# Route Leak Detection and Filtering using Roles in Update and Open messages

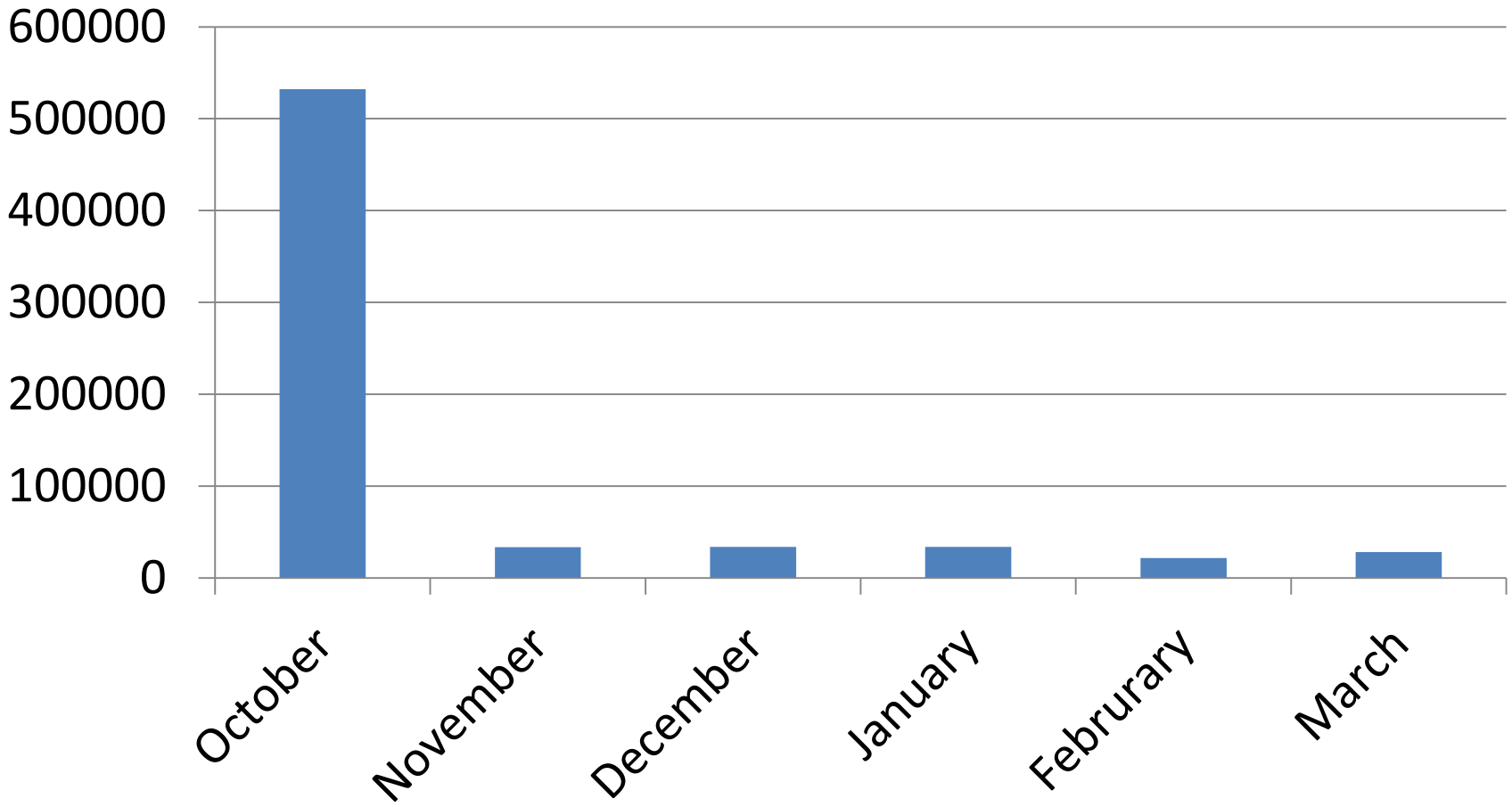
Alexander Azimov <aa@qrator.net>

Randy Bush <randy@psg.com>

