Simulations of uRPF and BAR-SAV

Presented by Amir Herzberg

Joint work by: Nick Scaglione*, Justin Furuness*, Yossi Gilad**,
Hemi Leibowitz***, Cameron Morris*, Bing Wang*, Sriram Kotikalapudi**** and Amir Herzberg*

*: Univ. Of Connecticut, **: Hebrew University,
: College of Management, Rishon, Israel, *: NIST

Scope

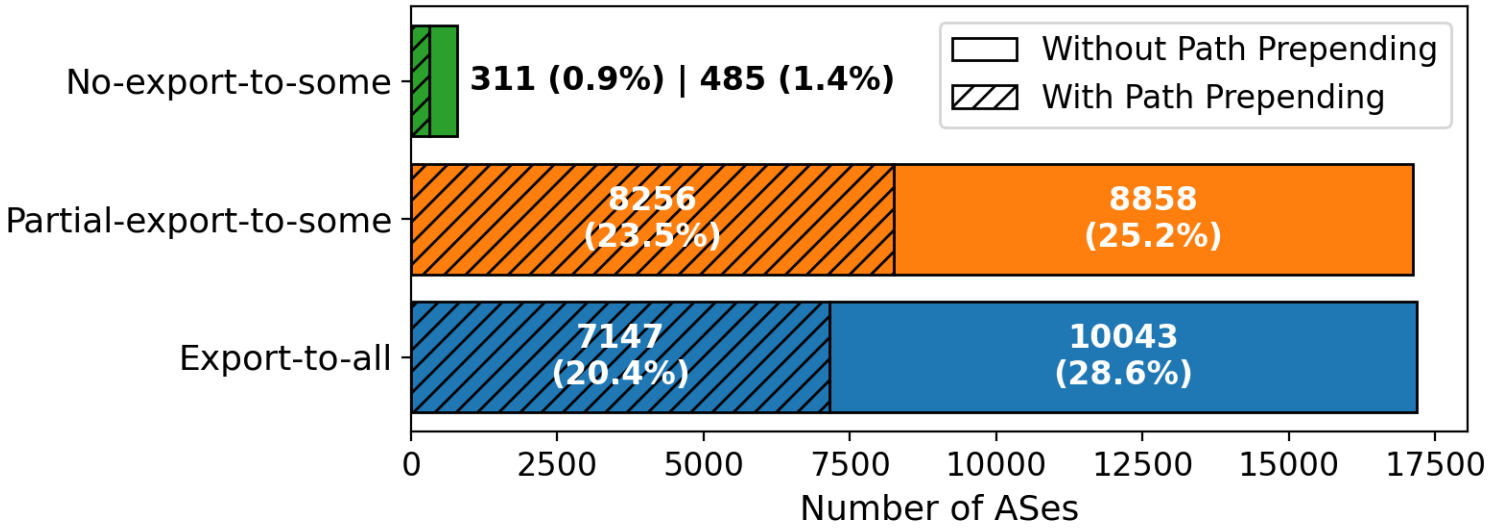
- **Simulation-based evaluation of SAV policies** over the Internet AS topology and relationships [as measured by CAIDA]
- Policies Evaluated
  - Strict uRPF
  - Feasible-Path uRPF (FP-uRPF)
  - Enhanced Feasible-Path uRPF (EFP-A and EFP-B)
  - BAR-SAV (with and without BAR-SAV-PI)
- Focus
  - Impact of (measured) traffic engineering methods [significant!!]
  - Performance under partial adoption
  - **False Positive** Rates vs **Detection Rates** (True Positive Rates)

Export Policies and TE Methods

- **Export-to-all** – export all prefixes to all eligible neighbors
  - Only model used by most published routing-security simulations
- **Partial-export-to-some** – export prefixes selectively to some providers
- **No-export-to-some** – do not export any prefix to some providers
- **AS path prepending** – prepend ASN multiple times to AS_PATH to deprefer route

Traffic-Engineering Measurement

- Use CAIDA's AS-level topology together with public routing data from RIPE and RouteViews BGPcollectors
- Measurement only of origin ASes, transit AS behaviors were not (yet) measured
- Under representative of no-export-to-some as most of these announcements would not propagate to the collectors



