
Efficient and Secure Source Identifiers via Packet Passports

Xiaowei Yang (UC Irvine)

NeXworking'07

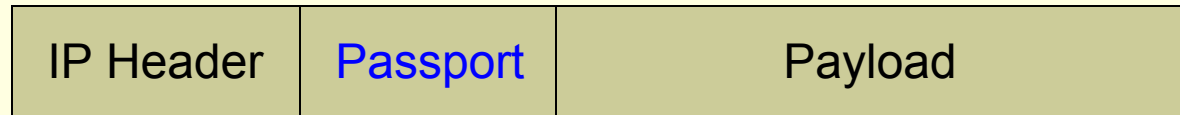
Xin Liu (UC Irvine), Jonathan Park (UC Irvine) and David
Wetherall (Intel and UW)

Source address spoofing complicates network security

- Reflector attacks
 - Recent DNS attacks in 2006, 63:1 amplification, 5+Gbps traffic
- Obstruct network intrusion detection and filtering
- Hijack two-way communications
 - DNS poisoning
 - TCP hijacking
- Complicate resource allocation
 - Active queue management
 - Fair queuing
- Little accountability

Our Proposal: Packet Passport System

IP Packet



- Goal of a passport: providing a cryptographic secure source identifier that routers can verify independently at packet forwarding time

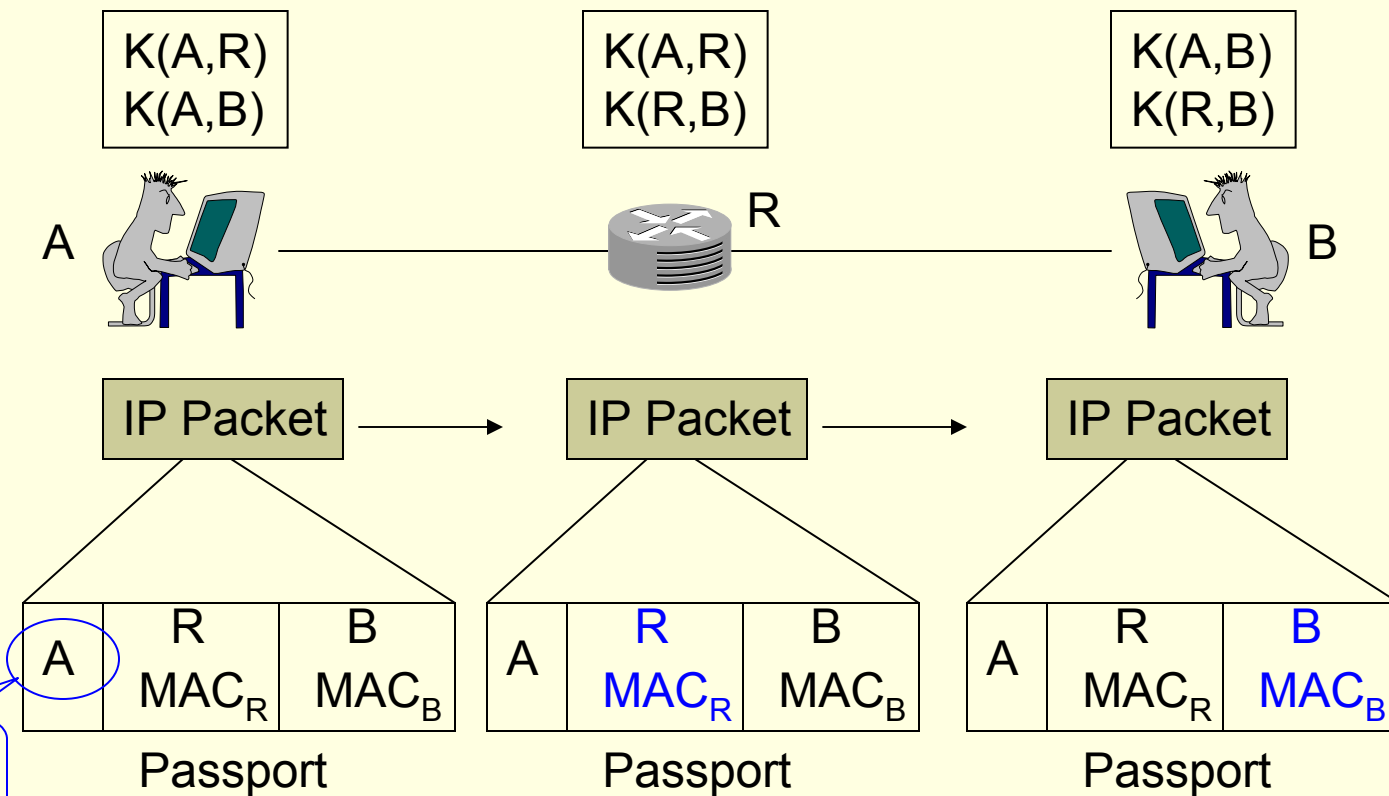
Challenges

- A passport must be:
 - Unspoofable
 - Efficient to generate and verify
 - Digital signature: computationally expensive
- The packet passport system must:
 - Bootstrap with minimum out-of-band communication
 - Be robust against attacks