# Route Leaks: Reasons

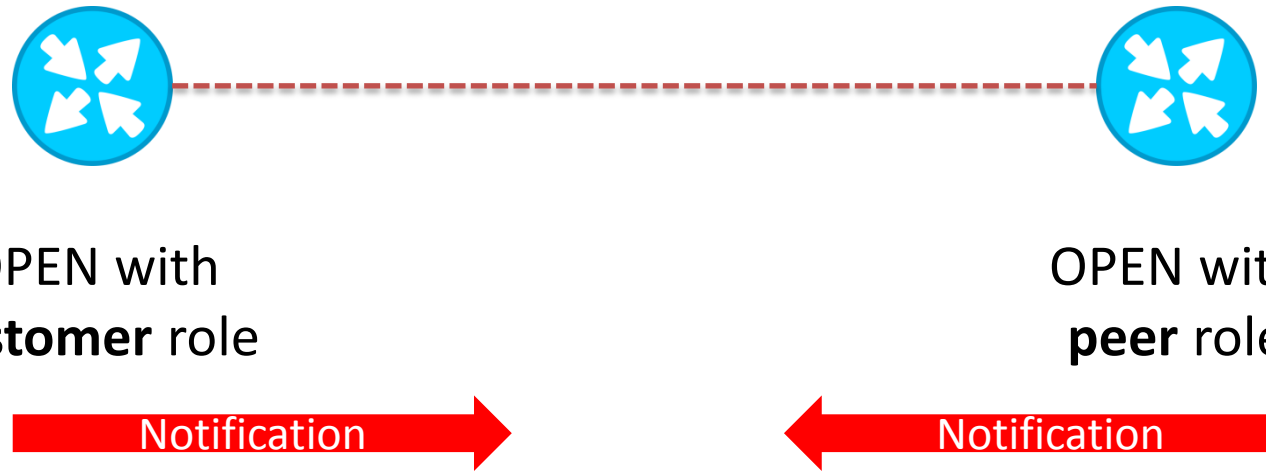
- Prefix lists/communities are optional
- Fat fingers
- MIT attacks
- Misunderstanding
- Misunderstanding
- Misunderstanding

