Resource Certification (RPKI) @AFRINIC

Amreesh Phokeer

Agenda

- What is the rationale behind RPKI?
- What is resource certification?
- How to get your resources certified?
- How to sign your routing announcements?
- How to make your router talk RPKI?
- How to build filters based on validated routes?
- Demo
- Current hot topics

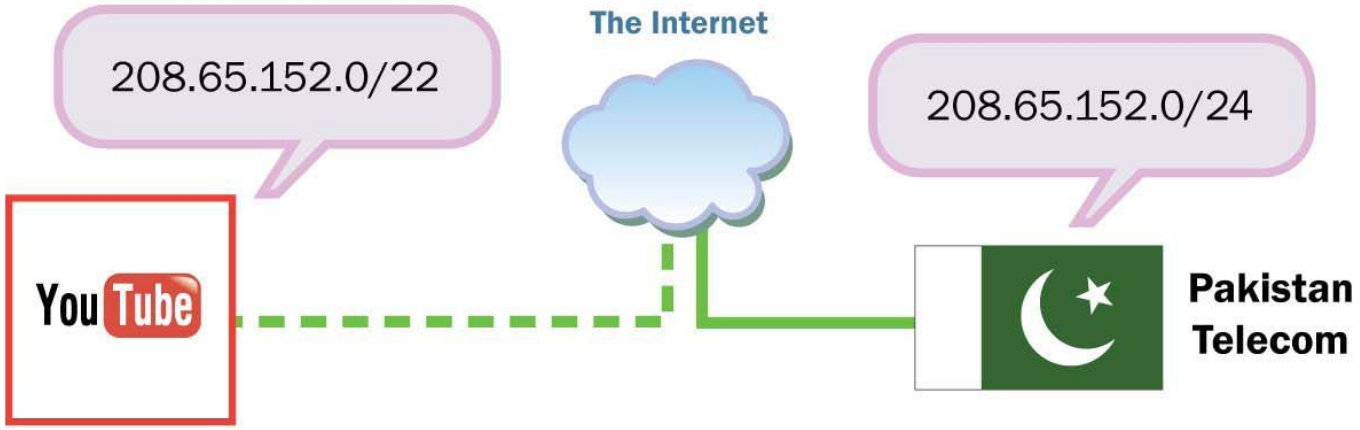
Rationale

- Routing mostly based on trust
- BGP offer amazing possibilities but poor security
- No systematic way to filter peers and customers
- Unreliable sources of policy information
- The Internet is full of stories of:
  - Route leaks you said?
  - BGP hijacks
  - Traffic redirection
  - Blackholing

