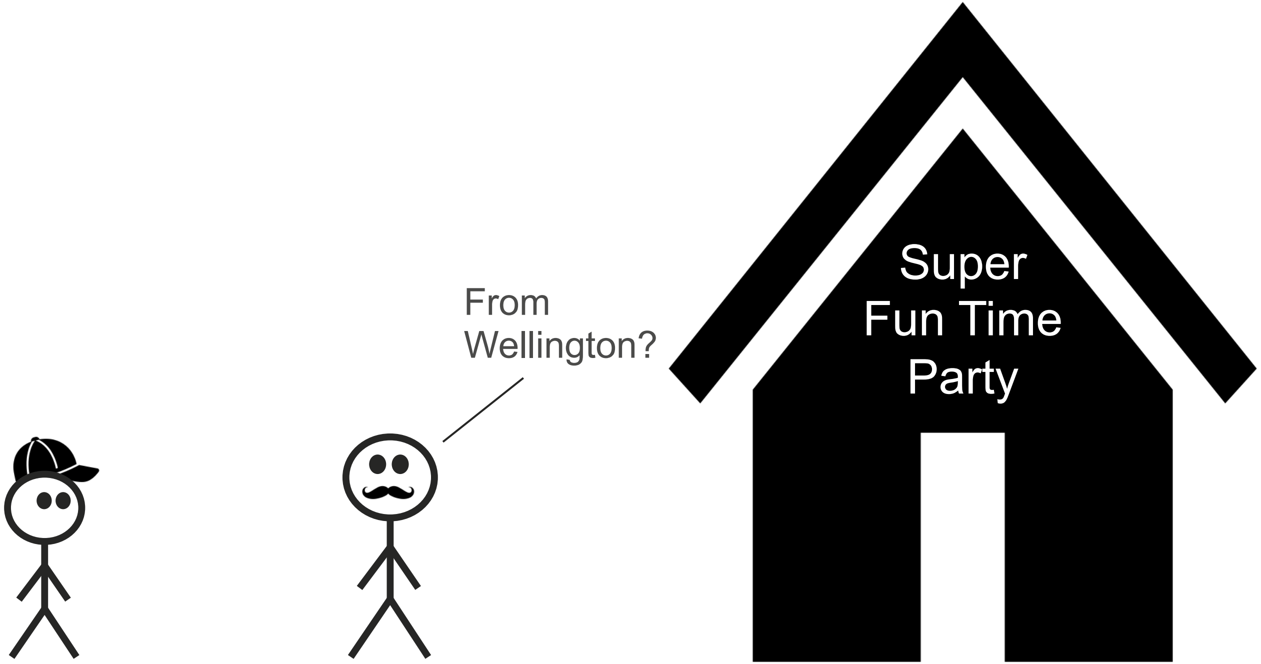
WHAT DOES RPKI PROTECT AGAINST (#1)



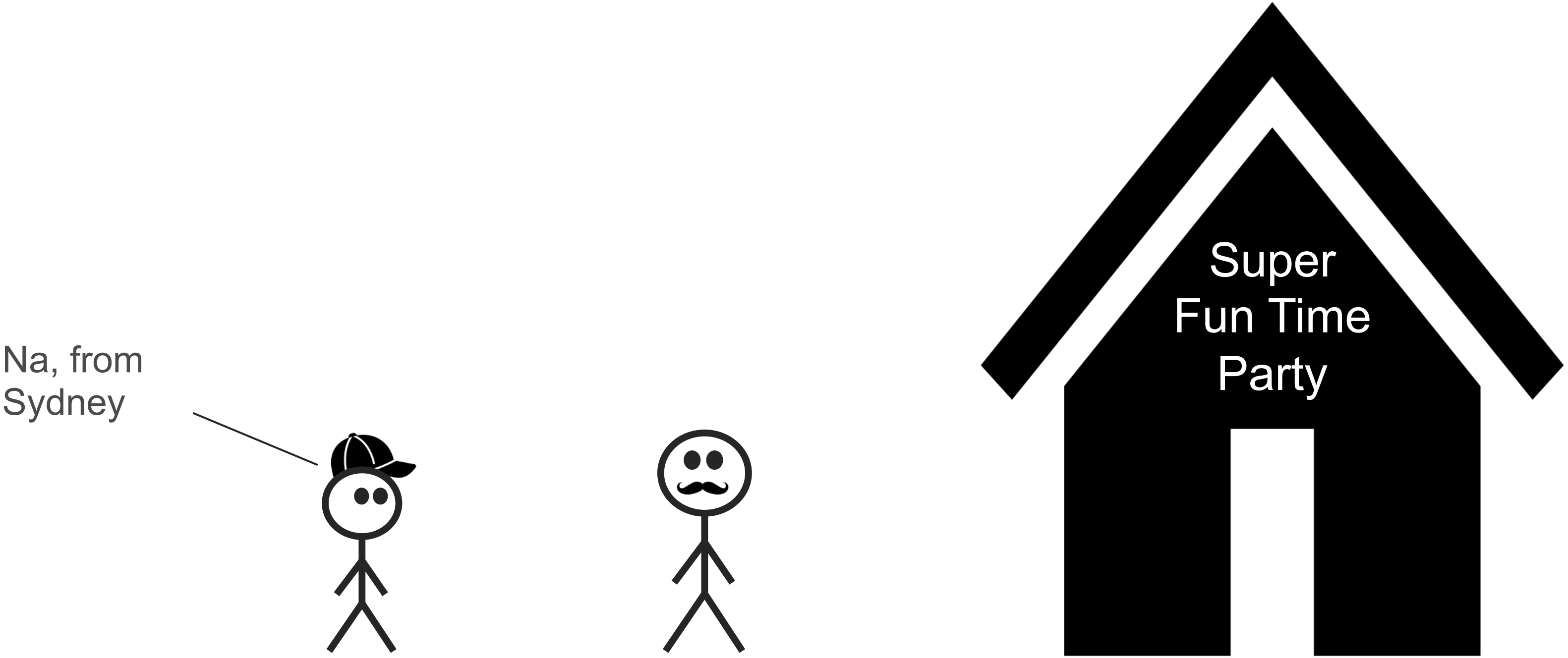
WHAT DOES RPKI PROTECT AGAINST (#1)



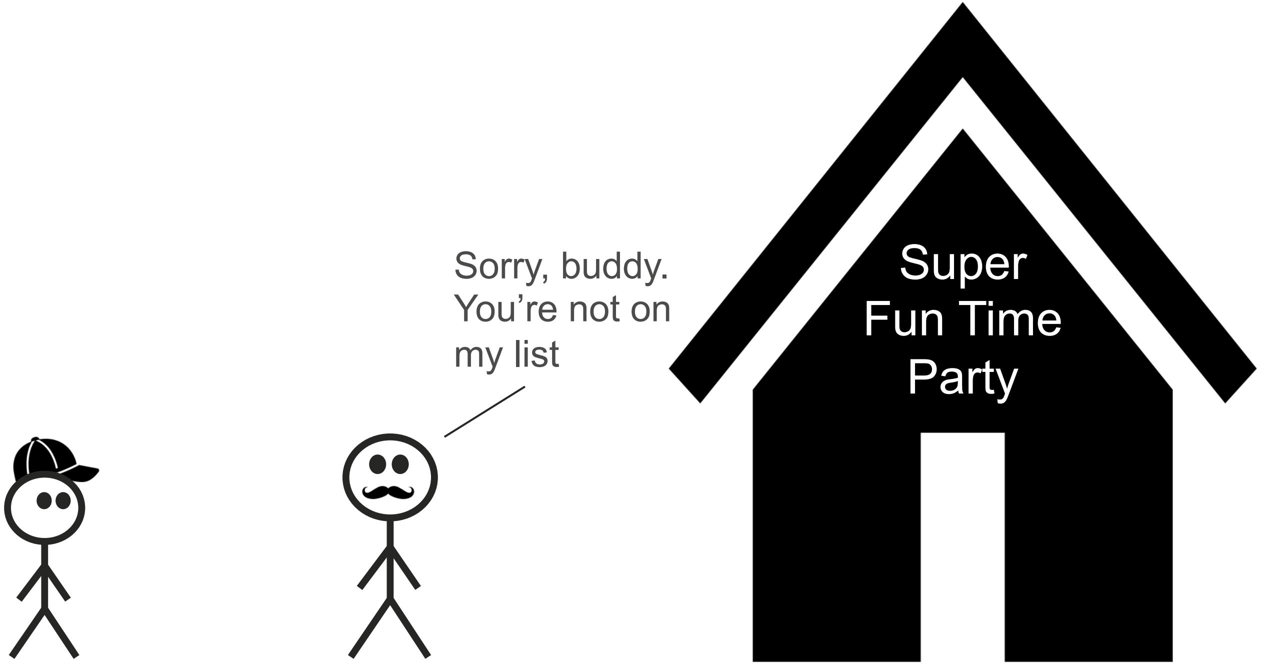
WHAT DOES RPKI PROTECT AGAINST (#1)



WHAT DOES RPKI PROTECT AGAINST (#1)

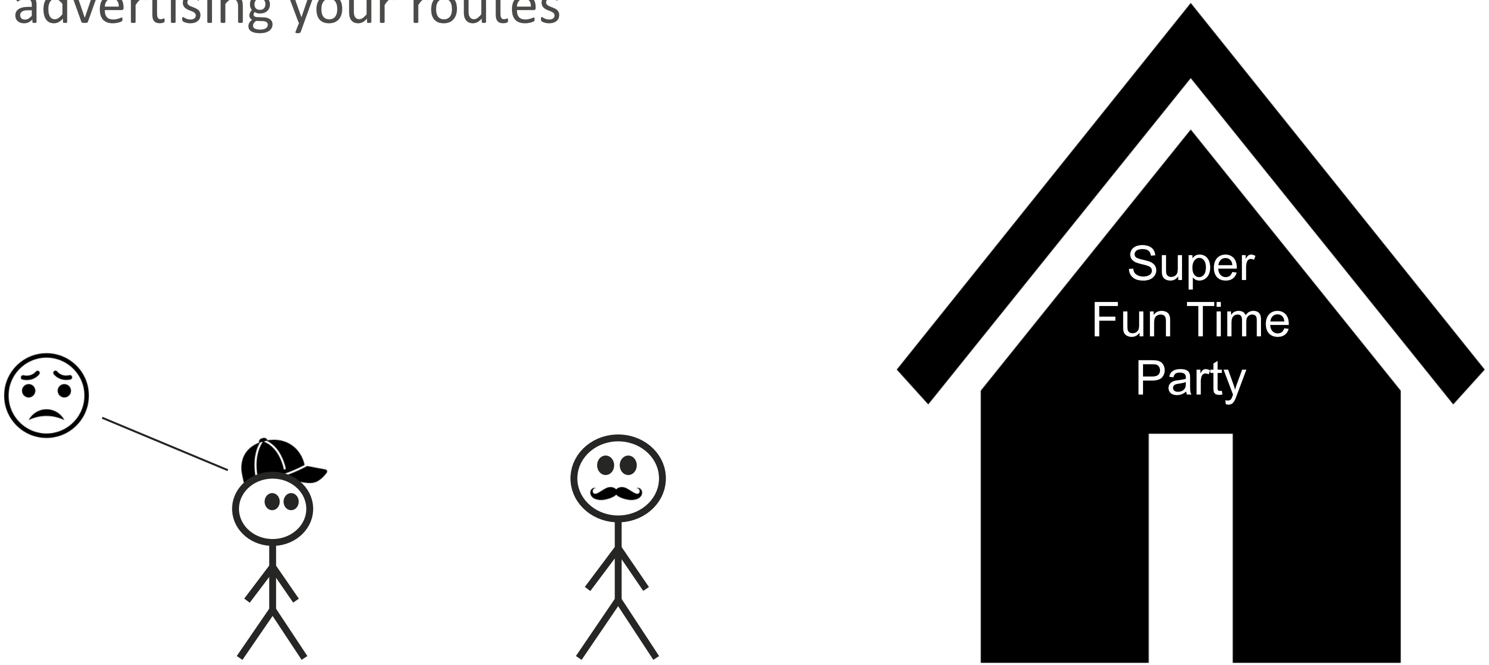


WHAT DOES RPKI PROTECT AGAINST (#1)