# Route Leak: stats




>30 000 prefixes each month

# Meet Neighbor Roles




**3 pairs** of non-conflict roles:

1. Peer <---> Peer
2. Customer <---> Provider
3. Internal <---> Internal

# Strict Mode

OPEN with
**no** role

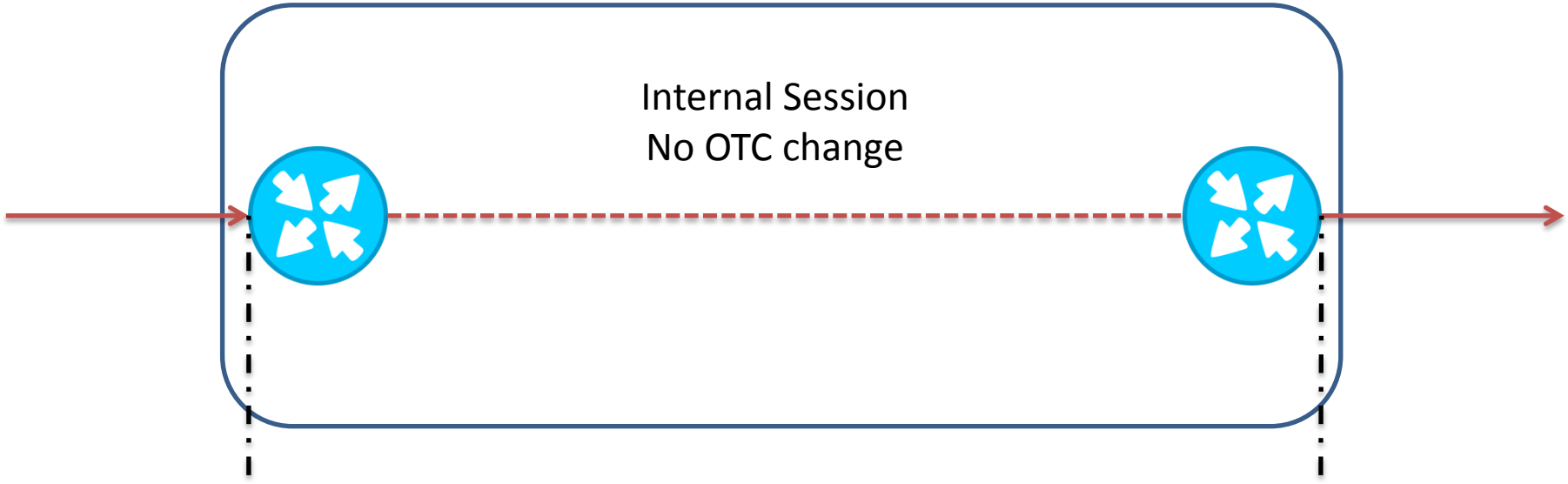
OPEN with
**peer** role

Notification

**Notification** if the role is not set in OPEN from the neighbor

# Preventing Route Leaks

Optional transit attribute – Only To Customer (OTC)

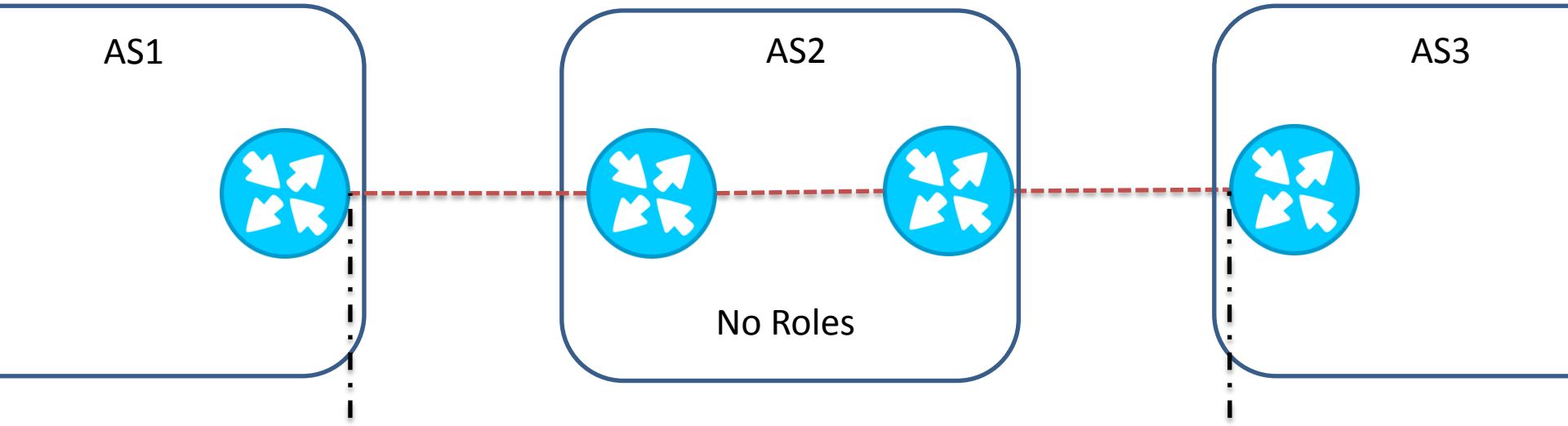



Set OTC if
role is customer or peer

Filter routes if OTC is set and
role is customer or peer

If route was learned from a provider or peer it should not be announced to another provider or peer

# OTC Attribute: Detect Leaks




Set OTC if no role capability in OPEN
and role is provider or peer

If OTC is set
and role is provider or peer

If route was learned from a customer or peer and OTC is set then
route was leaked

