Route Leak Prevention using Roles

Alexander Azimov
Randy Bush
Evgeniu Bogomozov
Keyur Patel
Few Examples

• 16.05.2017: leak by Incapsula (AS19551), ~1.5k prefixes in multiple directions;

• 24.05.2017: leak by Onlanta Ltd (AS56631) more than 50k prefixes between its providers;

• 29.06.2017: leak by BICS (AS6774) ~5k prefixes in multiple directions, including CW, Cogent and Swisscom;

• 13.07. 2017: leak by CDNNETWORKS (AS36408) ~7k prefixes from GTT and Telia to Megafon.
The Goal

One button to run it and without killing phones nearby!
Mandatory roles which describe peering relations: Customer, Provider, Peer, Internal, Complex

Attributes:
iOTC – route leak prevention;
Good Questions

• What happens after software update?
• Should we have *default* role?
• Can we verify per-prefix roles?
Mandatory roles which describe peering relations:
Customer, Provider, Peer, Internal, Complex

Attributes:
iOTC – route leak prevention;
Motivation to Use Roles

• Roles simplify configuration process;
• Strict mode;
• bgp-reject draft;
• And other roles applications...
Question #1: Notification Subcodes

First scenario:
Conflict pairing of roles;

Second scenario:
One side uses *strict mode*, other side doesn’t use roles;

Do we need two subcodes or one?
Question #2: Route Leak Mitigation

If we have widely deployed route leak prevention, do we need route leak detection and mitigation?