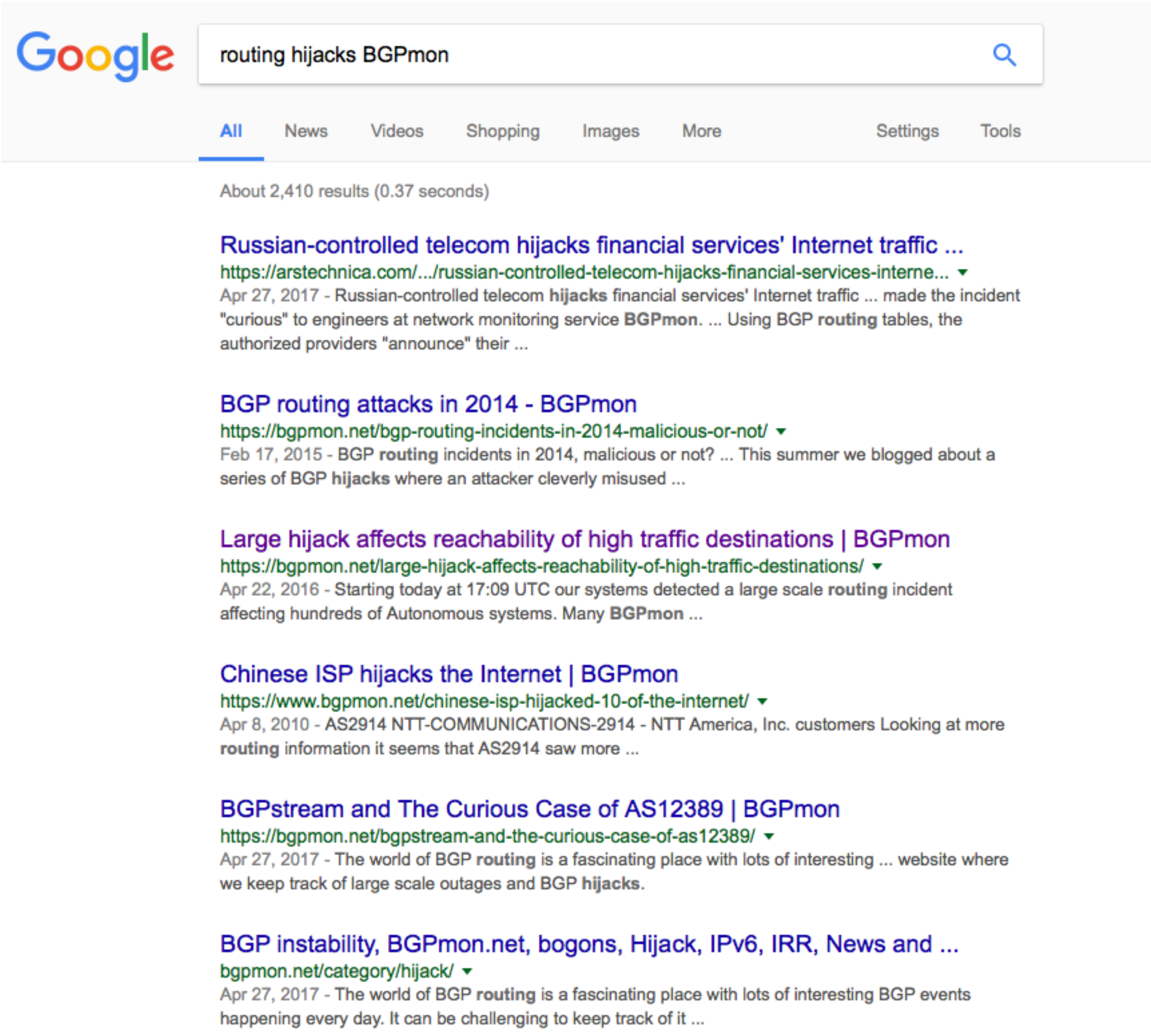
Securing BGP:
The current state of RPKI

Geoff Huston
Chief Scientist, APNIC

Incidents



About 2,410 results (0.37 seconds)

Russian-controlled telecom hijacks financial services' Internet traffic ...
https://arstechnica.com/.../russian-controlled-telecom-hijacks-financial-services-interne...
Apr 27, 2017 - Russian-controlled telecom **hijacks** financial services' Internet traffic ... made the incident "curious" to engineers at network monitoring service **BGPmon**. ... Using BGP **routing** tables, the authorized providers "announce" their ...

BGP routing attacks in 2014 - BGPmon
https://bgpmon.net/bgp-routing-incidents-in-2014-malicious-or-not/
Feb 17, 2015 - BGP **routing** incidents in 2014, malicious or not? ... This summer we blogged about a series of BGP **hijacks** where an attacker cleverly misused ...

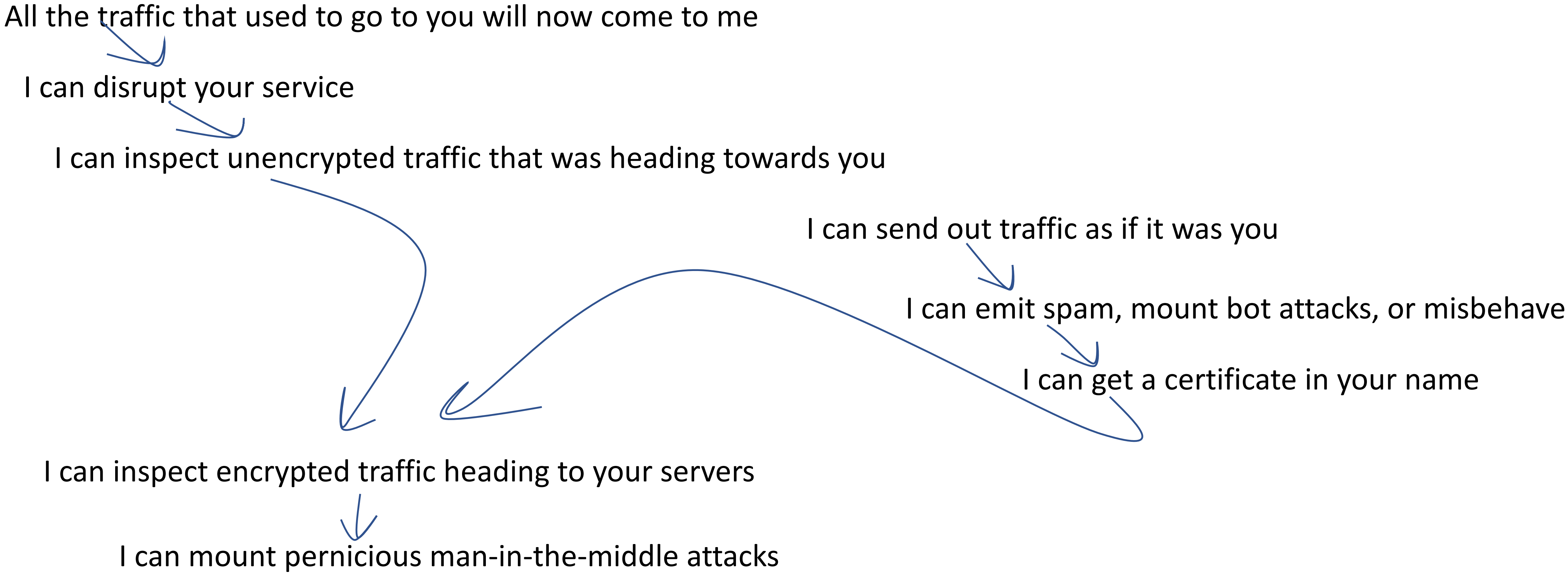
Large hijack affects reachability of high traffic destinations | BGPmon
https://bgpmon.net/large-hijack-affects-reachability-of-high-traffic-destinations/
Apr 22, 2016 - Starting today at 17:09 UTC our systems detected a large scale **routing** incident affecting hundreds of Autonomous systems. Many **BGPmon** ...

Chinese ISP hijacks the Internet | BGPmon
https://www.bgpmon.net/chinese-isp-hijacked-10-of-the-internet/
Apr 8, 2010 - AS2914 NTT-COMMUNICATIONS-2914 - NTT America, Inc. customers Looking at more **routing** information it seems that AS2914 saw more ...

BGPstream and The Curious Case of AS12389 | BGPmon
https://bgpmon.net/bgpstream-and-the-curious-case-of-as12389/
Apr 27, 2017 - The world of BGP **routing** is a fascinating place with lots of interesting ... website where we keep track of large scale outages and BGP **hijacks**.

