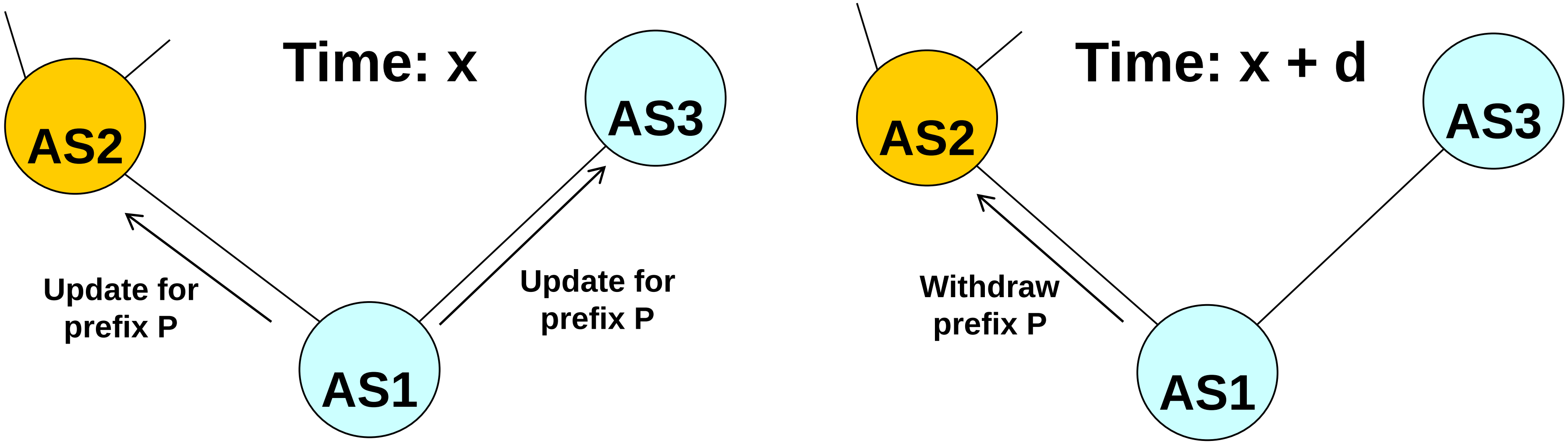
Comparison of Replay-Attack Protection Mechanisms for BGPSEC

September 20, 2012

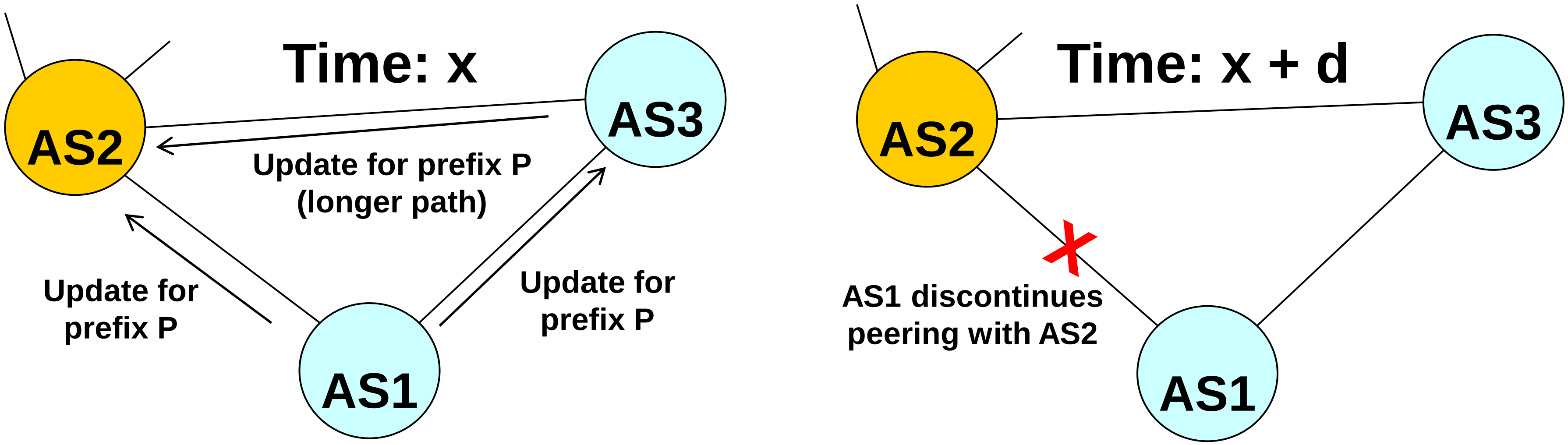
Kotikalapudi Sriram and Doug Montgomery
NIST
Contact: ksriram@nist.gov

