Definition and Classification of Route Leaks

draft-sriram-route-leak-problem-definition-00

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

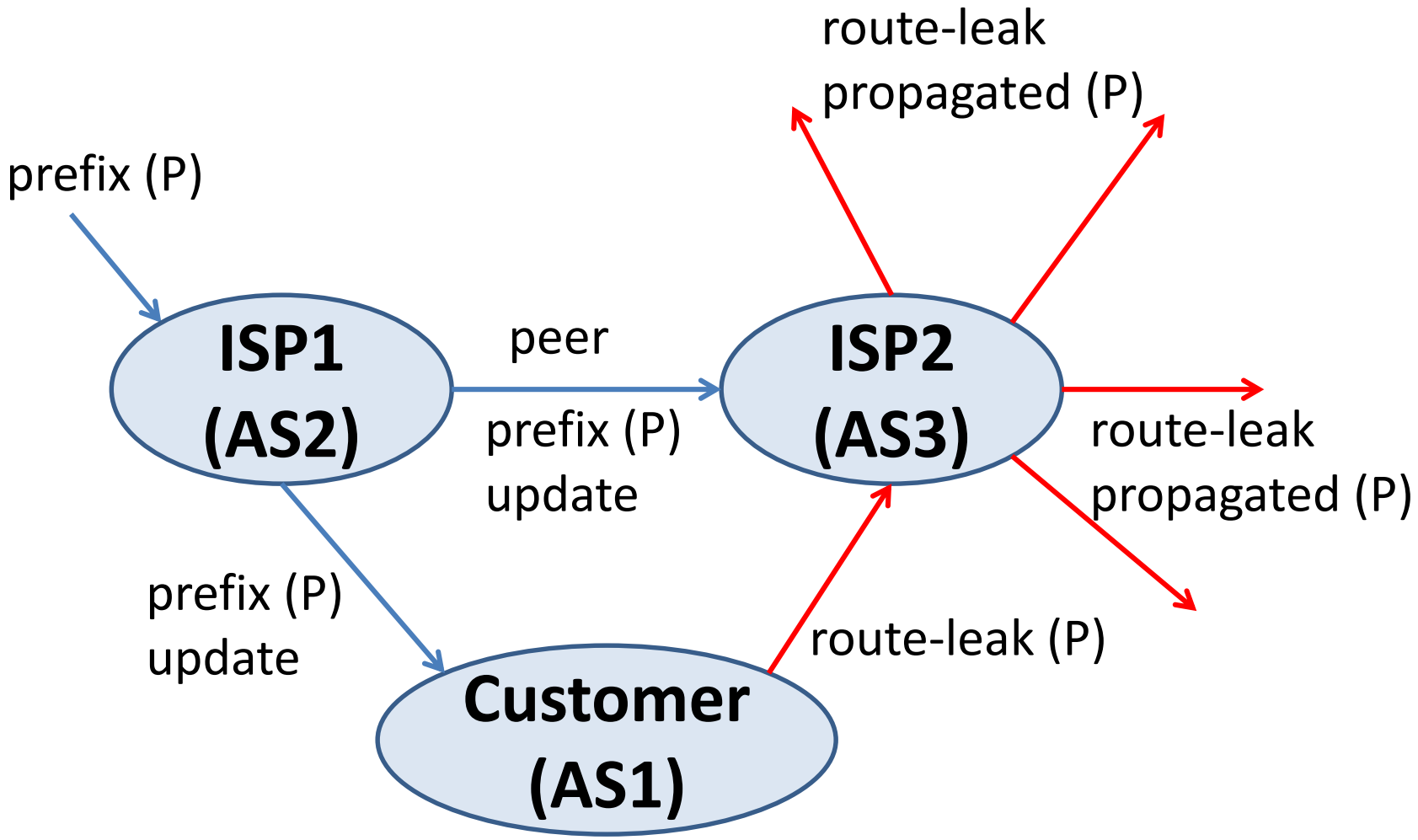
IETF 91, Honolulu, Hawaii
November 10, 2014

Acknowledgements: The authors would like to thank Jeff Haas, Wes George, Warren Kumari, Jared Mauch, Amogh Dhamdhere, Andrei Robachevsky, Randy Bush, Chris Morrow, and Sandy Murphy for comments and suggestions.

