RAPID7

THE STATE OF BGP SECURITY:

INTERNET PLUMBING FOR NETWORK SECURITY PROFESSIONALS

Wim Remes

Blackhat USA 2015

Agenda

- BGP Security History
- The BGP Threat Model
- Why do we care?
- How do we get better?

BGP Security

“The internet of things”

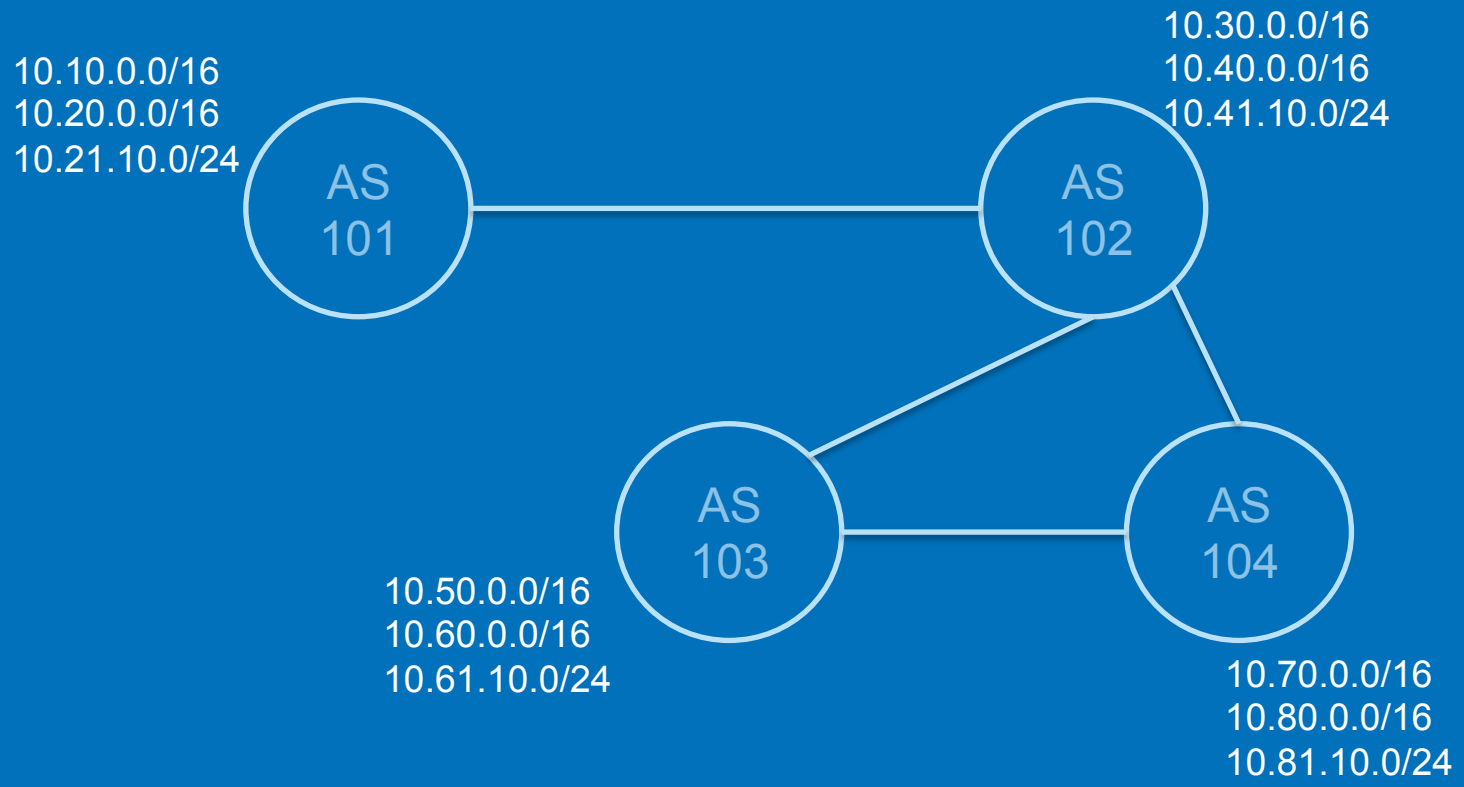
BGP Security

“The internet of your things”

