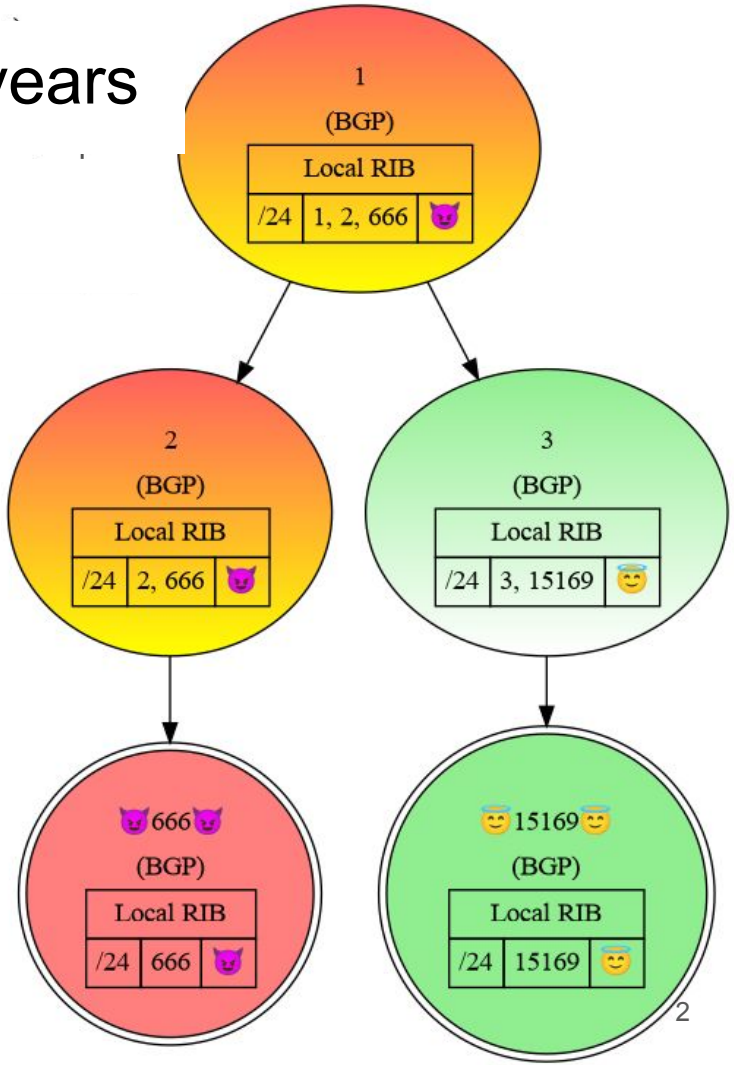
# Securing BGP ASAP: ASPA and Other Post-ROV Defenses

By: Dr. Justin Furuness, Dr. Cameron Morris, Dr. Reynaldo Morillo, Arvind Kasilya, Dr. Bing Wang, Dr. Amir Herzberg

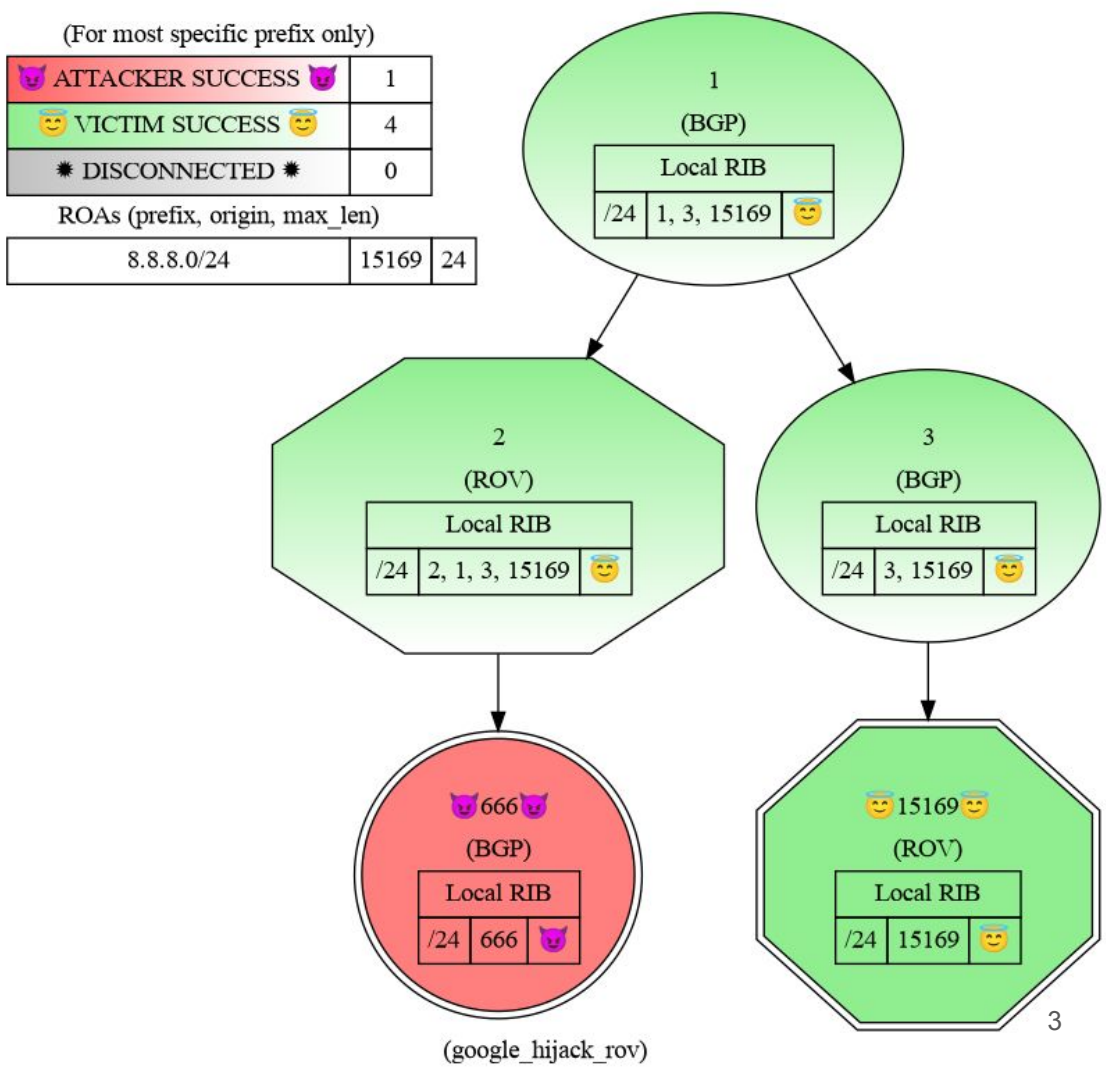
# BGP Hijacks: A Problem for over 30 years