BGP instability, BGPmon.net, bogons, Hijack, IPv6, IRR, News and ...
bgpmon.net/category/hijack/
Apr 27, 2017 - The world of BGP **routing** is a fascinating place with lots of interesting BGP events happening every day. It can be challenging to keep track of it ...

What happens when I announce your addresses in BGP?



All the traffic that used to go to you will now come to me

I can disrupt your service

I can inspect unencrypted traffic that was heading towards you

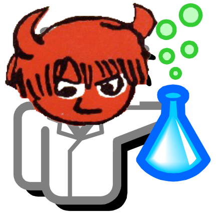
I can send out traffic as if it was you

I can emit spam, mount bot attacks, or misbehave

I can get a certificate in your name

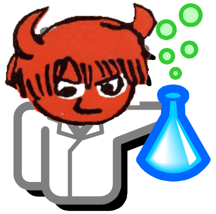
I can inspect encrypted traffic heading to your servers

I can mount pernicious man-in-the-middle attacks



If I were evil

- I’d announce your routes
- Use an automated cert issuer to get a certificate issued for your domain name
- Attract all secure traffic intended for your service and pass it on (man-in-the-middle)
  - But I use _MY_ encryption to the end user, so I can see everything the end users does with your service, including their passwords
  - And its not clear that they will notice anything amiss



If I were evil

- I’d announce your routes
- Use an autom

nd pass

to the end user, so I can see end users does with your service, including their passwords

  - And its not clear that they will notice anything amiss

This form of attack is challenging to prevent once the route hijack is installed

So a useful defence is to ensure that the routing system resists attempts to install route hijacks

If I were evil

- I'd announce your routes
- Use an autom

challenging to prevent once the route

system resists

pass

their

Th

hij

S

attempts

- And its not clear that they will notice anything

How can we counter route hijacks?

How can we tell what is a "genuine" route update and what's a fake?

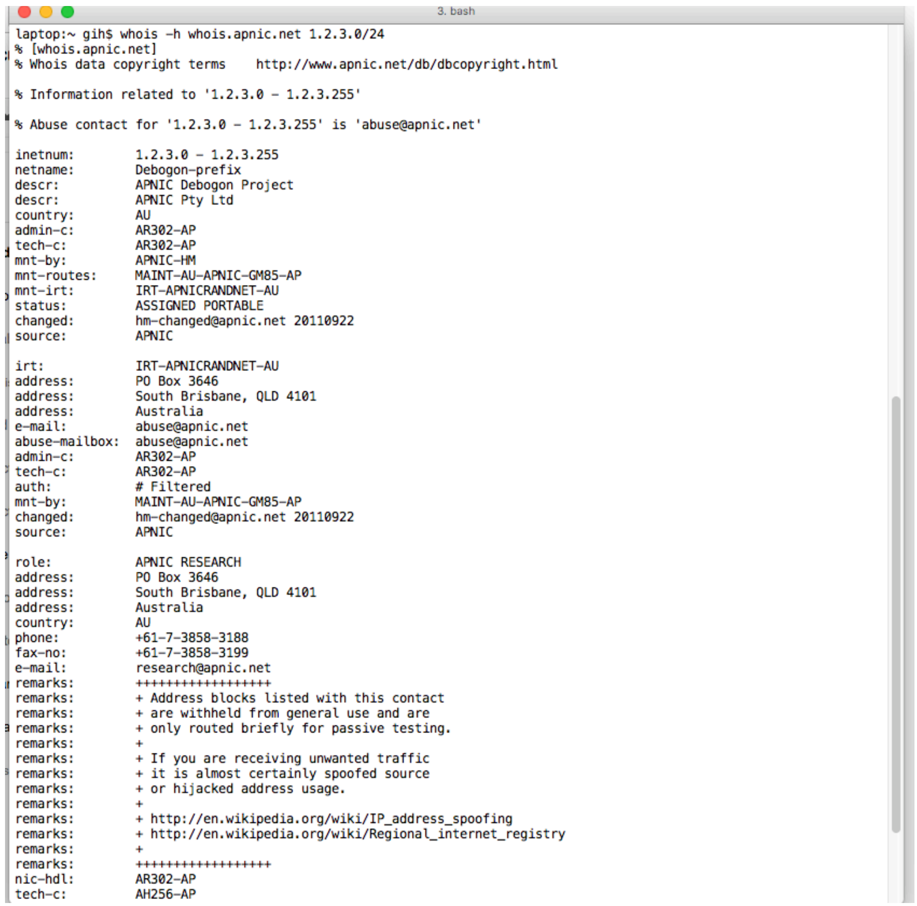
What do we do today?

What do we do today?

I ask you to route my net:

You look the net up on whois

If it all seems to match then accept the request and add it to the network filters for this customer



```
laptop:~ gih$ whois -h whois.apnic.net 1.2.3.0/24
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '1.2.3.0 - 1.2.3.255'

% Abuse contact for '1.2.3.0 - 1.2.3.255' is 'abuse@apnic.net'

inetnum:        1.2.3.0 - 1.2.3.255
netname:        Debogon-prefix
descr:          APNIC Debogon Project
descr:          APNIC Pty Ltd
country:        AU
admin-c:        AR302-AP
tech-c:         AR302-AP
mnt-by:         APNIC-HM
mnt-routes:     MAINT-AU-APNIC-GM85-AP
mnt-irt:        IRT-APNICRANDNET-AU
status:         ASSIGNED PORTABLE
changed:        hm-changed@apnic.net 20110922
source:         APNIC

irt:            IRT-APNICRANDNET-AU
address:        PO Box 3646
address:        South Brisbane, QLD 4101
address:        Australia
e-mail:         abuse@apnic.net
abuse-mailbox:  abuse@apnic.net
admin-c:        AR302-AP
tech-c:         AR302-AP
auth:           # Filtered
mnt-by:         MAINT-AU-APNIC-GM85-AP
changed:        hm-changed@apnic.net 20110922
source:         APNIC

role:           APNIC RESEARCH
address:        PO Box 3646
address:        South Brisbane, QLD 4101
address:        Australia
country:        AU
phone:          +61-7-3858-3188
fax-no:         +61-7-3858-3199
e-mail:         research@apnic.net
remarks:        ++++++++++++++++++
remarks:        + Address blocks listed with this contact
remarks:        + are withheld from general use and are
remarks:        + only routed briefly for passive testing.
remarks:        +
remarks:        + If you are receiving unwanted traffic
remarks:        + it is almost certainly spoofed source
remarks:        + or hijacked address usage.
remarks:        +
remarks:        + http://en.wikipedia.org/wiki/IP_address_spoofing
remarks:        + http://en.wikipedia.org/wiki/Regional_internet_registry
remarks:        +
remarks:        ++++++++++++++++++
nic-hdl:        AR302-AP
tech-c:         AH256-AP
```

What do we do today?

I ask you to route my net:

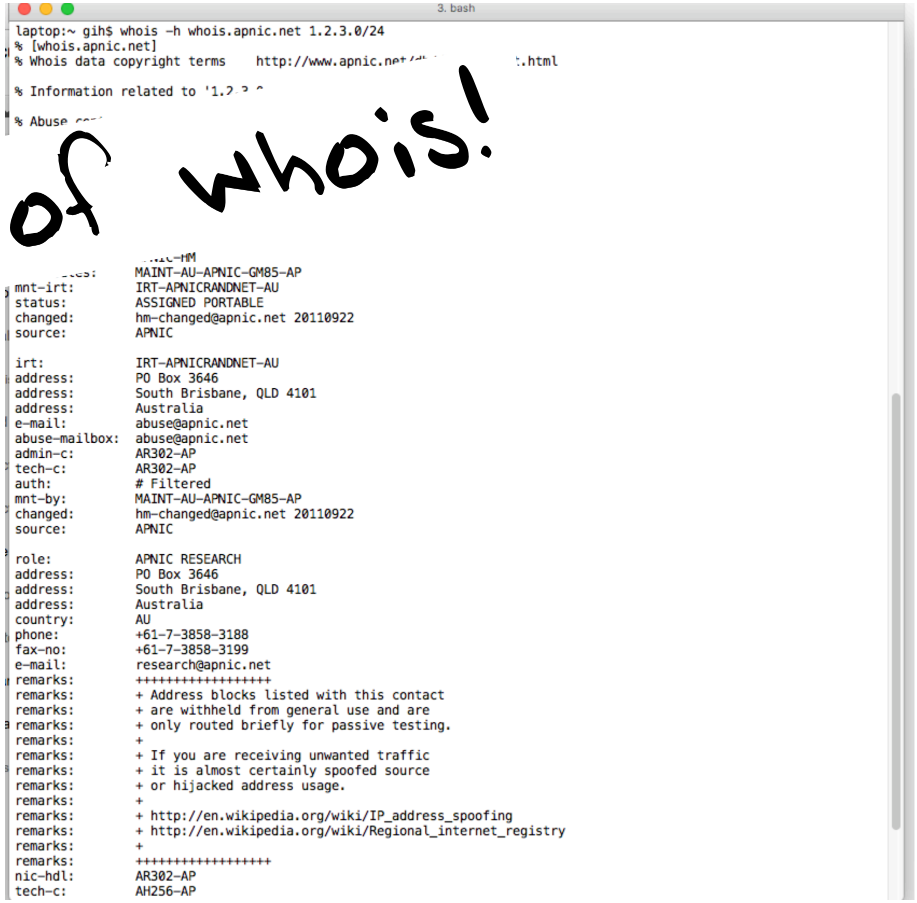
You look the net up on whois

If it all seems to match t

th the

ne filters for this customer

The awesome power of whois!



