Simulations of RPF SAV Methods (uRPF and BAR-SAV)

Presented by Amir Herzberg

Joint work with: Nick Scaglione*, Justin Furuness*, Yossi Gilad**, Hemi Leibowitz***, Cameron Morris*, Bing Wang*, Sriram Kotikalapudi****

*: Univ. Of Connecticut, **: Hebrew University,

: College of Management, Rishon, Israel, *: NIST

Goal: realistic, comprehensive simulations of Reverse Path Forwarding list SAV methods

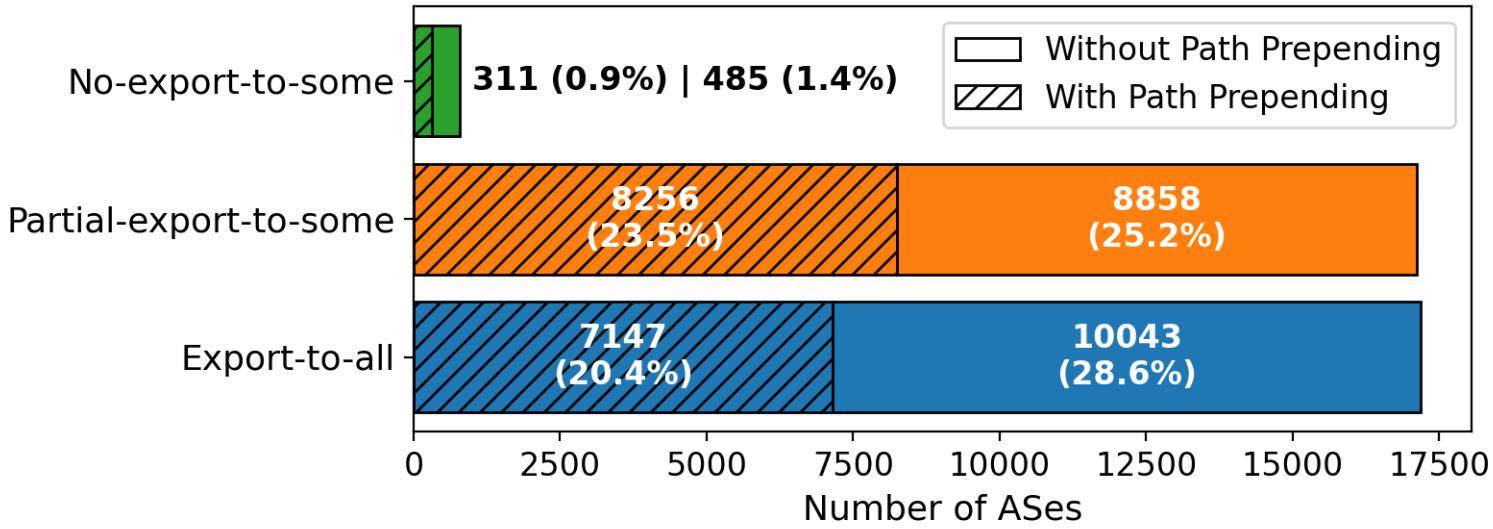
- **Evaluate different RPF-list SAV policies,** using Internet AS topology and relationships [as measured by CAIDA]
  - **False Positive Rates** vs **Detection Rates** (True Positive Rates)
  - Performance under **partial adoption**
  - Impact of (measured) **traffic engineering** methods [significant!!]
- Policies Evaluated [some results only in paper]
  - Strict uRPF
  - Feasible-Path uRPF (FP-uRPF)
  - Enhanced Feasible-Path uRPF (EFP-A and EFP-B)
  - BAR-SAV (with and without BAR-SAV-PI)

Export Policies and TE Methods

- **Export-to-all** – export all prefixes to all eligible neighbors
  - Only model used by most published routing-security simulations
- **AS path prepending** – prepend ASN multiple times to AS_PATH to deprefer route
- **Partial-export-to-some** – export prefixes selectively to some providers (some prefixes not exported or with NoExport)
- **No-export-to-some** – to some providers, export all prefixes with NoExport, or don't export at all
  - Mostly, **invisible** from MRT files (of RIPE RIS, RouteViews, etc.; not in CAIDA)
- **Direct Server Return (DSR)** – use prefix to send, without exporting it

Traffic-Engineering Measurement

- Use CAIDA's AS-level topology together with public routing data from RIPE and RouteViews BGP collectors
- ➔ Under representative of no-export-to-some policies, as (most of) these announcements do not propagate to the collectors
- Measurement only of edge Ases; transit AS behaviors not (yet) measured