BGP Security

“The internet of doing the right things”

BGP 101


10.10.0.0/16
10.20.0.0/16
10.21.10.0/24
AS
101
10.30.0.0/16
10.40.0.0/16
10.41.10.0/24
AS
102
AS
103
10.50.0.0/16
10.60.0.0/16
10.61.10.0/24
AS
104
10.70.0.0/16
10.80.0.0/16
10.81.10.0/24

BGP 101

AS 101:

how to get to 10.70.0.0/24?

AS 102, AS 104

AS 102, AS 103, AS 104

AS 104:

that link to AS 102 is too expensive

prepend 104, 104, 104 to the announcement

BGP 101

AS 101:

how to get to 10.70.0.0/24?

AS 102, AS 104, AS 104, AS 104, AS 104

AS 102, AS 103, AS 104

And then, there are routing policies …

filtering on reserved prefixes

filtering on attributed prefixes

filtering on too specific prefixes

etc. etc. etc.

BGP Security History

AS 7007 (1997)

Youtube hijacking (2008)

Chinese hijacking (2010)

BGP Security History

Malaysian route leak (2015)

Intentional BGP hijacking (2015)

(and numerous others, almost daily)

The BGP Threat Model

Anything is possible …

- Denial of service
- Router impersonation
- $big_service hijacking
- etc. etc.

But not everything is probable

Reality : attack surface is fairly limited

The BGP Threat Model

But :

Risk = impact x probability

The BGP Threat Model

But :

Risk = **impact** x probability

When it happens, it hurts.

- Directly involved parties
- Impacted ISPs
- Trust in the internet

The BGP Threat Model

Route hijacking

- through direct access to a router
- access to a router management computer
- collusion with an ASN owner

Why do we care?

BGP is foundational technology

- like DNS, SSL, HTTP, etc. etc.
- we expect it to “just work”
- “just working” depends on ASN owners

We need to be able to trust “our” internet.

Why do we care?

- Security technology exists!
  - Router authentication “just works”
    - it’s MD5, but it is better than nothing.
  - Resource Public Key Infrastructure “just works”
    - RIRs are ready to hand out ROAs
    - Routers are ready to use RPKI validation
    - RPKI validators exist
    - adoption rate, adoption rate, adoption rate, …

Why do we care?

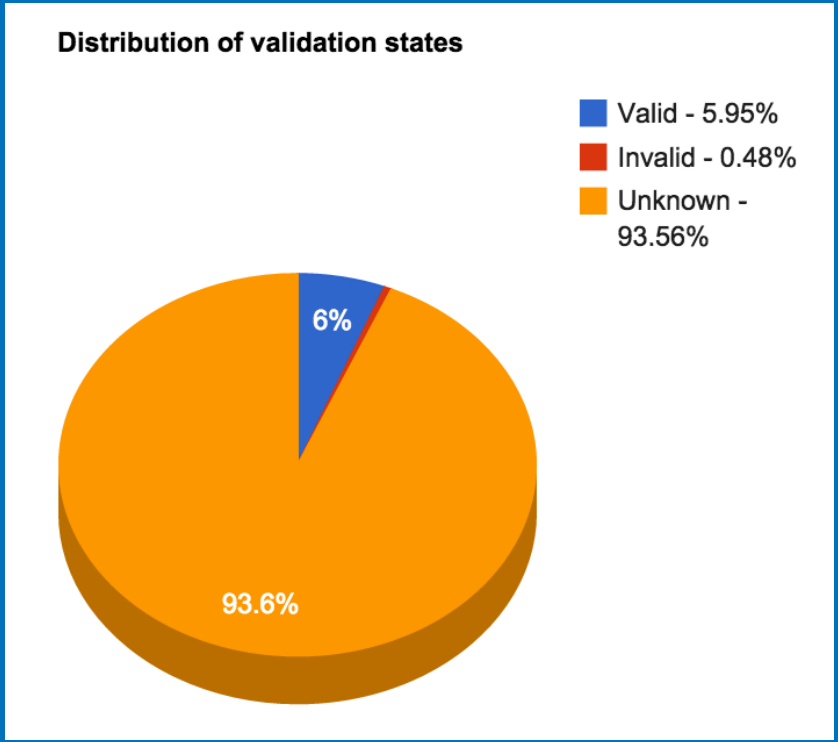
For you:

- the prefixes your infrastructure is hosted on.
- to prevent, to detect, to remediate

For “the cloud”:

- prefixes of any high value service you are using
- s/you/your constituents/g

Why do we care? (global)



Why do we care? (regional)

RIR	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
AFRINIC	13239 (100%)	100 (0.76%)	35 (0.26%)	13104 (98.98%)	74.07%	1.02%
APNIC	148044 (100%)	2166 (1.46%)	718 (0.48%)	145160 (98.05%)	75.1%	1.95%
ARIN	210163 (100%)	1391 (0.66%)	350 (0.17%)	208422 (99.17%)	79.9%	0.83%
LACNIC	75590 (100%)	17344 (22.94%)	772 (1.02%)	57474 (76.03%)	95.74%	23.97%
RIPE NCC	151526 (100%)	14627 (9.65%)	1021 (0.67%)	135878 (89.67%)	93.48%	10.33%

Why do we care? (per country)

Country	Total	Valid	Invalid	Unknown	Accuracy	RPKI Adoption Rate
BD	2373 (100%)	641 (27.01%)	6 (0.25%)	1726 (72.73%)	99.07%	27.27%
FR	5835 (100%)	1152 (19.74%)	105 (1.8%)	4578 (78.46%)	91.65%	21.54%
NL	5092 (100%)	686 (13.47%)	28 (0.55%)	4378 (85.98%)	96.08%	14.02%
US	174419 (100%)	984 (0.56%)	346 (0.2%)	173089 (99.24%)	73.98%	0.76%

Why do we care? (Alexa Top 500)

- Top 10
  - Only 1 (Facebook.com)
- Top 500
  - Only 16 (sixteen!)
  - 2 of them owned by Facebook
  - Most of them outside .com space
  - .ru, .fr, .de, .pl, …

BGP Security

“The internet of doing the right things”

How do we get better?