3. bash

```
laptop:~ gih$ whois -h whois.apnic.net 1.2.3.0/24
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/              .html

% Information related to '1.2.3

% Abuse

                 MAINT-AU-APNIC-GM85-AP
mnt-irt:         IRT-APNICRANDNET-AU
status:          ASSIGNED PORTABLE
changed:         hm-changed@apnic.net 20110922
source:          APNIC

irt:             IRT-APNICRANDNET-AU
address:         PO Box 3646
address:         South Brisbane, QLD 4101
address:         Australia
e-mail:          abuse@apnic.net
abuse-mailbox:   abuse@apnic.net
admin-c:         AR302-AP
tech-c:          AR302-AP
auth:            # Filtered
mnt-by:          MAINT-AU-APNIC-GM85-AP
changed:         hm-changed@apnic.net 20110922
source:          APNIC

role:            APNIC RESEARCH
address:         PO Box 3646
address:         South Brisbane, QLD 4101
address:         Australia
country:         AU
phone:           +61-7-3858-3188
fax-no:          +61-7-3858-3199
e-mail:          research@apnic.net
remarks:         +++++++++++++++++
remarks:         + Address blocks listed with this contact
remarks:         + are withheld from general use and are
remarks:         + only routed briefly for passive testing.
remarks:         +
remarks:         + If you are receiving unwanted traffic
remarks:         + it is almost certainly spoofed source
remarks:         + or hijacked address usage.
remarks:         +
remarks:         + http://en.wikipedia.org/wiki/IP_address_spoofing
remarks:         + http://en.wikipedia.org/wiki/Regional_internet_registry
remarks:         +
remarks:         +++++++++++++++++
nic-hdl:         AR302-AP
tech-c:          AH256-AP
```

What do we do today?

I ask you to route my net

You ask for me to provide a “Letter of Authority”

Which is an effort to absolve you of all liability that may arise from announcing this route

You then add the to the network filters for this customer

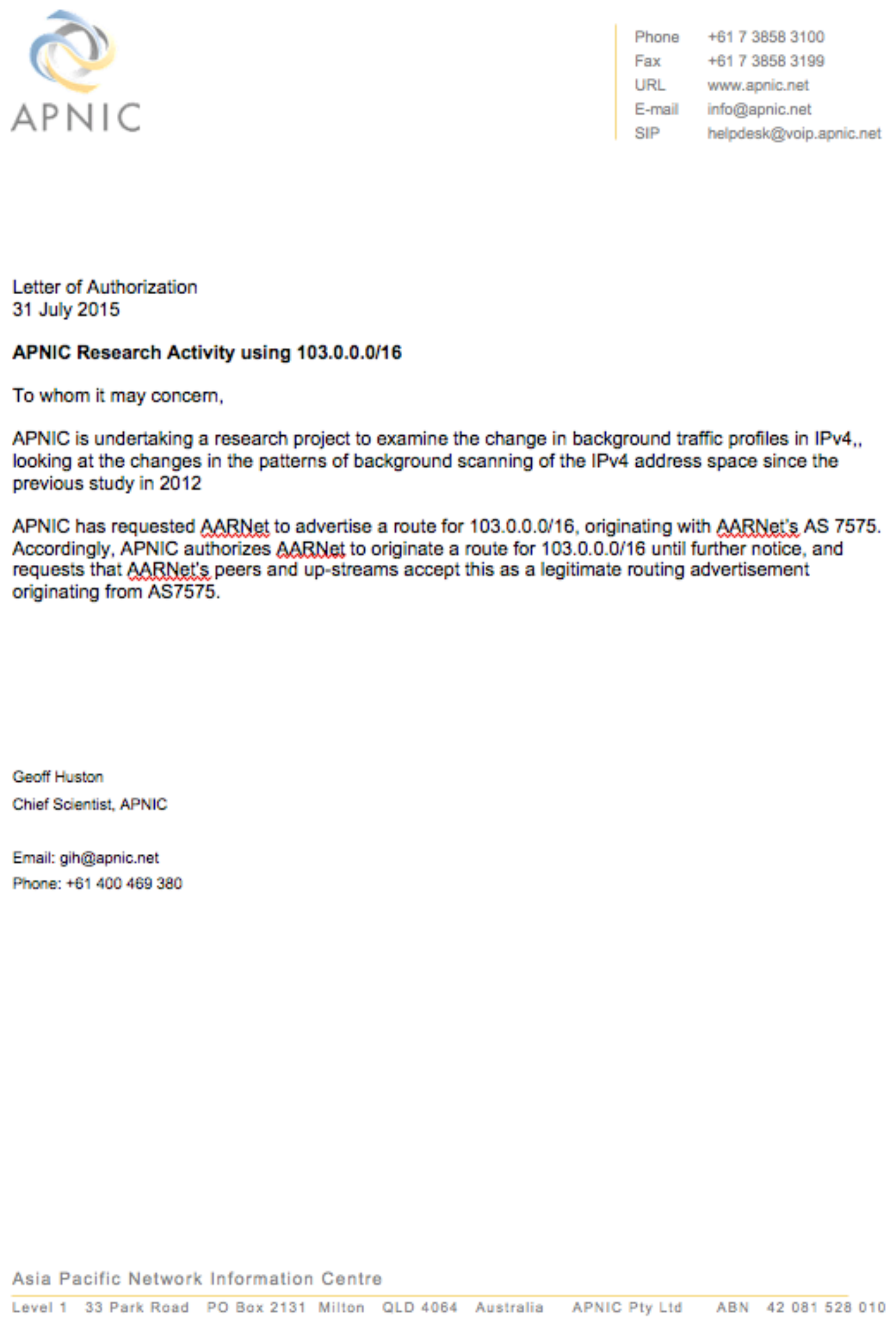
What do we

I ask you to route m

You ask for me to p

Which is an effort t nay arise from announcing this rou

You then add the tc mer



APNIC

Phone +61 7 3858 3100
Fax +61 7 3858 3199
URL www.apnic.net
E-mail info@apnic.net
SIP helpdesk@voip.apnic.net

Letter of Authorization
31 July 2015

APNIC Research Activity using 103.0.0.0/16

To whom it may concern,

APNIC is undertaking a research project to examine the change in background traffic profiles in IPv4,, looking at the changes in the patterns of background scanning of the IPv4 address space since the previous study in 2012

APNIC has requested AARNet to advertise a route for 103.0.0.0/16, originating with AARNet's AS 7575. Accordingly, APNIC authorizes AARNet to originate a route for 103.0.0.0/16 until further notice, and requests that AARNet's peers and up-streams accept this as a legitimate routing advertisement originating from AS7575.

