Minimal-Exposure AS-Path Verification against BGP Post-ROV Attacks

Zhongguancun Laboratory
Ziwei Li

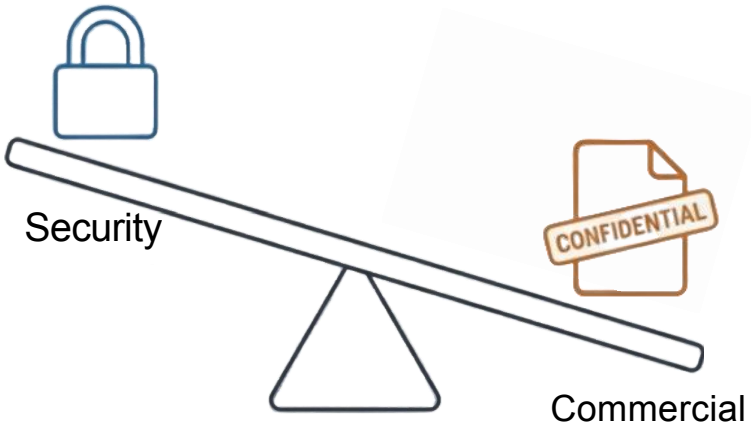
IETF 125 Hackathon, Shenzhen, China, 14-15 March 2026

The Adoption Dilemma: Path Security vs. Commercial Confidentiality

Problem:
Post-ROV attacks exploit unauthenticated AS-Paths

AS-Path Manipulation:
Forging paths to hijack traffic

Route Leaks:
Propagating routes in violation of policy



Existing Solutions & Trade-off:

BGPsec face high computational overhead
ASPA requires global publication of customer-provider relationships, exposing sensitive interconnection policies

Core Conflict: Mandatory transparency creates a major barrier to widespread adoption

Our Approach: MEASPV Decouples Validation from Disclosure

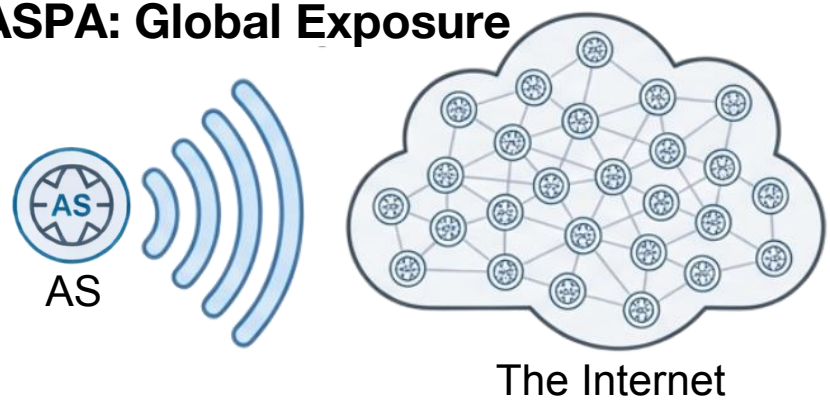
Core Principle:

Enable AS-Path verification, while limiting the visibility of relationship information only to relevant parties

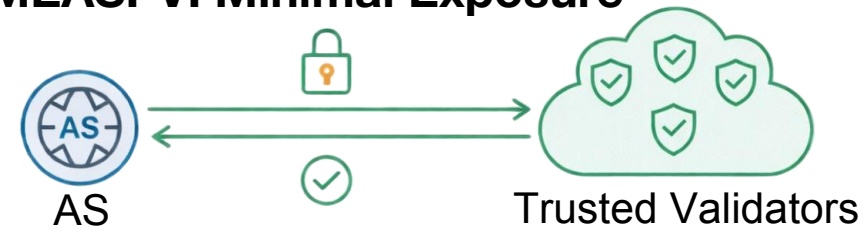
Design Goals:

- **Security:** Effective defense against path manipulation and route leaks.
- **Minimal Information Exposure:** Avoid global publication of AS topology.
- **Incremental Deployability:** Provide benefits even under partial adoption.
- **Low Overhead:** Negligible costs; no modifications to BGP-4 formats.