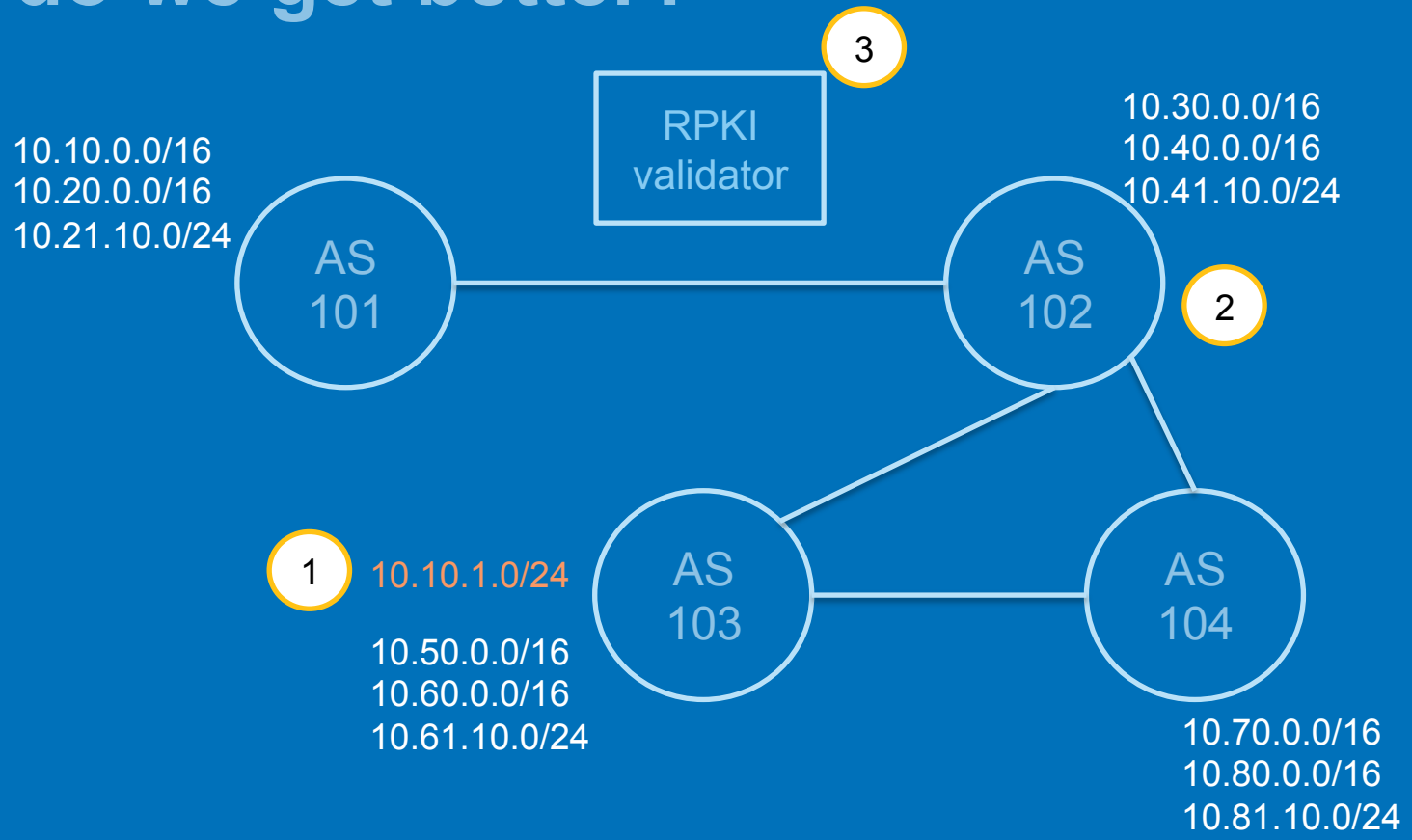
RPKI 101

Route Origin Associations (ROA)

```
Origin ASN       : 1234
Not valid before : 2015-08-05 00:00:00
Not valid after  : 2016-08-04 23:59:59
Prefixes         : 1.2.3.0/24 (max length /28)
                   2.3.4.0/18 (max length /32)
                   … … …
```

ASN owners request ROAs from RIRs

How do we get better?



How do we get better?

AS 103:

Yo, I have a route to 10.10.1.0/24 (1)

AS 102:

without RPKI (and no preventive routing policies)

Cool, here's the traffic!

with RPKI (and supportive routing policies)

102 : Hi validator, is 103 authorized for this prefix? (2)

Validator : heck no! (3)

102 : Ah, cool. Thanks!

How do we get better?

RPKI validator what?

RIPE open source validator.

<15 minutes to deploy (trust me, I've done it)

- install package

(ok, it requires java 7. /sadtrombone)

challenge : do better!

- configure router(s)
- done

https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources

How do we get better?

Monitoring what?

State University of Colorado

http://www.bgpmon.io/

livebgp.netsec.colostate.edu (port 50001)

XML data (reachability, withdraw, …)