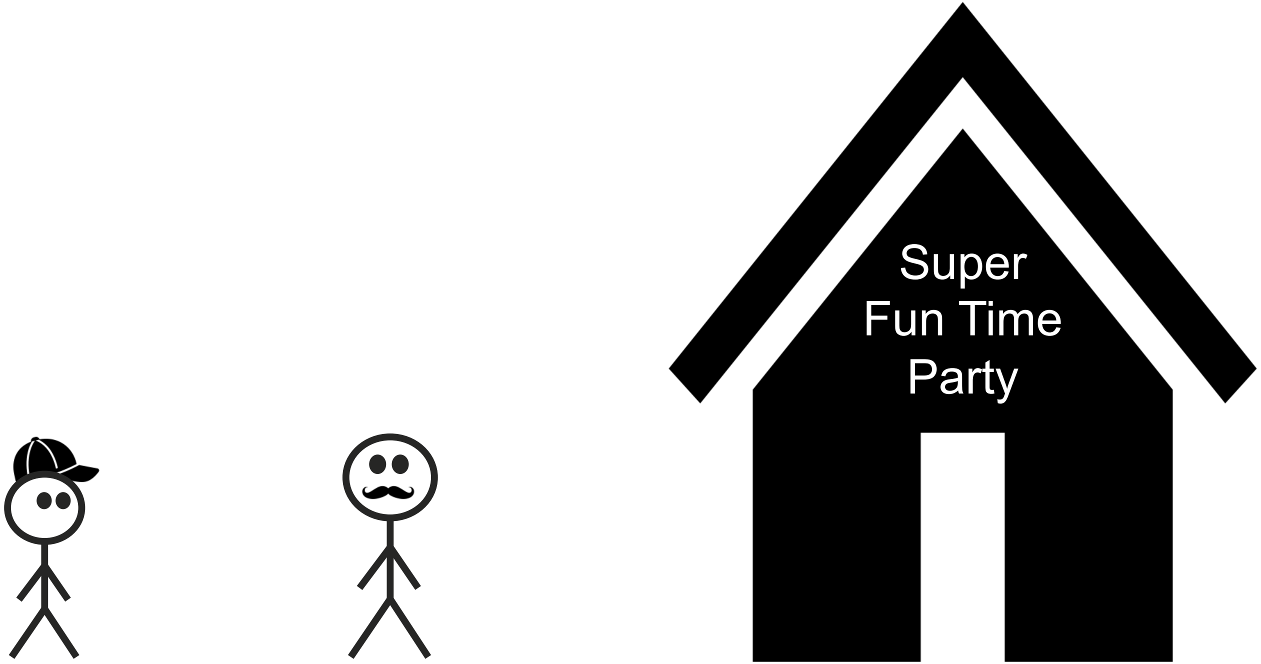


WHAT DOES RPKI PROTECT AGAINST (#1)

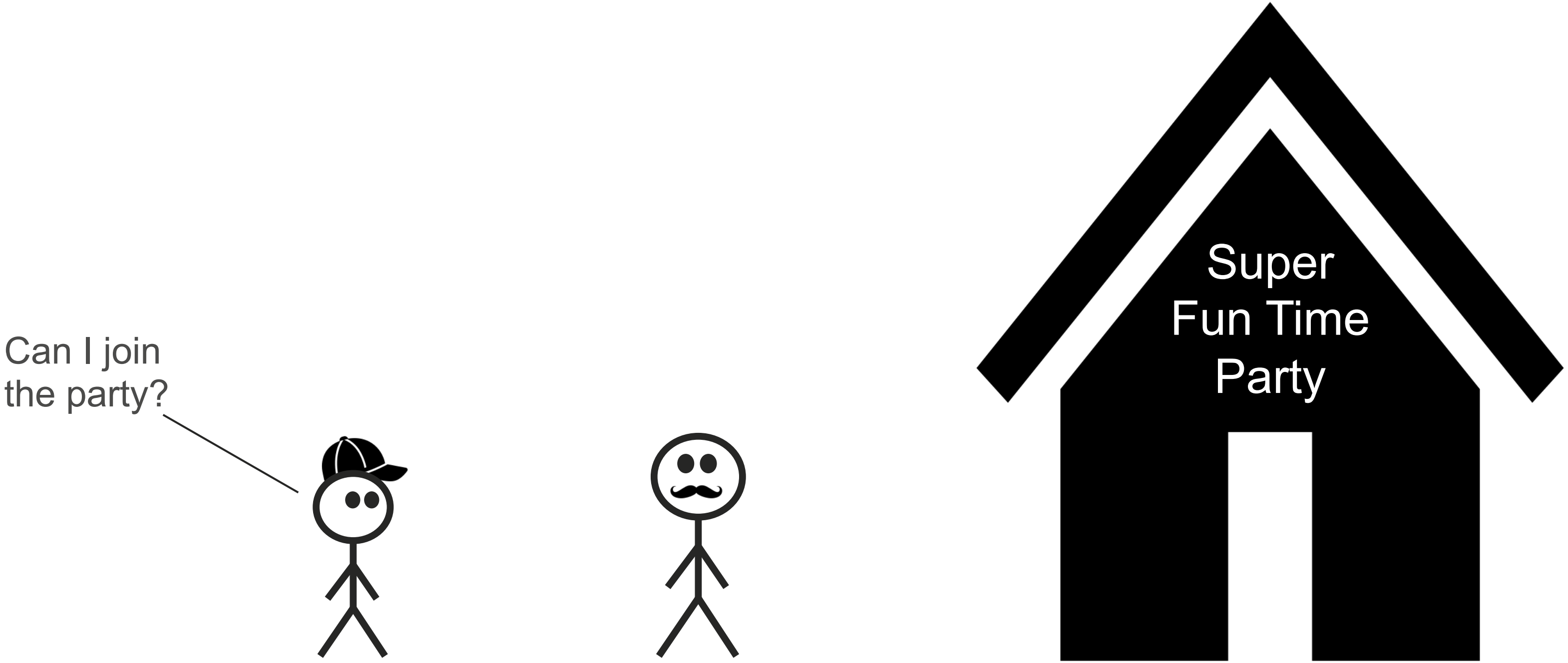
Another ASN advertising your routes



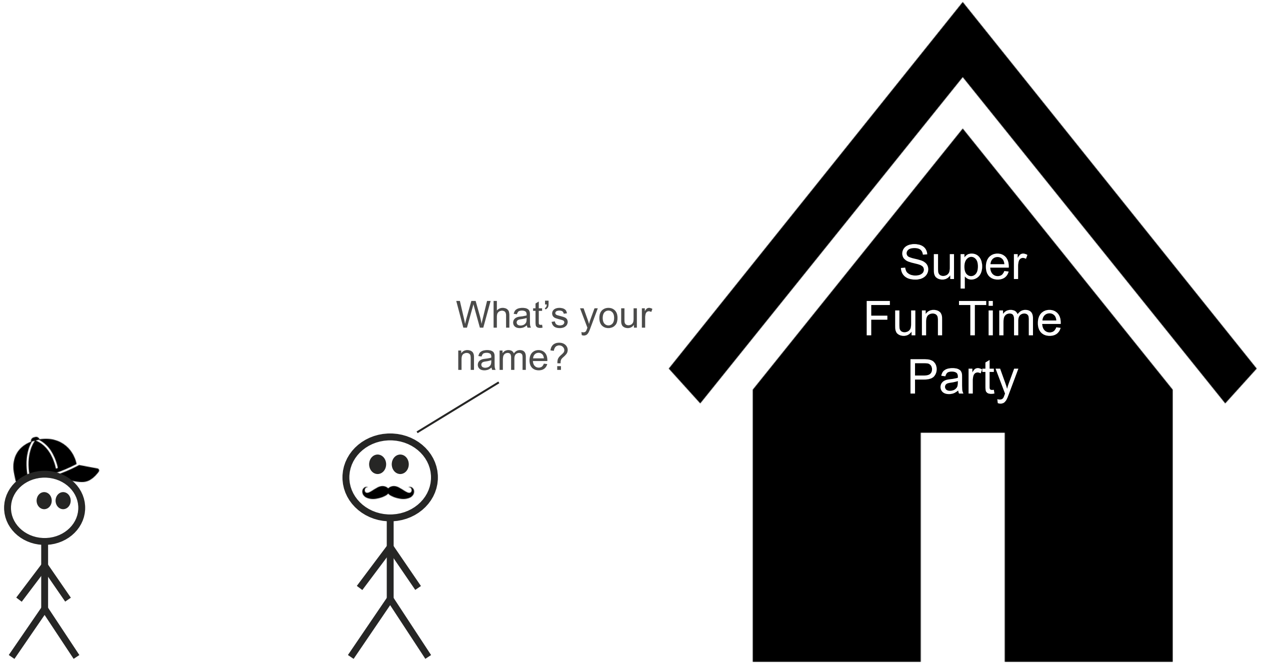
WHAT DOES RPKI PROTECT AGAINST (#2)