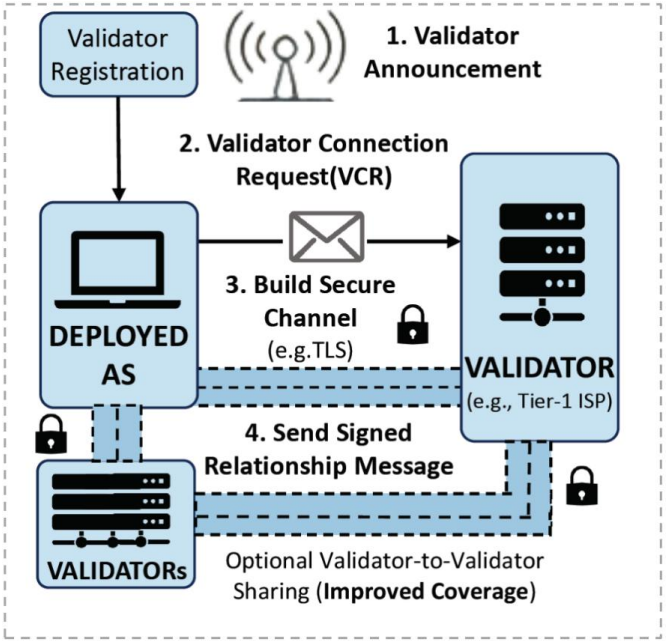
ASPA: Global Exposure

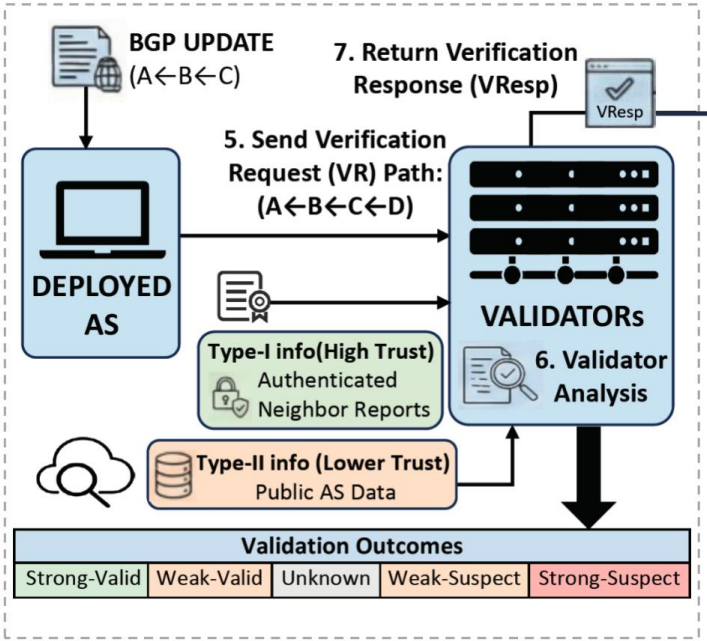


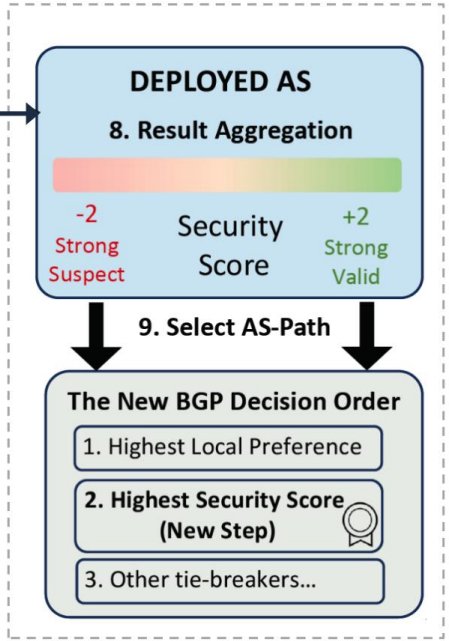
MEASPV: Minimal Exposure



MEASPV Employs a Validator-Assisted Architecture in Three Phases







Phase 1: Trust Establishment

High-tier ASes can register as validators, chosen validators and share encrypted, authenticated neighbor relationship data.