Geoff Huston
Chief Scientist, APNIC

Email: gih@apnic.net
Phone: +61 400 469 380

Asia Pacific Network Information Centre
Level 1 33 Park Road PO Box 2131 Milton QLD 4064 Australia APNIC Pty Ltd ABN 42 081 528 010

What do we

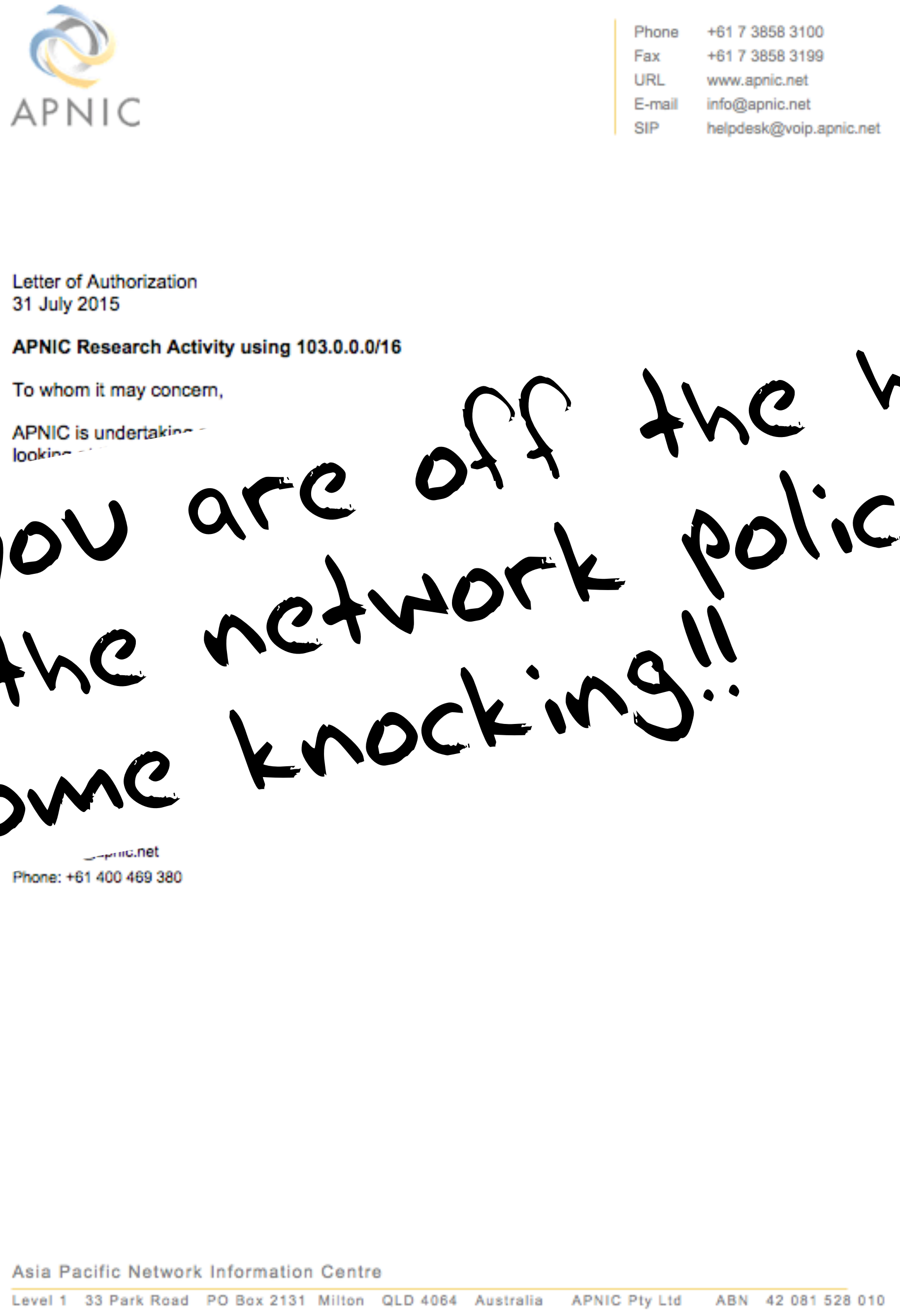
I ask you to route m

You ask for me to r

W' e from

an

You mer



APNIC

Phone +61 7 3858 3100
Fax +61 7 3858 3199
URL www.apnic.net
E-mail info@apnic.net
SIP helpdesk@voip.apnic.net

Letter of Authorization
31 July 2015

APNIC Research Activity using 103.0.0.0/16

To whom it may concern,

APNIC is undertakin
lookin

apnic.net
Phone: +61 400 469 380

Asia Pacific Network Information Centre
Level 1 33 Park Road PO Box 2131 Milton QLD 4064 Australia APNIC Pty Ltd ABN 42 081 528 010

At least you are off the hook
when the network police
come knocking!!

What do we do today?

I ask you to route my net

You ask for me to enter the details in a route registry

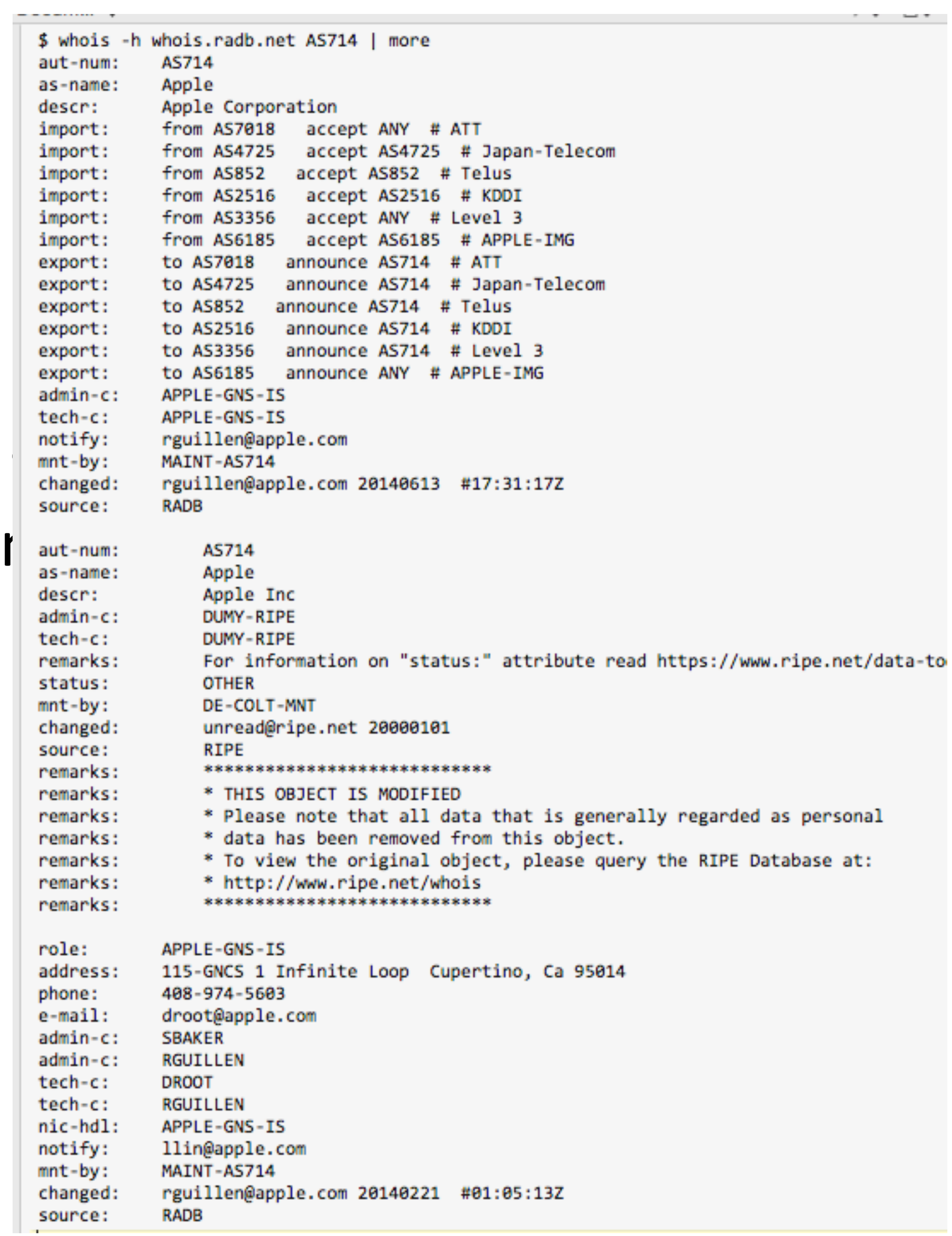
Access filters may be automatically generated from route registry data

What do we do today?