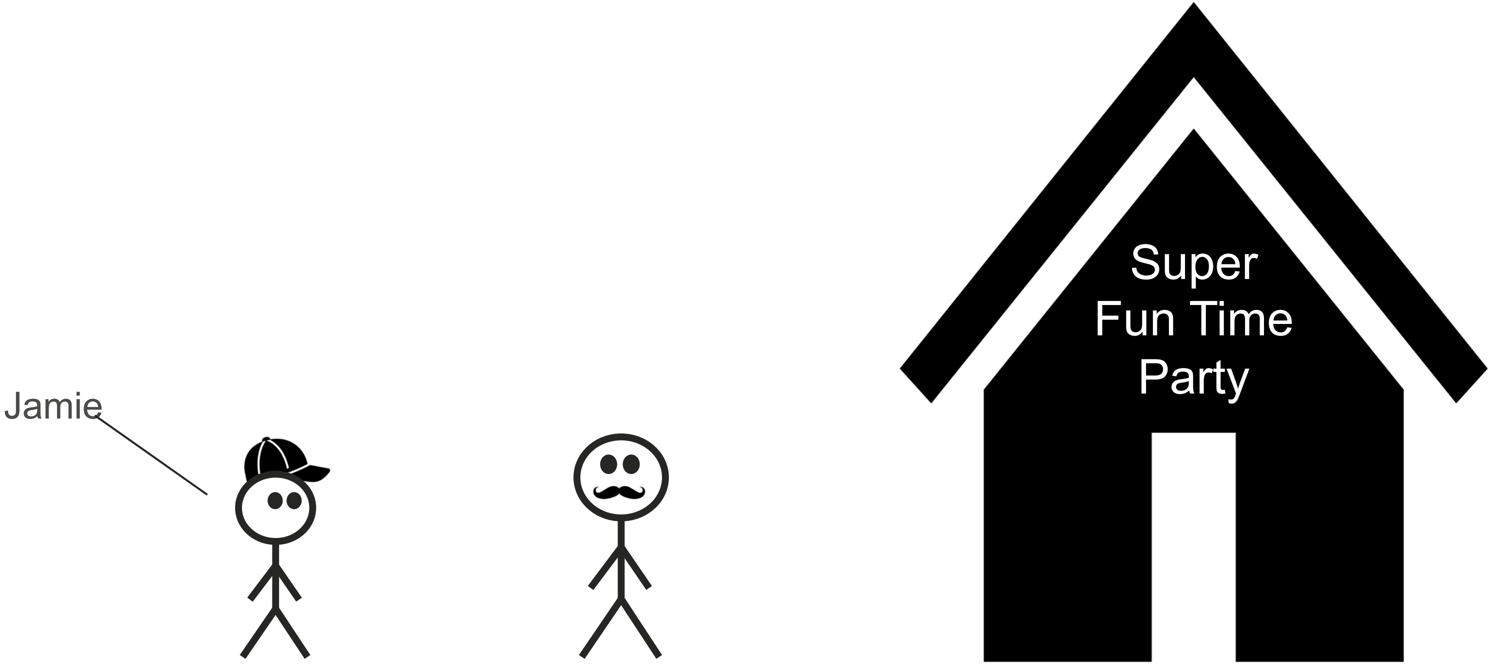
WHAT DOES RPKI PROTECT AGAINST (#2)



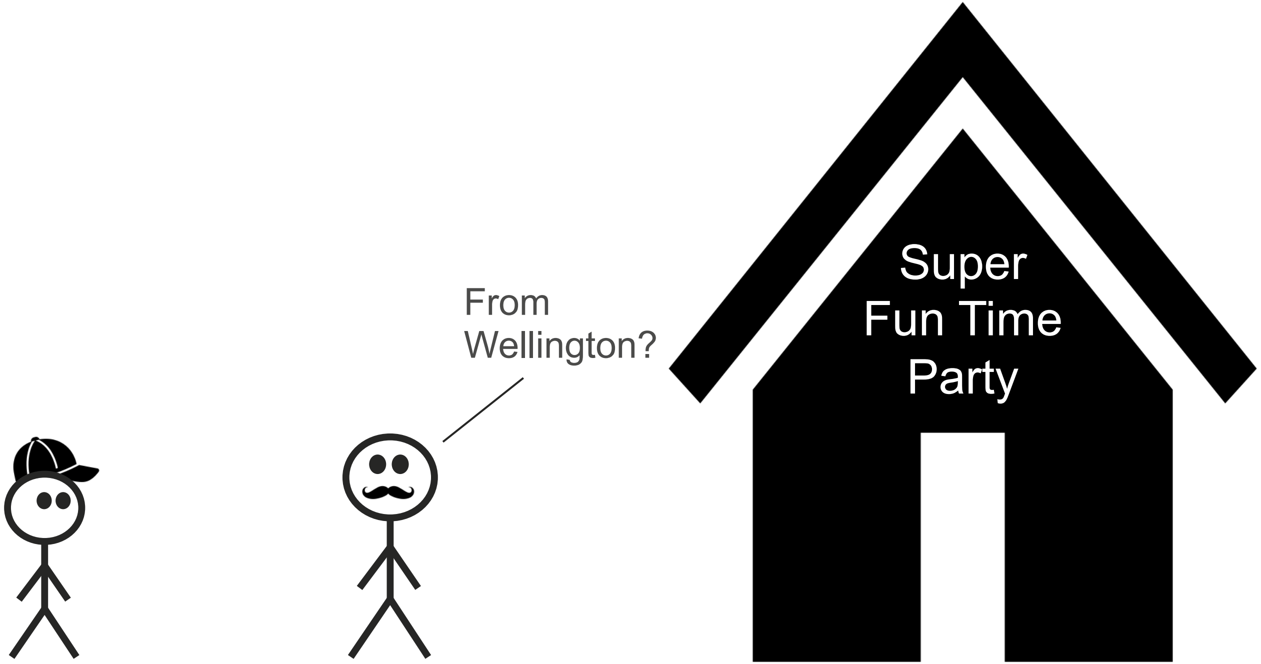
WHAT DOES RPKI PROTECT AGAINST (#2)



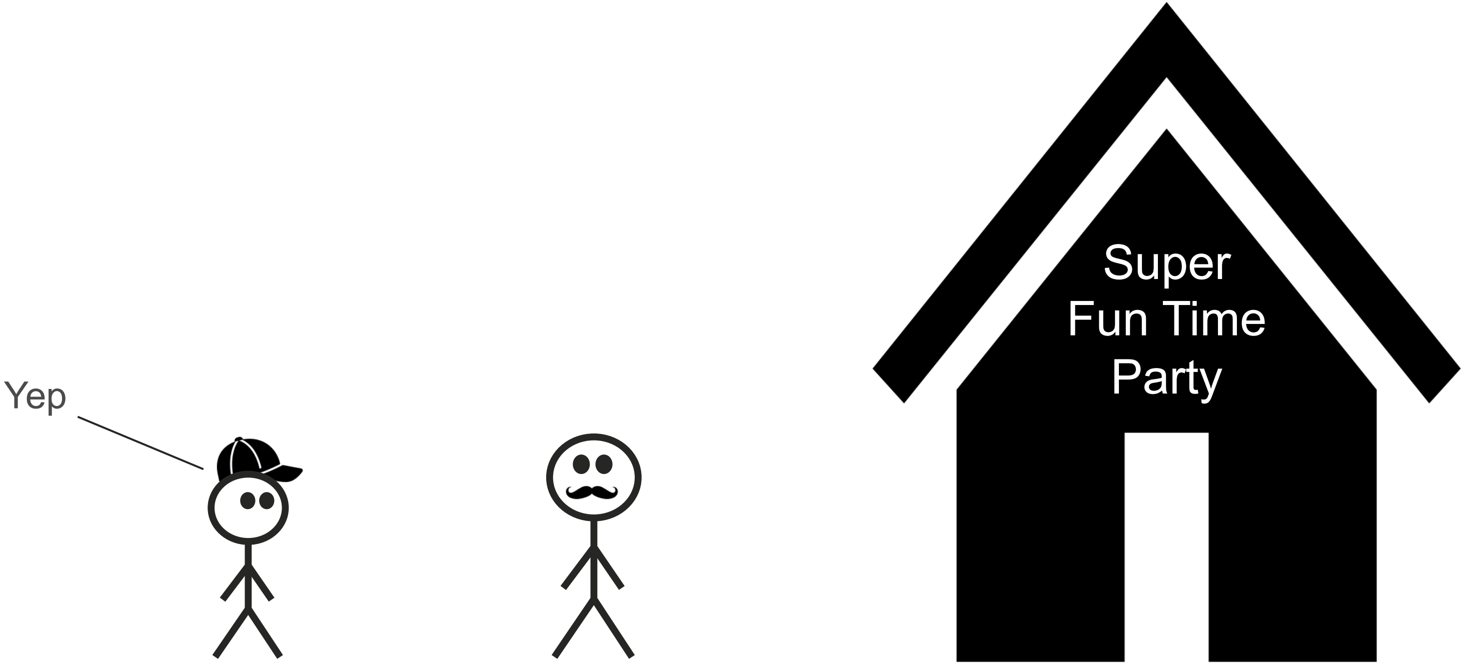
WHAT DOES RPKI PROTECT AGAINST (#2)



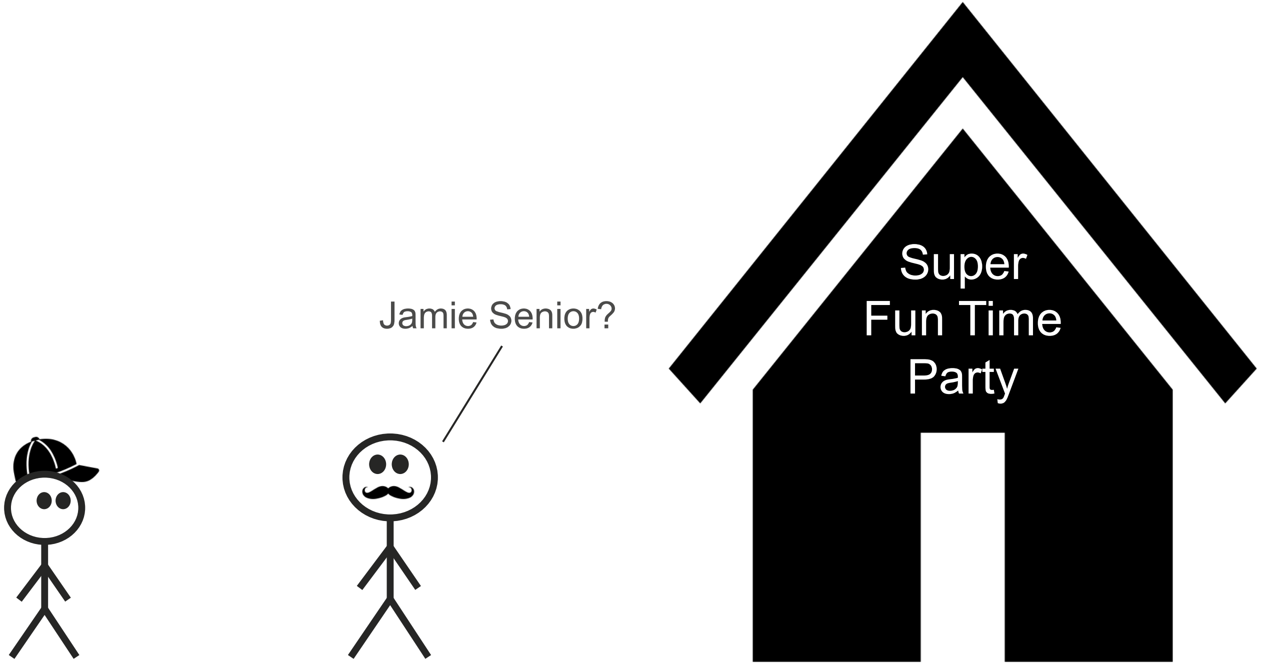
WHAT DOES RPKI PROTECT AGAINST (#2)



