Definition and Classification of Route Leaks

draft-ietf-grow-route-leak-problem-definition-01

- Update -

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

GROW WG Meeting, IETF 92, Dallas, Texas
March 25, 2015

Diffs Compared to the Previous Version

- draft-sriram-route-leak-problem-definition-00 was presented in Honolulu (IETF 91)
- Accepted as WG draft in January 2015
- Diffs are:
  - Two new types of route leaks added for completeness
    - Thanks to comments from Andrei and Brian
  - Several relevant new references added

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 Hijack 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-01

Route Leaks - Types 6 & 7

- Type 6 "Leak of Provider Prefixes to Peer":
  - ➢ This type of route leak occurs when an offending AS leaks prefix-routes learned from its provider to a lateral peer.
- Type 7 “Type 7 "Leak of Peer Prefixes to Provider":
  - ➢ This type of route leak occurs when an offending AS leaks prefix-routes learned from a lateral peer to its (the AS's) own provider. These leaked prefix-routes typically originate from the customer cone of the lateral peer.

The detection-mitigation draft has also been revised to extend solutions to address Types 6 and 7.
http://tools.ietf.org/html/draft-sriram-idr-route-leak-detection-mitigation-00