Simulation Architecture

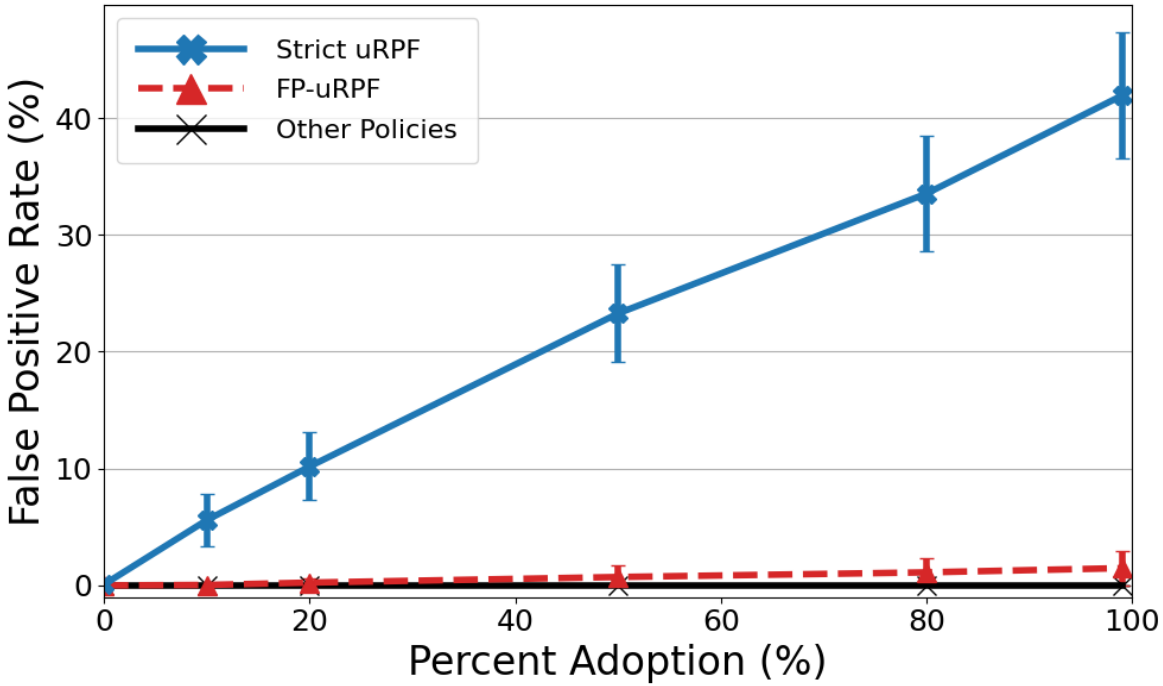
- BGPy Simulator Extension
  - Implemented SAV policies, data-plane traceback and performance metric tracking
  - Integrated TE measurement data into routing models
  - Open-sourced (anonymized repository until paper release)
- Modeled the Internet as a graph of ASes and inter-AS relationships based on CAIDA (2025)
  - CAIDA dataset may miss some links, leading to false in the case of disconnections
  - Only customer-provider and peer-peer relationships are modeled, sibling and other relationship types excluded due to insufficient data
  - IXPs are not explicitly represented in the topology