Replay Attack Example 1



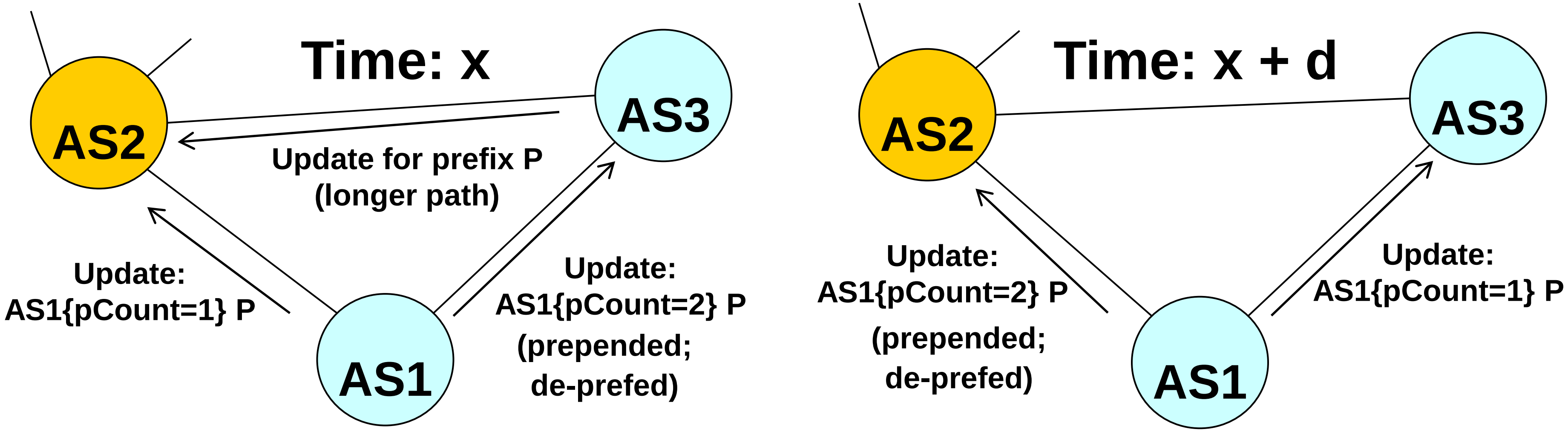
- All AS peers here are eBGPSEC peers
- AS1 had announced a prefix P to AS2 at time x
- At a later time x+d, AS1 sends a Withdraw for prefix P to AS2
- AS2 suppresses the Withdraw (does not send to its peers any explicit or implicit Withdraw)