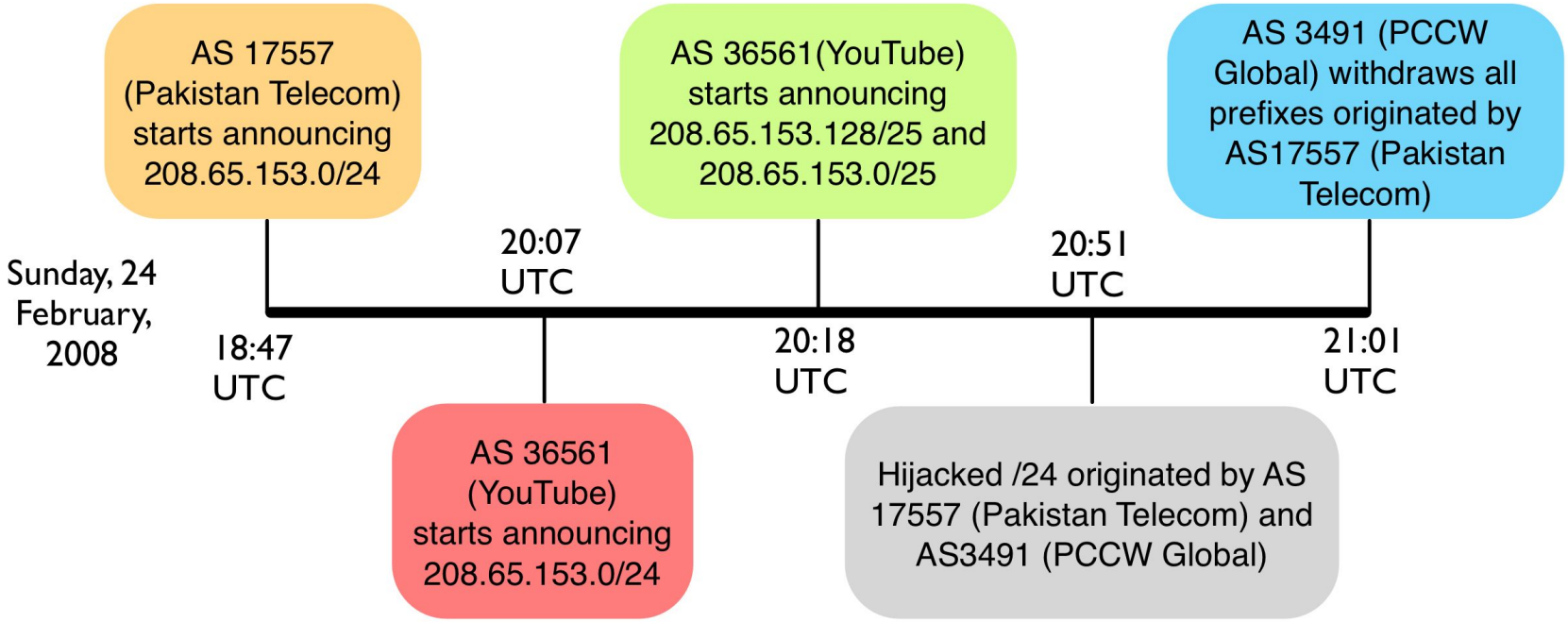
Mitigation techniques

- Conservative filtering
- Use of Routing Registries but:
  - Do not have all routing information