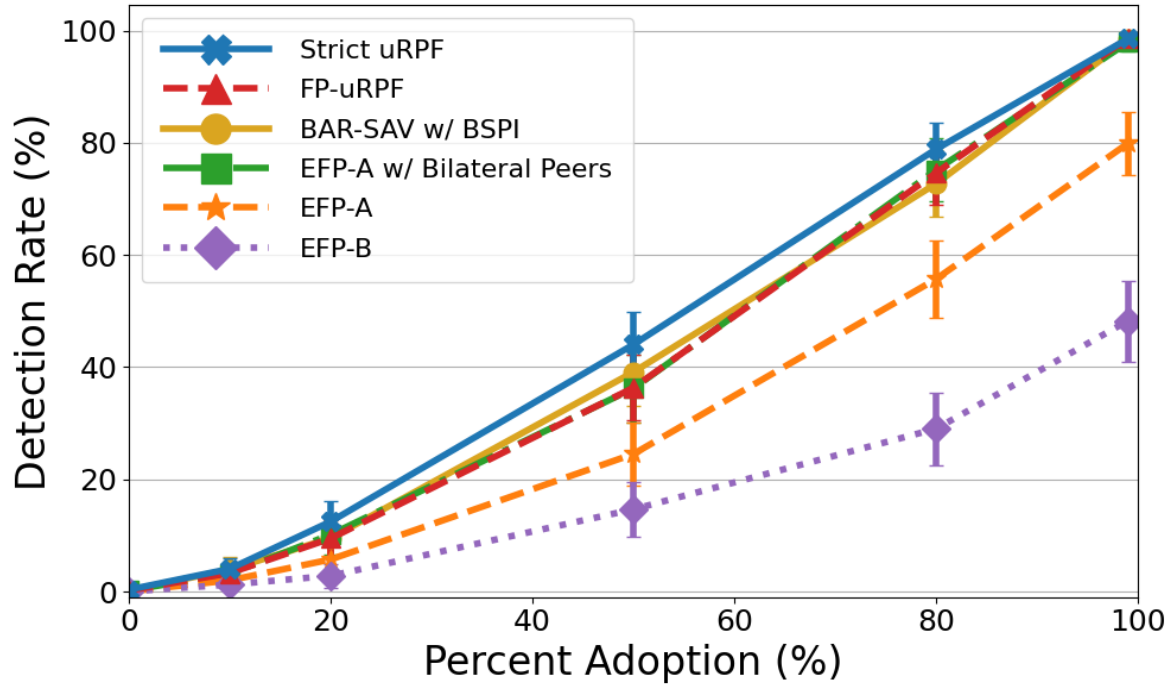
Simulation Setup

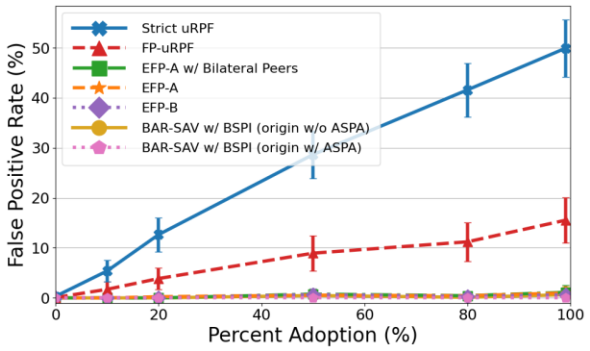
- Scenarios
  - Export-to-all
  - Traffic-Engineering (includes all measured TE behaviors)
  - Partial-export-to-some (comparable results to TE, see paper)
  - No-export-to-some
  - Direct Server Return (DSR)
- Varying percent adoption 0%-99%
- Spoofing Host (see paper) and Spoofing AS attacker models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