- The internet is comprised of over 100k Autonomous Systems (ASes) and >500k connections
- These ASes communicate using the Border Gateway Protocol (BGP)
- From a high level, ASes announce which prefixes they own to the rest of the internet
  - For example, Google's AS of 15169 announces prefixes such as 8.8.8.0/24
- BGP was not designed with security in mind
  - Other ASes can claim to own google.com and reroute the traffic through themselves
  - These hijacks happen nearly every day: https://x.com/bgpstream



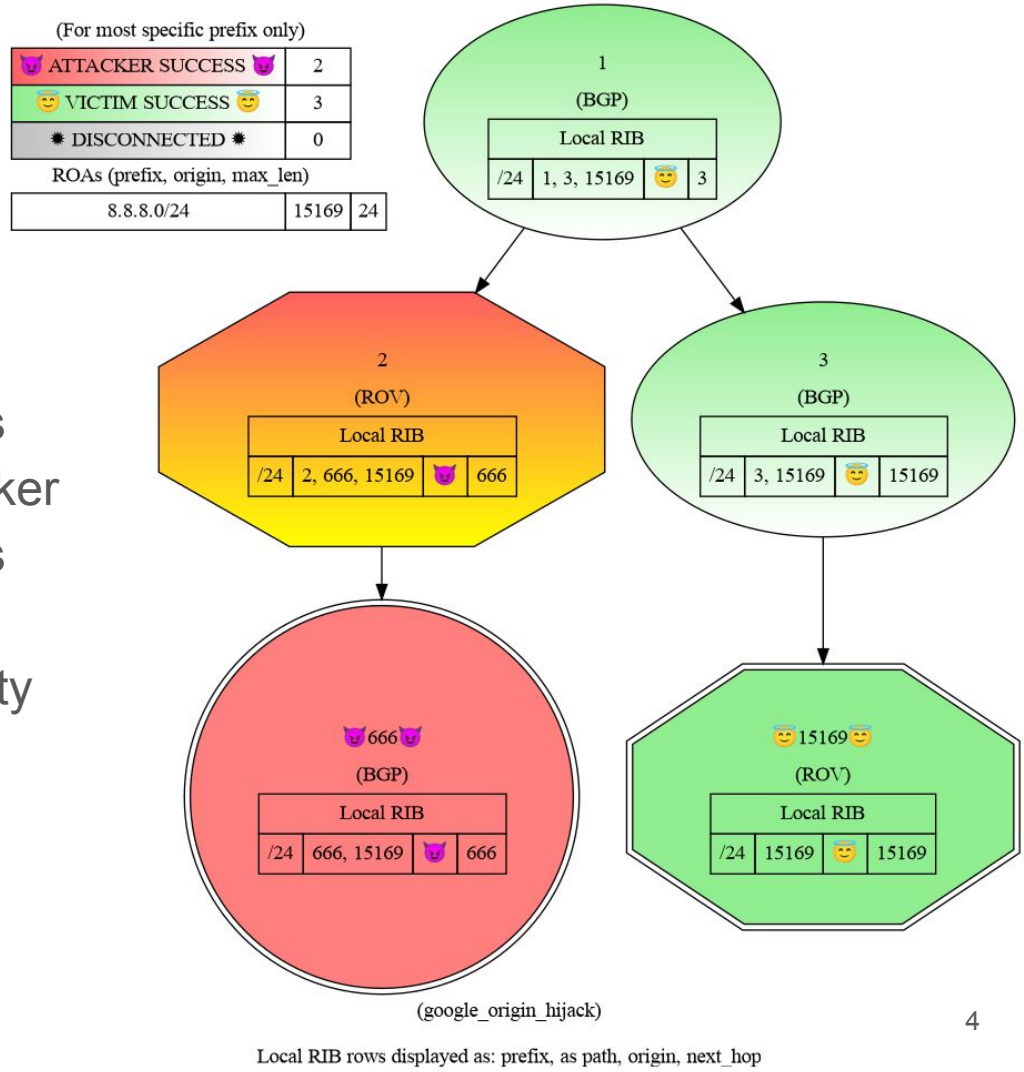
# Route Origin Validation (ROV)

- Internet Engineering Task Force (IETF) proposed standard to secure BGP
- From a high level, you can think of ROV using the RPKI to keep a list of valid prefix-origin pairs
  - The origin here is the AS number (or ASN for short)