Simulation Methodology

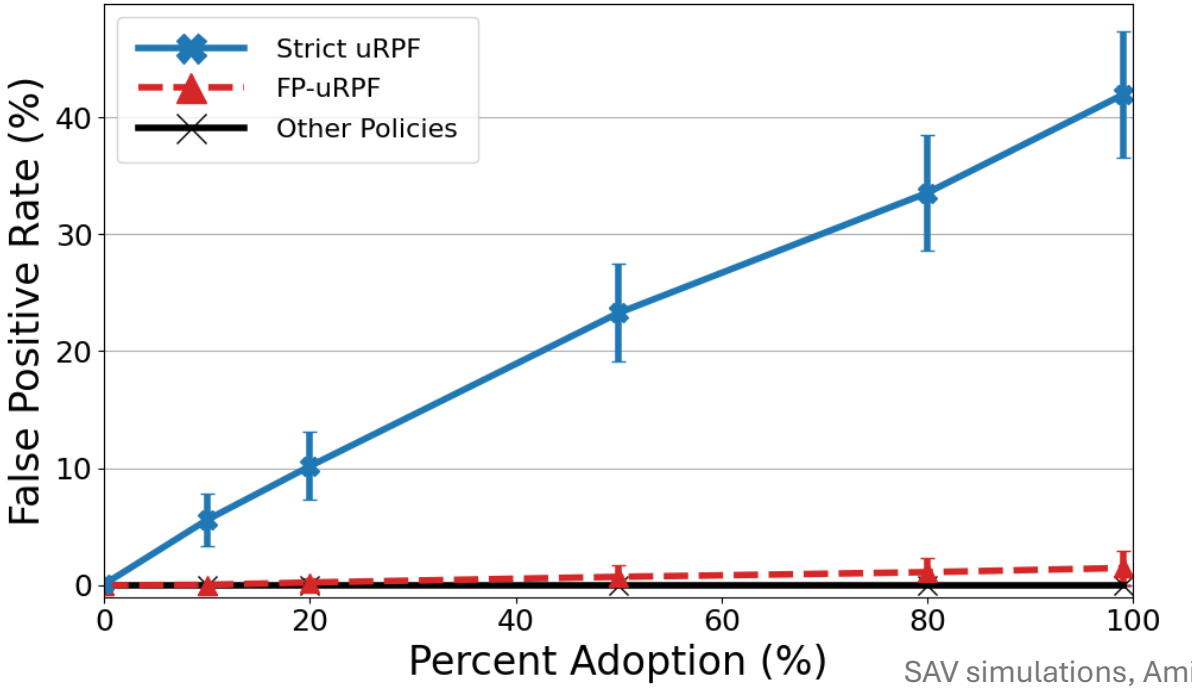
- We developed, use, extend the **BGPy simulator**
  - We (and others) use BGPy to study different SIDR attacks/defenses
  - In this study, we implemented SAV policies, data-plane traceback and performance metric tracking
  - Integrated TE measurement data into routing models (only for origins)
  - Open-sourced (anonymized repository until paper release)
- Modeled the Internet as a graph of ASes and inter-AS relationships based on CAIDA (2025)
  - CAIDA dataset may miss some relationships or have wrong relationships ➔ disconnections ➔ incorrect losses ➔ ignored
  - Only customer-provider and peer-peer relationships are modeled
    - Sibling, IXPs/RSs and complex relationship excluded (insufficient data)
- Random edge ASes used as legit-origin and as spoofer (attacker)