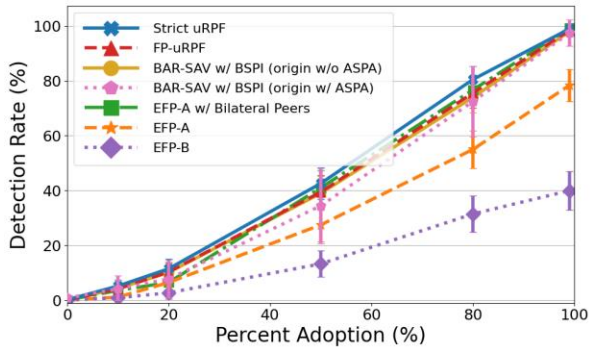
Export-to-all

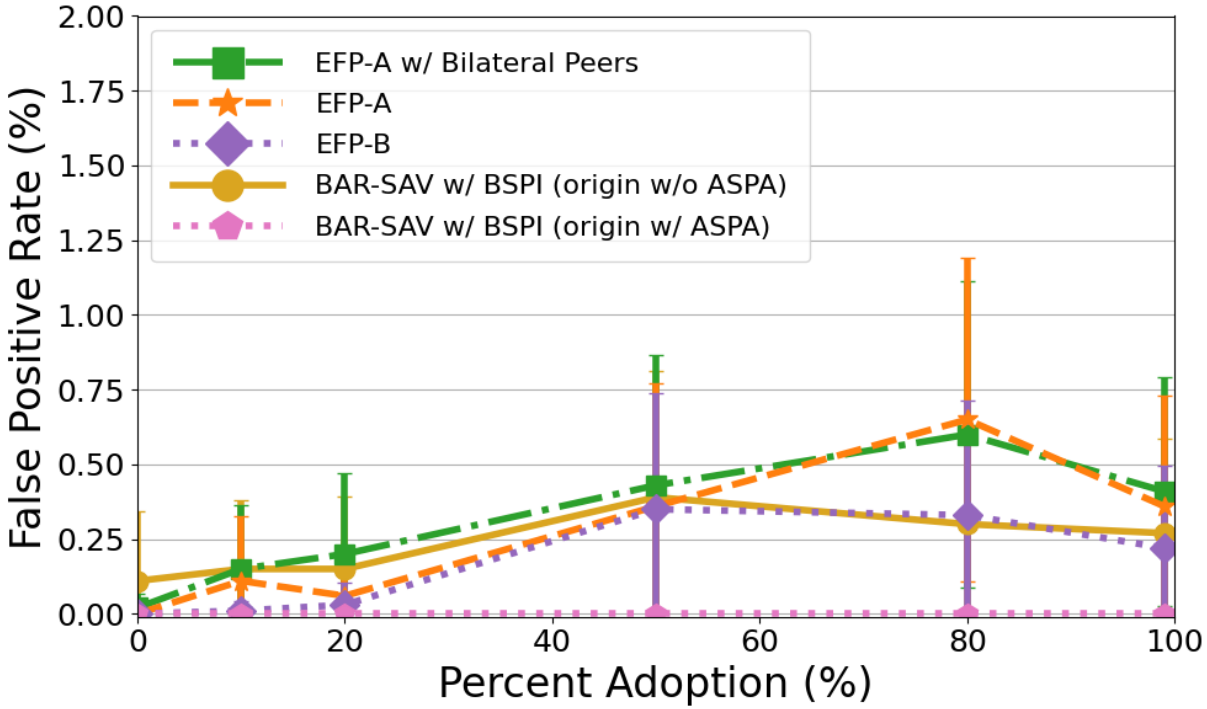
- Default assumption in (most?) prior works
- Idealized routing environment for SAV policies
- Strict and FP-uRPF are the only two policies with False Positives
- BAR-SAV & EFP-A scale best with adoption while having no false positives