  - Do not necessarily mirror each other
  - Routing policies not kept up-to-date
  - Error-prone

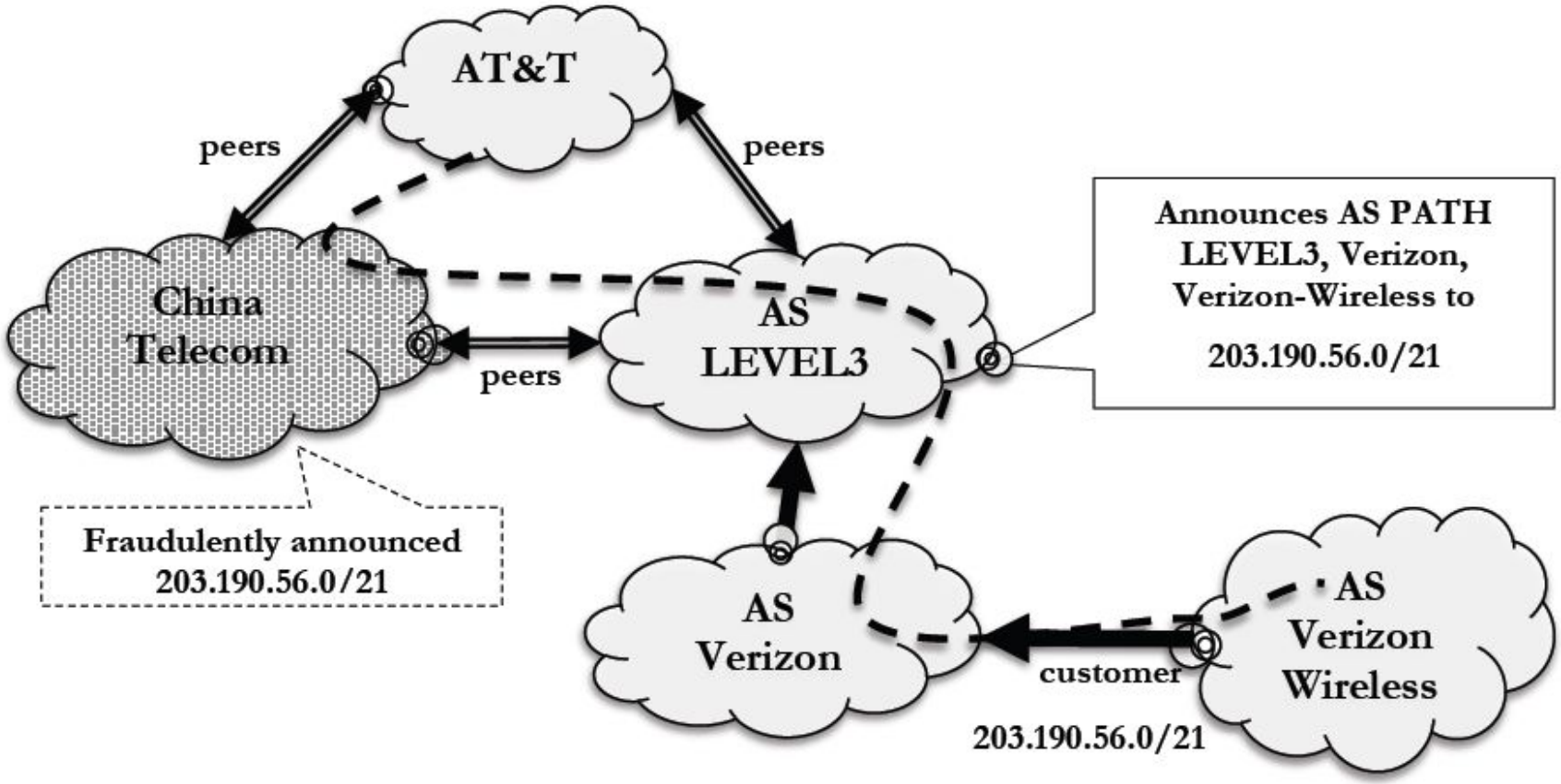
Youtube and Pakistan Telecom (2008)