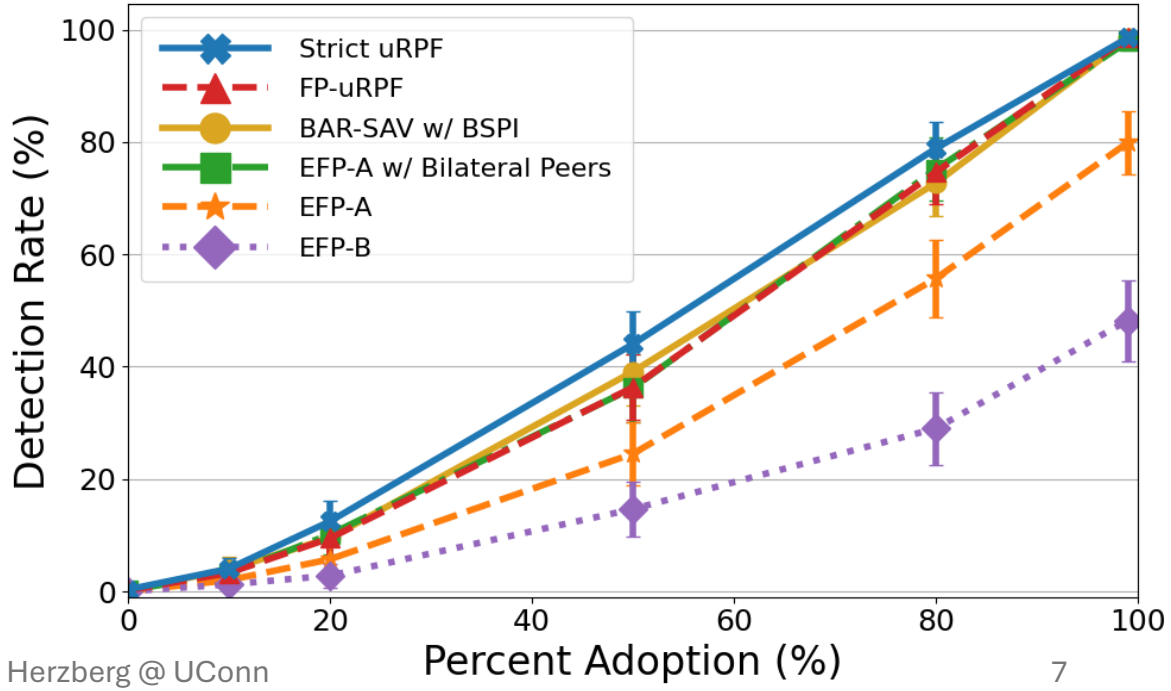
Simulation Setup

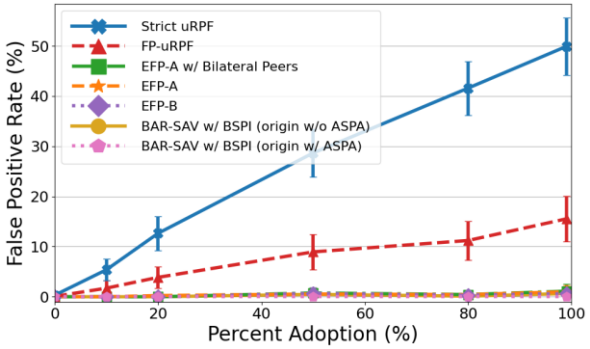
- Scenarios
  - Export-to-all
  - Traffic-Engineering (includes all measured TE behaviors)
  - Focus on Partial-export-to-some (comparable results to TE, see paper)
  - No-export-to-some
  - Direct Server Return (DSR)
- Varying percent of adoption 0%-99%
- Attacker models: **Spoofing Host** and **Spoofing AS**
- 5 destinations, 1000 trials
- Results presented with 95% confidence interval