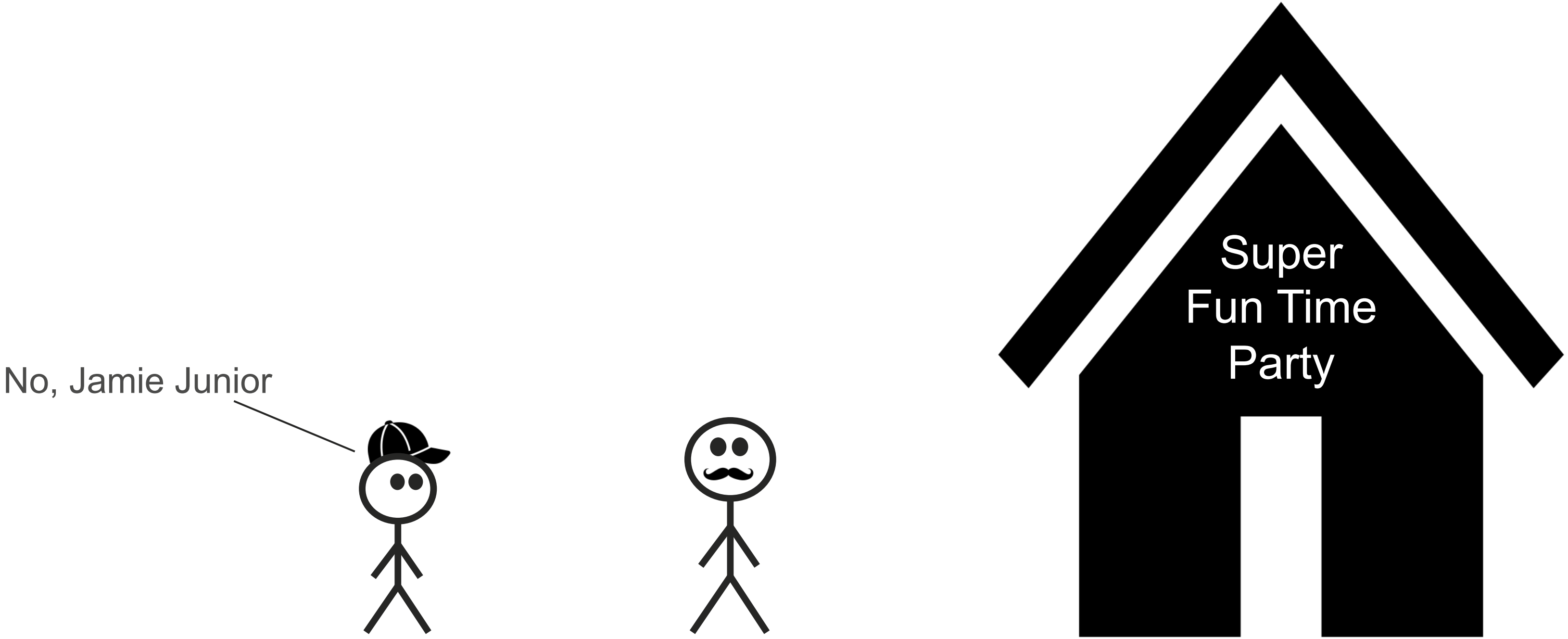
WHAT DOES RPKI PROTECT AGAINST (#2)



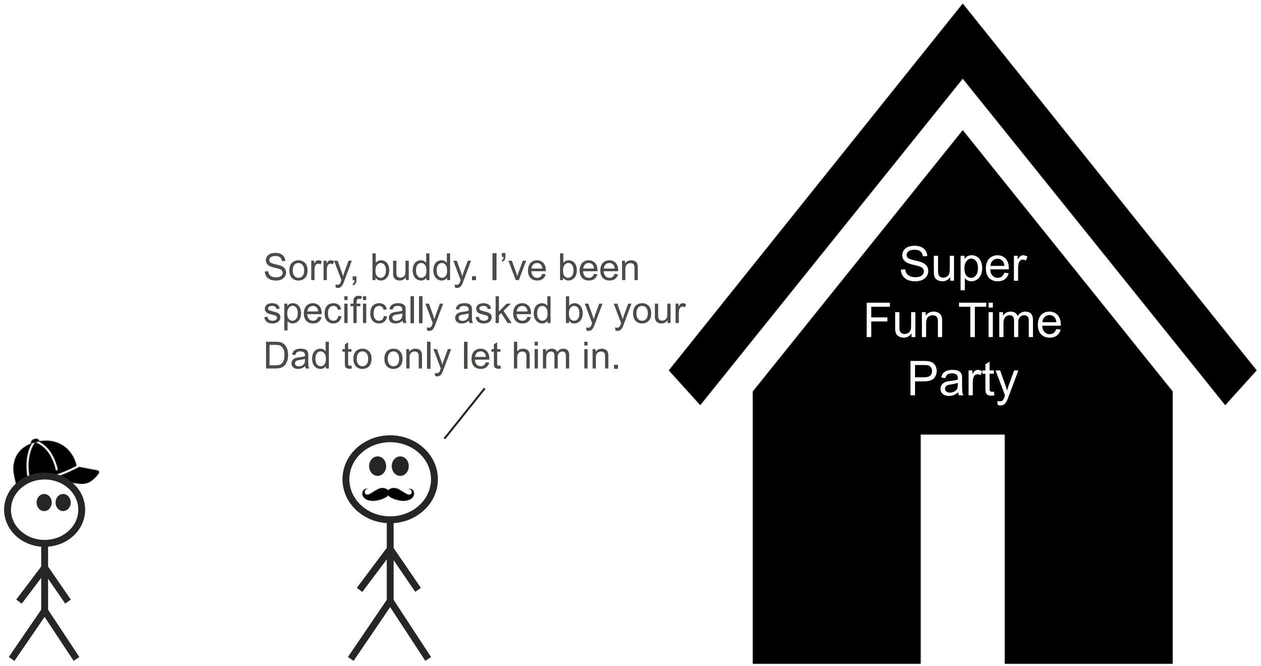
WHAT DOES RPKI PROTECT AGAINST (#2)



WHAT DOES RPKI PROTECT AGAINST (#2)

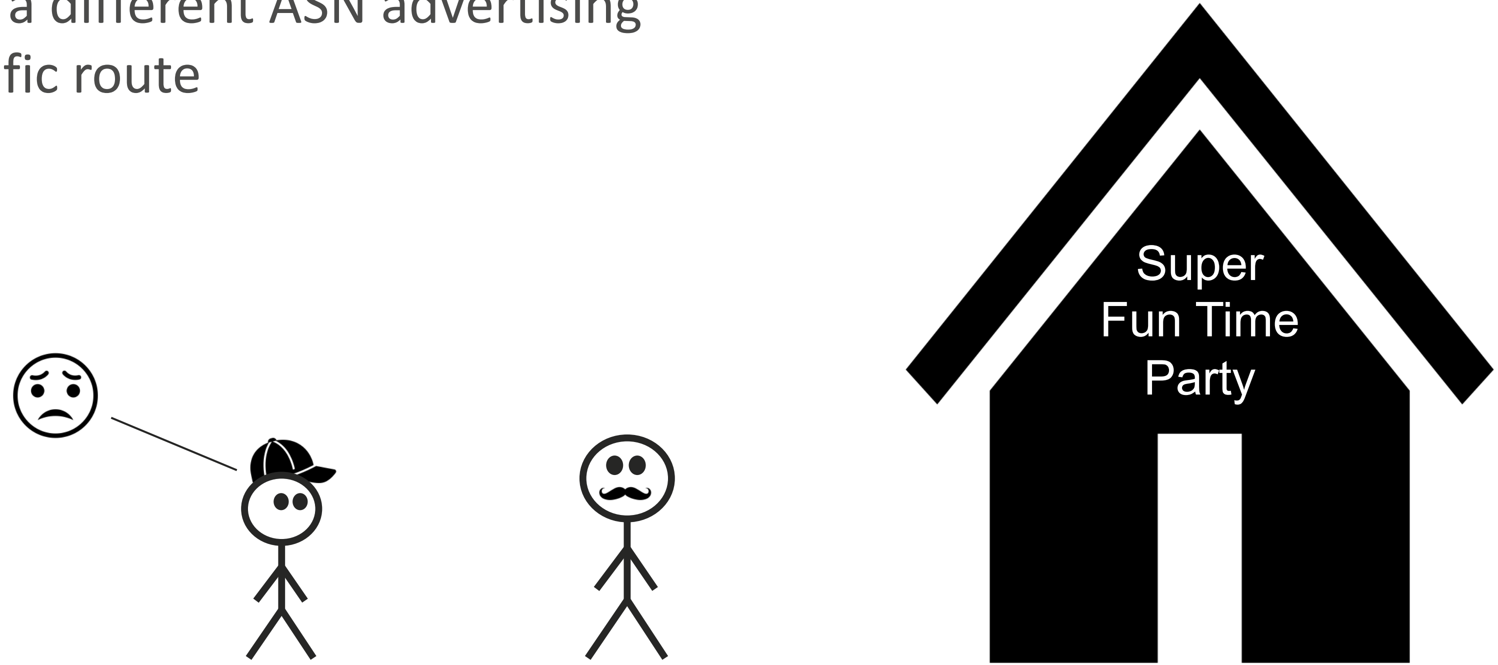


WHAT DOES RPKI PROTECT AGAINST (#2)