Replay Attack Example 2



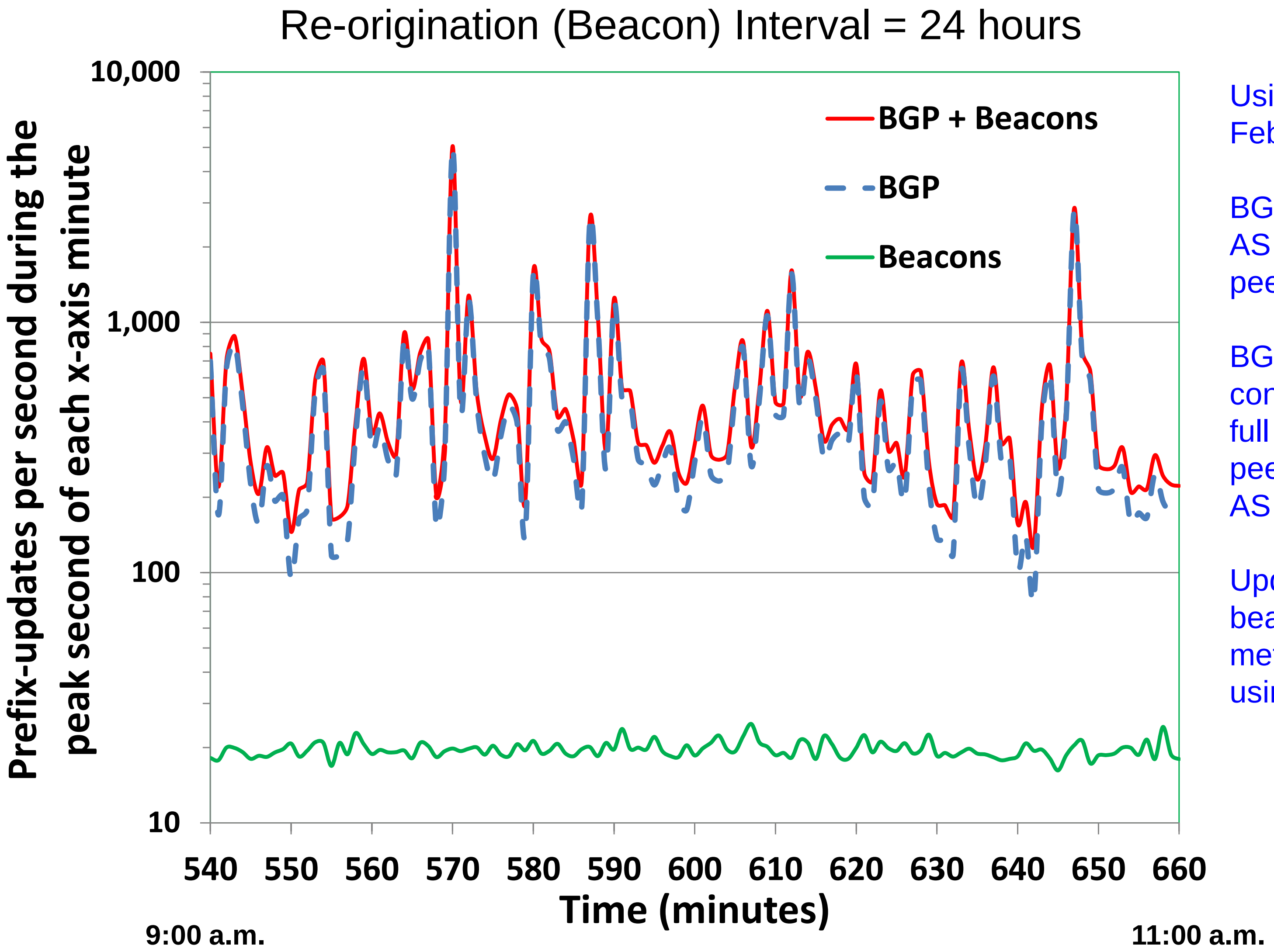
- All AS peers here are eBGPSEC peers
- AS1 had announced a prefix P to AS2 at time x
- At a later time x+d, AS1 discontinues peering with AS2
- AS2 suppresses the Withdraw (does not send to its peers any explicit or implicit Withdraw)

Replay Attack Example 3



- All AS peers here are eBGPSEC peers
- AS1 had announced a prefix P; prefers ingress data path via AS2 over that via AS3
- At a later time x+d, AS1 switches ingress data path preference to AS3 over AS2
- AS2 suppresses the new prepended path announcement (does not send to its peers any update about P)

Load Due to BGP and Periodic Re-Originations (i.e. Beacons) for 3 Peers (Same Results Apply to ET and PKR Methods)



Using Routeviews data, Feb 1, 2012.