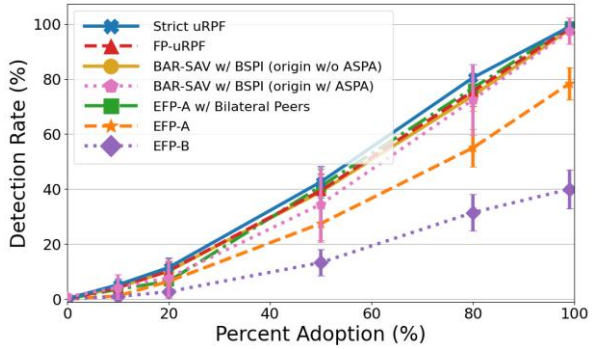
Export-to-all

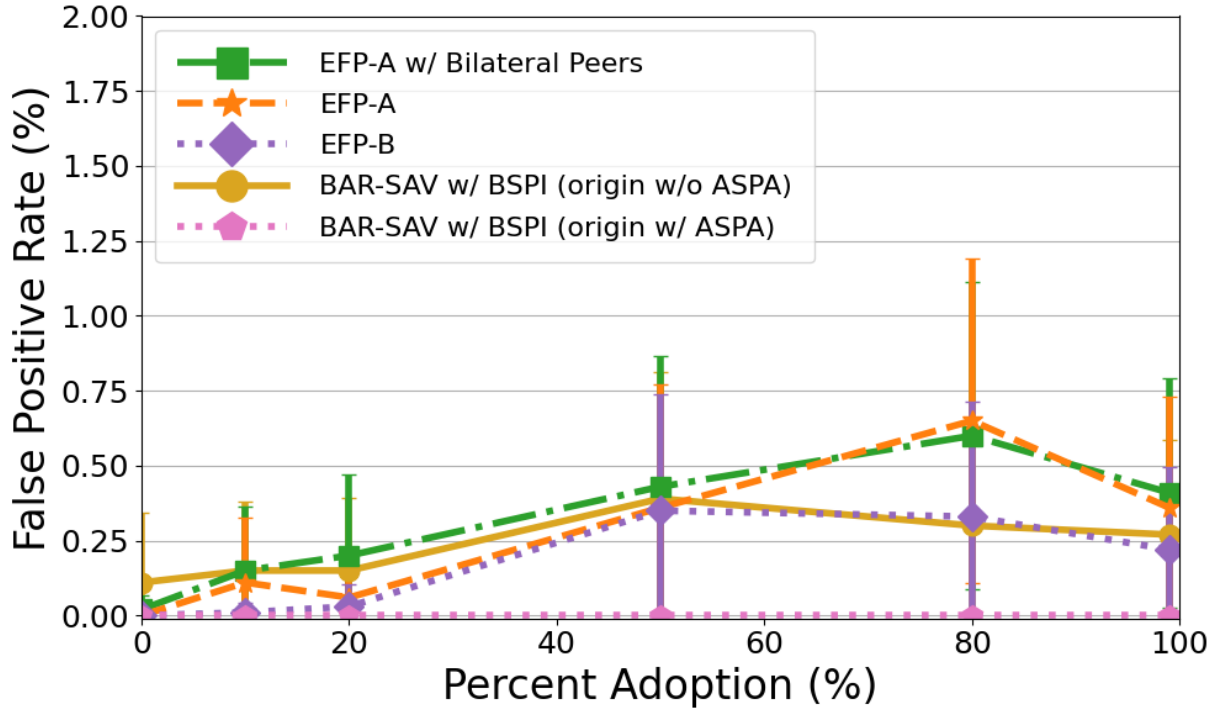
- Default assumption in (most?) prior works
- Idealized routing environment for SAV policies
- Strict and FP-uRPF (cust.+peers) are the only two policies with False Positives
- BAR-SAV (w/ BSPI) & EFP-A (w/BiPeers): good detection and no false positives









