Definition and Classification of Route Leaks

draft-ietf-grow-route-leak-problem-definition-02

- Update -

K. Sriram, D. Montgomery, D. McPherson,
E. Osterweil, and B. Dickson

GROW WG Meeting, IETF 93, Prague, Czech Republic
July 20, 2015

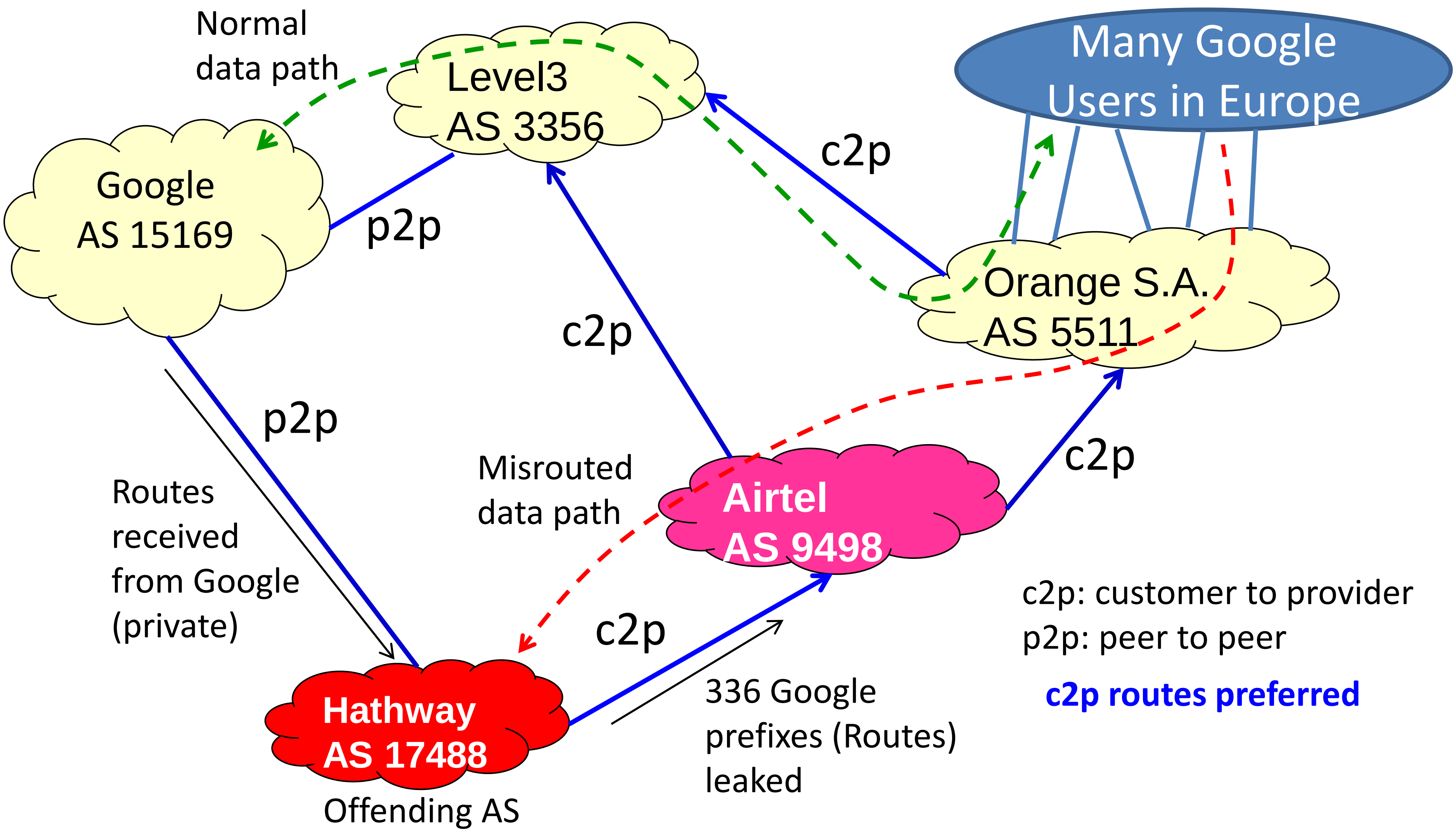
Diffs Compared to the Previous Version

- Added new examples of route leaks incidents:
  - In Type 1:
    - Hathway-Airtel caused route-leaks of 336 Google prefixes (Mach 2015)
    - Telekom Malaysia caused route-leaks of about 179,000 prefixes, which in turn Level3 accepted and propagated (June 2015)
  - In Type 2:
    - Telekom Malaysia via Level3; out of about 179,000 total route-leaked prefixes, about 10,000 were more specifics of previously announced aggregates
- Brian Dickson is included as an author
- New references added

References: http://research.dyn.com/2015/03/routing-leak-briefly-takes-google/
http://www.bgpmon.net/massive-route-leak-cause-internet-slowdown/

Hathway / Airtel Route Leaks of Google Prefixes

March 12, 2015



c2p: customer to provider
p2p: peer to peer

c2p routes preferred

Incident analysis: http://research.dyn.com/2015/03/routing-leak-briefly-takes-google/

Accidental vs. Intentional (Malicious) Route Leaks

- Most route leaks are accidental (99% ?)
- Small fraction may be intentional or malicious (1% ?)
  - Intentional leak of a more specific prefix as in Kapela-Pilosov demo at DEFCON-16
  - Attacker keeps the legitimate origin AS but removes all other preceding ASes in the AS_PATH before leaking or announcing the route to its other provider ISP
    - Deceives origin validation (assuming RPKI & origin validation are deployed)
  - New attack vector: If an unsecured solution contains unprotected Route Leak Protection bits, a determined attacker would alter them to avoid detection

Accidental vs. Intentional (Malicious) Route Leaks

Solution Steps

Today: Current BGP (without route leak solution; assuming prefix filters aren’t doing job adequately)

- Vulnerable to accidental (99%) and malicious (1%) route leaks

⇩

Step 1: BGP with proposed route leak solution (with RPKI/OV but without BGPsec)

- Detects/mitigates accidental (99%) but not malicious (1%)

⇩

Step 2: BGP with proposed route leak solution (with RPKI/OV and BGPsec)

- Detects/mitigates accidental (99%) as well as malicious (1%)

Route Leaks Solution Draft in IDR

- https://tools.ietf.org/html/draft-sriram-idr-route-leak-detection-mitigation-01

- Adopted as a WG draft (7/19/2015)

Back to Route Leaks Definition Draft

- All comments received so far have been addressed
- Is this possibly a good time to request WGLC?

- Authors could possibly include a section to discuss accidental vs. malicious route leaks (minor change)
  - ➢ But that starts to get into solution space a little

Backup Slides

Anatomy of a Route Leak: Seven Types

Type 1: Type 1: U-Turn with Full Prefix

Type 2: U-Turn with More Specific Prefix

Type 3: Prefix Reorigination with Data Path to Legitimate Origin

Type 4: Leak of Internal Prefixes and Accidental Deaggregation

Type 5: Lateral ISP-ISP-ISP Leak

Type 6: Leak of Provider Prefixes to Peer

Type 7: Leak of Peer Prefixes to Provider

Details and example incidents provided in:
draft-ietf-grow-route-leak-problem-definition-02