Diffs Compared to the Previous Version

- draft-sriram-route-leak-protection-00 was presented in Toronto (IETF 90)
- Diffs are:
  - Separated the problem definition draft from the solution draft
  - Added a working definition of route leaks
  - Added Type 5: Lateral ISP to ISP Leak
  - Included accidental deaggregation also (in Type 4)
  - Some more reported incidents added as examples

Illustration of Basic Notion of a Route Leak



In general, ISPs prefer customer route announcements over those from others.

A Proposed Working Definition of Route Leak

A "route leak" is the propagation of routing announcement(s) beyond their intended scope. That is, an AS's announcement of a learned BGP route to another AS is in violation of the intended policies of the receiver, the sender and/or one of the ASes along the preceding AS path. The intended scope is usually defined by a set of local redistribution/filtering policies distributed among the ASes involved. Often, these intended policies are defined in terms of the pair-wise peering business relationship between ASes (e.g., customer, provider, peer).

Anatomy of a Route Leak: Classification

Type 1: U-Turn with Full Prefix

A multi-homed AS learns a prefix route from one upstream ISP and simply propagates the prefix to another upstream ISP.

- The update basically makes a U-turn at the attacker's multi-homed AS.
- Neither the prefix nor the AS path in the update is altered.
- This is similar to a straight forward path-poisoning attack [Kapela-Pilosov], but with full prefix.
- Example incidents: Google-Moratel (2012), Dodo-Telstra (2012), VolumeDrive-Atrato (2014).

Anatomy of a Route Leak: Classification

Type 2: U-Turn with More Specific Prefix

A multi-homed AS learns a prefix route from one upstream ISP and announces a sub-prefix (subsumed in the prefix) to another upstream ISP.

- The update basically makes a U-turn at the attacker's multi-homed AS but a subprefix is propagated. Having the subprefix maximizes the success of the attack.
- Reverse path is kept open by the path poisoning techniques as in [Kapela-Pilosov].
- Example: Demo at DEFCON-16 in 2008 causing live DEFCON attendees' traffic to detour via an offending AS.

Anatomy of a Route Leak: Classification

Type 3: Prefix Hijack with Data Path to Legitimate Origin

A multi-homed AS learns a prefix route from one upstream ISP and re-originates it towards another upstream ISP. This amounts to straightforward hijacking.

- Somehow (not attributable to path poisoning by the attacker) a reverse path is present, and data packets reach the legitimate destination via the offending AS.
- Example incidents: China Telecom (2008), Belarusian GlobalOneBel (February-March 2013 and May 2013), Icelandic Opin Kerfi-Simmin (July-August 2013) the Indosat (2014)

Anatomy of a Route Leak: Classification

Type 4: Leak of Internal Prefixes and Accidental Deaggregation

An offending AS simply leaks its internal prefixes to one or more of its provider ASes. The leaked internal prefixes are often deaggregated subprefixes (i.e. more specifics) of already announced aggregate prefixes.

- Typically these leaked announcements are due to some transient failures within the AS; they are short-lived, and typically withdrawn quickly following the announcements.
- Example incidents: Leaks of internal prefix-routes occur frequently (e.g. multiple times in a week). AS701 and AS705 leaked about 22,000 more specifics of already announced aggregates (2014).

Anatomy of a Route Leak: Classification

Type 5: Lateral ISP to ISP Leak

This type of route leak typically occurs when, for example, three sequential ISP peers (e.g. ISP-A, ISP-B and ISP-C) are involved, and ISP-B receives a prefix-route from ISP-A and in turn leaks it to ISP-C.

- The typical routing policy between laterally (i.e. non-hierarchically) peering ISPs is that they should only propagate to each other their respective customer prefixes.
- Example incidents: In [Mauch-nanog][Mauch], route leaks of this type are reported by monitoring updates in the global BGP system and finding three or more very large ISP ASNs in a sequence in a BGP update's AS path.
- However, [Mauch] also notes that there are exceptions when one very large ISP does indeed buy transit from another very large ISP.

Not Claiming to Be Exhaustive

- The five types identified here are by no means indented to be exhaustive
- We simply observe that most attacks that have caused significant concern and been called route leaks in recent years seem to fit into this taxonomy
- We are open to further suggestions/comments

Thank you.

Is this a good time to request WG adoption of this problem definition I-D draft-sriram-route-leak-problem-definition-00?