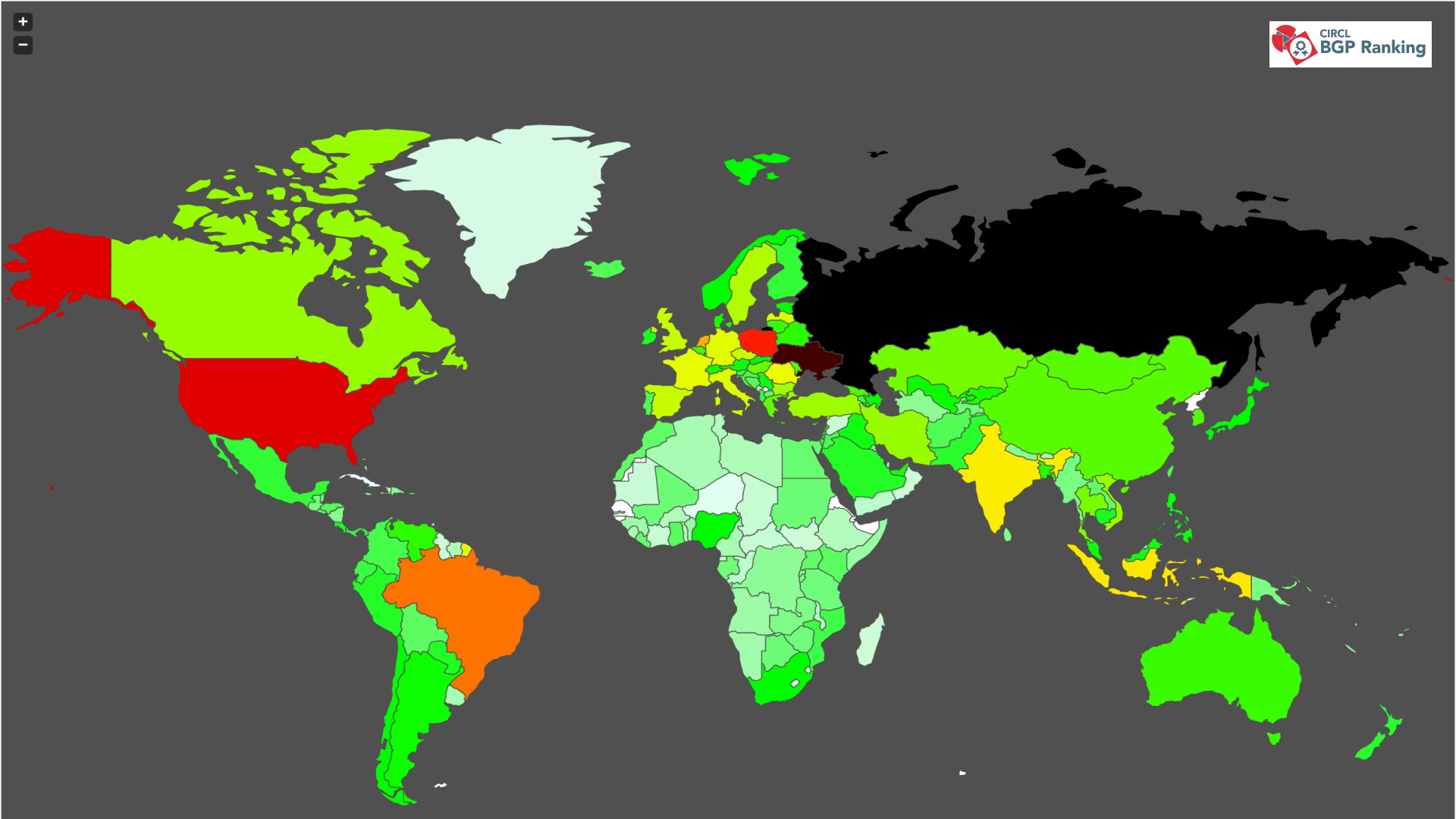
How do we get better?

Monitoring what?

CIRCL

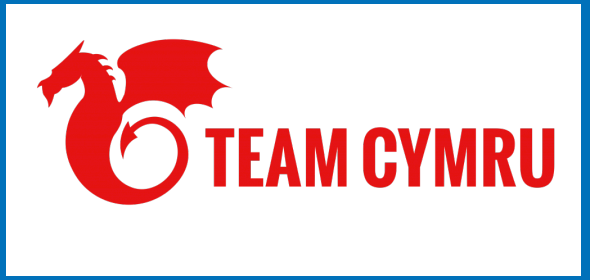
Computer Incident Response Center Luxembourg

https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources


CIRCL
BGP Ranking

How do we get better?

Monitoring what?



Conclusion

- BGP is important, for everybody
- We have to look beyond direct incentives
- We have the technology, let’s use it
- Let’s work together to make this happen

Thank you! Let’s DO this!

QUESTIONS?

Wim Remes
Manager Strategic Service EMEA
wim_remes@rapid7.com
@wimremes on twitter