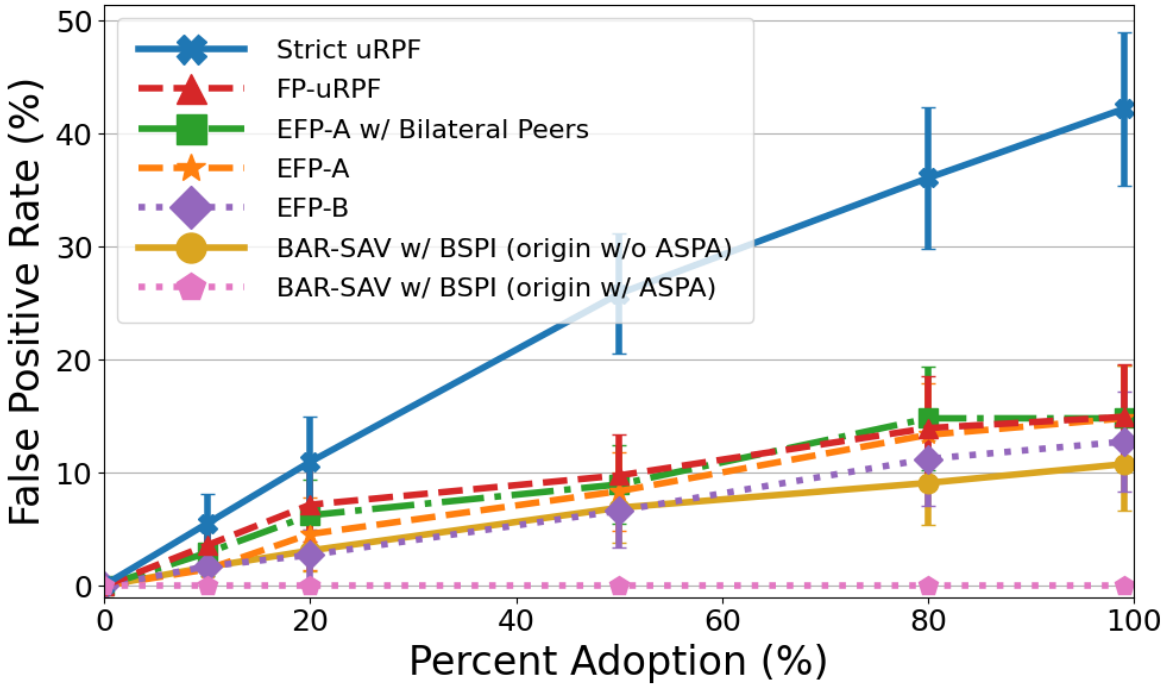


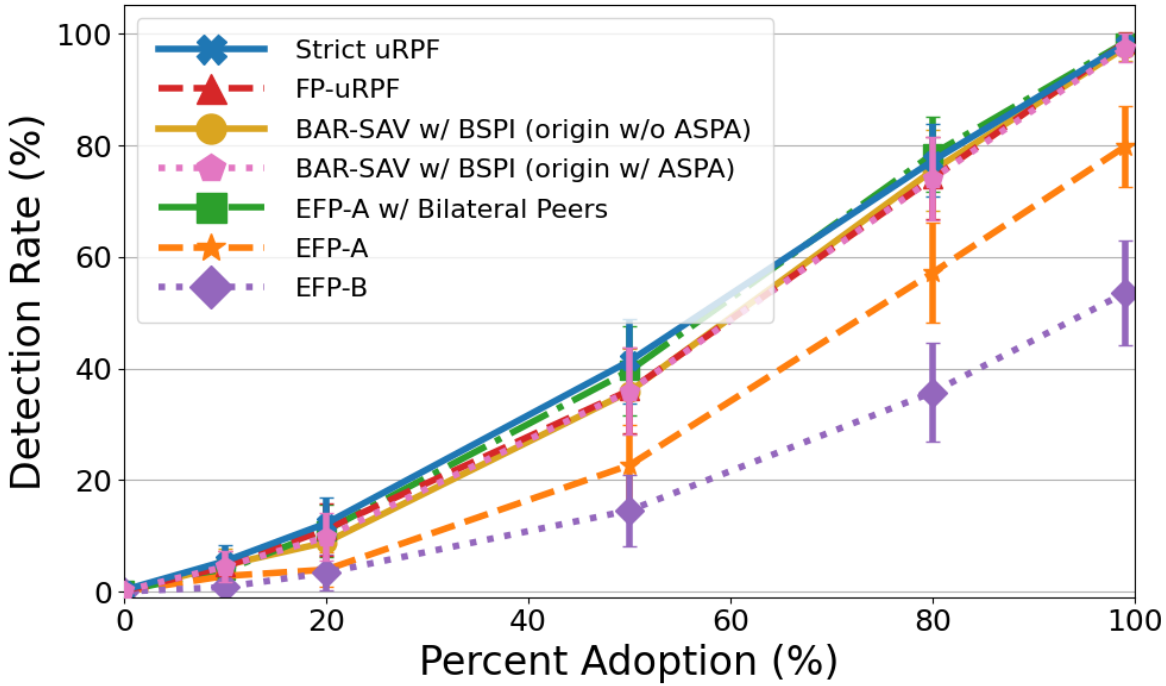
Traffic-Engineering

- Incorporates all measured TE behaviors
  - I.e., Export-to-all, Partial-export-to-some, No-export-to-some, 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** and detection rate almost as good as Strict uRPF

