Routing Security

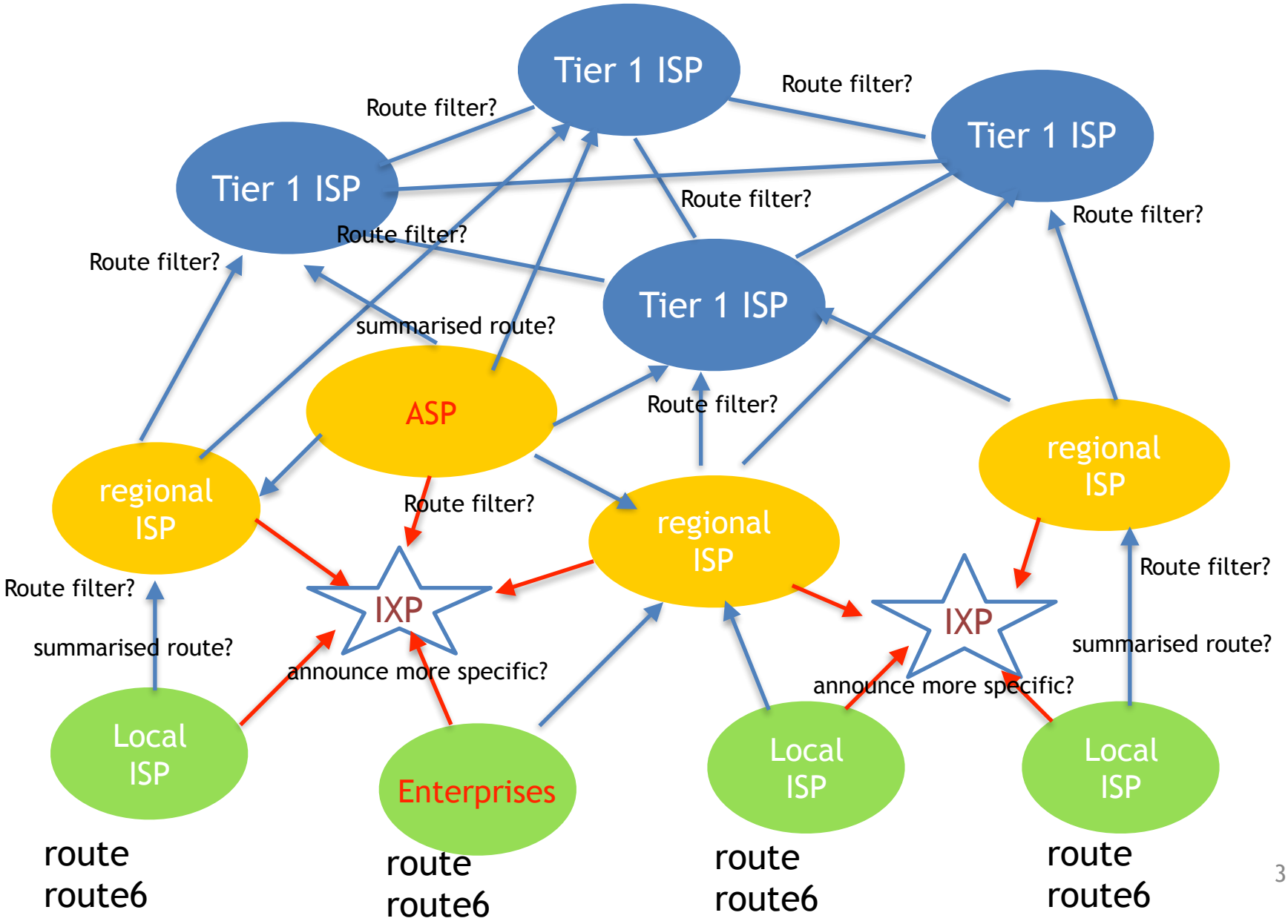
NTT Communications (AS2914)
Binh Lam
#lighttalk #Ausnog2018

Routing Security

1. What happened?

2. How to prevent?

What is your current route announcement & route filter policies?



Amazon

hijacked

24 April 2018:

AWS DNS network hijack turns MyEtherWallet into ThievesEtherWallet - 2hours!
> over 17millions USD stolen

More info: https://www.internetsociety.org/blog/2018/04/amazons-route-53-bgp-hijack/

Auth Nameserver	Original	Hijacked
205.251.192.73 ns-73.awsdns-09.com	205.251.192.0/23 AS16509	205.251.192.0/24 AS10297 205.251.193.0/24 AS10297
205.251.195.239 ns-1007.awsdns-61.net	205.251.194.0/23 AS16509	205.251.195.0/24 AS10297
205.251.197.218 ns-1498.awsdns-59.org	205.251.196.0/23 AS16509	205.251.197.0/24 AS10297
205.251.199.201 ns-1993.awsdns-57.co.uk	205.251.198.0/23 AS 16509	205.251.199.0/24 AS10297

- The AS 10297 upstreams (NTT, Cogent, Level3) & Equinix route server blocked the hijack attack
- Some peers of AS 10297 (Google, HE, BBOI-AS19151) accepted the hijack.

Prevent Route Hijacked

- Create & Manage your own valid Whois Route Object in IRR
- Enabling Resource Public Key Infrastructure certification RPKI and enable ROA

https://www.apnic.net/wp-content/uploads/2017/01/route-roa-management-guide.pdf

- Announce /24 route for your critical infrastructure to the Global Internet Routing

Route Object

```
whois -h rr.ntt.net 202.9.112.0/22
route:      202.9.112.0/22
descr:      NTT-AU-IP
origin:     AS23918
notify:     ip-eng@au.ntt.com
mnt-by:     MAINT-AU-NTTAUS
changed:    binh.lam@au.ntt.com 20180605
source:     NTTCOM

route:      202.9.112.0/22
descr:      RPKI ROA for 202.9.112.0/22
remarks:    This route object represents routing data retrieved from the
RPKI
remarks:    The original data can be found here: https://
rpki.gin.ntt.net/r/AS23918/202.9.112.0/22
remarks:    This route object is the result of an automated RPKI-to-IRR
conversion process.
remarks:    maxLength 22
origin:     AS23918
mnt-by:     MAINT-JOB
changed:    job@ntt.net 20180830
source:     RPKI  # Trust Anchor: APNIC RPKI Root
```

Route CIDR

AS-Origin

Maintainer

Prefix length

AS-Origin

RPKI ROA

Update Your Filter

1) Reject RFC 1918 (private) IP space

https://www.apnic.net/get-ip/faqs/resource-quality-assurance/

2) Reject Bogon/Private ASNs

http://as2914.net/bogon_asns/configuration_examples.txt

3) Reject IXP Nets

http://bgpfilterguide.nlnog.net/guides/no_transit_leaks/

4) Allow what is registered in IRR, WHOIS, RPKI

http://ix.br/pttforum/9/slides/ixbr9-irr.pdf

5) Reject all other BGP announcements

Thank you

Question?

Please contact: binh.lam@nttict.com