I ask you to route my net

You ask for me to enter the details in

Access filters may be automatically gen



```
$ whois -h whois.radb.net AS714 | more
aut-num:     AS714
as-name:     Apple
descr:       Apple Corporation
import:      from AS7018   accept ANY  # ATT
import:      from AS4725   accept AS4725  # Japan-Telecom
import:      from AS852   accept AS852  # Telus
import:      from AS2516   accept AS2516  # KDDI
import:      from AS3356   accept ANY  # Level 3
import:      from AS6185   accept AS6185  # APPLE-IMG
export:      to AS7018   announce AS714  # ATT
export:      to AS4725   announce AS714  # Japan-Telecom
export:      to AS852   announce AS714  # Telus
export:      to AS2516   announce AS714  # KDDI
export:      to AS3356   announce AS714  # Level 3
export:      to AS6185   announce ANY  # APPLE-IMG
admin-c:     APPLE-GNS-IS
tech-c:      APPLE-GNS-IS
notify:      rguillen@apple.com
mnt-by:      MAINT-AS714
changed:     rguillen@apple.com 20140613  #17:31:17Z
source:      RADB

aut-num:         AS714
as-name:         Apple
descr:           Apple Inc
admin-c:         DUMY-RIPE
tech-c:          DUMY-RIPE
remarks:         For information on "status:" attribute read https://www.ripe.net/data-to
status:          OTHER
mnt-by:          DE-COLT-MNT
changed:         unread@ripe.net 20000101
source:          RIPE
remarks:         ****************************
remarks:         * THIS OBJECT IS MODIFIED
remarks:         * Please note that all data that is generally regarded as personal
remarks:         * data has been removed from this object.
remarks:         * To view the original object, please query the RIPE Database at:
remarks:         * http://www.ripe.net/whois
remarks:         ****************************

role:        APPLE-GNS-IS
address:     115-GNCS 1 Infinite Loop  Cupertino, Ca 95014
phone:       408-974-5603
e-mail:      droot@apple.com
admin-c:     SBAKER
admin-c:     RGUILLEN
tech-c:      DROOT
tech-c:      RGUILLEN
nic-hdl:     APPLE-GNS-IS
notify:      llin@apple.com
mnt-by:      MAINT-AS714
changed:     rguillen@apple.com 20140221  #01:05:13Z
source:      RADB
```

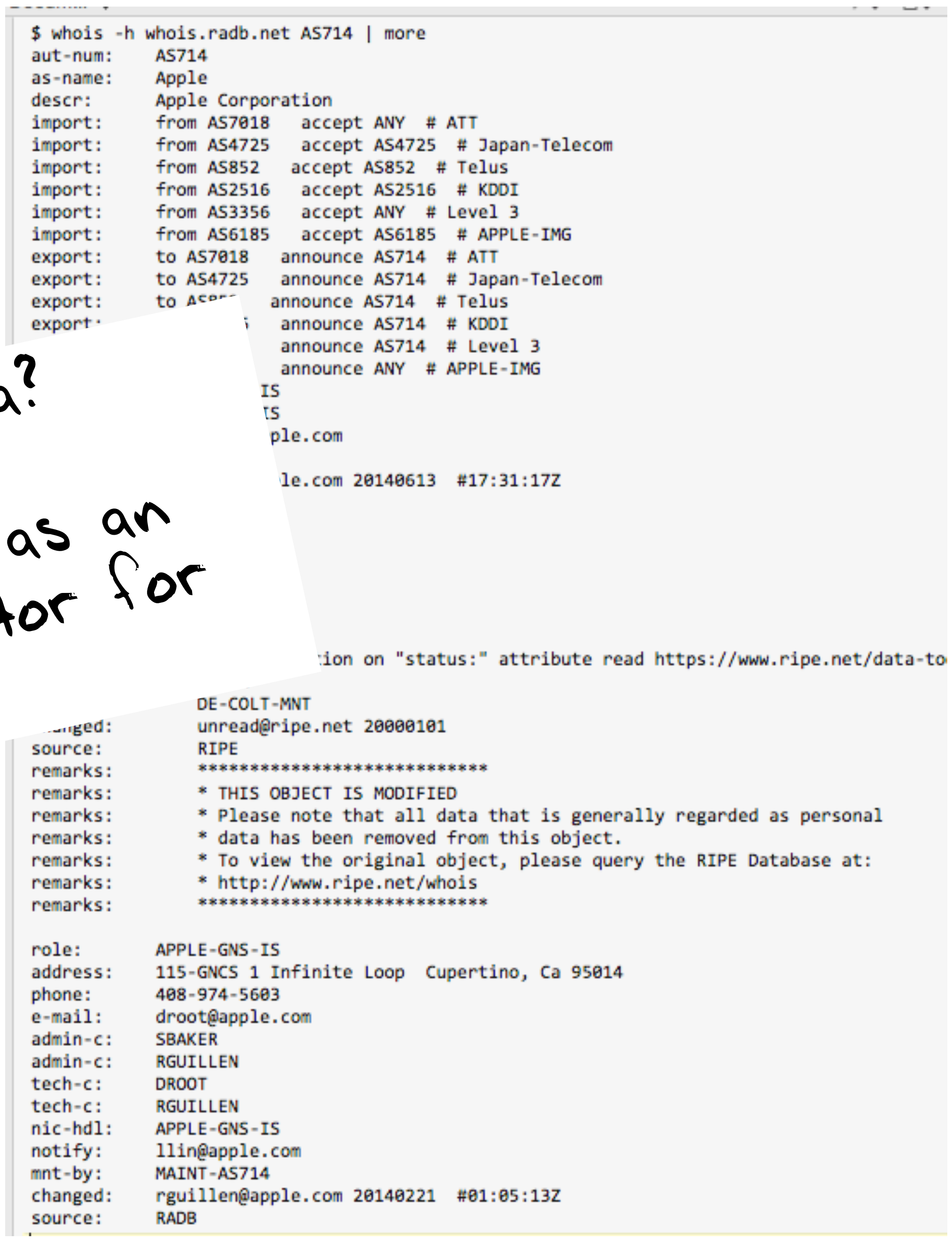
What do we do today?

I ask you to route my net

You ask for me to ente

Access fil

- How current is this data?
- is it complete?
- Can i trust it to use as an automatic filter generator for my routers?



```
$ whois -h whois.radb.net AS714 | more
aut-num:     AS714
as-name:     Apple
descr:       Apple Corporation
import:      from AS7018   accept ANY  # ATT
import:      from AS4725   accept AS4725  # Japan-Telecom
import:      from AS852   accept AS852  # Telus
import:      from AS2516   accept AS2516  # KDDI
import:      from AS3356   accept ANY  # Level 3
import:      from AS6185   accept AS6185  # APPLE-IMG
export:      to AS7018   announce AS714  # ATT
export:      to AS4725   announce AS714  # Japan-Telecom
export:      to AS8   announce AS714  # Telus
export              announce AS714  # KDDI
                    announce AS714  # Level 3
                    announce ANY  # APPLE-IMG
                  IS
                  IS
                  ple.com

                  le.com 20140613  #17:31:17Z

                    ion on "status:" attribute read https://www.ripe.net/data-to

                 DE-COLT-MNT
  nged:          unread@ripe.net 20000101
source:          RIPE
remarks:         ****************************
remarks:         * THIS OBJECT IS MODIFIED
remarks:         * Please note that all data that is generally regarded as personal
remarks:         * data has been removed from this object.
remarks:         * To view the original object, please query the RIPE Database at:
remarks:         * http://www.ripe.net/whois
remarks:         ****************************

role:        APPLE-GNS-IS
address:     115-GNCS 1 Infinite Loop  Cupertino, Ca 95014
phone:       408-974-5603
e-mail:      droot@apple.com
admin-c:     SBAKER
admin-c:     RGUILLEN
tech-c:      DROOT
tech-c:      RGUILLEN
nic-hdl:     APPLE-GNS-IS
notify:      llin@apple.com
mnt-by:      MAINT-AS714
changed:     rguillen@apple.com 20140221  #01:05:13Z
source:      RADB
```

What do we do today?