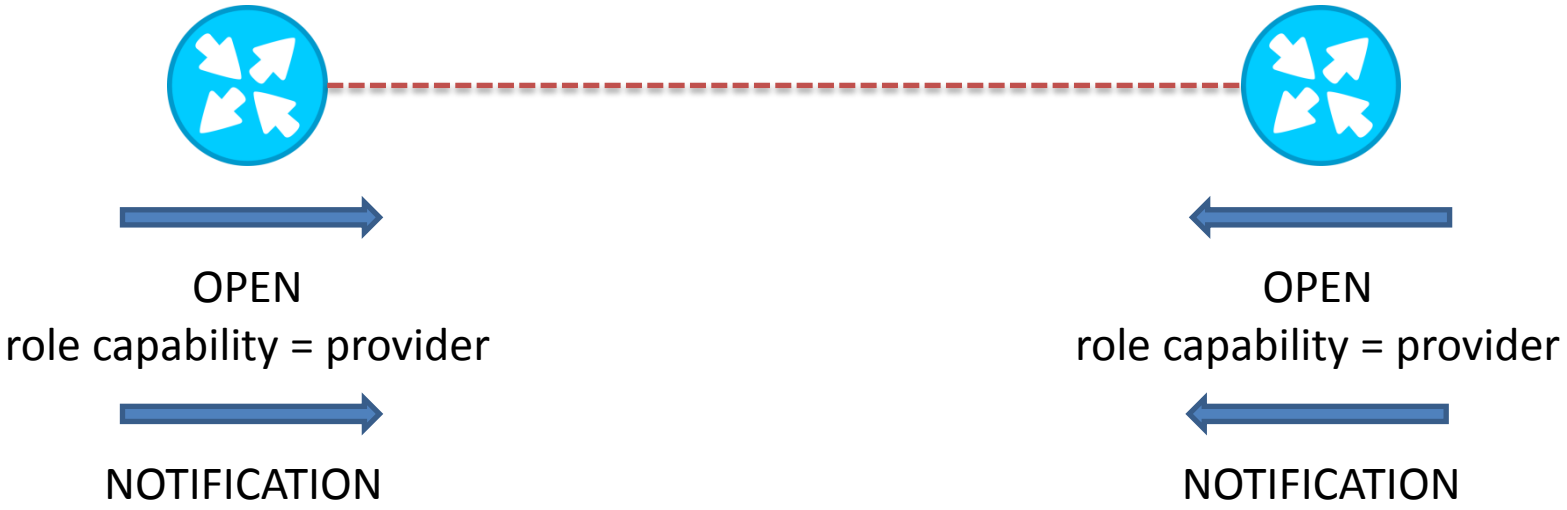
# Proposed Draft

Key ideas:

1. BGP Roles to control/help/check configuration of directly connected neighbors
2. Only To Customer (OTC) attribute to control announce propagation and detect route leaks
3. Strict mode to make newcomers adopt new version of protocol

# Security Considerations: Roles

Mismatch role:




Result: no BGP session, easy to detect

# Security Considerations: OTC

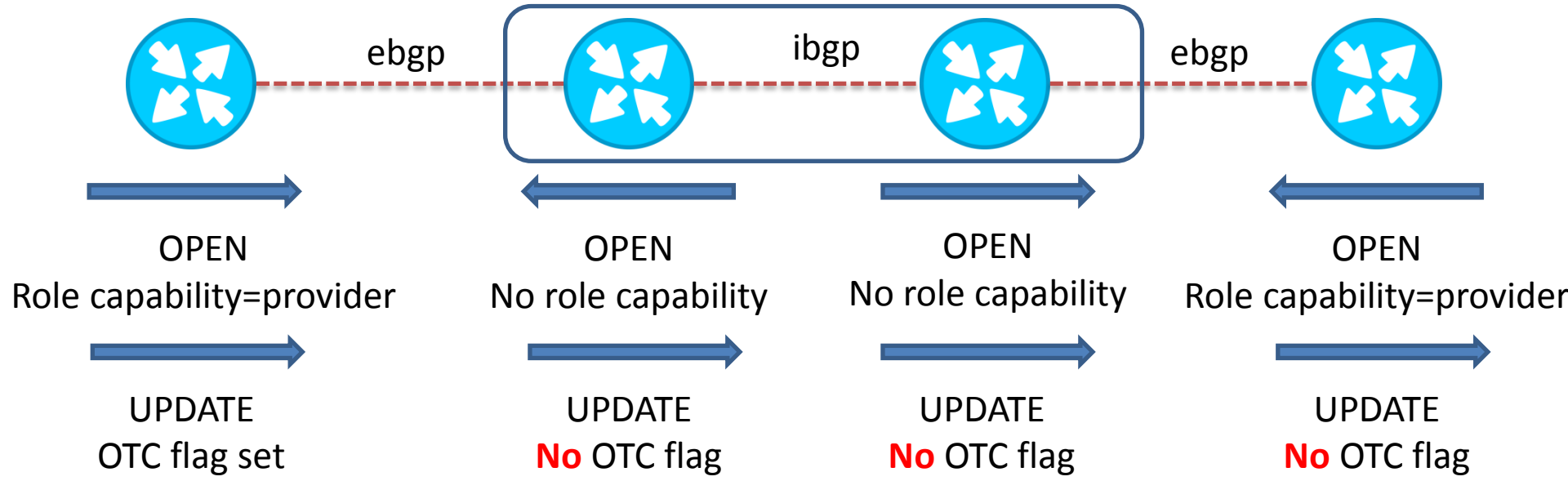
№1 OTC flag is set in violation of roles