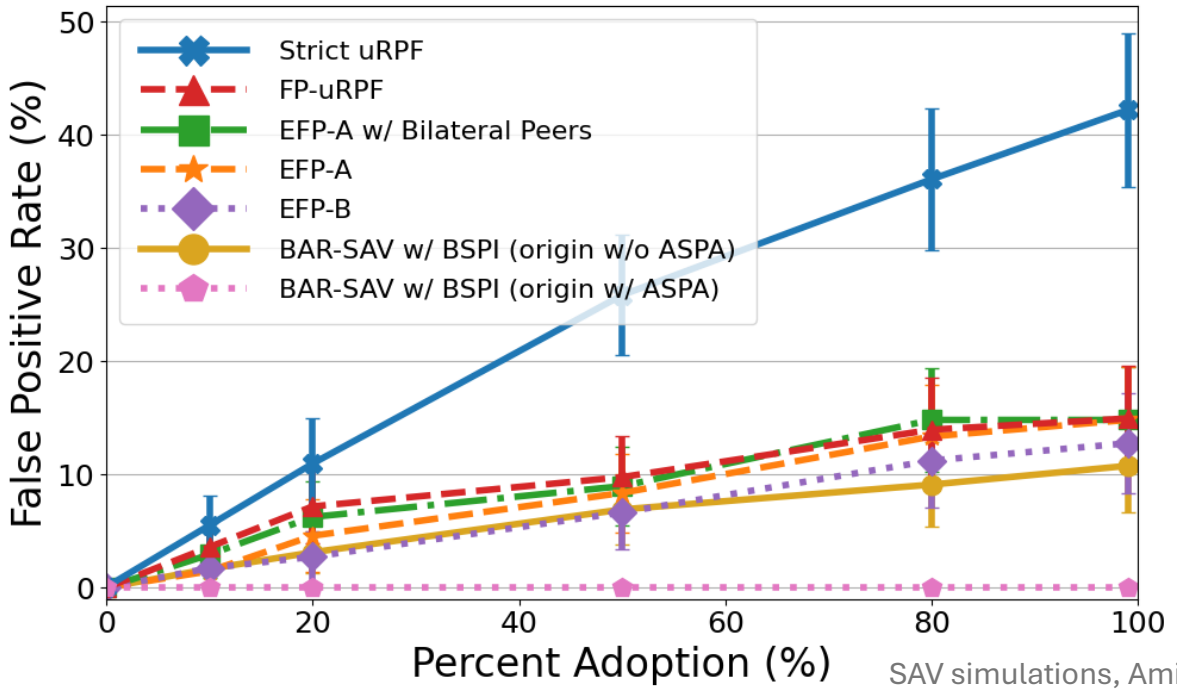


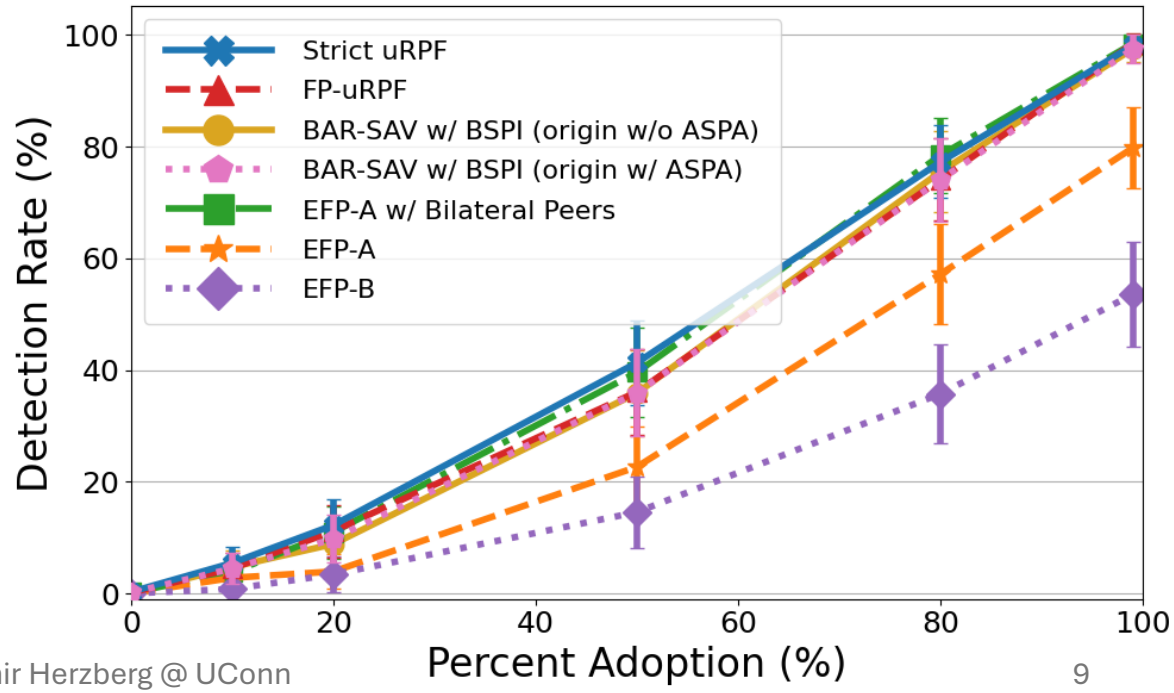
Traffic-Engineering

- We measured TE use by origins (edge ASes)
- Incorporates all measured TE behaviors
  - Export-to-all, Partial-export-to-some, No-export-to-some (under-represented), and path prepending
- Increased routing asymmetry and multiple prefixes from the same origin AS
- BAR-SAV, with only the origin adopting ASPA, results in **no false positives** [if origin publishes ASPA] and **great detection rate** (almost as good as Strict uRPF) [esp. – as shown – w/ BSPI]