No-export-to-some

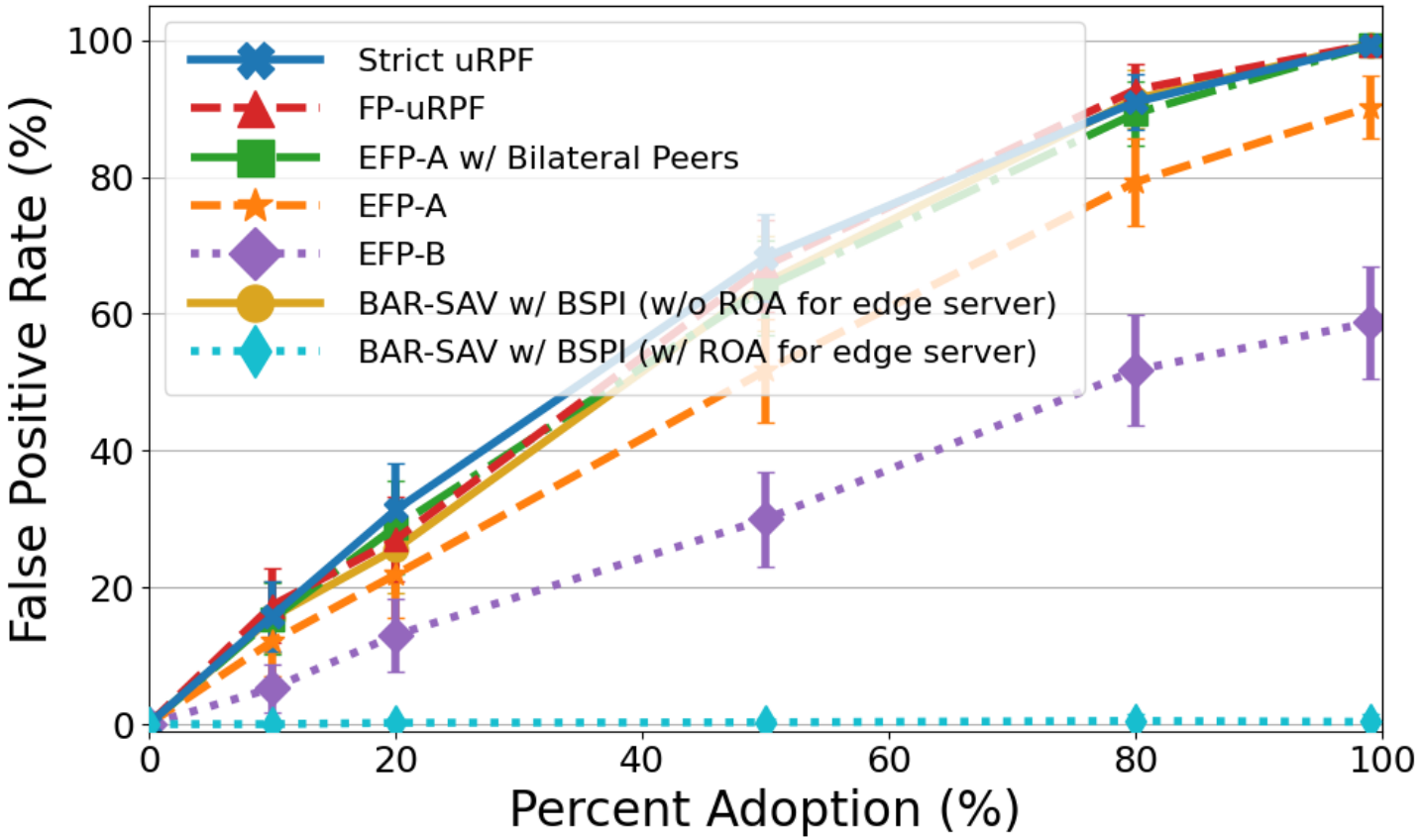
- No-export to at least one provider results in the lowest route visibility
  - Can't rely on measurements (would mostly be invisible), so: random provider
  - Other ASes export as measured (no TE for transit ASes)
- Without RPKI, there are significant false positives for all policies
- With ASPA, BAR-SAV 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: probably recommendations should consider TE in use

- BAR-SAV consistently results in the lowest/zero false positive rates and is also among the best in detection rates
  - Requires minimal assumptions to achieve this: ROA + ASPA at the origin (broader adoption is not necessary)

Thank you!

- If you would like a copy of our paper or a link to our SAV extension repo, please contact:
  - nicholas.scaglione@uconn.edu
  - amir.herzberg@uconn.edu
- Questions?