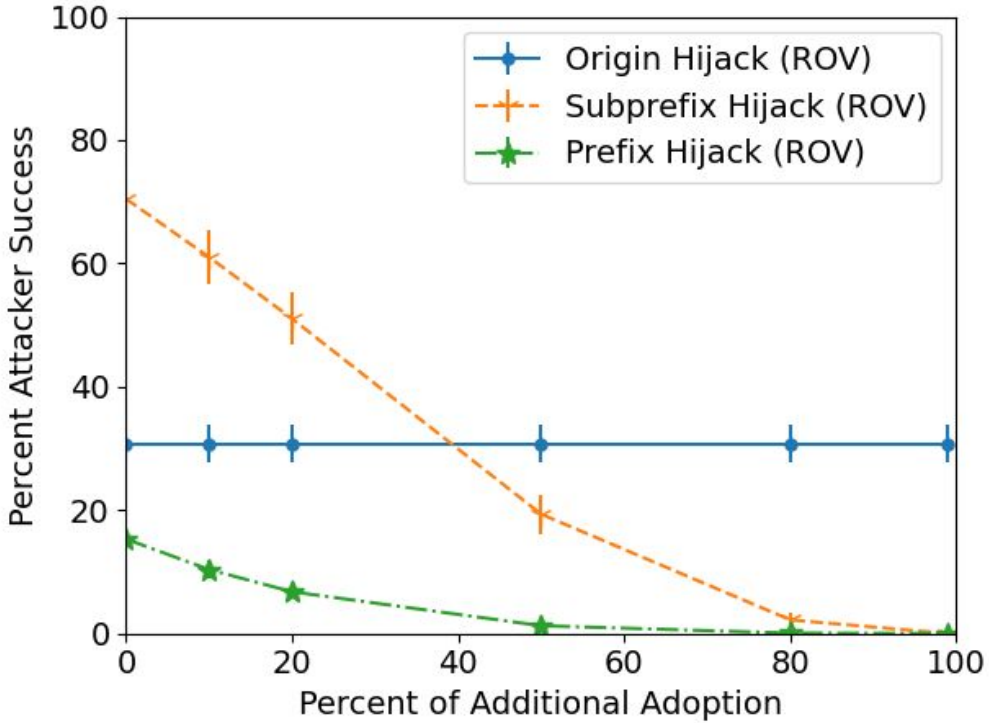
# Forged-Origin Hijacks

- While ROV deployment is widespread, unfortunately, ROV does not cover all types of attacks
- In a forged-origin hijack, the attacker can fake the AS-Path, and bypass ROV
- The attacker does incur the penalty of a longer AS-Path
- When sent to the attacker's providers, this powerful hijack propagates to the entire internet



# Is ROV Good Enough?

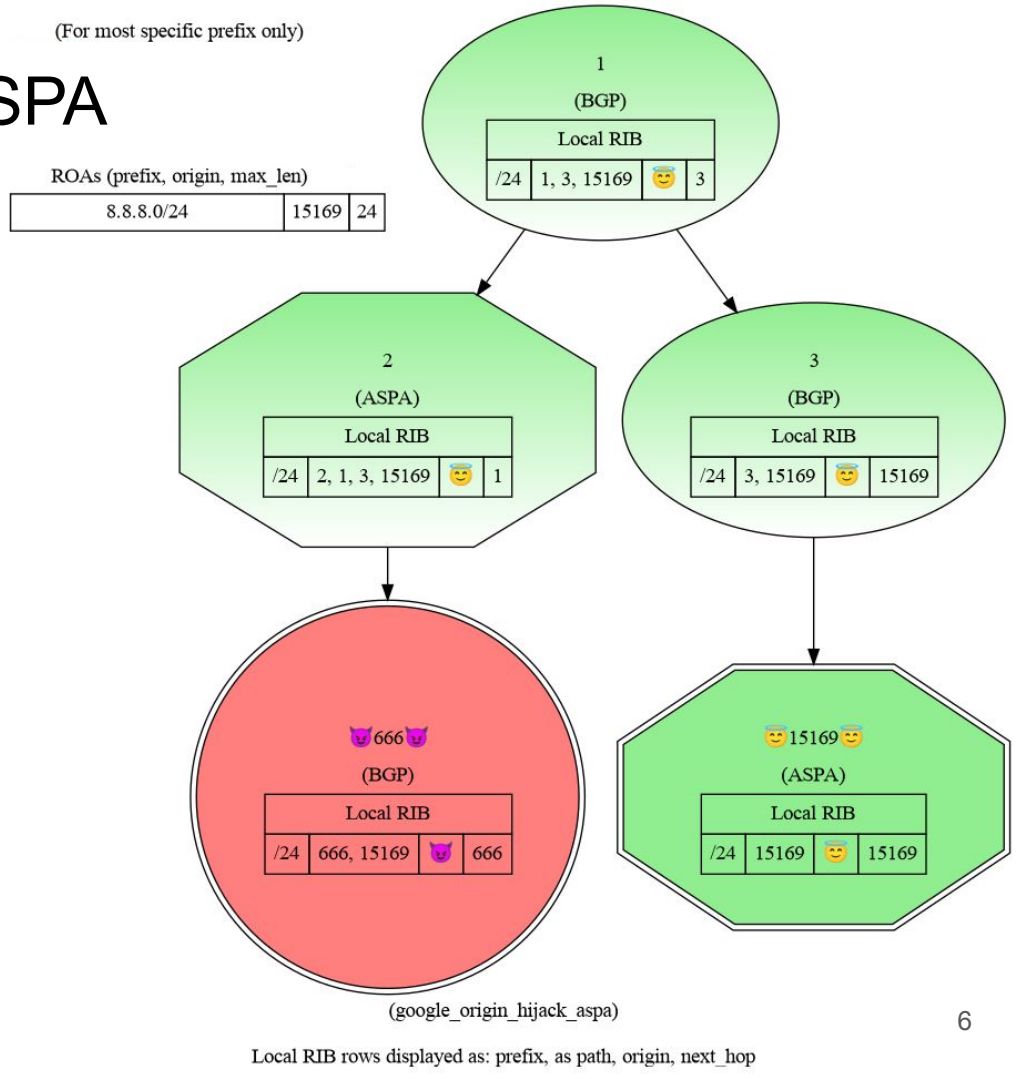
- To test this, in a first, we simulated the current internet with real-world AS and ROV data
- We discovered that already, today, forged-origin hijacks are more powerful than prefix-hijacks, even with ROV deployment!
  - Subprefix hijacks (which we don't have time to get into) are not possible for /24 prefixes
- So how can we defend against this powerful forged-origin attack?




Categories 3, 6, 7 from "Keep Your Friends Close, but Your Route Servers Closer"

# IETF Proposed Defense: ASPA

- ASPA functions by publishing a list of your providers in ASPA records
  - Customer-provider
  - peer-peer
- Whenever an ASPA AS receives a BGP announcement from a customer or peer:
  - If the provider chain is not possible, the announcement is rejected
  - ASPA also protects against leaks
- ASPA is readily deployable and already in the wild!