Phase 2: Path Verification :

An AS receives a BGP UPDATE, sends a verification request to its validators, and receives a verification response.

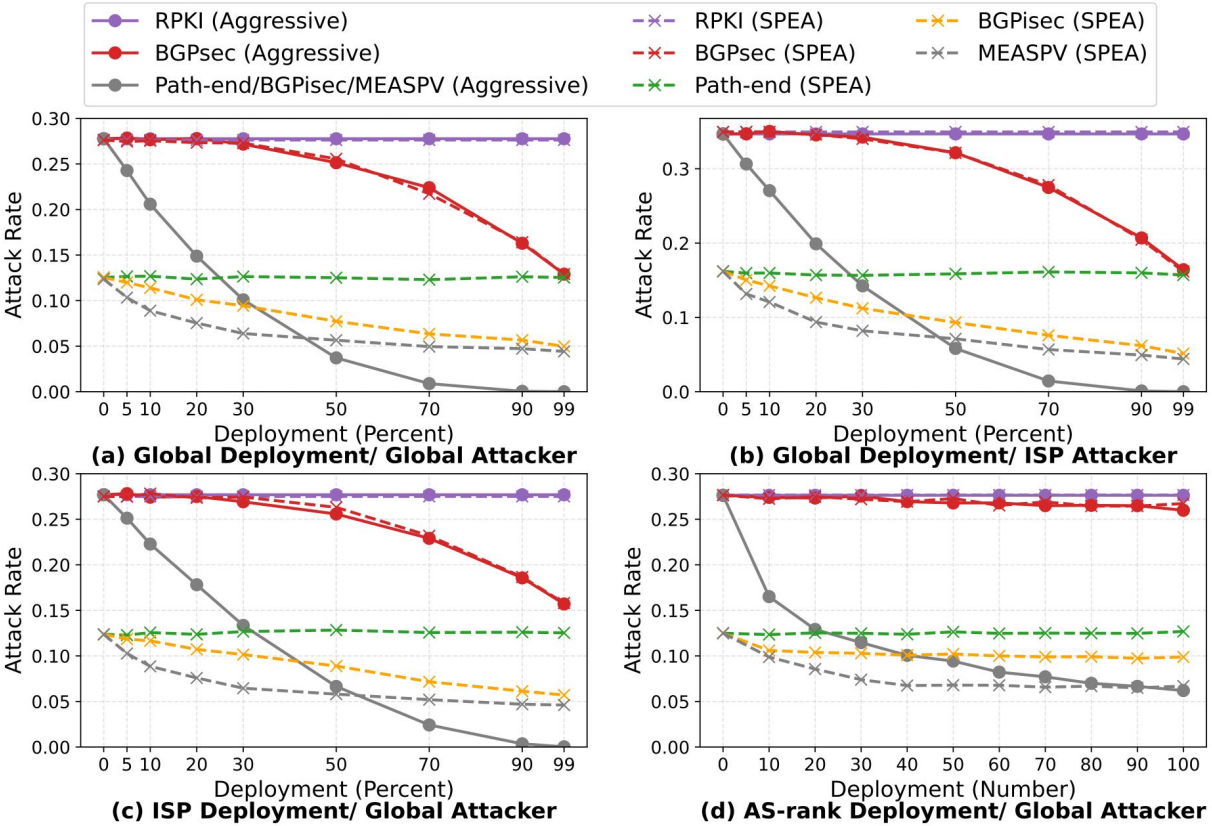
Phase 3: Secure Route Selection:

The AS aggregates responses into a security score.

