AS Hijack Detection and Mitigation

https://tools.ietf.org/id/draft-sriram-sidrops-as-hijack-detection-00.txt

K. Sriram and Doug Montgomery

ksriram@nist.gov, dougm@nist.gov

US National Institute of Standards and Technology

https://www.nist.gov/programs-projects/robust-inter-domain-routing

SIDROPS Meeting

IETF 108

July 2020

What is AS hijacking?

- Recent NANOG thread:

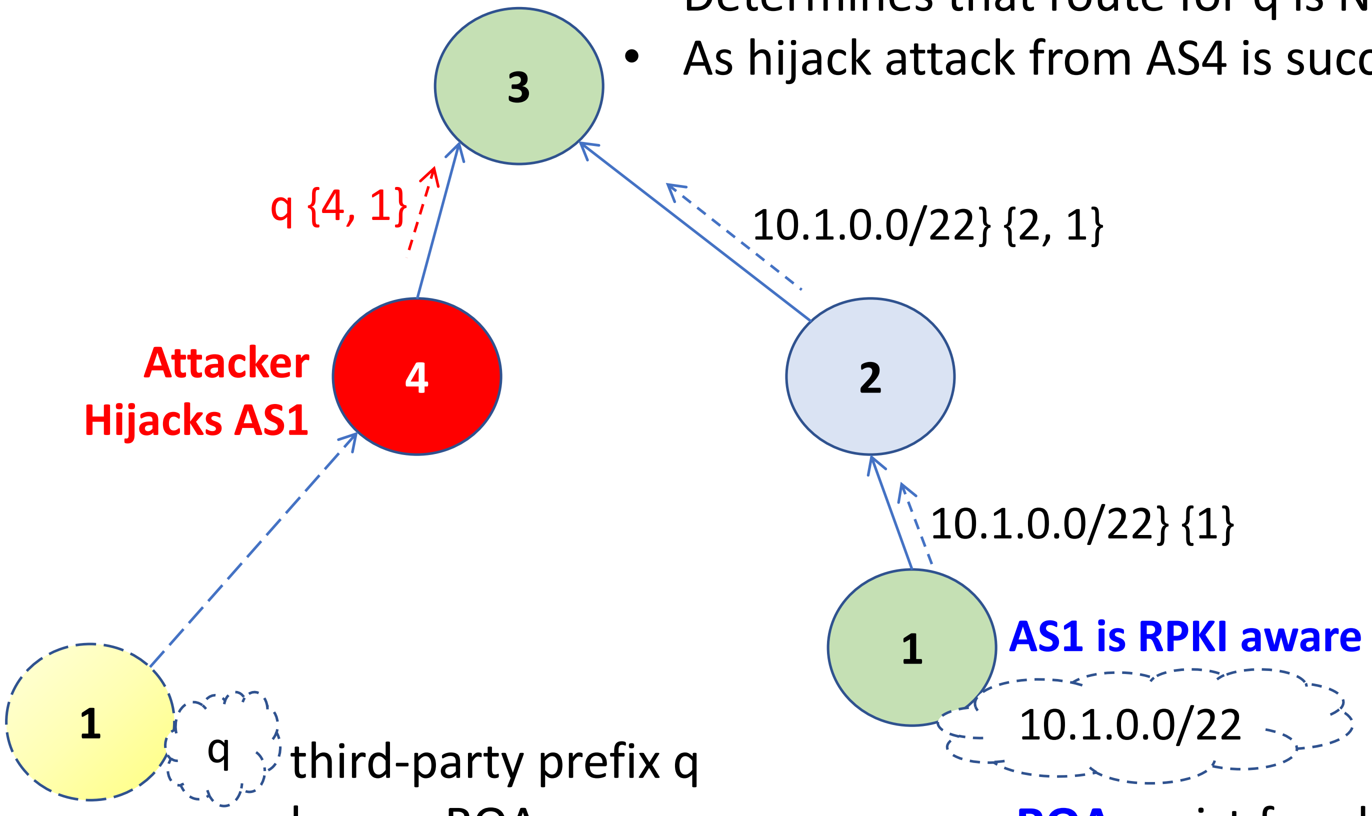
  https://mailman.nanog.org/pipermail/nanog/2020-June/thread.html#207797

  https://mailman.nanog.org/pipermail/nanog/2020-May/thread.html#207763

- Definition: “**AS hijacking**” occurs when one AS uses another AS's number (ASN) as the origin ASN in a BGP announcement.
  - Could be accidental (misconfiguration) or malicious.
  - The prefix in the announcement may sometimes belong to the hijacker.
  - But AS hijacking is often done in conjunction with hijacking a third-party prefix.