Only c2p and p2p could be affected

It could have significantly impact on route propagation

# Security Considerations: OTC

№2 OTC flag is removed in violation of roles




Could be used to create route leaks by purpose (man in the middle attacks)

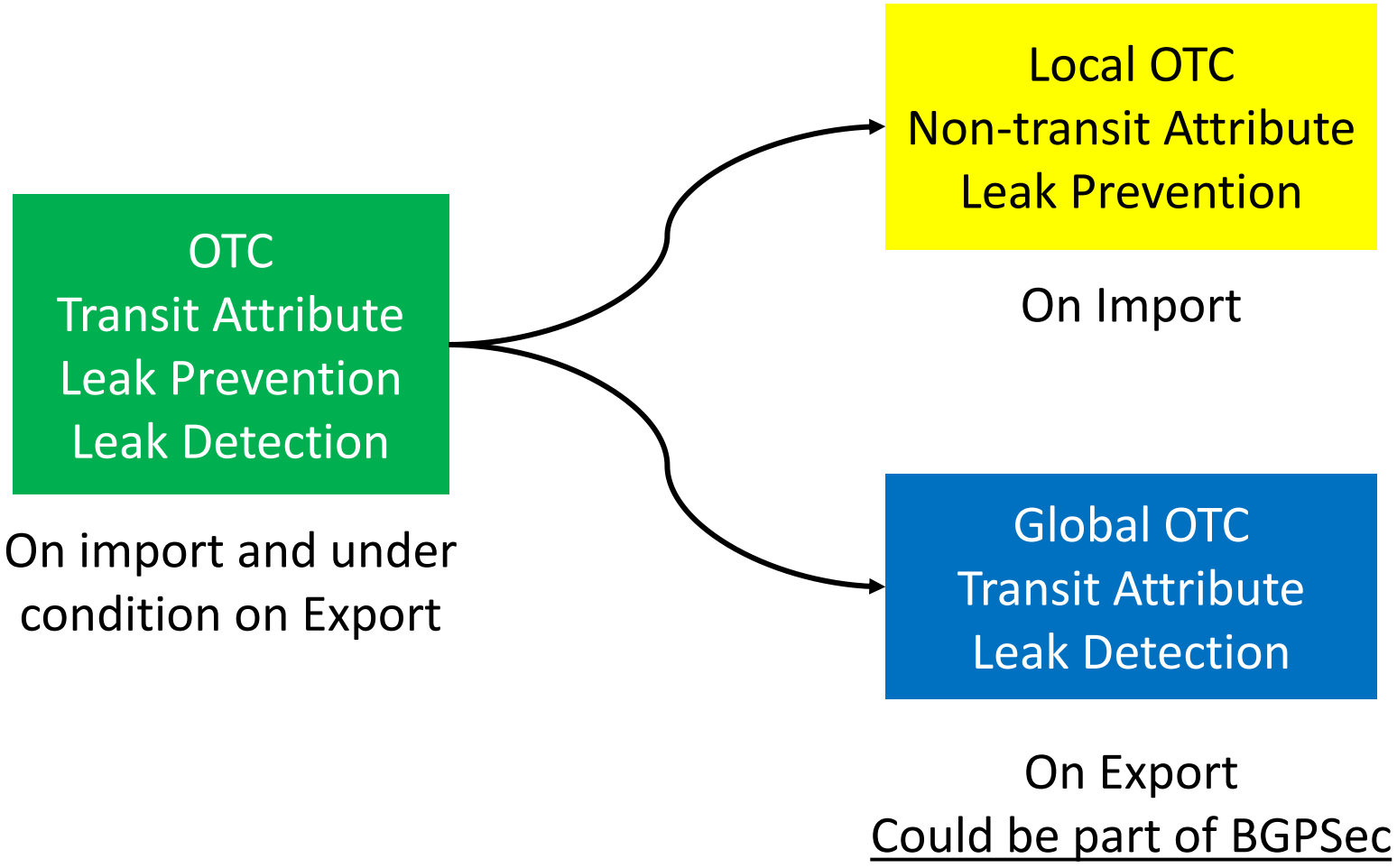
# BGPSec

Protect changes in OTC attribute using BGPSec

1. When a given BGP speaker advertises the route to an internal peer, the advertising speaker SHALL NOT modify the AS_PATH attribute associated with the route (rfc4271)