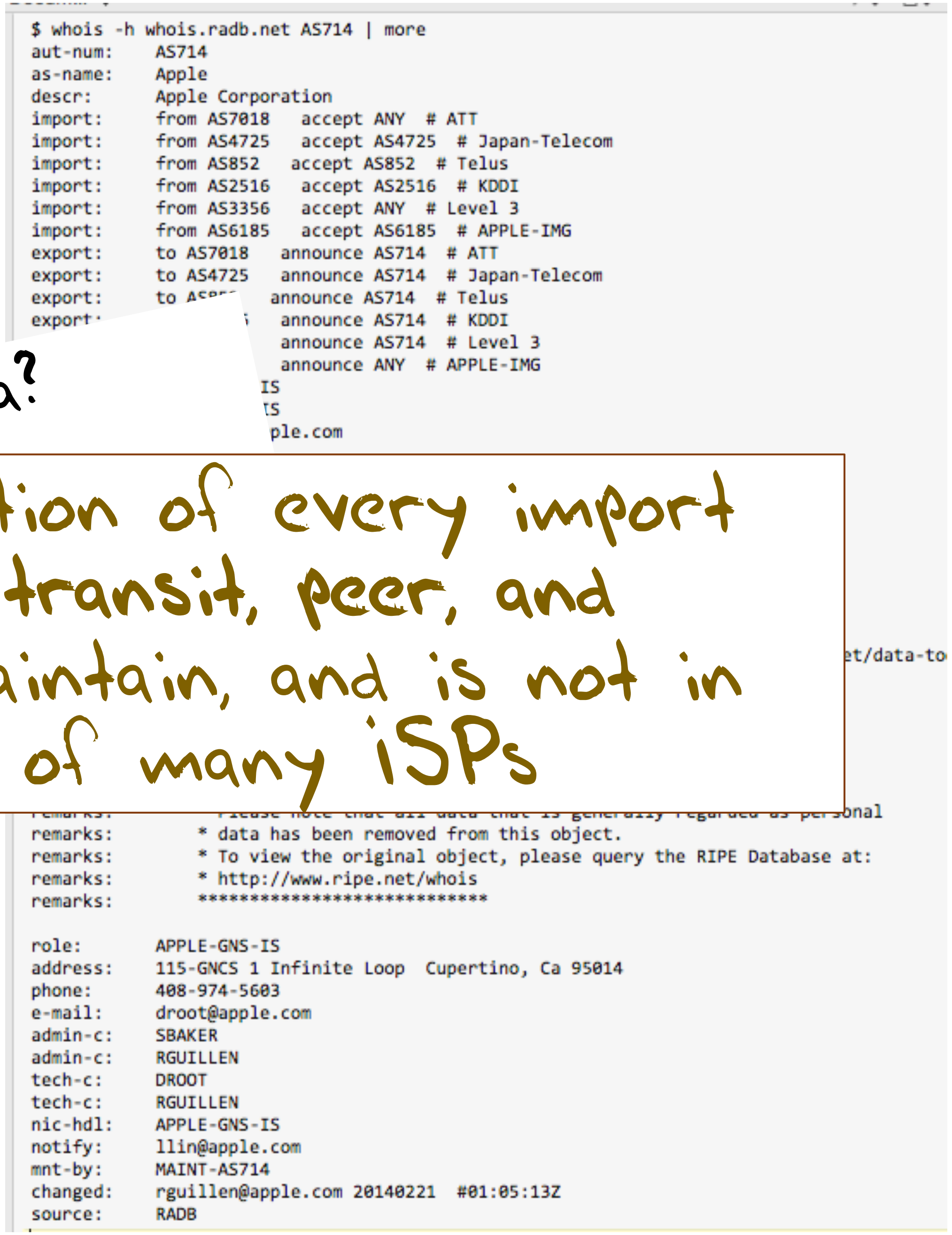
I ask you to route my net

You ask for me to enter is this data?

Ac

my

A publicly accessible description of every import and export policy to every transit, peer, and customer, is difficult to maintain, and is not in the best business interests of many iSPs



```
$ whois -h whois.radb.net AS714 | more
aut-num:    AS714
as-name:    Apple
descr:      Apple Corporation
import:     from AS7018   accept ANY  # ATT
import:     from AS4725   accept AS4725  # Japan-Telecom
import:     from AS852   accept AS852  # Telus
import:     from AS2516   accept AS2516  # KDDI
import:     from AS3356   accept ANY  # Level 3
import:     from AS6185   accept AS6185  # APPLE-IMG
export:     to AS7018   announce AS714  # ATT
export:     to AS4725   announce AS714  # Japan-Telecom
export:     to AS8   announce AS714  # Telus
export:            announce AS714  # KDDI
                   announce AS714  # Level 3
                   announce ANY  # APPLE-IMG
                 IS
                 IS
                 ple.com

                                                                    et/data-to

remarks:        * data has been removed from this object.
remarks:        * To view the original object, please query the RIPE Database at:
remarks:        * http://www.ripe.net/whois
remarks:        ****************************

role:       APPLE-GNS-IS
address:    115-GNCS 1 Infinite Loop  Cupertino, Ca 95014
phone:      408-974-5603
e-mail:     droot@apple.com
admin-c:    SBAKER
admin-c:    RGUILLEN
tech-c:     DROOT
tech-c:     RGUILLEN
nic-hdl:    APPLE-GNS-IS
notify:     llin@apple.com
mnt-by:     MAINT-AS714
changed:    rguillen@apple.com 20140221  #01:05:13Z
source:     RADB
```

What’s the problem here?

- Whois lookups typically require manual processing.
  - This information is also somewhat informal so it often requires some level of interpretation and judgment
  - Whois lookups are an admission process, not a means to maintain route filters
- Letters of Authority are just a way to try and avoid liabilities – they are not a useful tool to manage routing
- Routing Registries come in all shapes and sizes!
  - Which is itself a problem – there is no single authoritative source
  - The expression of routing policies quickly becomes complex and error prone
  - Is this a case of attempting to harness too much information?

The RPKI Approach

- None of these approaches are very satisfactory as a complete solution to this problem
- Let’s take a step back and see if we can use digital signature technology to assist here.
- If we can, then we can construct automated systems that will recognise validly signed attestations about addresses and their use

Using Cryptography to tell “Good” from “Bad”

This looks a lot like an application of public/private key cryptography, with “authority to use” conveyed by a digital signature

- Using a private key to sign the authority, and the public key to validate the authority
- If the private key was held by the address holder then we have the notion of binding the control over an address to holding the private key
- We can use a conventional certificate infrastructure to support public key validation at the scale of the Internet
- But how can we inject trustable authority into this framework?

Trustable Credentials

How can we inject trustable authority into this framework?

Trustable Credentials

How can we inject trustable authority into this framework?

Bind the Registry and the key structure together:

- Use the existing address allocation hierarchy
  - IANA, RIRs, NIRs & LIRs, End holders
- Describe this address allocation structure using digital certificates
- The certificates do not introduce additional data – they are a representation of registry information in a particular digital format

Resource Certificates

- A resource certificate is a digital document that binds together an IP address block with the IP address holder’s public key, signed by the certification authority’s private key
- The certificate set can be used to validate that the holder of a particular private key is held by the current legitimate holder of a particular number resource – or not!

- Community driven approach
  - Collaboration between the RIRs since 2006
  - Based on open IETF standards
    - Based on work undertaken in the Public Key Infrastructure (PKIX) and Secure Inter-Domain Routing (SIDR) Working Groups of the IETF

The RPKI Certificate Service

- Enhancement to the RIR Registry
  - Offers verifiable proof of the number holdings described in the RIR registry
- Resource Certification is an opt-in service
  - Number Holders choose to request a certificate
    - Derived from registration data

What Can we Sign?

- One approach is to look at the process of “permissions” that add an advertised address prefix to the routing system:
  - The address holder is “authorising” a network to “originate” a route advertisement into the routing system
- The ‘ROA’ is a digitally signed version of this authority. It contains
  - An address prefix (and range of ‘allowed’ prefix sixes
  - An ‘originating address’
- This allows others to check the validity of a BGP route announcement:
  - If there is a valid ROA, and the origin AS matches the AS in the ROA, and the prefix length is within the bounds of the ROA, then the announcement has been entered into the routing system with the appropriate permissions

