# Route Hijack Prevention via Pins

stable routing to stable prefixes

Jared Mauch

NTT America

# Pins you say? Won't that hurt?

- Google SSL Certificate Attacks
  - via DigiNotar SSL CA
  - https://www.imperialviolet.org/2011/05/04/pinning.html
- Chrome 13+ Protects against this
- Firefox 32+
- Android 4.0 (ICS)+

# History Lesson (brief)

- Peers are often not filtered
  - Certainly at the SFI-core
  - Max-prefix sometimes best-effort
  - Sanity Filters (rfc1918/rfc3330)
- Bogon filters
- As-path filters
- RIR Boundary Filters
  - Dating back to Sean Doran @ ICP
- IRR Filtering (is seen as) difficult

# Application for Routing

- Prefixes are periodically mis-routed
  - Youtube Hijack
    - 2008 - AS17557 announces 208.65.153.0/24
    - http://www.ripe.net/internet-coordination/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study
    - Youtube now in AS43515 (vs AS36561)
  - Recent SpetsEnergo abuse
    - http://www.bgpmon.net/using-bgp-data-to-find-spammers/
    - http://seclists.org/nanog/2014/Aug/479
- Goal
  - Prevent customer calls (FB, YT, Google down!)
- Does not address MITM (outside scope)
  - Plus RIB may not always align with FIB

# What does it look like

- Resurrect Golden-Nets (RIPE-229/210)
  - Dates to route flap dampening days
- Tie Prefix + Origin AS together
  - 36619 - 198.41.0.0/24 (A.ROOT)
  - 4 - 192.228.79.0/24 (B.ROOT)
  - 2149 - 192.33.4.0/24 (C.ROOT)
  - 27 - 199.7.91.0/24 (D.ROOT)
  - 3557 - 192.5.4.0/23 (F.ROOT)
  - …
  - 15169 - 216.239.32.0/24 (NS1.GOOGLE)
  - 15169 - 74.125.225.0/24 (www.youtube.com)

# Short, Simple, Static (mostly)

- Can build policy to join AS +Prefix
- Youtube Example:

```
route-policy golden-prefix-list
 if destination in AS43515 and as-path originates-from ’43515' then pass exit
 if destination in AS43515 drop exit
!
prefix-set AS43515
 64.15.112.0/20,
 208.65.152.0/22,
 208.117.224.0/19,
 208.117.236.0/24,
 208.117.238.0/24,
 208.117.240.0/24,
 208.117.242.0/24,
 208.117.248.0/24,
 208.117.249.0/24,
 208.117.250.0/24,
 208.117.251.0/24,
 208.117.254.0/24,
 208.117.255.0/24,
 216.239.60.0/24
end-set
!
```

# Golden ASN list (Alexa top 10 + Key Resources)

- 19836 (A)
- 2149 (C)
- 27 (D)
- 297 (E)
- 3557 (F)
- 5927 (G)
- 13 (H)
- 29216 (I)
- 26415 (J)
- 25152 (K)
- 20144 (L)
- 7500 (M)
- 15169 (Google)
- 32934 (FB)
- 26101 (Y!)
- 55967(Baidu)
- 14907 (Wikimedia)
- 13414 (Twitter)
- 16509 (Amazon)
- 20049 (LinkedIn)

# Example Reference List

- Web 2.0 way?
  - https://github.com/hmproject/goldenprefixes
  - Please contribute ideas/lists/code
- Old fashioned way:
  - http://puck.nether.net/~jared/golden-list.txt
    - Built from actual BGP RIB snapshot with automation
      - ASN can announce new prefixes, then can be later promoted to stable/golden via cron + clogin
    - Input: List of ASNs, Output: IOS-XR Policy
      - Code ugly, needs quick rewrite (why do you hate my perl?)

# Why not me?

- $CDN
- $CCtld
- $Gtld
- $my_content_startup

- Could build your own list, this is just a reference idea to protect those that drive customer calls/complaints.

# Thank You (feedback)

- Job Snijders
- Chris Morrow
- Warren Kumari
- Tony Kapela

Please follow-up on Hijack Mitigation List:

http://puck.nether.net/mailman/listinfo/hmproject

# Questions?

Jared Mauch
NTT America
jmauch@us.ntt.net
jared@puck.nether.net