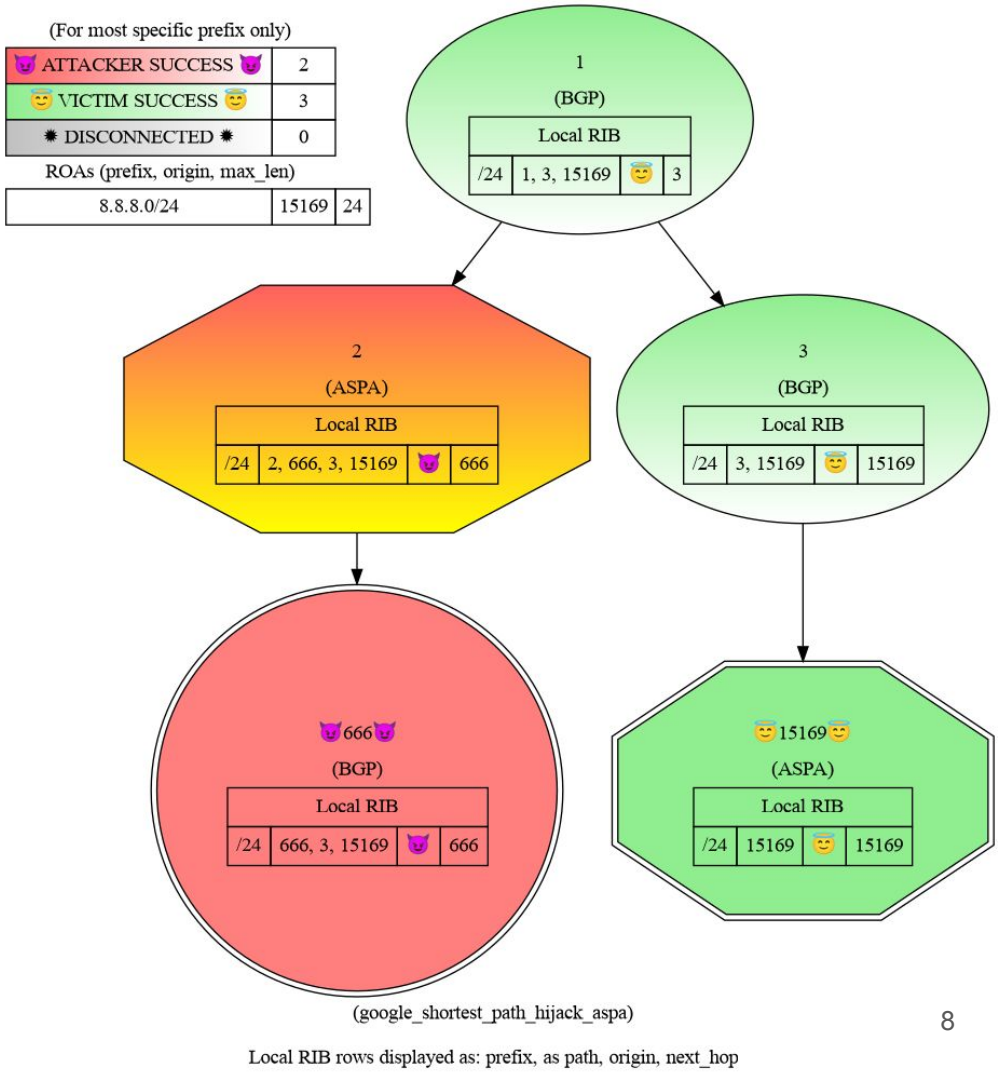


# Securing BGP ASAP: ASPA and Other Post-ROV Defenses

- In our work, we evaluate ASPA against other Post-ROV defenses (that can be found in our paper) and propose extensions to it that we call ASPA with Neighbors (ASPAwN)
- We find that ASPA is very effective at preventing:
  - Forged-Origin hijacks
  - Shortest-Path hijacks (we are the first to evaluate this)
  - Route Leaks
    - In a first, we find that ASPA is better than OTC (another IETF RFC)!
- Prior works came to the conclusion that ASPA is not effective at intermediate ASes, or without tier-1 adoption - a conclusion that may deter would-be adopters.
  - In our work, we show that ASPA is effective regardless of tier-1 adoption, motivating ASPA adoption at all transit ASes
- We discuss vulnerabilities relating to the novel First-ASN-Stripping Hijack
- Our work is fully reproducible and open-source (links at the end)

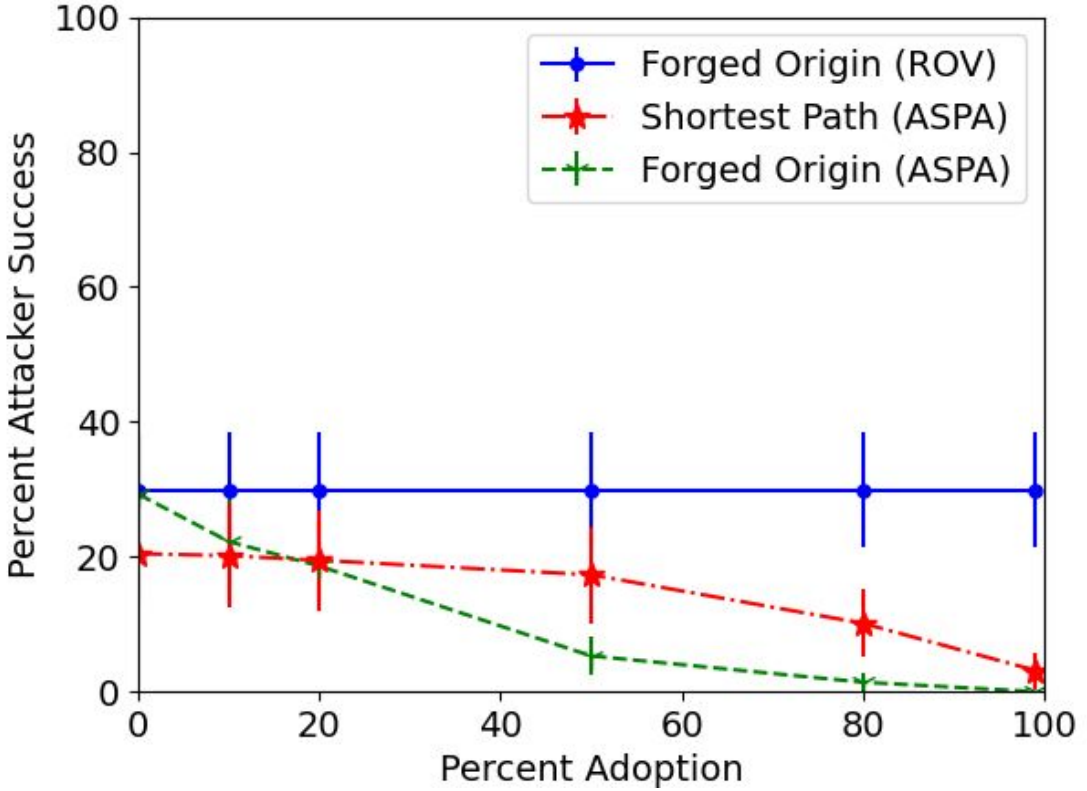
# Shortest Path Hijack

- There is another type of hijack designed to work against ASPA
- The Shortest-Path hijack keeps adding ASes to the AS-Path until there is an AS that does not adopt ASPA
  - When this occurs, ASPA can not detect the hijack, since the last AS in the AS-Path does not announce their providers and does not have ASPA records