No-export-to-some

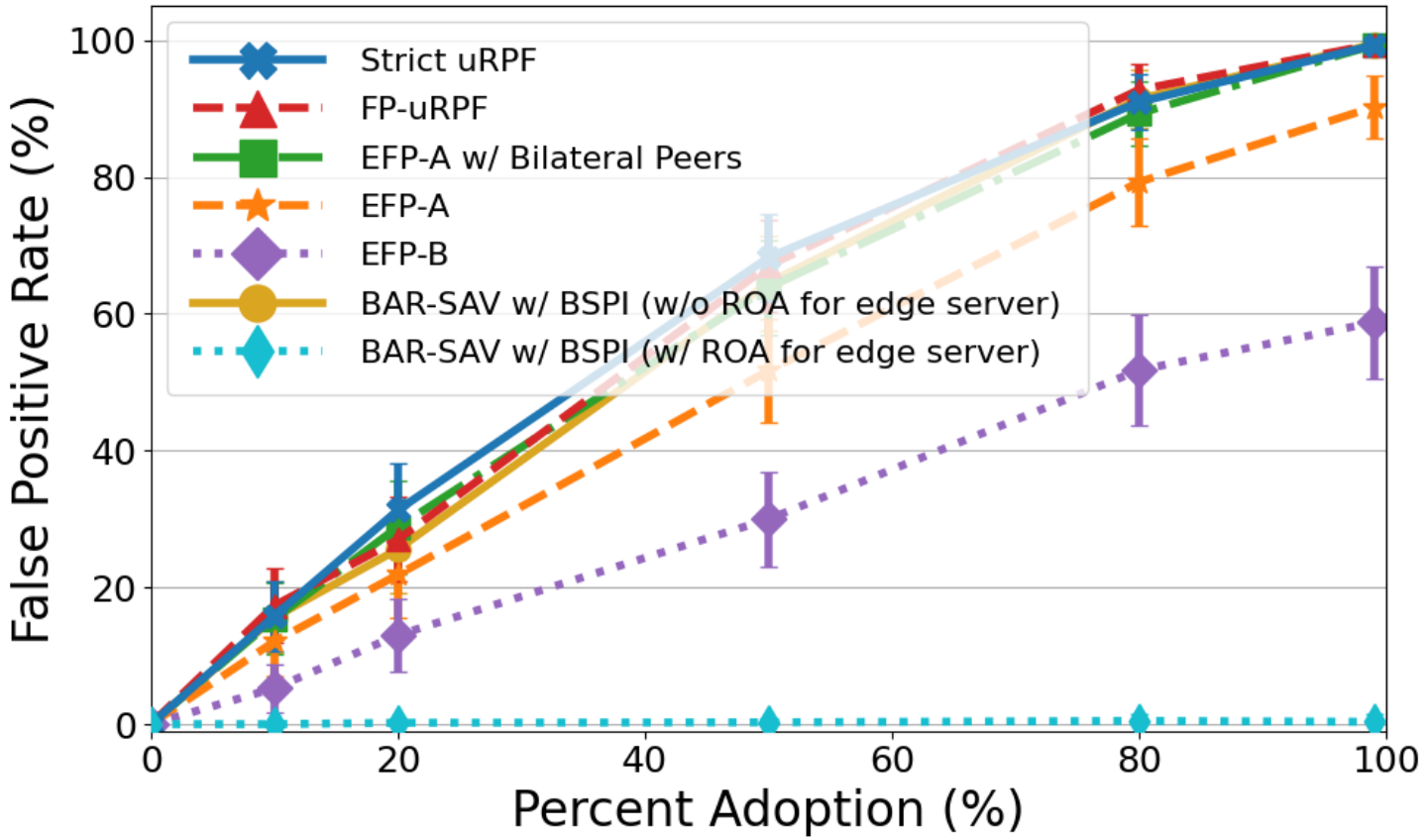
- No-export to at least one provider results in the lowest route visibility
  - Can't rely on measurements (would mostly be invisible), so: random provider
  - Other ASes export as measured, but no TE for transit ASes (not yet measured)
- Without RPKI, there are significant false positives for all policies
- With ASPA, BAR-SAV has no false positives whiles maintaining a high spoofing detection rate





Direct Server Return (DSR)

- Routing scenario in which AS sending data traffic does not announce the source prefix used
- BAR-SAV with the origin having a valid ROA for the source prefix results in **no false positives**



Key Takeaways

- Traffic-engineering has a significant impact on SAV policies: recommendations should probably consider TE in use
  - More false positives (even a bit for BAR-SAV) in additional simulations (not shown) with random TE by transit ASes [see paper and/or ask us]
- BAR-SAV consistently results in the lowest/zero false positive rates and has great detection rates [esp. with BSPI]
  - ZFP for: export-to-all, partial-export-to-some, or if ASPA published
  - ZFP even for DSR, if origin authorized by ROA (or TOA)

Thank you!

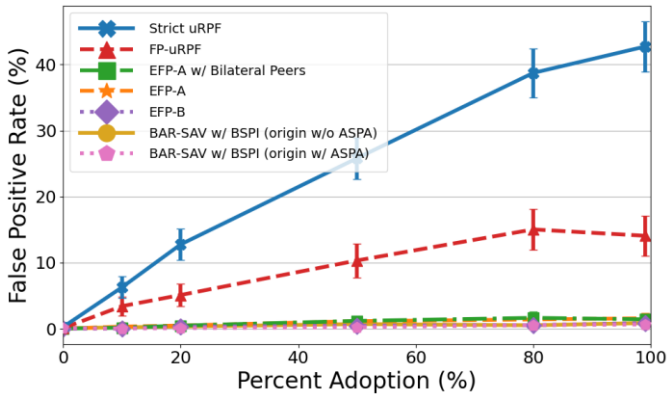
- For a copy of the paper, please contact:
  - nicholas.scaglione@uconn.edu
  - amir.herzberg@uconn.edu
  - Or other authors: Justin Furuness, Yossi Gilad, Hemi Leibowitz, Cameron Morris, Bing Wang, and Sriram Kotikalapudi
- Talk to us also about other works on SIDR (e.g., extensions to ASPA) and improved PKI
- Questions?