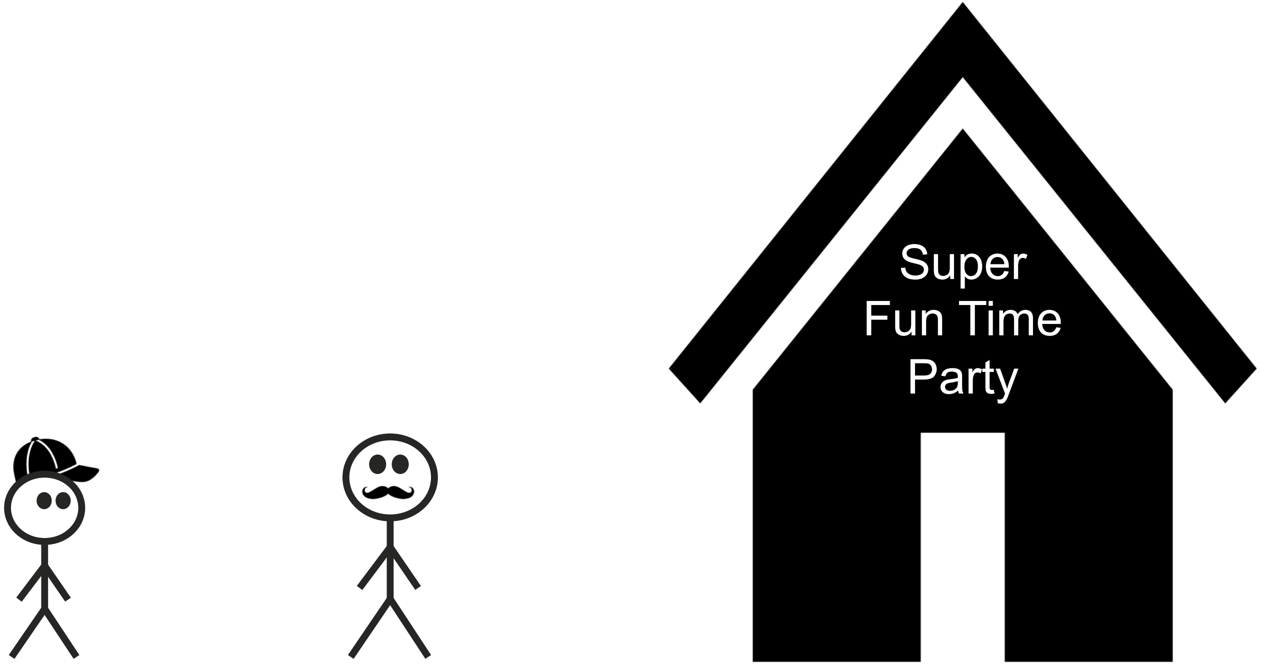

Sorry, buddy. I’ve been specifically asked by your Dad to only let him in.
Super Fun Time Party

WHAT DOES RPKI PROTECT AGAINST (#2)

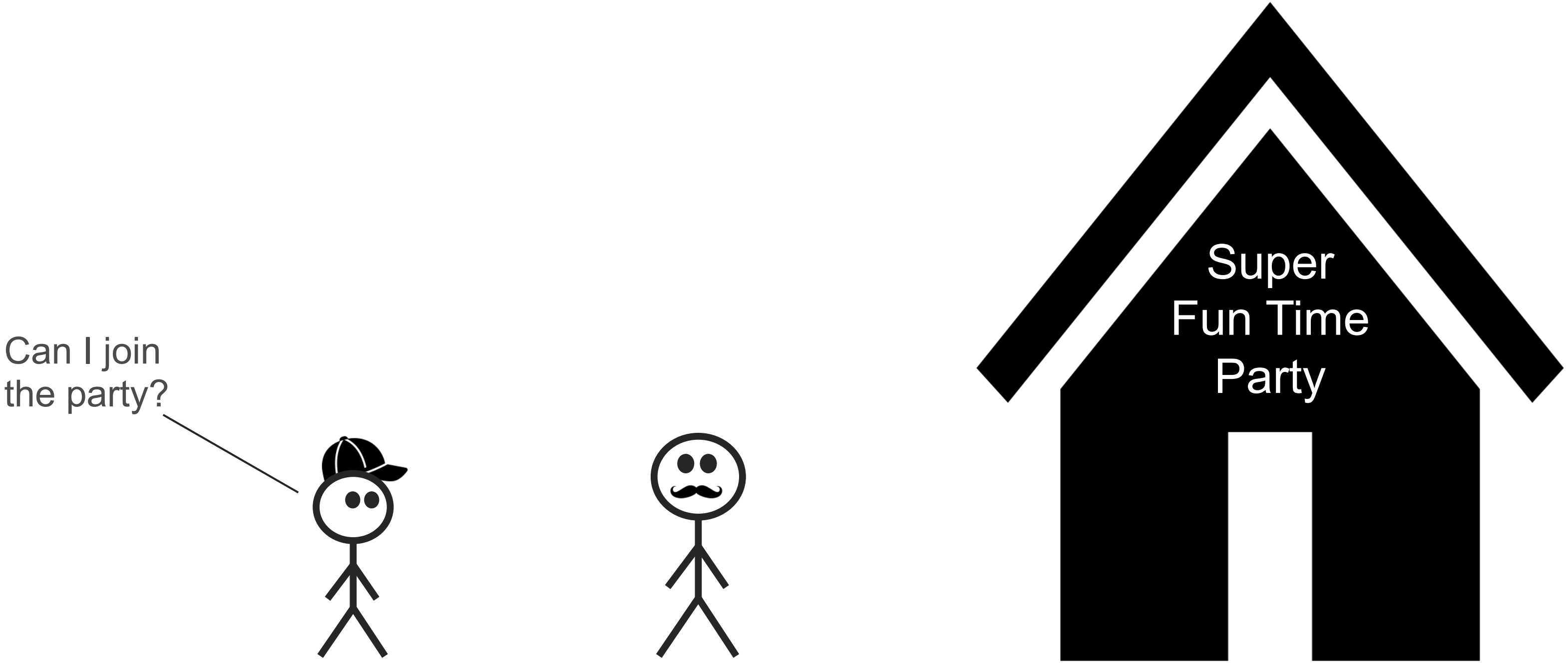
The same or a different ASN advertising a more specific route