2. BGPsec_Path keeps this idea

But OTC is different…

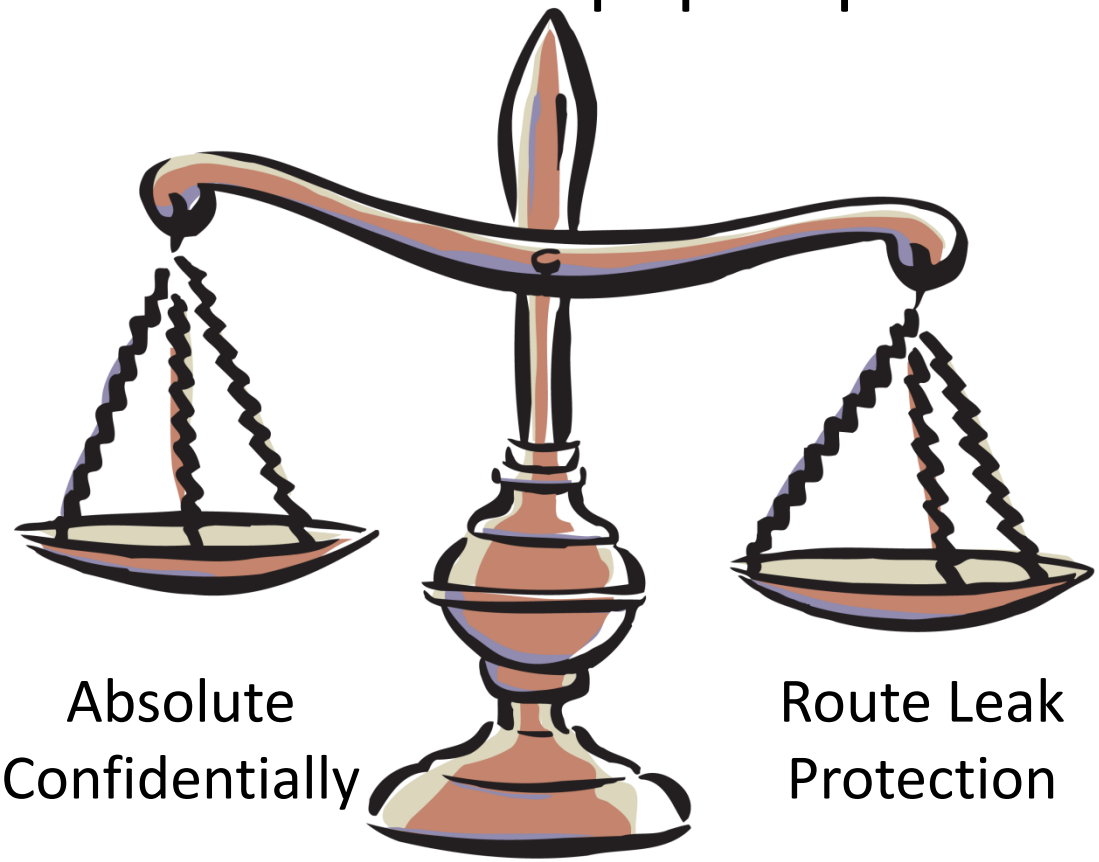
# OTC transformation



# Business Confidentiality

OTC reveals that some link isn't c2p

OTC don't reveal if link is p2p or p2c



# Conclusion

- BGP Roles – new mechanism to track down misconfigurations is automatic way
- OTC attribute – solves the problem: prevention and detection of route leaks that are result of mistakes
- OTC integration with BGPSec is part of future work