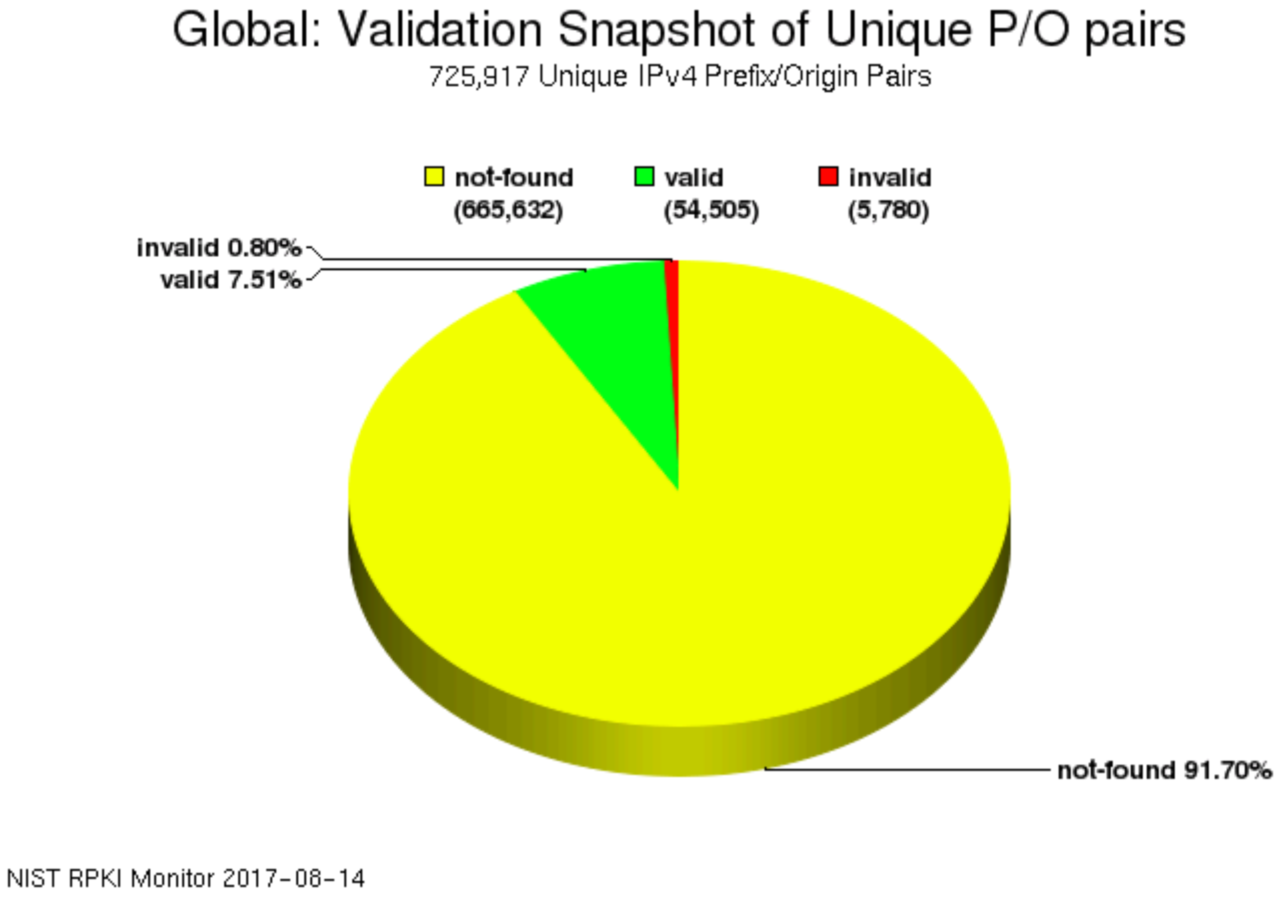
So ROAs can help

- An automated solution that checks the validity of a route announcement against a local repository of digital certificates:
  - Which can be used to feed a BGP routing filter that can isolate certain instances of what looks like attempted route hijack

Are we using RPKI and ROAS

- Two questions:
  - What proportion of existing route advertisements have associated published ROAs?
  - What proportion of network operators will reject a route if the associated ROA set indicates an invalid route advertisement (possible route hijack)