Timeline


AS 17557 (Pakistan Telecom) starts announcing 208.65.153.0/24
AS 36561(YouTube) starts announcing 208.65.153.128/25 and 208.65.153.0/25
AS 3491 (PCCW Global) withdraws all prefixes originated by AS17557 (Pakistan Telecom)
Sunday, 24 February, 2008
18:47 UTC
20:07 UTC
20:18 UTC
20:51 UTC
21:01 UTC
AS 36561 (YouTube) starts announcing 208.65.153.0/24
Hijacked /24 originated by AS 17557 (Pakistan Telecom) and AS3491 (PCCW Global)

China Telecom - Traffic redirection



How do we securing Internet Routing?

Network	Next Hop	Metric	LocPrf	Weight	Path
192.0.2.0/24	1.1.1.1	20		0	1010 1011 286 4040 i
	2.2.2.2	20		0	2020 1011 4040 i
	3.3.3.3	10	100	0	2020 702 4040 i
	4.4.4.4	0	90	0	4040 i
	5.5.5.5	2659		0	5050 1011 4040 i
	6.6.6.6		80	0	6060 4040 i
	7.7.7.7	10	100	0	7070 3356 3356 4040 i

How do we securing Internet Routing?

Network	Next Hop	Metric	LocPrf	Weight	Path
192.0.2.0/24	1.1.1.1	20		0	1010 1011 286 4040 i
	2.2.2.2	20		0	2020 1011 4040 i
	3.3.3.3	10	100	0	2020 702 4040 i
	4.4.4.4	0	90	0	4040 i
	5.5.5.5	2659		0	5050 1011 4040 i
	6.6.6.6		80	0	6060 4040 i
	7.7.7.7	10	100	0	7070 3356 3356 4040 i

How do we securing Internet Routing?

Network	Next Hop	Metric	LocPrf	Weight	Path
192.0.2.0/24	1.1.1.1	20		0	1010 1011 286 4040 i
	2.2.2.2	20		0	2020 1011 4040 i
	3.3.3.3	10	100	0	2020 702 4040 i
	4.4.4.4	0	90	0	4040 i
	5.5.5.5	2659		0	5050 1011 4040 i
	6.6.6.6		80	0	6060 4040 i
	7.7.7.7	10	100	0	7070 3356 3356 4040 i