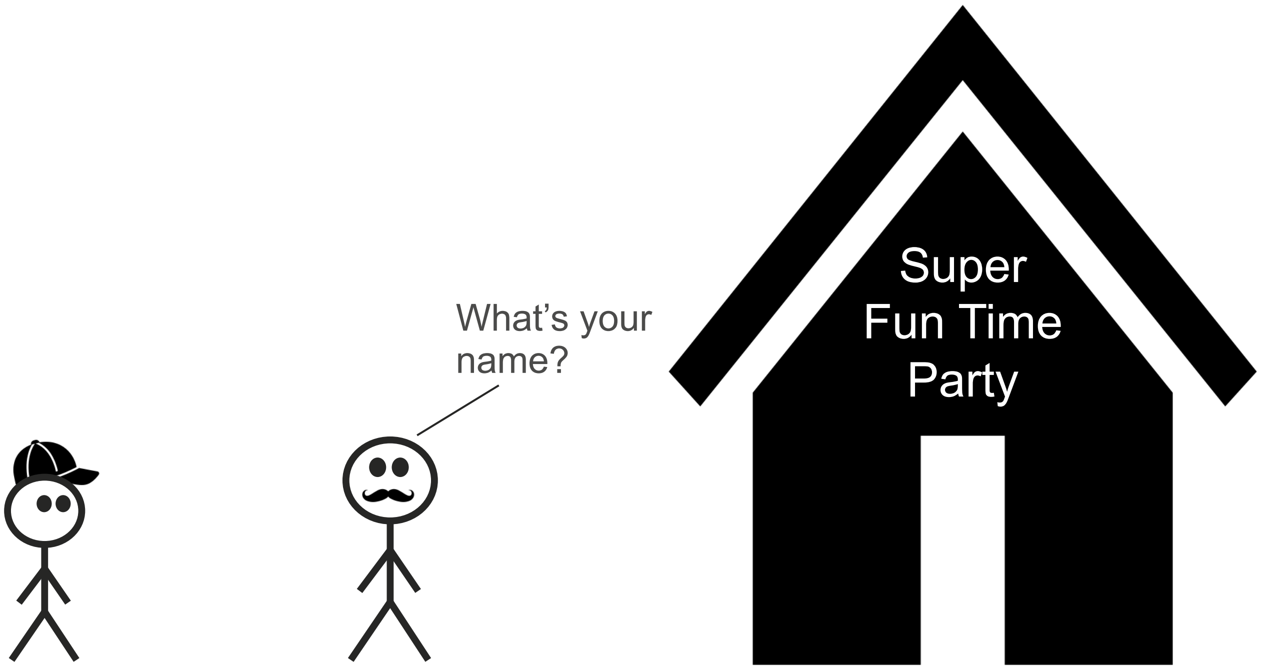
WHAT DOESN’T RPKI PROTECT AGAINST



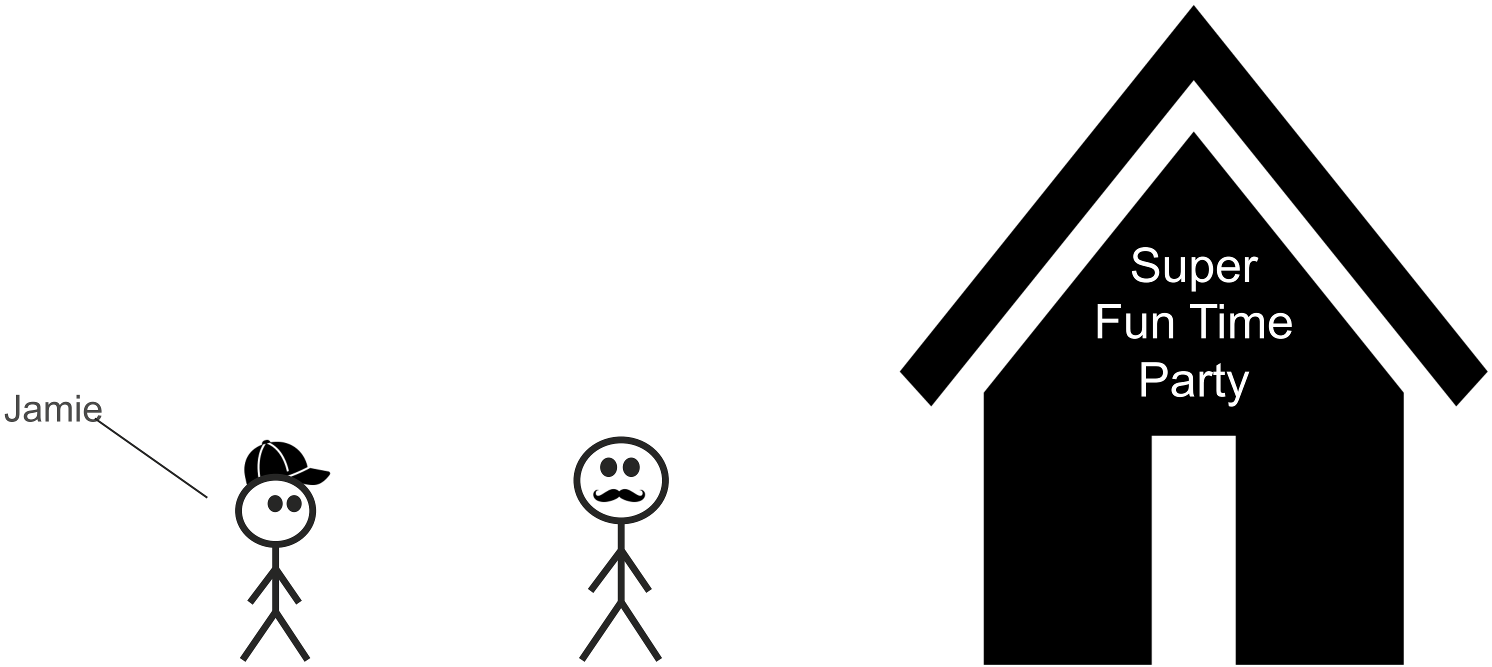
WHAT DOESN'T RPKI PROTECT AGAINST



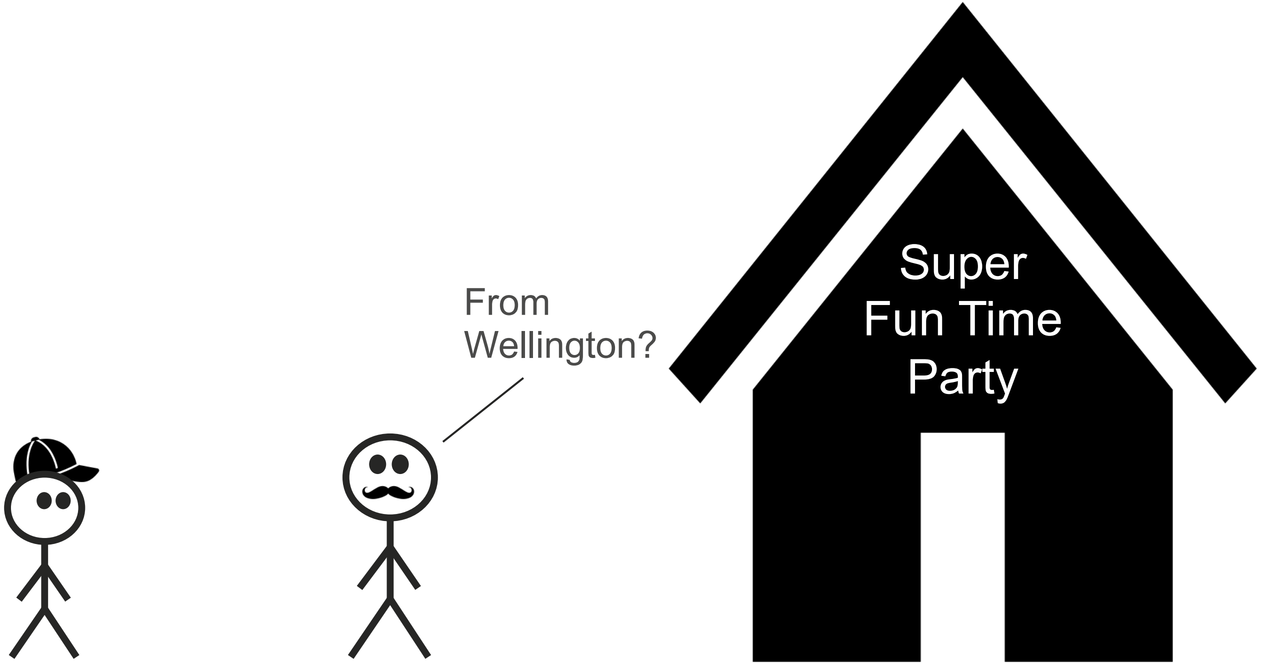
WHAT DOESN’T RPKI PROTECT AGAINST



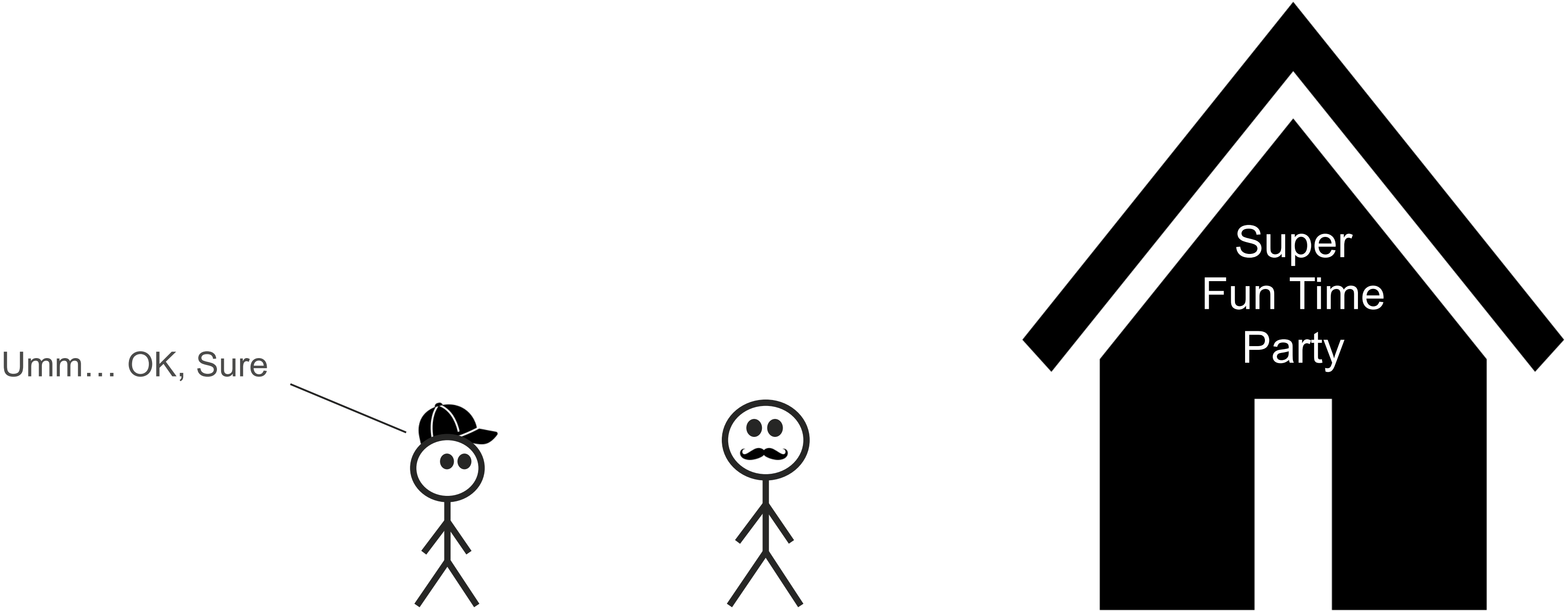
WHAT DOESN’T RPKI PROTECT AGAINST



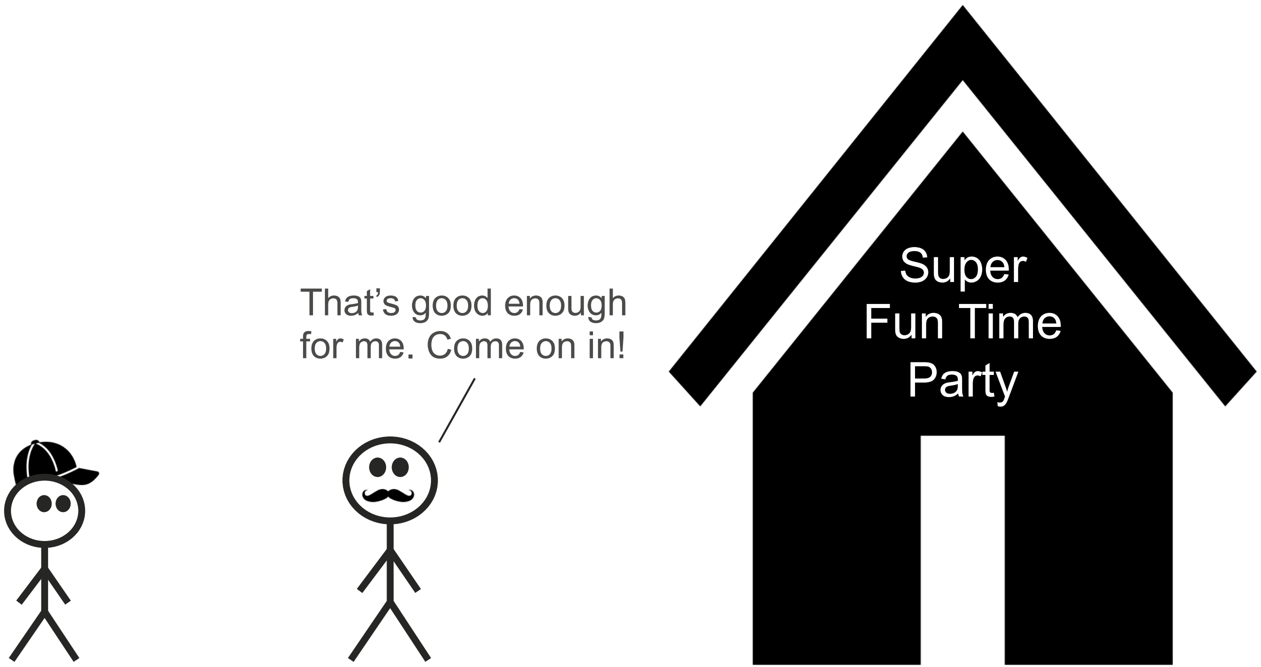
WHAT DOESN'T RPKI PROTECT AGAINST



WHAT DOESN'T RPKI PROTECT AGAINST

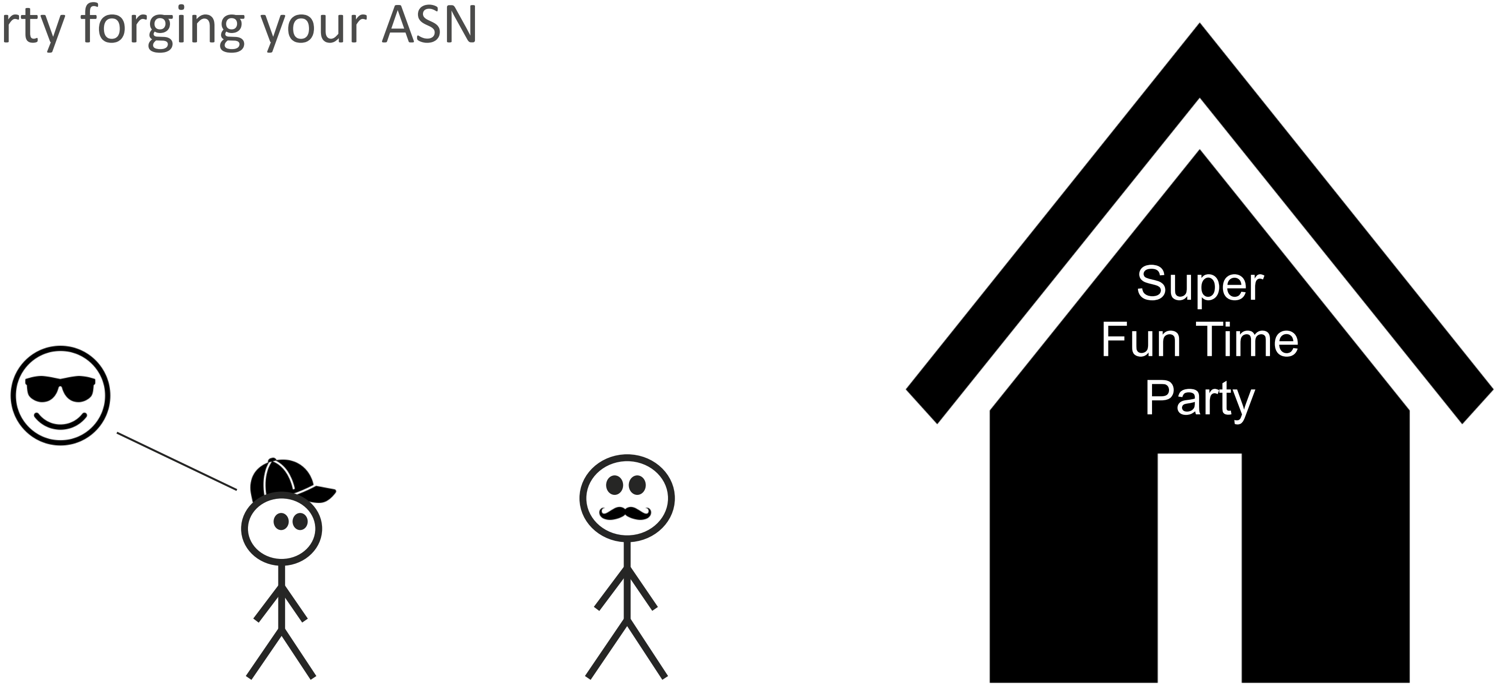


WHAT DOESN'T RPKI PROTECT AGAINST



WHAT DOESN'T RPKI PROTECT AGAINST

Malicious party forging your ASN as the origin



TLDR

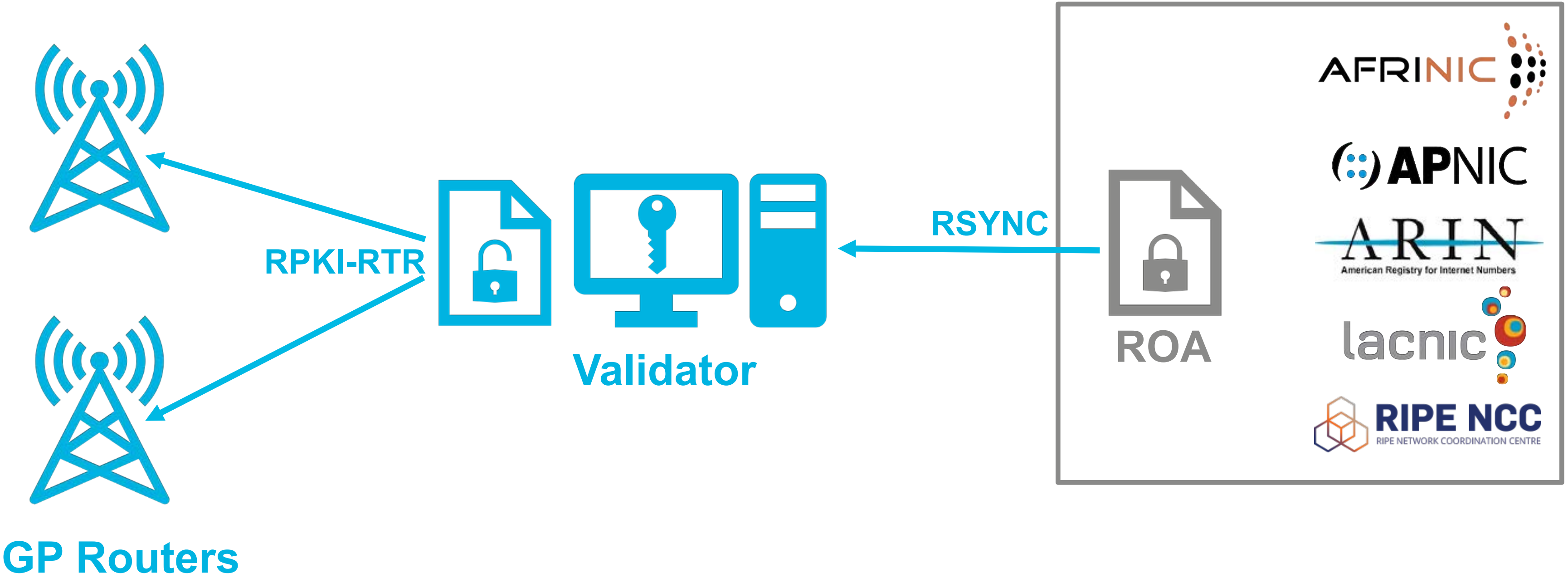
- Protects against
  - accidental advertisement of incorrect routes
  - route hijacking with more specific prefixes

- Doesn’t protect against
  - malicious advertisement of routes with impersonated origin ASN