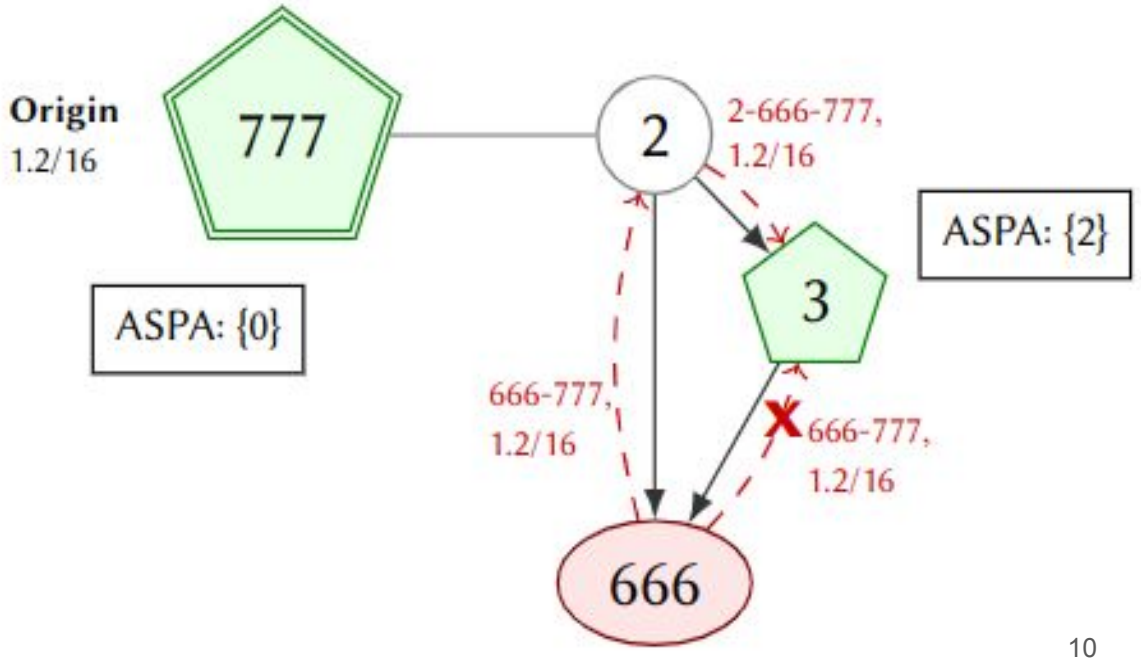
# Forged-Origin and Shortest-Path Hijack Simulations

- As we can see, ASPA is highly effective against both of these attacks
  - Significantly better than ROV
- Initially the forged-origin hijack is the strongest due to the shorter AS-Path
- Once ASPA adoption is high, the shortest-path hijack is stronger
  - (Since this bypasses ASPA with the longer AS-Path)



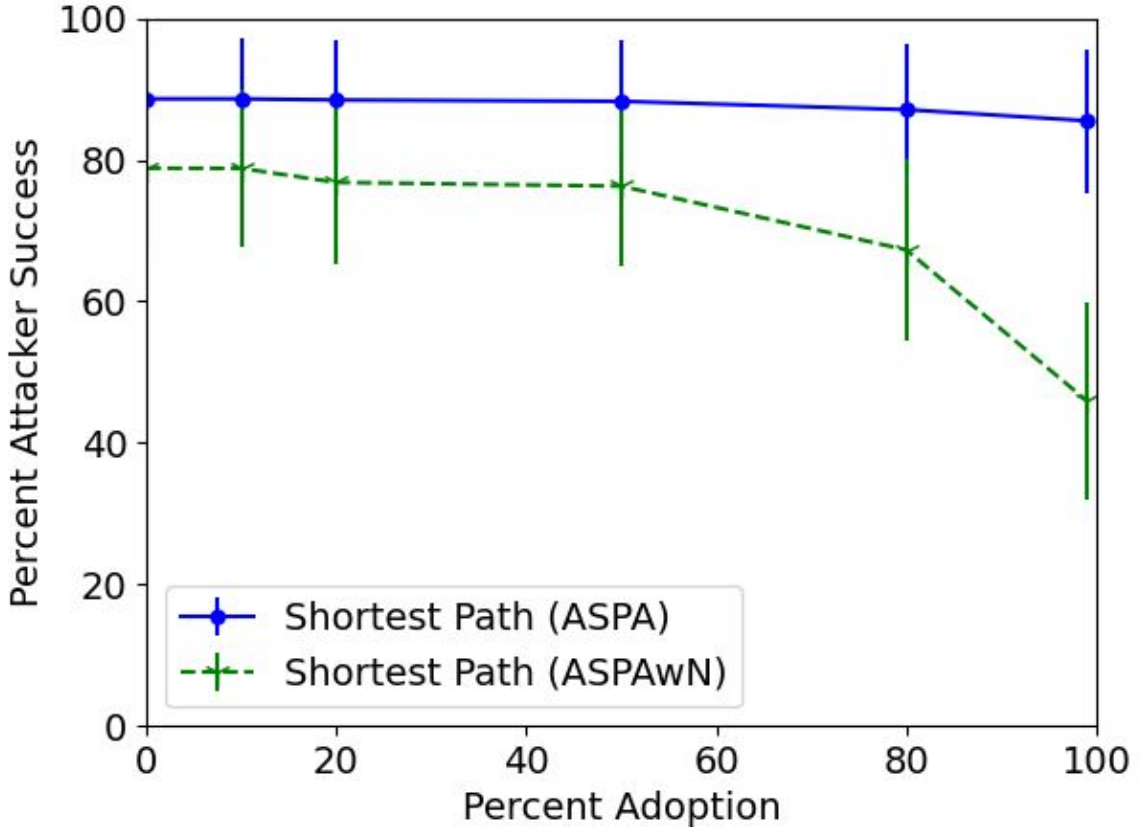
# ASPA with Neighbors (ASPAwN)