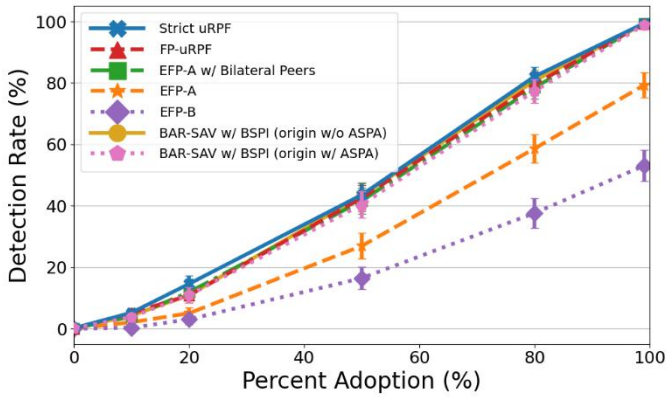
Additional slides:

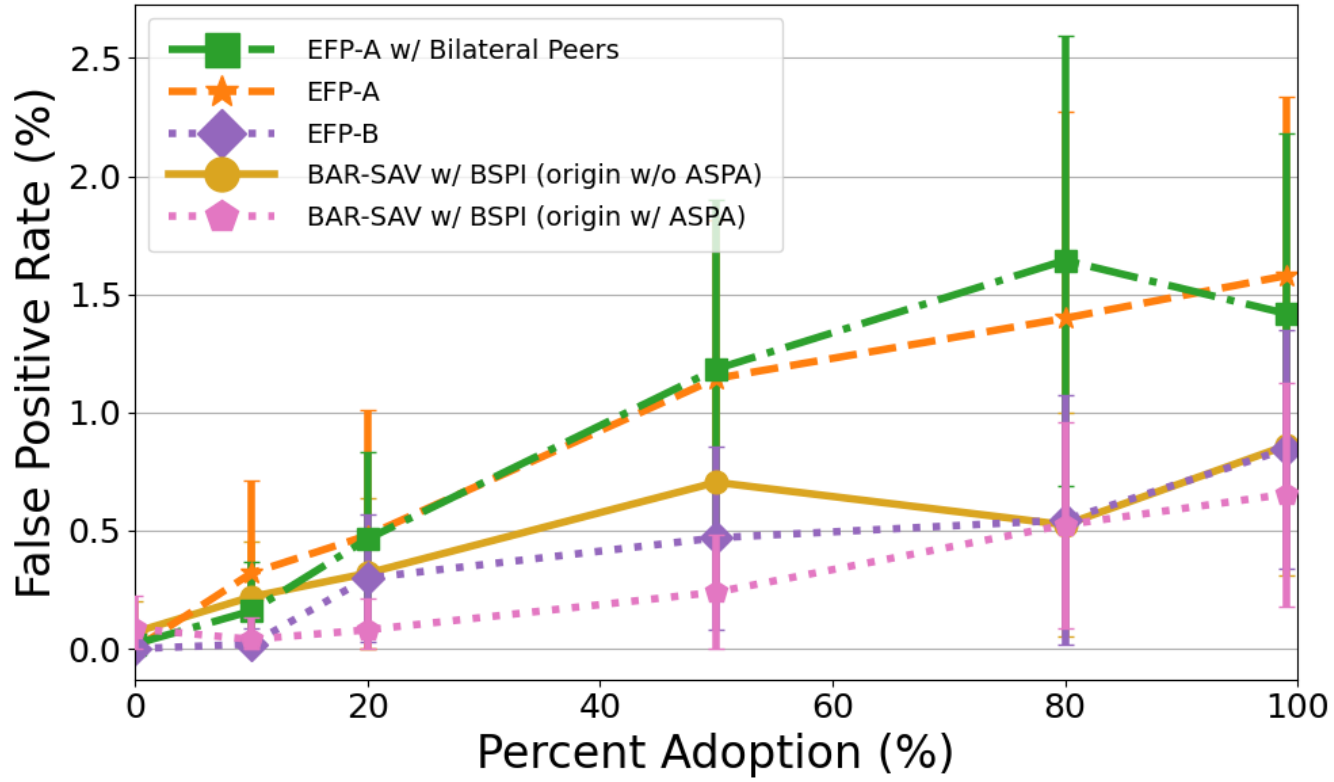
- Initial results for TE by transit Ases
- Example of BAR-SAV false positive (with transit AS not-exporting to a provider)