  - accidental transit of peer routes

Validating the AS path is a whole other kettle of cryptographic fish

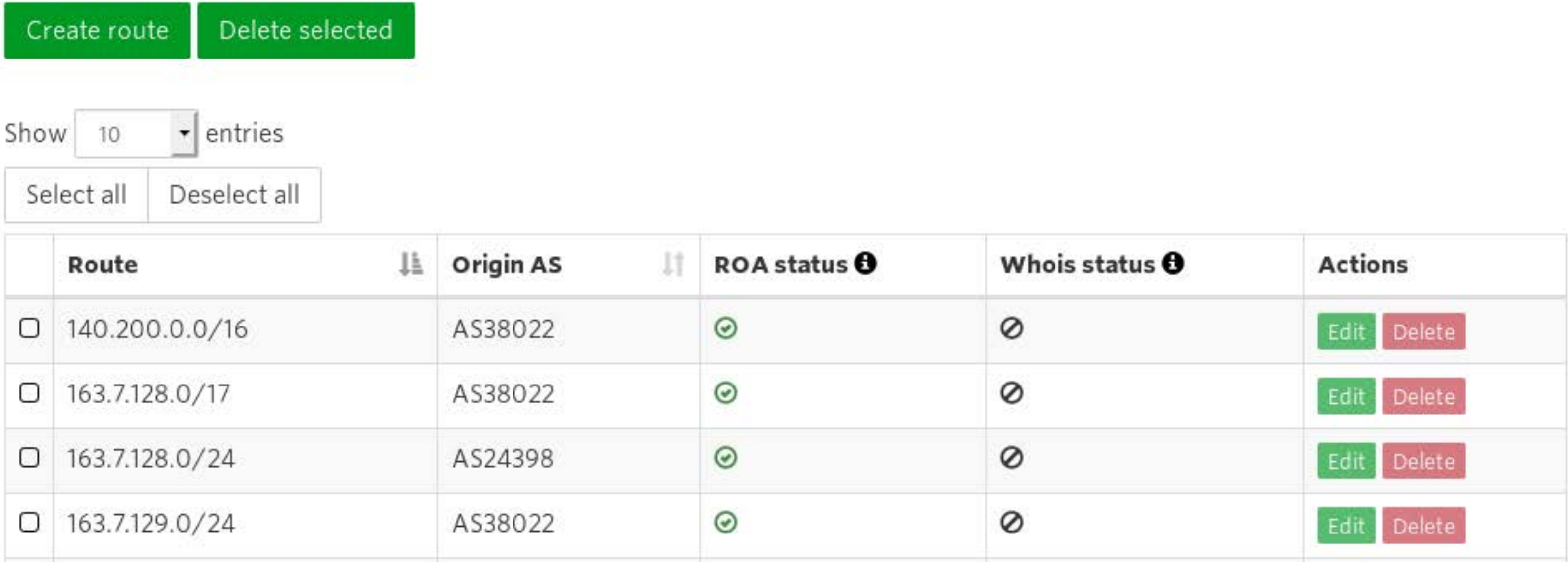
RPKI IMPLEMENTATION

RPKI ARCHITECTURE


AFRINIC
APNIC
ARIN
American Registry for Internet Numbers
lacnic
RIPE NCC
RIPE NETWORK COORDINATION CENTRE
ROA
RSYNC
Validator
RPKI-RTR
BGP Routers

ROA

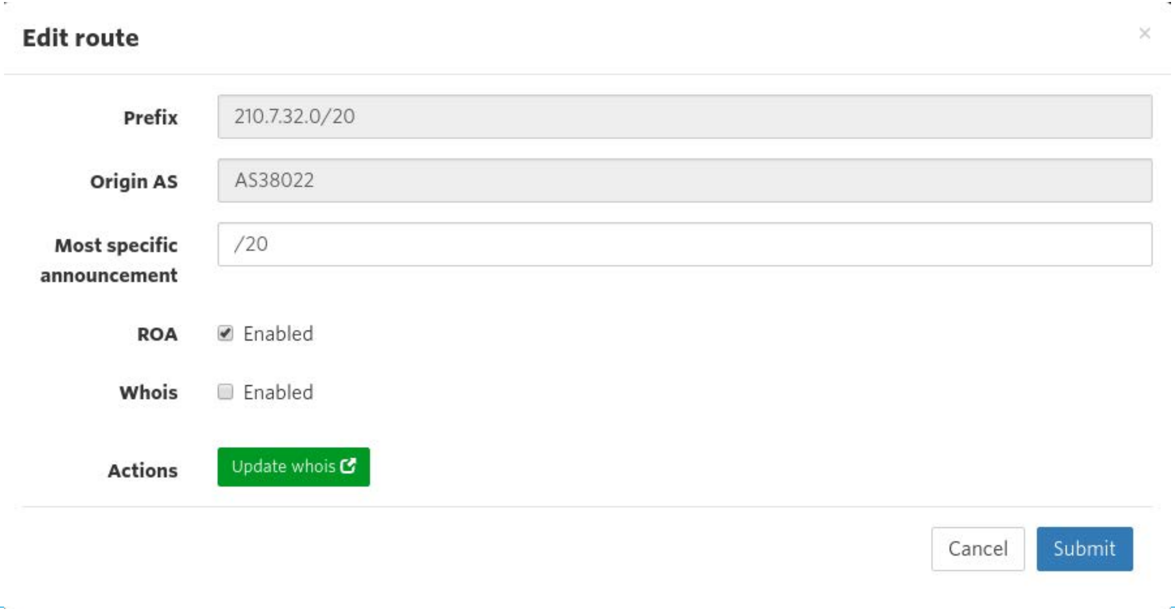
https://myapnic.net -> Resources -> (Route Management) Routes



	Route	Origin AS	ROA status	Whois status	Actions
□	140.200.0.0/16	AS38022	✓	⊘	Edit Delete
□	163.7.128.0/17	AS38022	✓	⊘	Edit Delete
□	163.7.128.0/24	AS24398	✓	⊘	Edit Delete
□	163.7.129.0/24	AS38022	✓	⊘	Edit Delete

ROA

Just tick the ROA option - trivial



Edit route

Prefix	210.7.32.0/20
Origin AS	AS38022
Most specific announcement	/20
ROA	☑ Enabled
Whois	□ Enabled

VALIDATOR (RELYING PARTY)