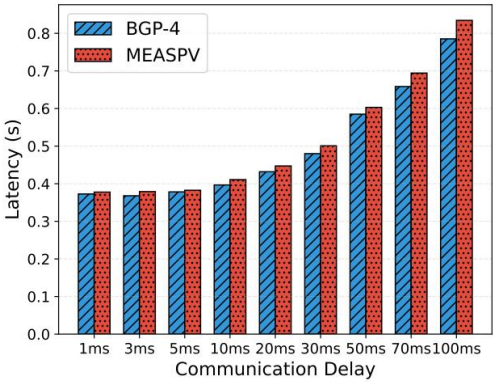
Evaluation: Path Manipulation

Metric: Attack Rate (% of legitimate ASes selecting a malicious path).

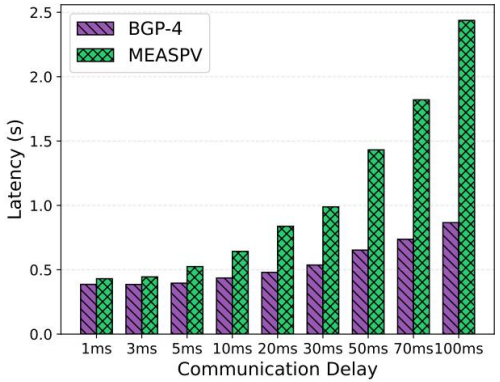
Key Result: MEASPV has achieved better defense effect in several deployment scenarios, especially in SPEA scenarios.



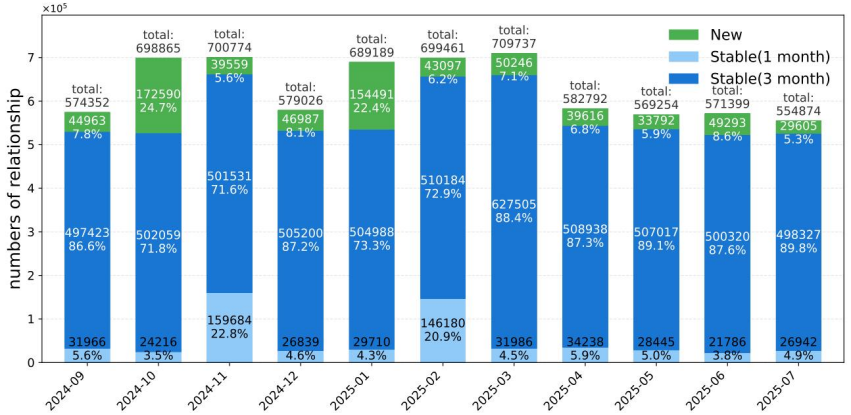
Performance: MEASPV Adds Negligible Latency Overhead



(a) BGP-4 vs MEASPV Stable Latency



(b) Cold Start Latency



- **Stable State(Cache-hit):** Convergence latency is nearly identical to native BGP-4.
- **Cold Start (Cache-miss):** A rare, one-time cost as AS topology changes infrequently.

- The Monthly change of AS relationship
- The vast majority of AS relationships remain stable over long periods, with only a small fraction of new relationships emerging each month.

MEASPV is operationally feasible and avoids the high performance costs that hindered BGPsec

Conclusion: Minimal-Exposure AS-Path Verification

The Problem Revisited

Global transparency is not a prerequisite for routing security. The need to protect commercial relationships is a fundamental adoption barrier.

MEASPV's Contribution

We resolve the tension between robust route verification and business confidentiality. By decoupling path validation from global disclosure, MEASPV provides security comparable to ASPA while minimal information exposure.

MEASPV offers a security, pragmatic, deployable, and less exposure path toward securing inter-domain routing

THANK YOU !