- ASPA only validates announcements sent to providers
- ASPA rejects the hijack from a customer - but accepts from a provider!
- ASPAwN adds an **optional** set of valid next-hops to the ASPA record to prevent this
- This was developed in parallel to ASRA and has equivalent security properties



# Shortest-Path Hijack from a Transit AS

- Here a transit AS performs the shortest-path hijack against ASPA and ASPAwN adopting ASes
- We are measuring the customer cone of the transit AS
- ASPAwN is significantly more effective at protecting customers
- (About 50% of ASes go through the attacker passively)



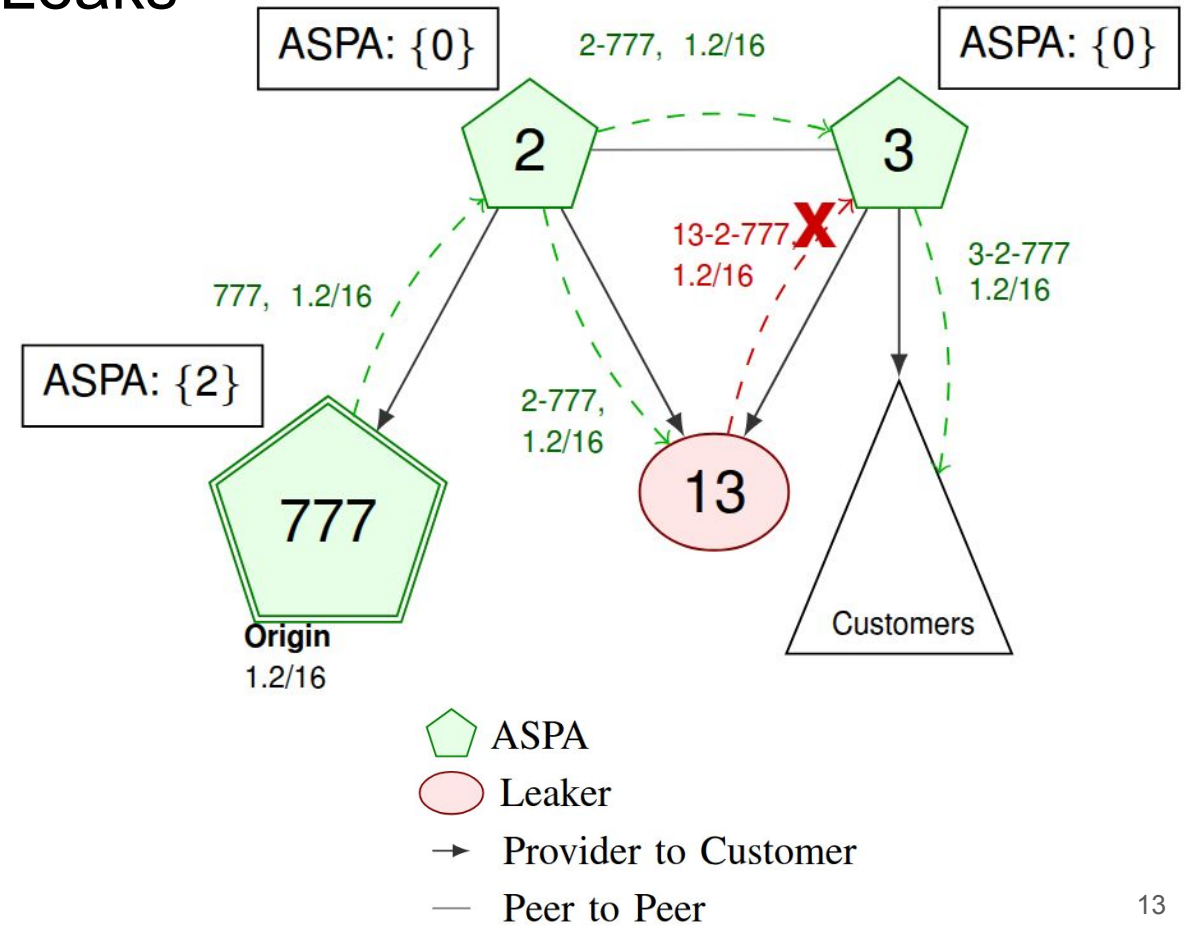
# Enforce-first-as & First-ASN-Stripping Hijack

- ASPA states that the first ASN in the AS-Path must be the ASN of the neighbor
  - This just makes common sense to check that your neighbor is the last ASN on the AS-Path
  - This is using the enforce-first-as option on routers
- However - we discovered this behavior is not the default on several routing vendors!
- What's worse, this is a global setting for Cisco
  - A bug for over 10 years, updated 2023
- Attackers can exploit this in what we call the first-asn-stripping hijack, where they strip their own ASN from the AS-Path
  - This reduces the AS-path length and attracts more traffic to the attacker

| Vendor | Default | Global |
|---|---|---|
| Cisco | Y | Y |
| Juniper | N | N |
| Arista | Y | N |
| BIRD | N | N |