Prefix origination
AS_PATH

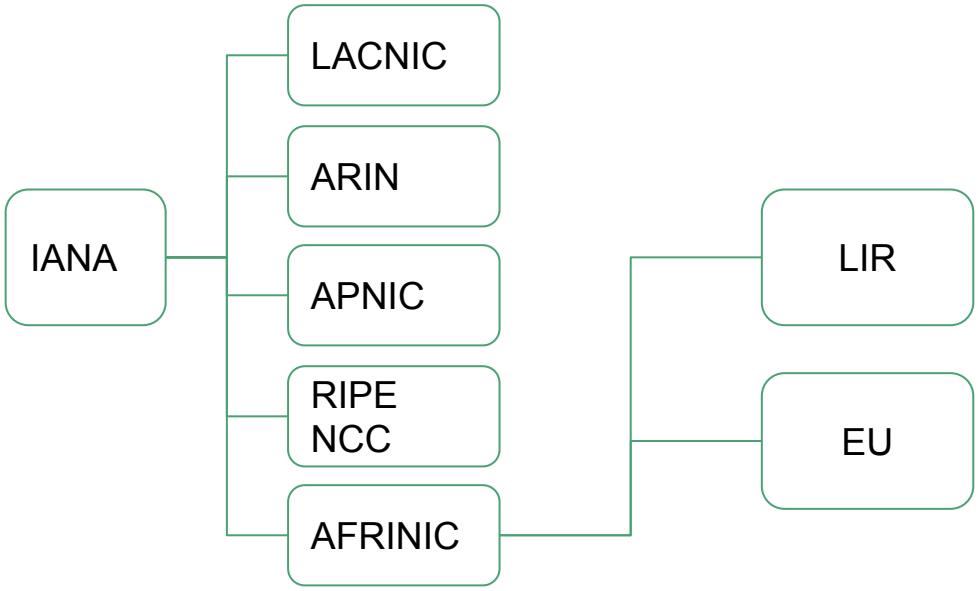
You need to secure both!!!

Solution - RPKI

- SIDR group at the IETF
  - How to securely verify that an AS is authorised to announce a prefix? (Origin Validation)
  - How to make sure that the AS_PATH has not been modified? (BGPSEC)
- Origin validation
  - RFC 5280: X.509 Public Key Infrastructure
  - RFC 3779: Extensions for IP addresses and ASN
- BGPSEC (still on-going)

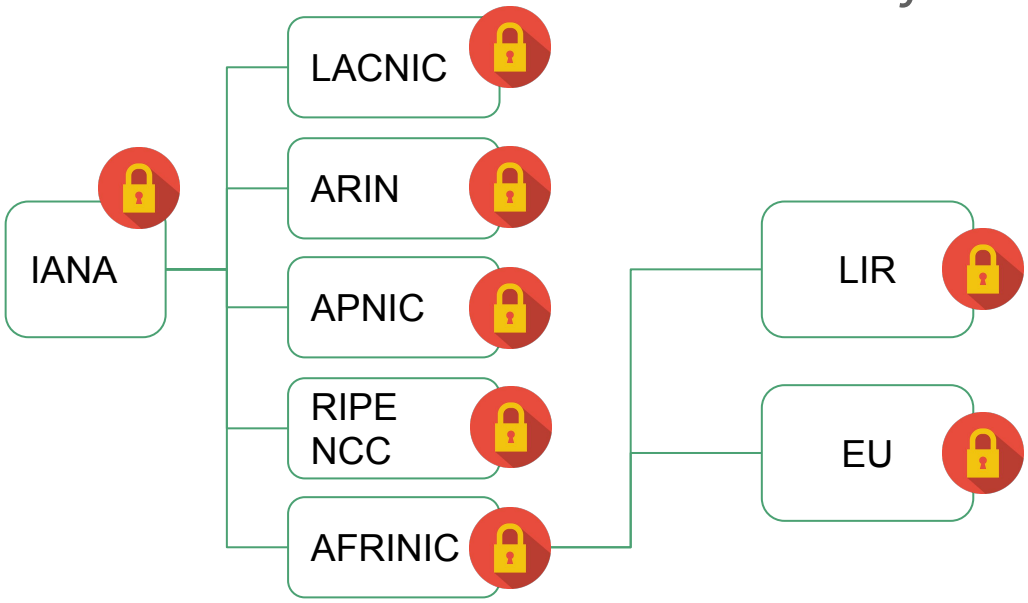
Role of the RIR

- Receives global allocations from IANA
- Distribute and manage resources at a regional level
- Make sure information are up-to-date and accurate
- Becomes the de-facto authority as sole registry regionally