ROA publication

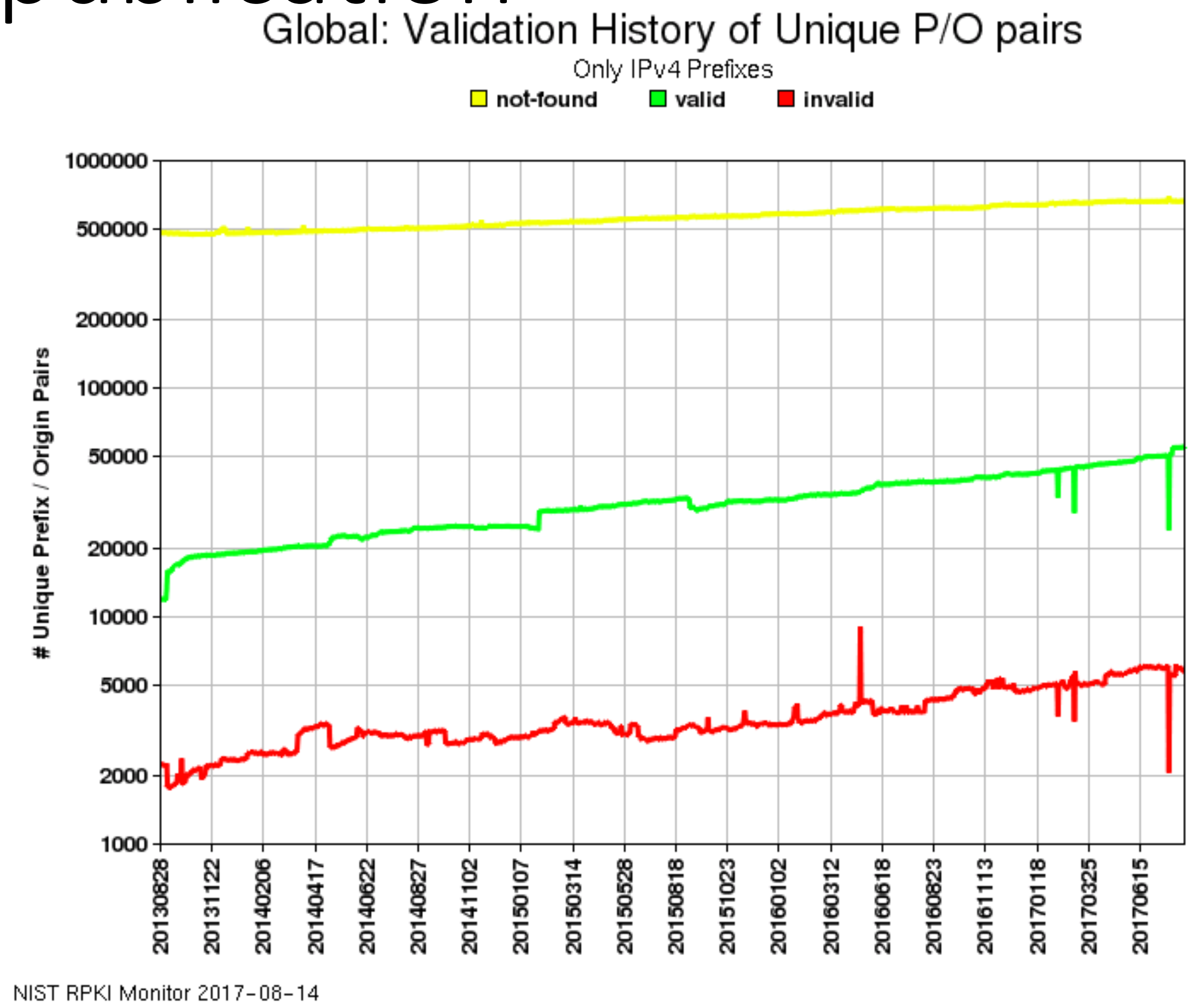

Global: Validation Snapshot of Unique P/O pairs

725,917 Unique IPv4 Prefix/Origin Pairs

NIST RPKI Monitor 2017-08-14

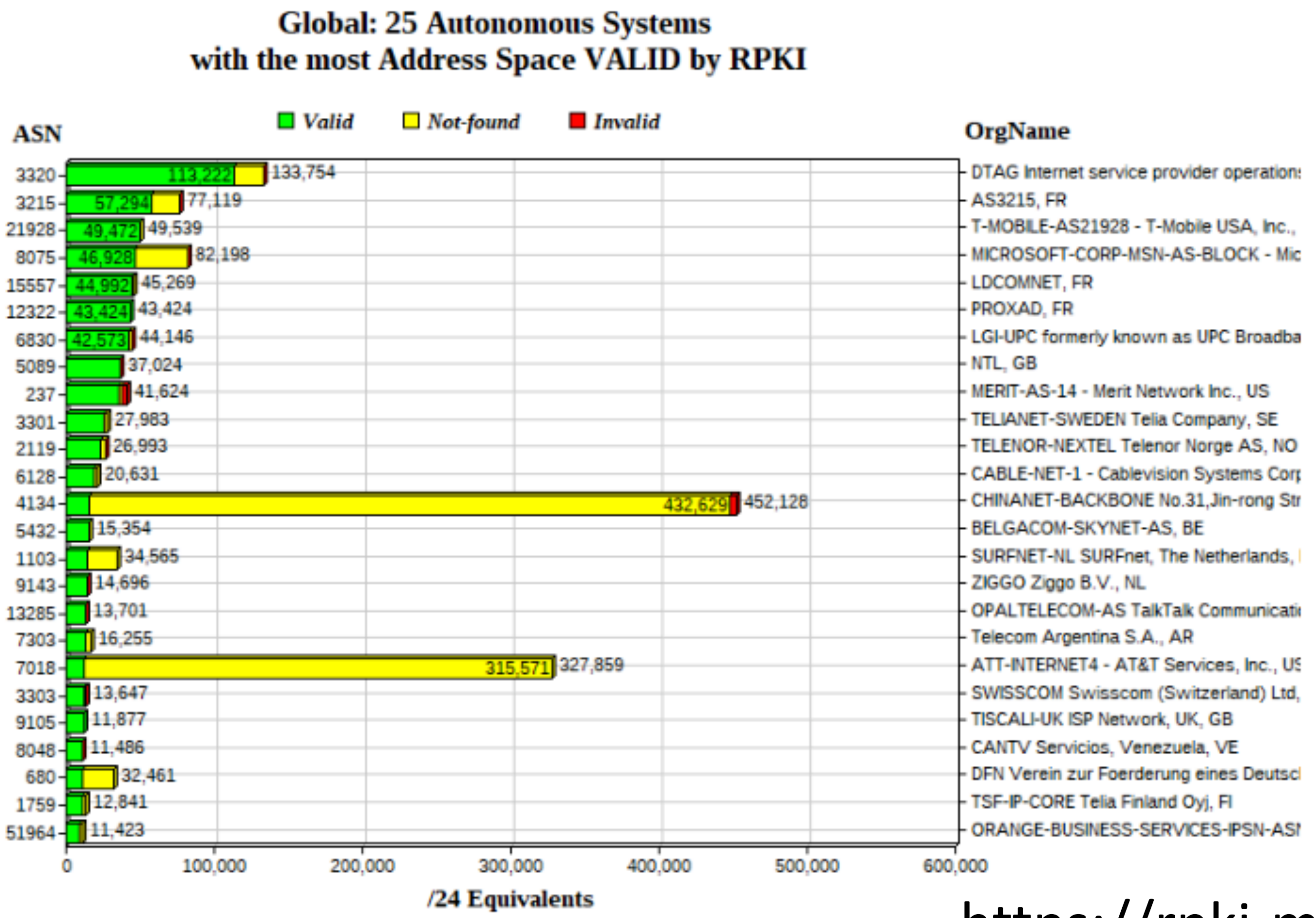
https://rpki-monitor.antd.nist.gov

ROA publication



https://rpki-monitor.antd.nist.gov

ROA publication

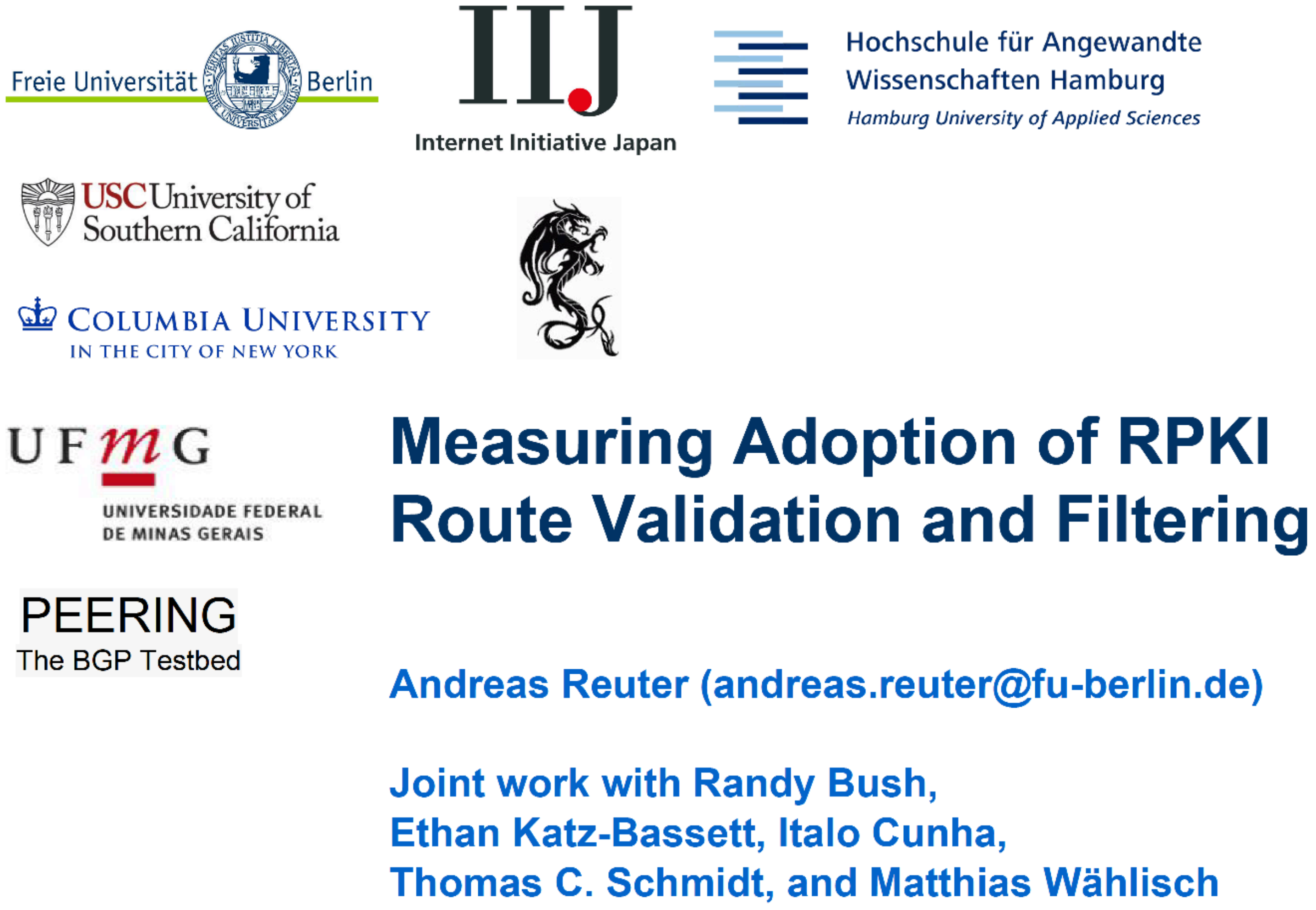


Global: 25 Autonomous Systems
with the most Address Space VALID by RPKI

NIST RPKI Monitor: 2017-08-14

https://rpki-monitor.antd.nist.gov

ROA Use



Freie Universität Berlin

IIJ
Internet Initiative Japan

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

USC University of Southern California

Columbia University
in the City of New York

UFMG
Universidade Federal de Minas Gerais

PEERING
The BGP Testbed

Measuring Adoption of RPKI Route Validation and Filtering

Andreas Reuter (andreas.reuter@fu-berlin.de)

Joint work with Randy Bush,
Ethan Katz-Bassett, Italo Cunha,
Thomas C. Schmidt, and Matthias Wählisch

https://ripe74.ripe.net/presentations/43-ovs-study-ripe74-plen-final.pdf

ROA Use

Results

We found at least 3 AS that deployed RPKI-based filtering!

None of them are large providers ...

2 AS filtered all invalid routes

1 AS filtered selectively

Conclusion

➔ There are ASes that do RPKI-based filtering.
Not many, not the big ones, but at least some (>3).

➔ Uncontrolled experiments are unsuited to infer RPKI-based filtering policies

➔ Controlled experiments are crucial to measuring adoption of RPKI-based filtering policies

Internet infrastructure requires proper monitoring.

https://ripe74.ripe.net/presentations/43-ovs-study-ripe74-plen-final.pdf

Errrr

- If route hijacking is such a problem then why aren’t we all publishing ROAs and running ROA filters on our routers?

- Cryptography and Certificate management operationally challenging

  which is often seen as one more thing to go wrong!

- Without everybody running BGPsec that it is not a very robust defence

  As long as a hijacker includes your ROA-described originating AS in the faked AS PATH the hijacker can still inject a false route

- If ROAs are challenging for operators, then BGPsec is far more so!

The Perfect can be the enemy of the Good

Maybe there are some “Good” things we can do right now instead of just waiting for BGPsec to work!

More Ideas?

- Waiting for everyone to adopt a complex and challenging technology solution is probably not going to happen anytime soon
- Are that other things we can do that leverage the RPKI in ways that improve upon existing measures?
  - Use ROAs to digitally sign a LOA?
  - Digitally sign whois entries?
  - Digitally sign Routing Policy descriptions in IRRs

  - Signed data could help a user to determine if the information is current and genuine
  - This would not directly impact routing infrastructure, but instead would improve the operators' route admission process to automatically identify routing requests that do not match signed registry / routing database information

Thanks!