Transit AS performing TE: Simulation Results

- 50% of Transit ASes perform no-export to one provider
- Origin AS performs any TE technique
  - Partial-export-to-some, No-export-to-some, path prepending
- BAR-SAV has false positives even under the assumptions:
  - Origin adopting ASPA
  - Providers of the victim originating their own announcements

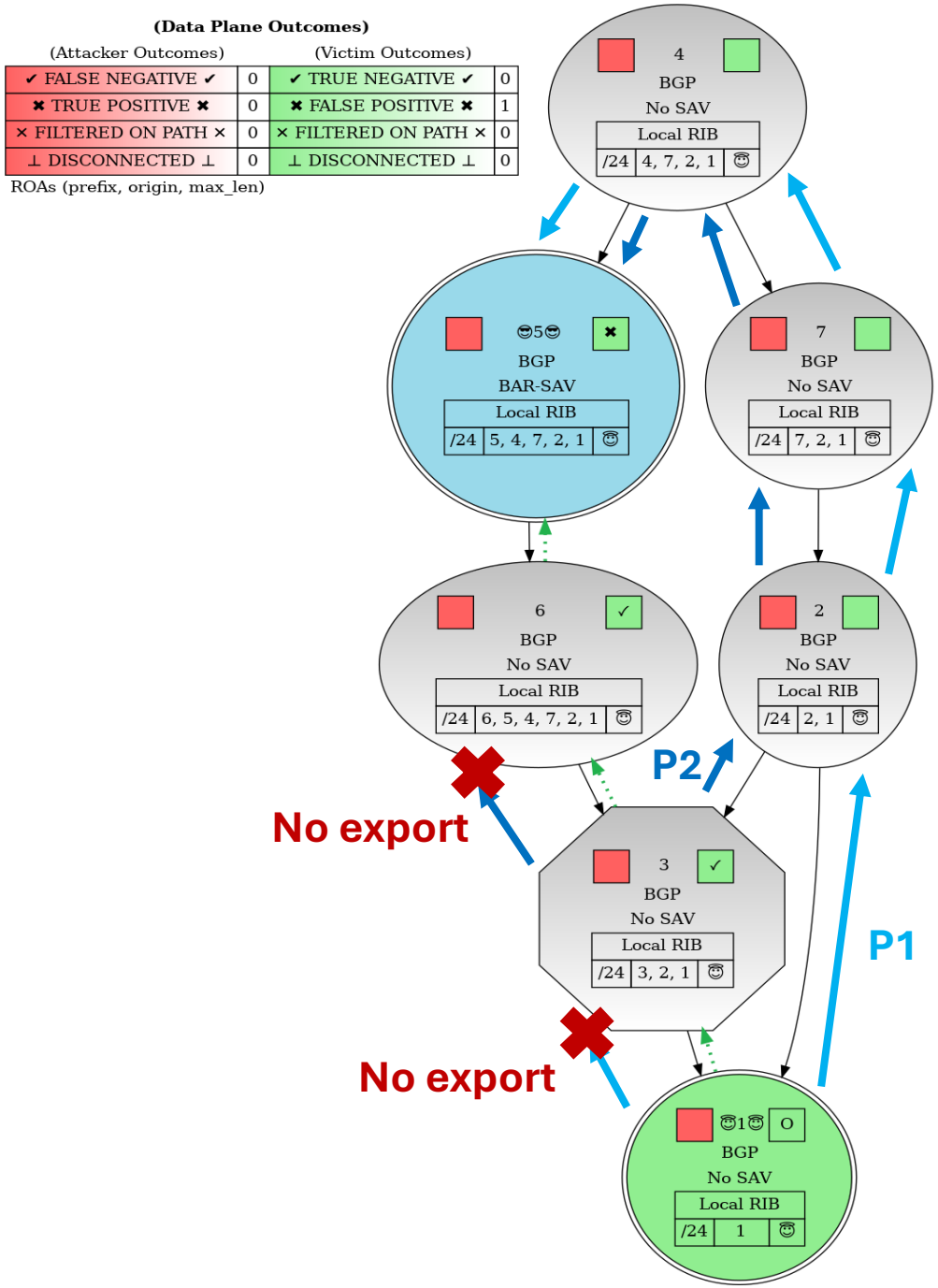






BAR SAV False Positive Example

- Origin AS (AS 1) adopts ASPA and performs no export to AS 3
- AS 3 announces, however, unlike in our simulations, performs traffic engineering (no export to AS 6)
- Origin's announcement is received through a provider interface (preserves connectivity), but data traffic flows through a customer interface



(config_006)
False Positive scenario for BAR-SAV w/ ASPA & providers announce, origin and transit AS export-to-some