Role of the RIR

- Receives global allocations from IANA
- Distribute and manage resources at a regional level
- Make sure information are up-to-date and accurate
- Becomes the de-facto authority as sole registry regionally

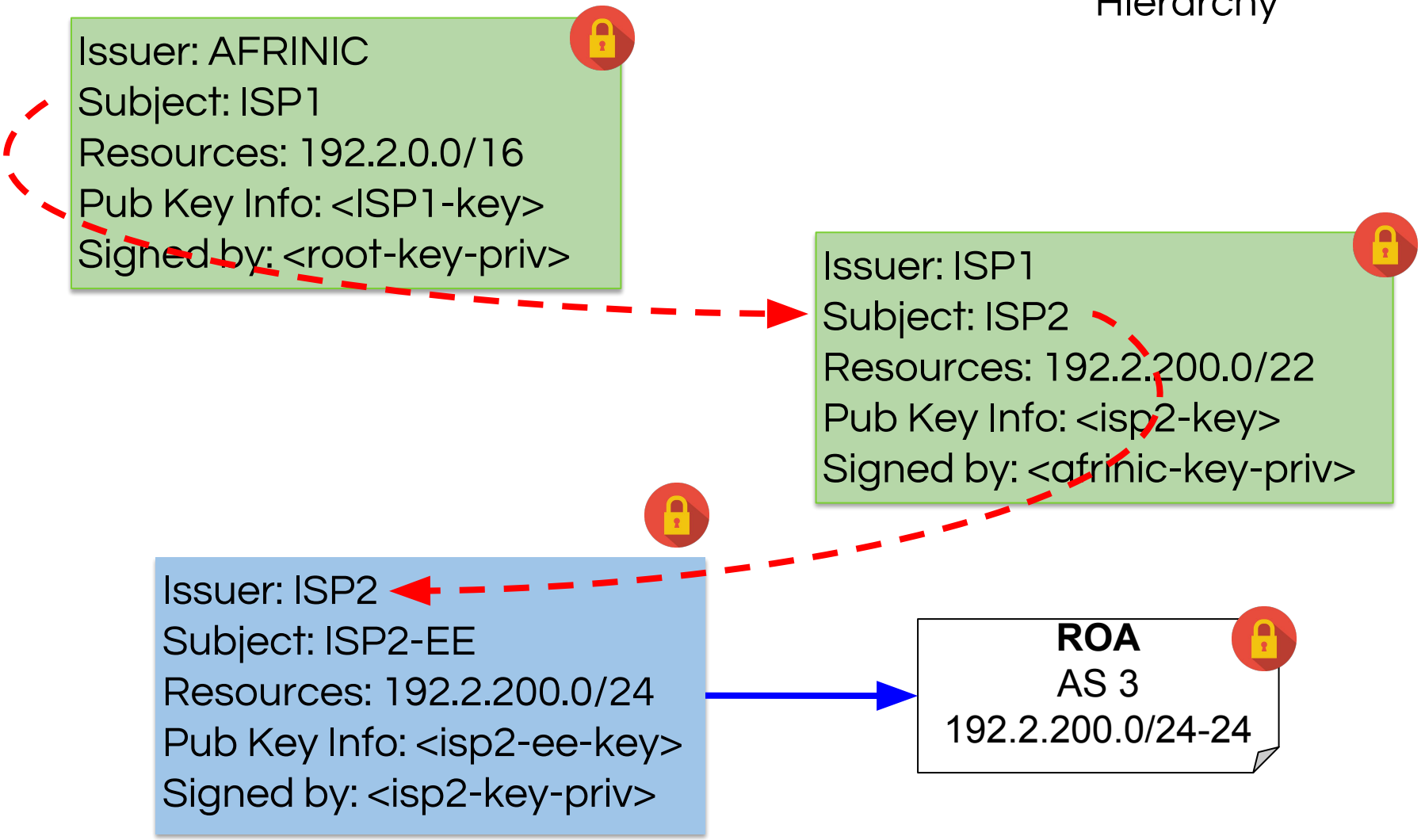


Resource Certificates

- RPKI defines two types of certificates:
  - CA - Certificate Authority (to issue CA or EE)
  - EE - End-entity (digital signature, etc)
- Certify resources - verifiable ownership!
- AFRINIC has a self-signed root certificate
- IANA one-day!
- Opt-in service, one year validity
- Exclude legacy space/members