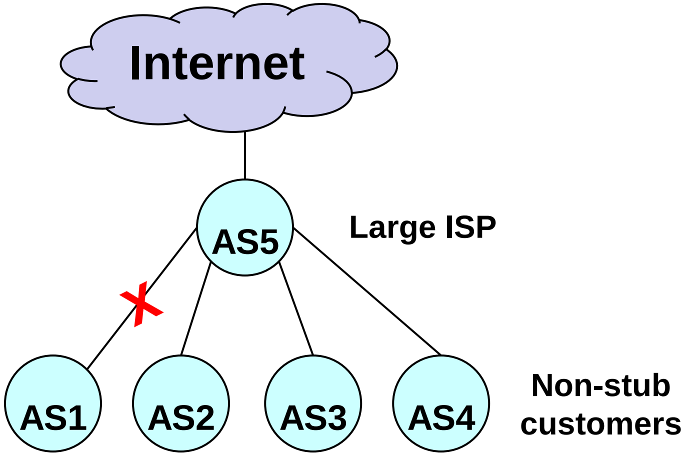
BGP feeds from AS7018, AS 701, and AS 3356 peer routers combined.

BGPSEC router in consideration receives full tables from three peers in AS7018, AS 701, AS 3356.

Update load due to beacons in PKR or ET method is estimated using a Poisson model.

Comparison of PKR vs. EKR: Scenario 1

Peering Change Event Scenario 1:



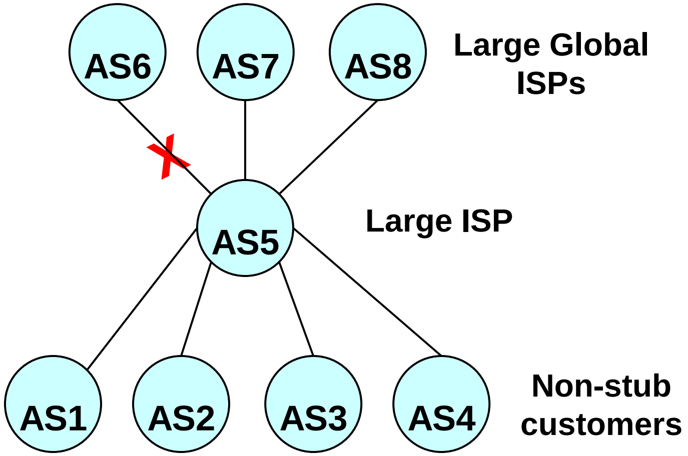
- Assume each AS in this figure also represents a single BGPSEC router
- We focus on workload at the router in AS5
- AS1 thru AS4 are non-stub customers of AS5; Each receives almost full table (400K signed prefix updates) from AS5
- Assume: AS1 and its customers together originate 100 prefixes total; likewise for AS2, AS3, AS4
- Event: Peering between AS1 and AS5 is discontinued

Workload Comparison:

- When the peering (AS5-AS1) is discontinued:
  - ❖ In the PKR method, the router at AS5 sends only 4x100 = 400 Withdraws in total and signs/re-propagates ZERO prefix updates
  - ❖ In contrast, in the EKR method (EKR-A or EKR-B), the router at AS5 sends those same 400 Withdraws but also signs and re-propagates 3x400K +3*200 +300 = 1.2 MILLION signed prefix updates in total

Comparison of PKR vs. EKR: Scenario 2

Peering Change Event Scenario 2:

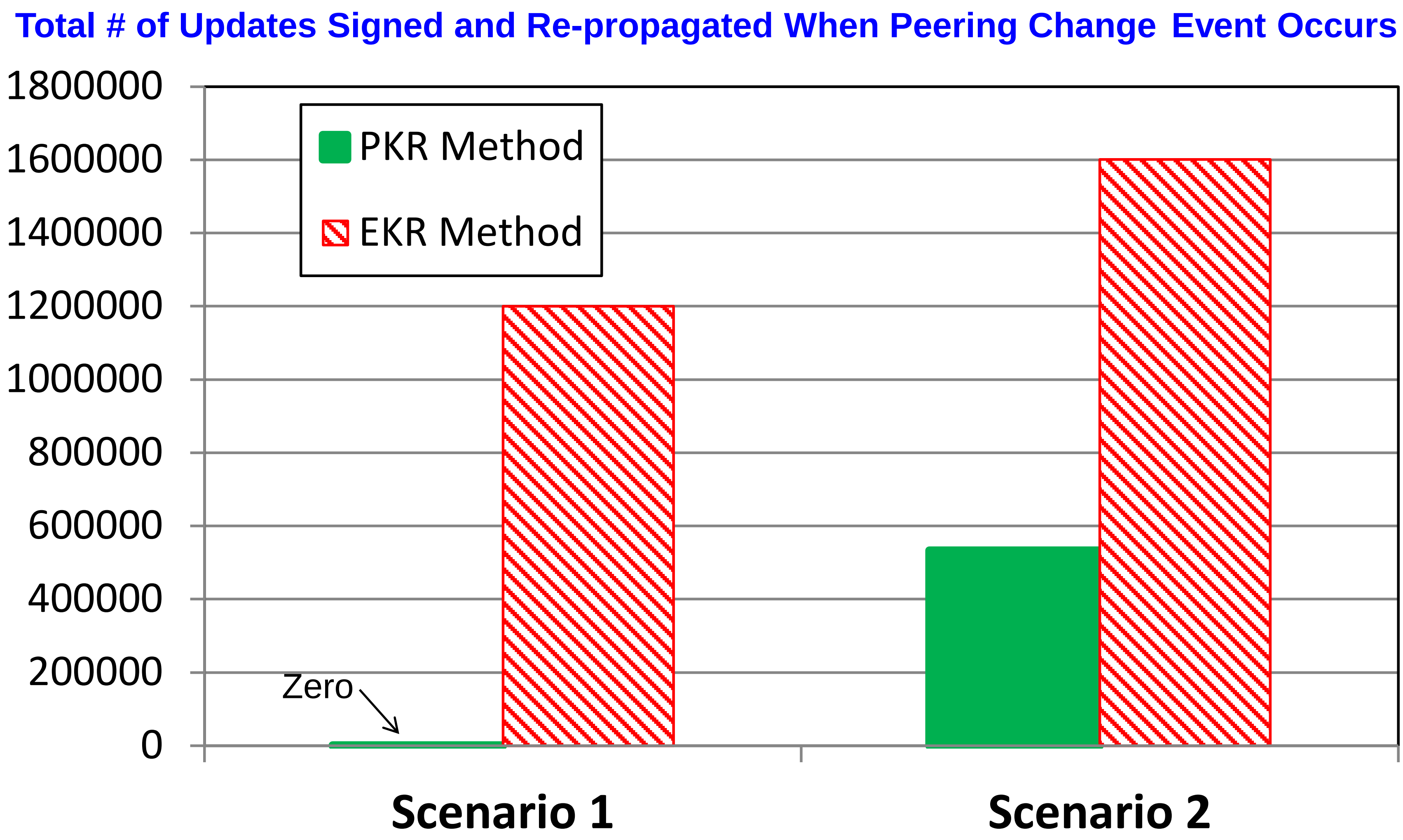


- Same assupmtions apply for AS1 through AS5 as in Scenario 1 except AS5 is multi-homed
- AS6 through AS8 give almost full table (400K signed prefixe updates) to AS5
- AS5 does not announce routes learned from one ISP to another (policy)
- Assume AS5's best path routes to the 400K prefixes are evenly distributed (i.e., 133.3K routes each) via AS6, AS7, and AS8
- Event: Peering between AS6 and AS5 is discontinued

Workload Comparison:

- When the peering (AS5-AS6) is discontinued:
  - ❖ In the PKR method, the router at AS5 signs and re-propagates 4x133.3K = 533K prefix updates in total
  - ❖ In contrast, in the EKR method (EKR-A or EKR-B), the router at AS5 signs and re-propagates 4x400K = 1.6 MILLION signed prefix updates

Summary of Comparison of PKR vs. EKR: Scenarios 1 & 2



- BGPSEC with PKR generates the same number of prefix-route re-propagations as BGP-4 when a peering/policy change event occurs
- BGPSEC with EKR typically generates far more for the same scenario