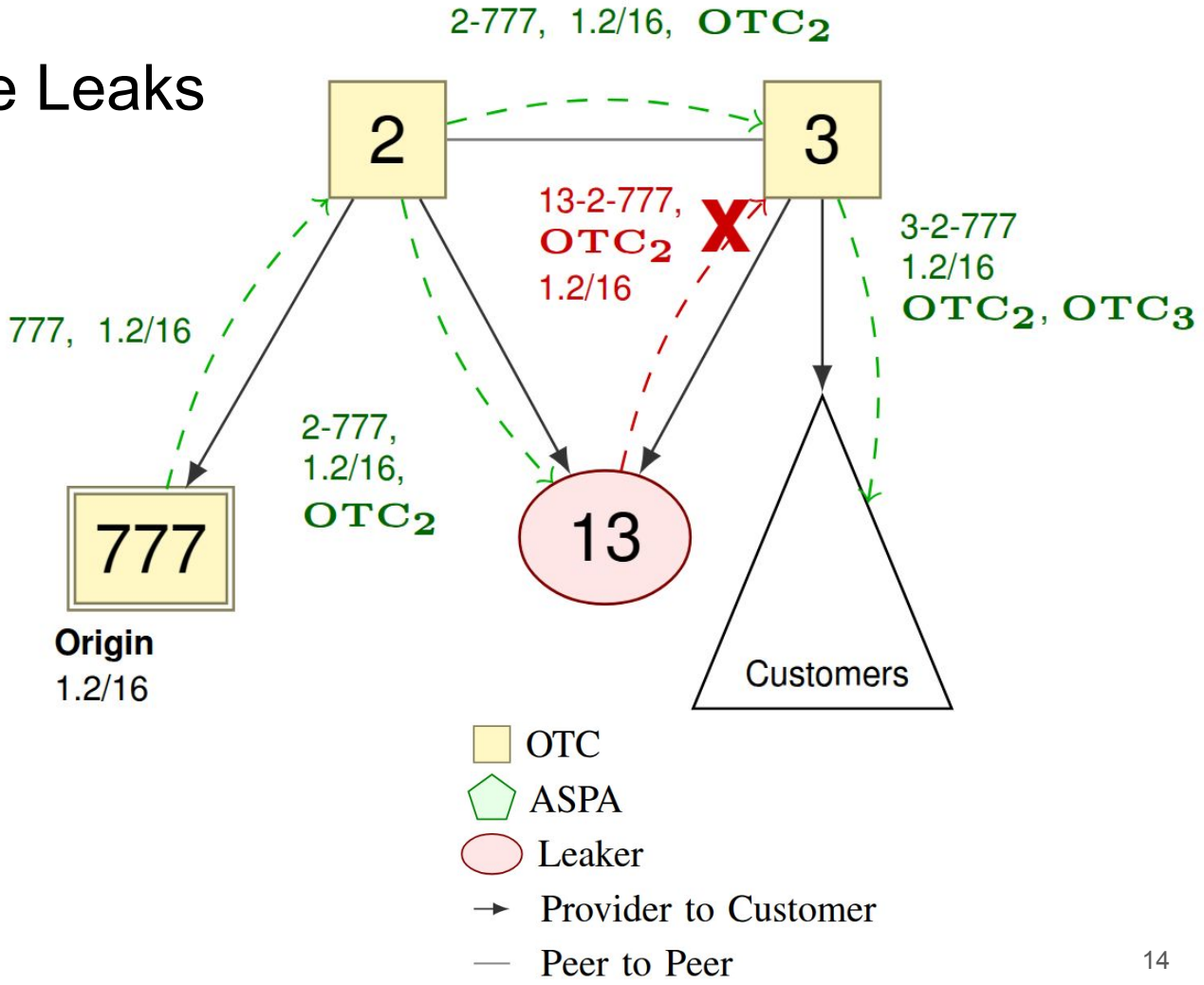
# ASPA Against Route Leaks

- Beyond hijacks, ASPA also protects against route leakage
- These are commonly misconfigurations that violate valley free routing
- ASPA uses special algorithms outlined in the draft by the IETF to detect route leaks
  - In short - ensure valley free routing is taking place



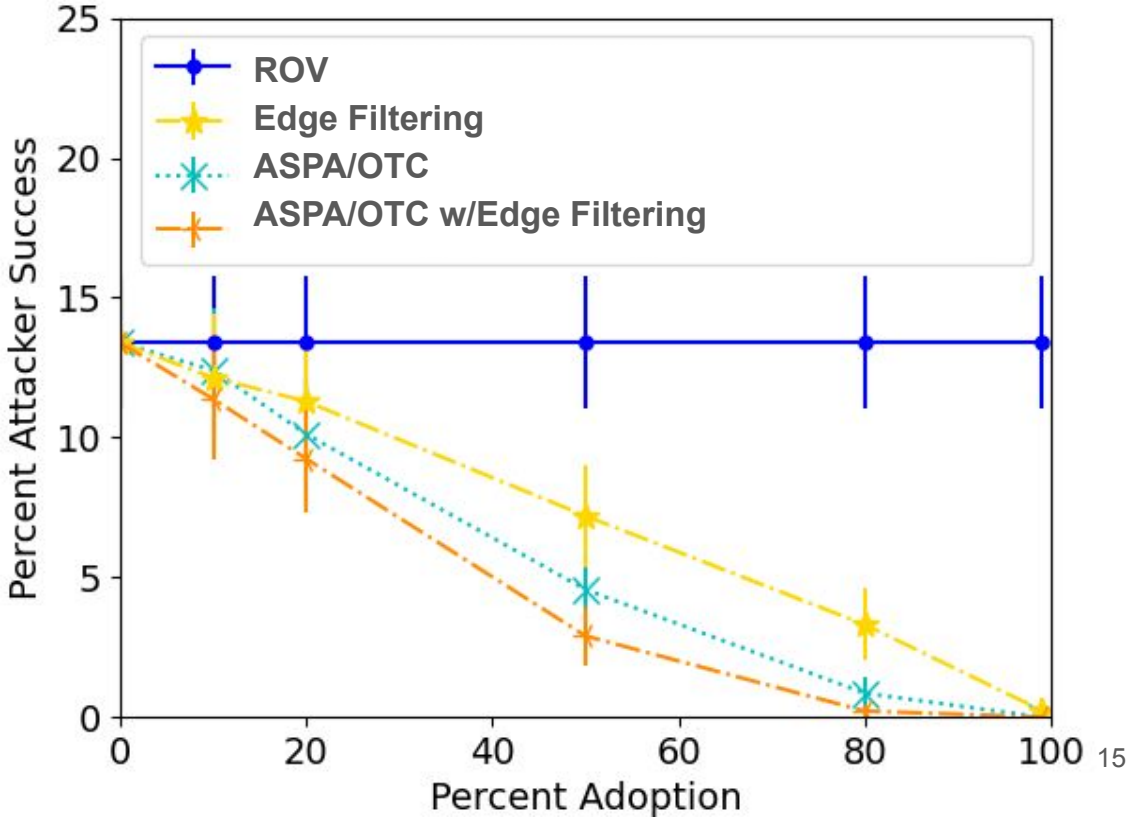
# OTC Against Route Leaks

- OTC is another IETF proposed RFC
  - From a high level, announcements with OTC should only be sent to customers
- OTC is already deployed, but only by a few smaller ASes