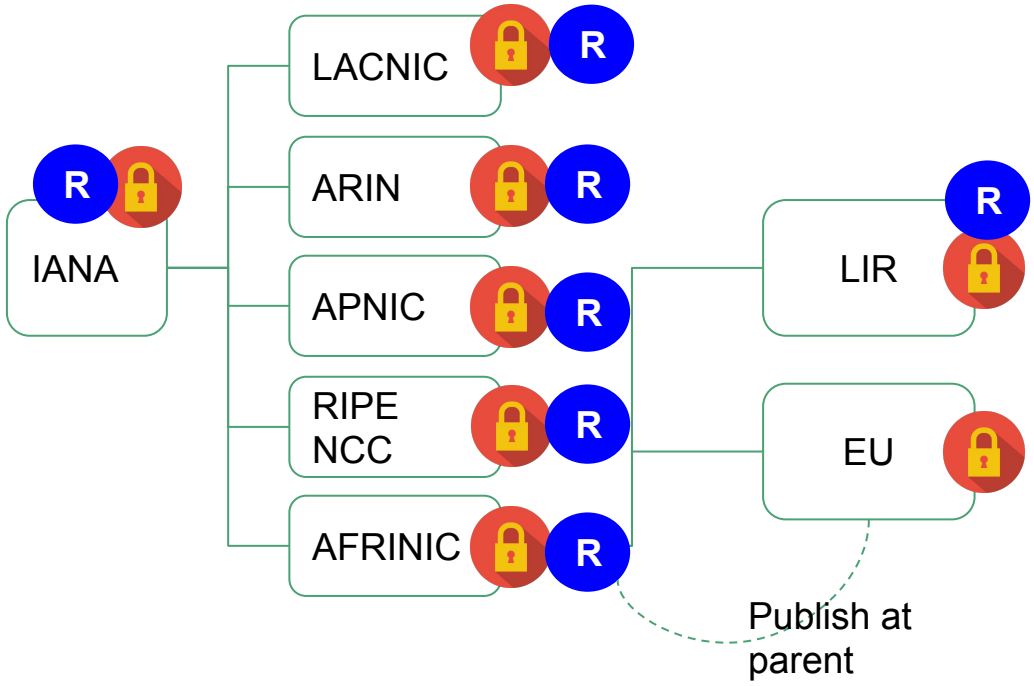
Certificate hierarchy

Resource Allocation Hierarchy

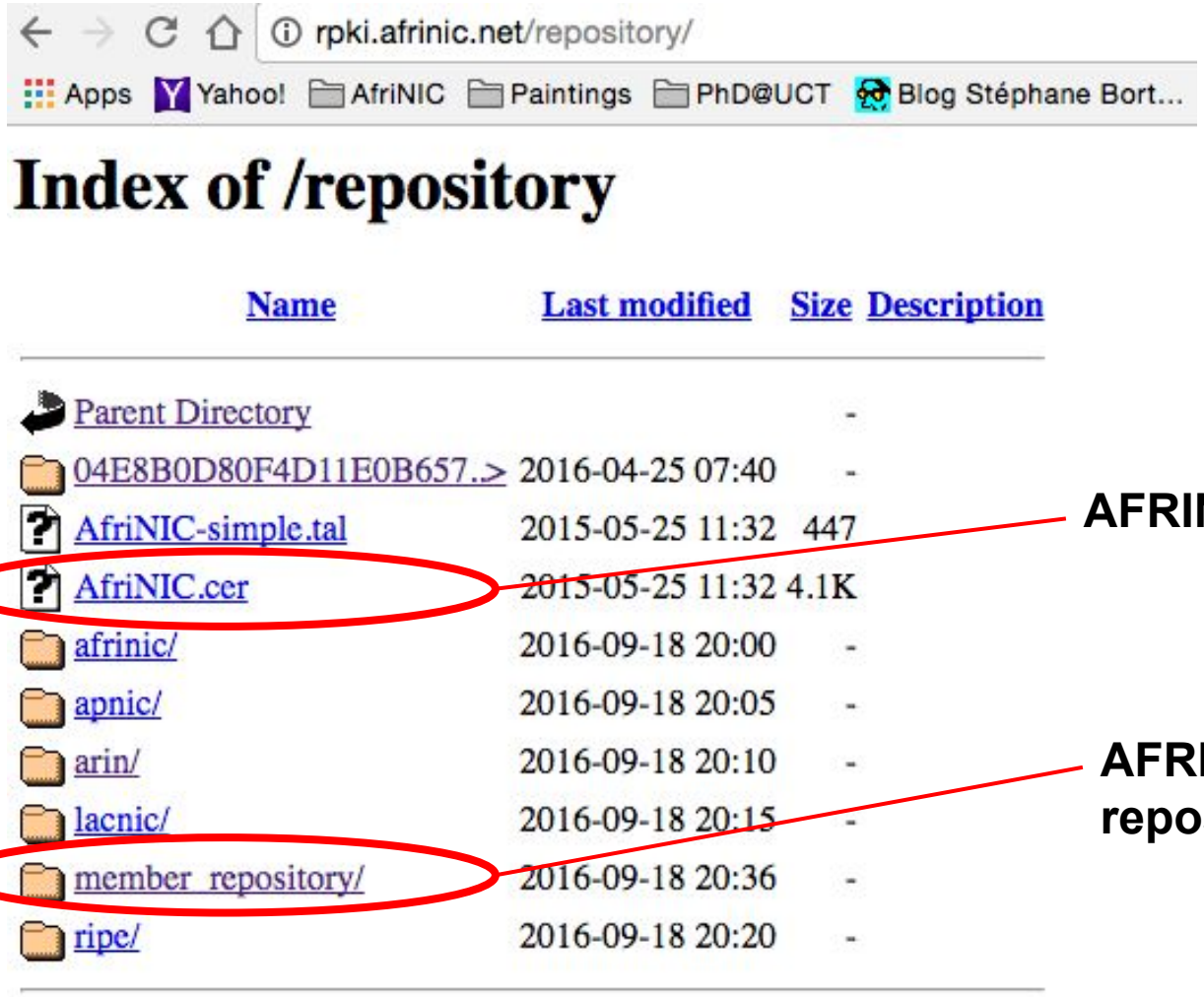


Repositories

- Public
- Certificates and ROA
- CRL and MFT
- Hosted or delegated
- HOSTED MODE only