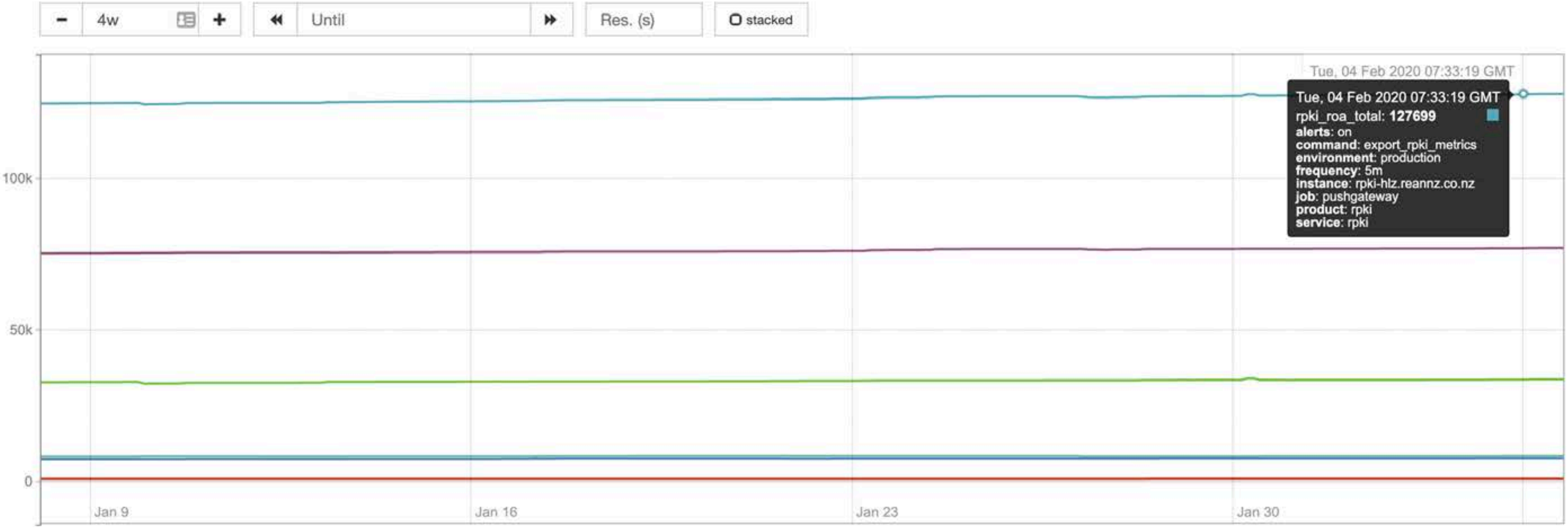
RIPE RPKI Validator

- Infrastructure
  - Java
  - 2 x containers
  - Ansible-managed
  - Memory-hungry (~6GB)
- Capability
  - Downloads ROAs with RSYNC
  - Validates ROAs cryptographically
  - ROA overrides (Ignore, Whitelist)
  - Performs the RTR transfer to your BGP routers
  - Validated data can be exposed via JSON API

https://blog.apnic.net/2019/10/28/how-to-installing-an-rpki-validator/

RPKI IMPLEMENTATION

VALIDATOR (RELYING PARTY)

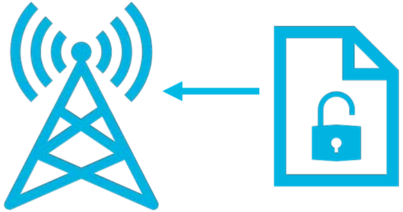


Tue, 04 Feb 2020 07:33:19 GMT
rpki_roa_total: **127699**
alerts: on
command: export_rpki_metrics
environment: production
frequency: 5m
instance: rpki-hlz.reannz.co.nz
job: pushgateway
product: rpki
service: rpki

ADVERTISE VALIDATED DATA TO NETWORK

RPKI to Router (RTR) protocol

- RFC6810
- Unencrypted



```
routing-options {
    validation {
        notification-rib [ some-inet.0 some-inet6.0 ];
        group rpki-wlg {
            session 203.0.113.14 {
                port 8282;
                local-address 192.0.2.1
            }
        }
    }
}
```

```
filter protect-re {
  term rpki-rtr {
    from {
      source-prefix-list {
        rpki-rtr-validators;
      }
      protocol tcp;
      source-port 8282;
    }
    then accept;
  }
}
```

ENABLING RPKI POLICY

Just add an import filter to your peering policy

```
term valid {
    from {
        protocol bgp;
        validation-database valid;
    }
    then {
        validation-state valid;
        next policy;
    }
}
```

```
term invalid {
    from {
        protocol bgp;
        validation-database invalid;
    }
    then {
        validation-state invalid;
        reject;
    }
}
```

```
term unknown {
    from {
        protocol bgp;
        validation-database unknown;
    }
    then {
        validation-state unknown;
        next policy;
    }
}
```

REANNZ RPKI BEST PRACTICE

- Apply on external BGP feeds
  - Peerings, Transit Providers, R&E
- Not applying to customers
  - Exact route filters already in place (built from IPAM)
- Begin by logging invalid routes
- Then act on RPKI validation
  - Valid == Accept
  - Invalid == Reject
  - Unknown == Accept

REANNZ RPKI BEST PRACTICE

- Use exact prefix lengths for ROAs
- Automate regular checks of your configured ROAs

```
aaron@nms-wlg:~$ check_reannz_roas
Missing ROAs:
 140.200.0.0/24 AS38022
 140.200.1.0/24 AS38299
Extra ROA's:
 140.200.1.0/24 AS38022
```

SHOULD I ENABLE RPKI VALIDATION?

- Pro
  - Gain benefit without full (internet-wide) implementation
  - Security improves as adoption increases
  - BGP performance/reliability unaffected
  - Cleanly handles failure
  - Operationally, pretty simple to implement/run

- Con
  - Requires ensuring ROAs are kept up-to-date
  - Some extra training for the NOC

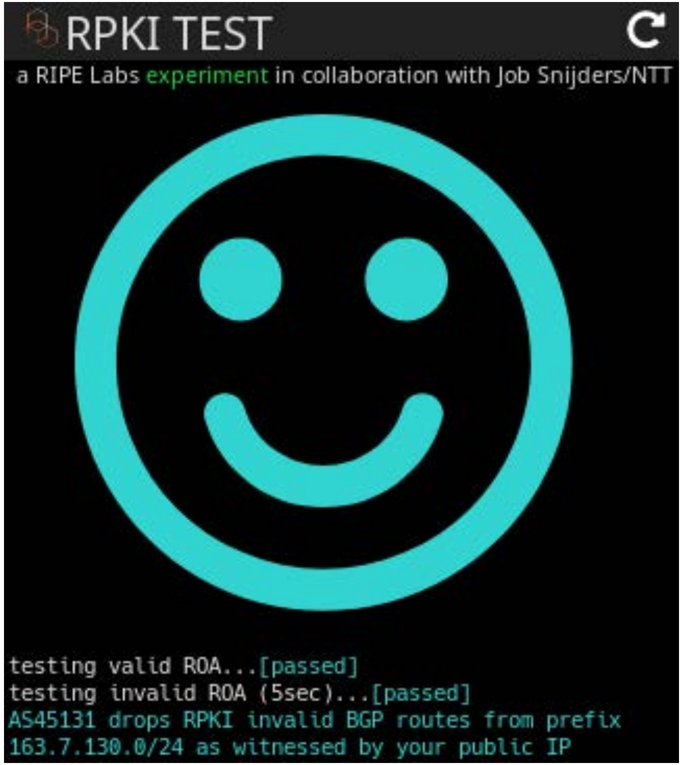
SHOULD I ENABLE RPKI VALIDATION?

- Pro
  - Gain benefit without full (internet-wide) implementation
  - Security improves as adoption increases
  - BGP performance/reliability unaffected
  - Cleanly handles failure
  - Operationally, pretty simple to implement/run

Not if you receive the default route!

- Con
  - Requires ensuring ROAs are kept up-to-date
  - Some extra training for the NOC

RPKI IMPLEMENTATION



RPKI TEST
a RIPE Labs experiment in collaboration with Job Snijders/NTT

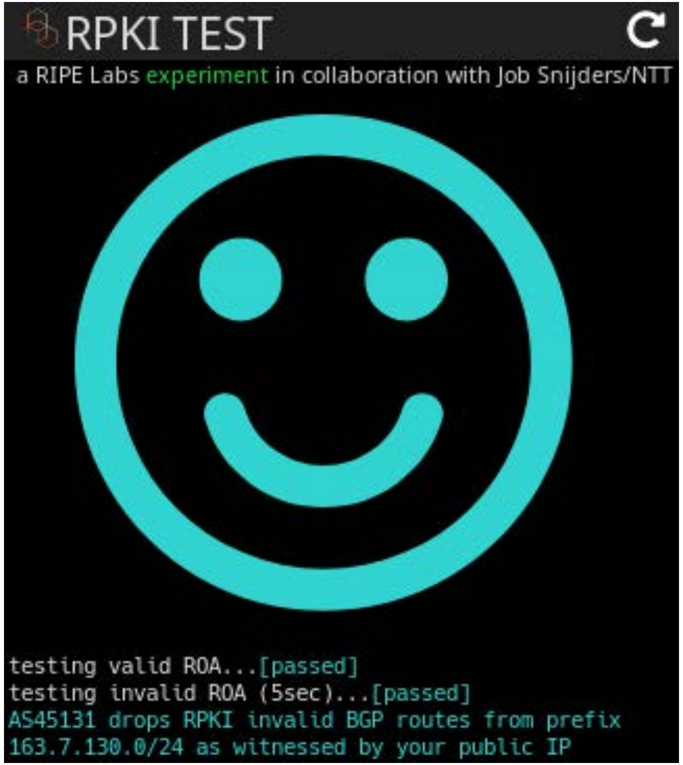
```
testing valid ROA...[passed]
testing invalid ROA (5sec)...[passed]
AS45131 drops RPKI invalid BGP routes from prefix
163.7.130.0/24 as witnessed by your public IP
```

http://sg-pub.ripe.net/jasper/rpki-web-test

Number of reported faults:

0

RPKI IMPLEMENTATION



RPKI TEST

a RIPE Labs experiment in collaboration with Job Snijders/NTT

```
testing valid ROA...[passed]
testing invalid ROA (5sec)...[passed]
AS45131 drops RPKI invalid BGP routes from prefix
163.7.130.0/24 as witnessed by your public IP
```

http://sg-pub.ripe.net/jasper/rpki-web-test

Number of reported faults:

2

LESSONS LEARNED

- Keep your WHOIS contact details up-to-date
- Automate checks of validity of your ROAs
  - https://github.com/taiji-k/roamon-verify
- Implement a check of what IP space disappears when rejecting invalid routes
  - Ignore where there is a valid covering route
  - https://nusenu.github.io/RPKI-Observatory/unreachable-networks.html

IT ALL KINDA JUST WORKED

REANNZ