RPKI ROV is not sufficient to mitigate AS hijacking

- **AS3 Implements RPKI-OV**
- Determines that route for q is NotFound
- As hijack attack from AS4 is successful at AS3 and it propagates



third-party prefix q
has no ROA

ROAs exist for all prefixes
originated by AS1

New RPKI Object REAP for AS Hijack Detection/Mitigation

- REAP: ROAs Exist for All Prefixes (REAP) – RPKI object digitally signed by an AS
- The AS is asserting that ROAs Exist for All Prefixes that are originated by it
- REAP object contains only an AS number

Detection algorithm:

1. Perform the RPKI-OV process [RFC6811] as normal.
2. If the result of RPKI-OV is NotFound and the origin AS has a REAP object, then replace NotFound with Invalid.

Mitigation:

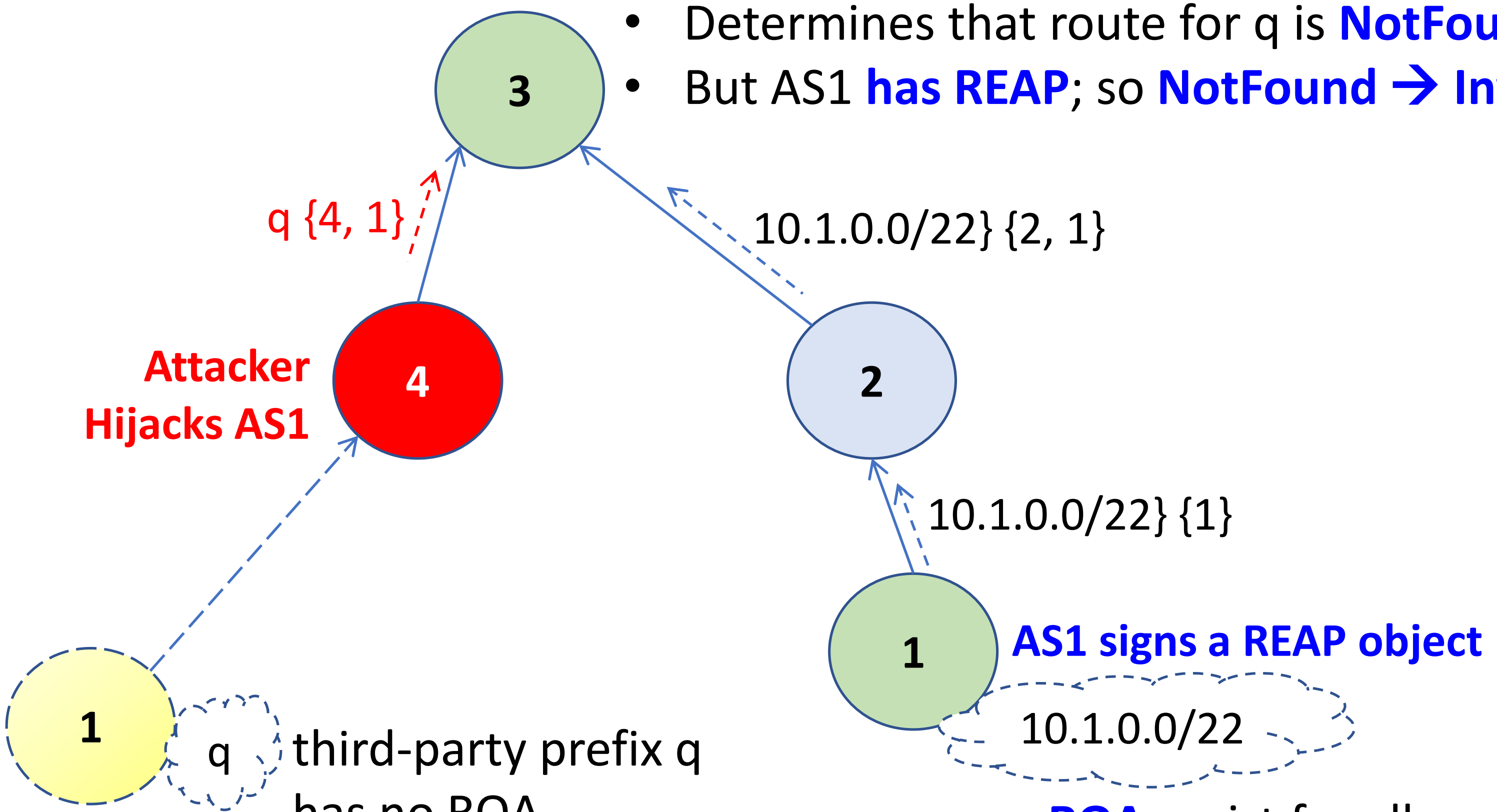
Operator SHOULD reject Invalid.