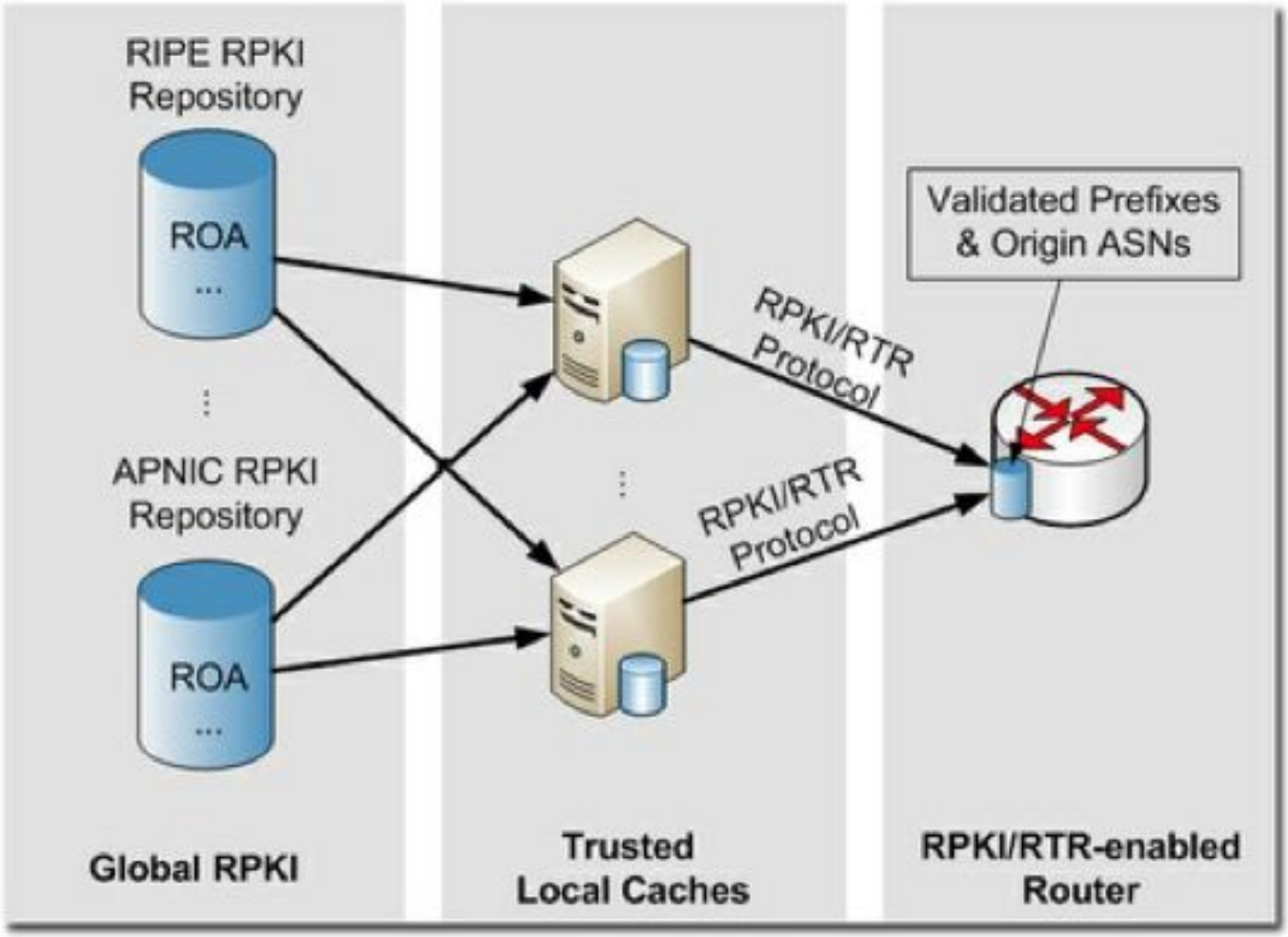
AFRINIC's Repository



Demo

https://my.afrinic.net

Validated caches



AFRINIC Validator Host: **validator.afrinic.net** Port: **8080**

Configure your router

```
router bgp 12345
…
bgp rpki server tcp 192.168.179.3 port 43779 refresh 60
bgp rpki server tcp 147.28.0.84 port 93920 refresh 60
```

Route announcement status

- **Valid** – A matching/covering prefix was found with a matching AS number
- **Invalid** – A covering prefix was found, but the AS number did not match, and there was no other matching one
- **NotFound** – No matching or covering prefix was found, same as today

You define your own policy

Fairly Secure

```
route-map validity-0
    match rpki valid
    set local-preference 100
route-map validity-1
    match rpki not-found
    set local-preference 50
! invalid is dropped
```

Paranoid

```
route-map validity-0
match rpki valid
set local-preference 110
! everything else dropped
```

Security Geek

```
route-map validity-0
match rpki invalid
set local-preference 110
! everything else dropped
```

RPKI tools

- Validators:
  - RIPE Validator
  - Rcynic - www.rpki.net (CA+Validator)
  - RPSTIR
- Looking glasses:
  - bgp.he.net
  - Bgpmon
  - RIPEStat

RPKI Hot topics

- Global trust anchor
  - ICANN/IANA/NRO
  - Support from local RIR community
- RPKI Adverse actions
- RPKI Validation considered
  - Transfers of resources
  - ERX spaces

Questions

rpki-help@afrinic.net