# ASPA vs. OTC Route Leak Simulations

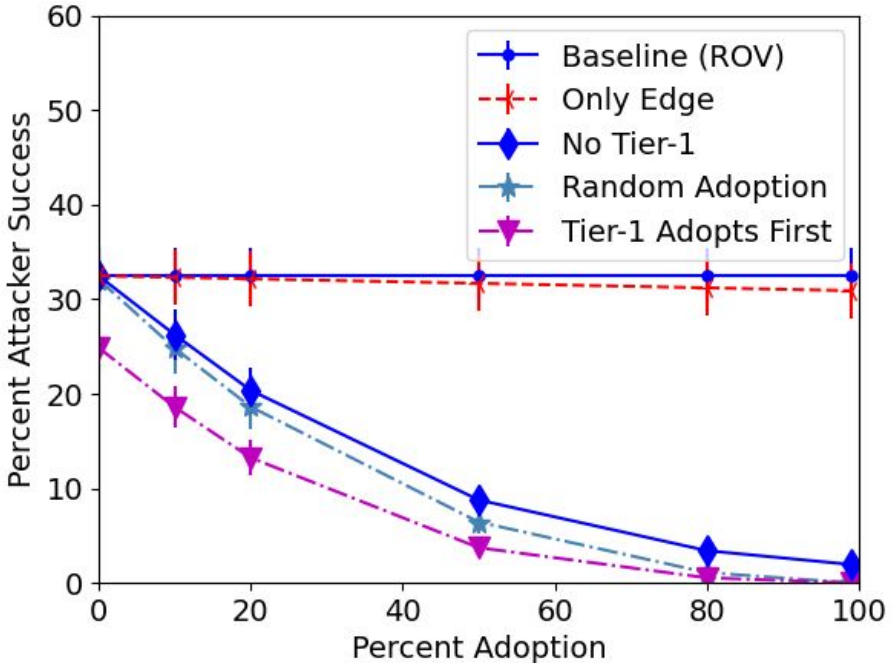
- We prove in a first that ASPA is equivalent to OTC for misconfigurations
- ASPA also protects against intentional leaks
  - (where an attacker would simply remove OTC)
- ASPA outperforms OTC when ASes drop transitive attributes
  - 1-3% of ASes do this



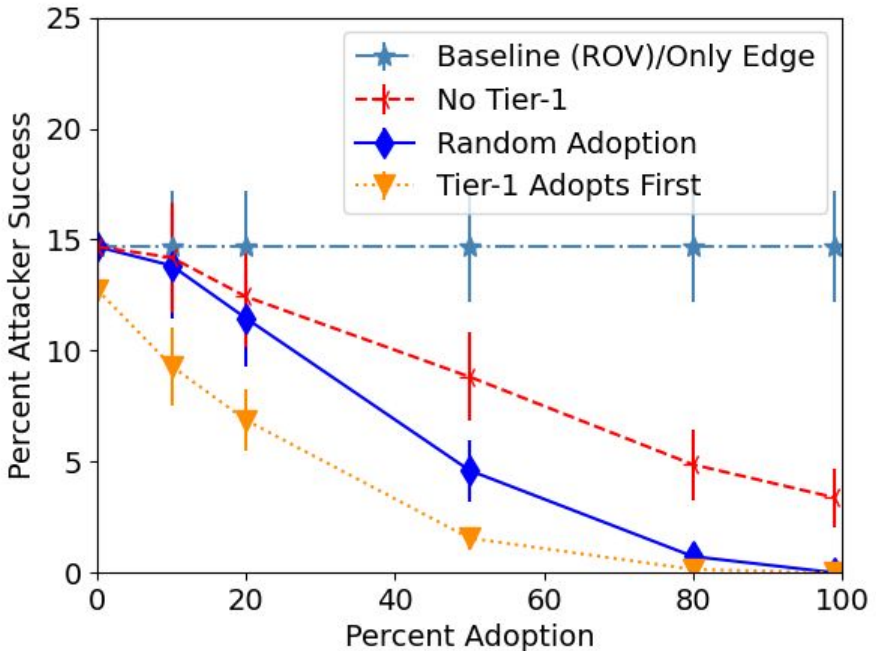
# ASPA Adoption Scenarios

Contrary to prior works, we show that ASes benefit from ASPA even when tier-1 ASes do not adopt, motivating ASPA adoption throughout transit ASes and the internet at large

Forged-Origin Hijack




Multihomed Route Leak



# Reproducibility

All our simulations and everything in this work is **fully reproducible**

- Our simulations run off of BGPy, a leading Python BGP Security Simulator: github.com/jfuruness/bgpy_pkg
  - BGPy has been used in 5+ publications already with many more ongoing
  - It has been used by teams all around the world - including NIST!
  - It is actively maintained by me, any questions just reach out :)
- We open-source our ROV collection tool here: github.com/jfuruness/rov_collector
  - We parse real-world ROV data from every known ROV data source
- We also open-source our code to run our simulations:
  - github.com/jfuruness/aspa_eval
- We'd love to hear from you if you want to try it out, extend this, and implement some simulations to answer any unanswered questions!

# Thank You!

## Securing BGP ASAP: ASPA and Other Post-ROV Defenses


- Dr. Justin Furuness (jfuruness@gmail.com)
- Dr. Cameron Morris (cameron.morris@uconn.edu)
- Dr. Reynaldo Morillo (reynaldo.morillo@uconn.edu)
- Arvind Kasilya (arvind.kasilya@uconn.edu)
- Dr. Bing Wang (bing@uconn.edu)
- Dr. Amir Herzberg (amir.herzberg@uconn.edu)


- Links:
  - BGPy:
    - github.com/jfuruness/bgpy_pkg
  - ROV Collector:
    - github.com/jfuruness/rov_collector
  - ASPA Eval:
    - github.com/jfuruness/aspa_eval
- I was also limited due to the time constraints, for more (especially comparison to other policies), read our paper :)
- Any questions?