Benefit of REAP Accrues Right Away

- For the ASes that sign REAP objects and the ISPs that deploy RPKI-OV and REAP detection
- The benefit does not depend on whether other ASes adopt

Example with REAP solution

- **AS3 implements RPKI-OV and REAP**
- Determines that route for q is **NotFound** (per RPKI-OV)
- But AS1 **has REAP**; so **NotFound → Invalid**



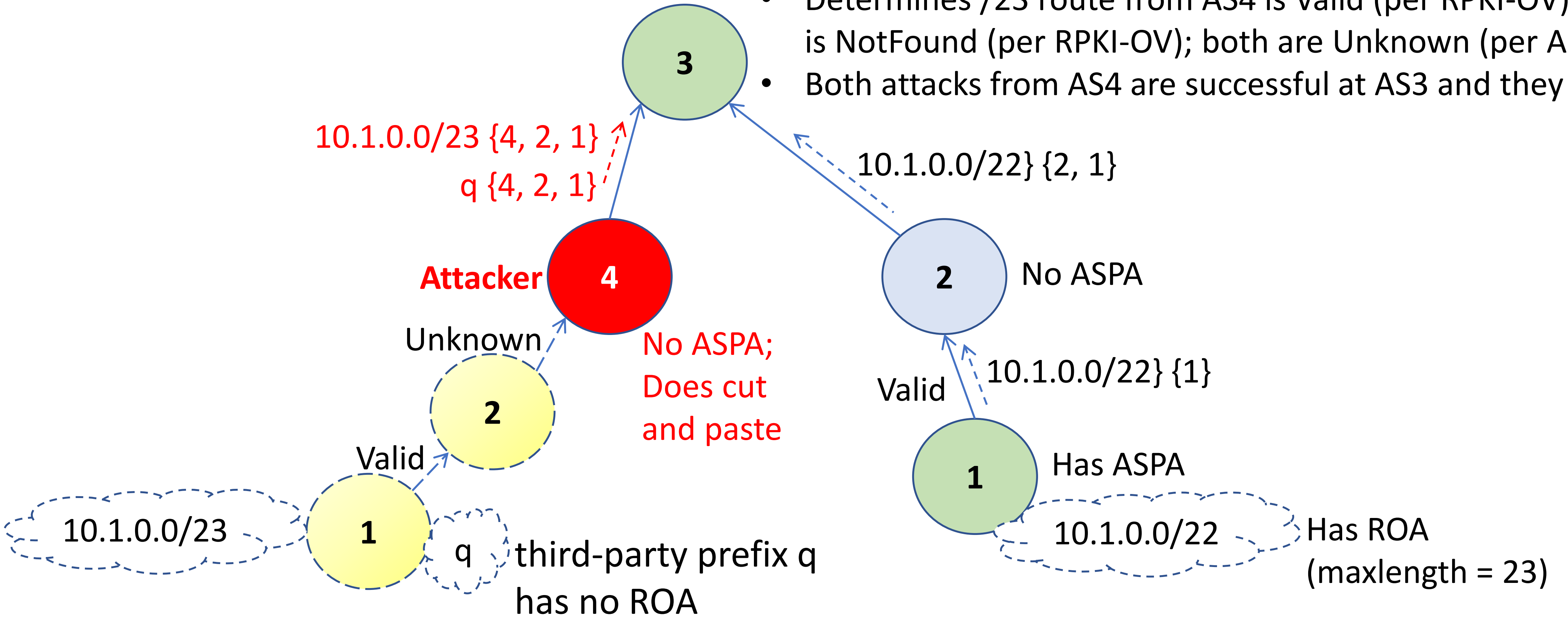
ROAs exist for all prefixes originated by AS1

Other Mechanisms that do AS Hijack Detection/Prevention

- BGPsec – requirement of path signatures prevents AS hijacks … but adoption?
- ASPA – vulnerable to cut and paste attacks in partial deployment

Example with ASPA solution

- AS3 Implements RPKI-OV and ASPA;
- Determines /23 route from AS4 is Valid (per RPKI-OV) and route for q is NotFound (per RPKI-OV); both are Unknown (per ASPA)
- Both attacks from AS4 are successful at AS3 and they propagate



Summary

- AS hijacking is a concern for AS operators (NANOG discussion)
- AS owner signs a REAP object
- REAP implementation in ISPs helps detect and mitigate the commonly occurring AS hijacking with a third-party prefix (accidental or malicious)
- Benefit accrues immediately for anyone participating
- REAP and ASPA are complementary for AS hijack detection