Replacing digital signatures with MACs

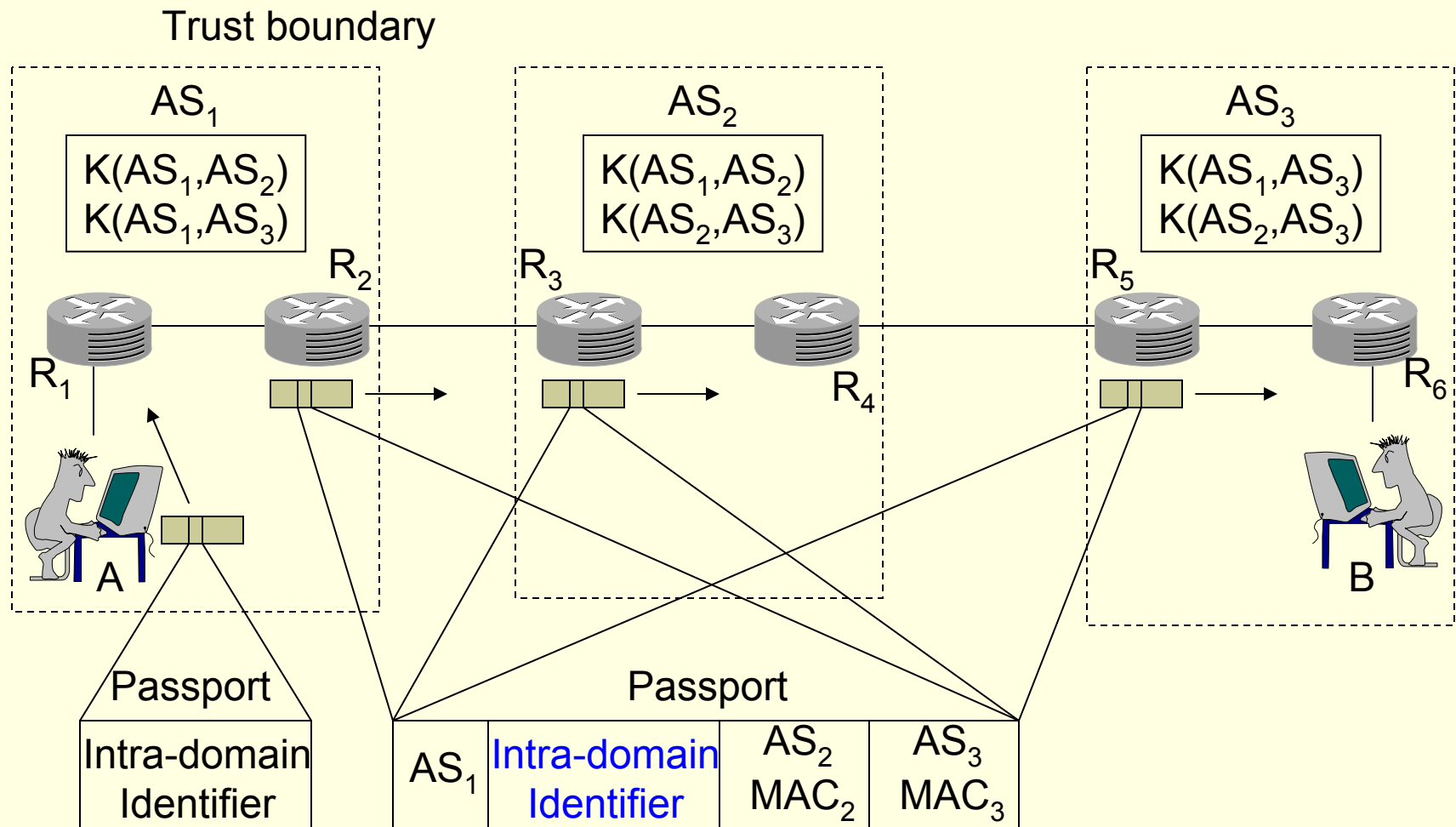
MAC: Message Authentication Code

$K(X,Y)$: Symmetric key shared between two nodes X and Y



$$MAC_R = MAC_{K(A,R)}(A, R, B, SrcIP, DstIP, \dots)$$

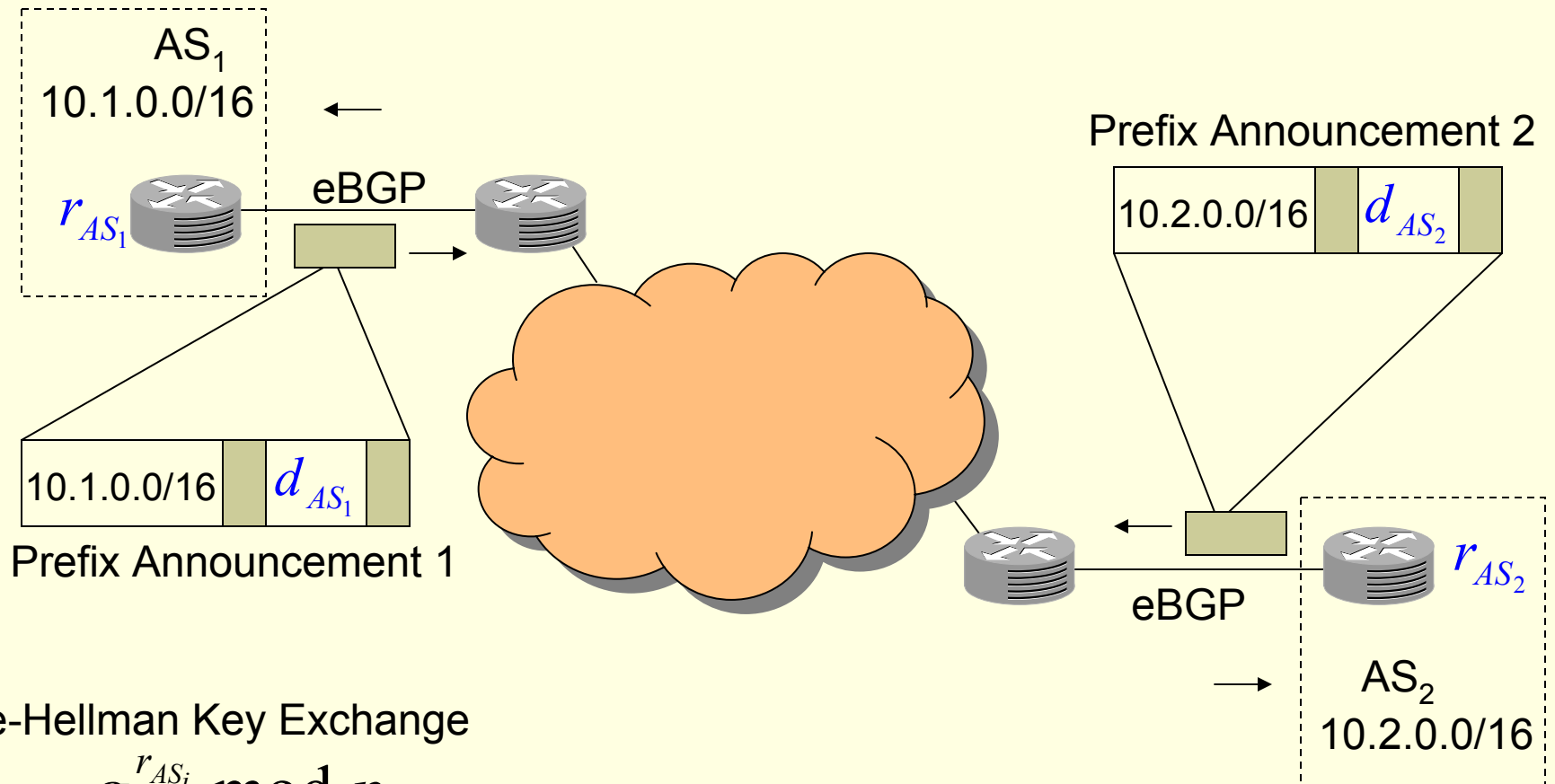
Two-Level Hierarchy for Scalability



Two-Level Identifiers

- Only the source domain can verify intra-domain identifiers
 - Filters may not be effective when source domain forges arbitrary intra-domain identifiers
 - Counter-measure: blocking the source domain
- Each domain can implement intra-domain identifier in its own way
 - Source IP address (if source spoofing is prevented inside a domain)
 - Message authentication code

Key Distribution via Routing (BGP)



Diffie-Hellman Key Exchange

$$d_{AS_i} = g^{r_{AS_i}} \text{ mod } p$$

$$K(AS_1, AS_2) = d_{AS_1}^{r_{AS_2}} \text{ mod } p = d_{AS_2}^{r_{AS_1}} \text{ mod } p$$

Benefits of Key Distribution via BGP

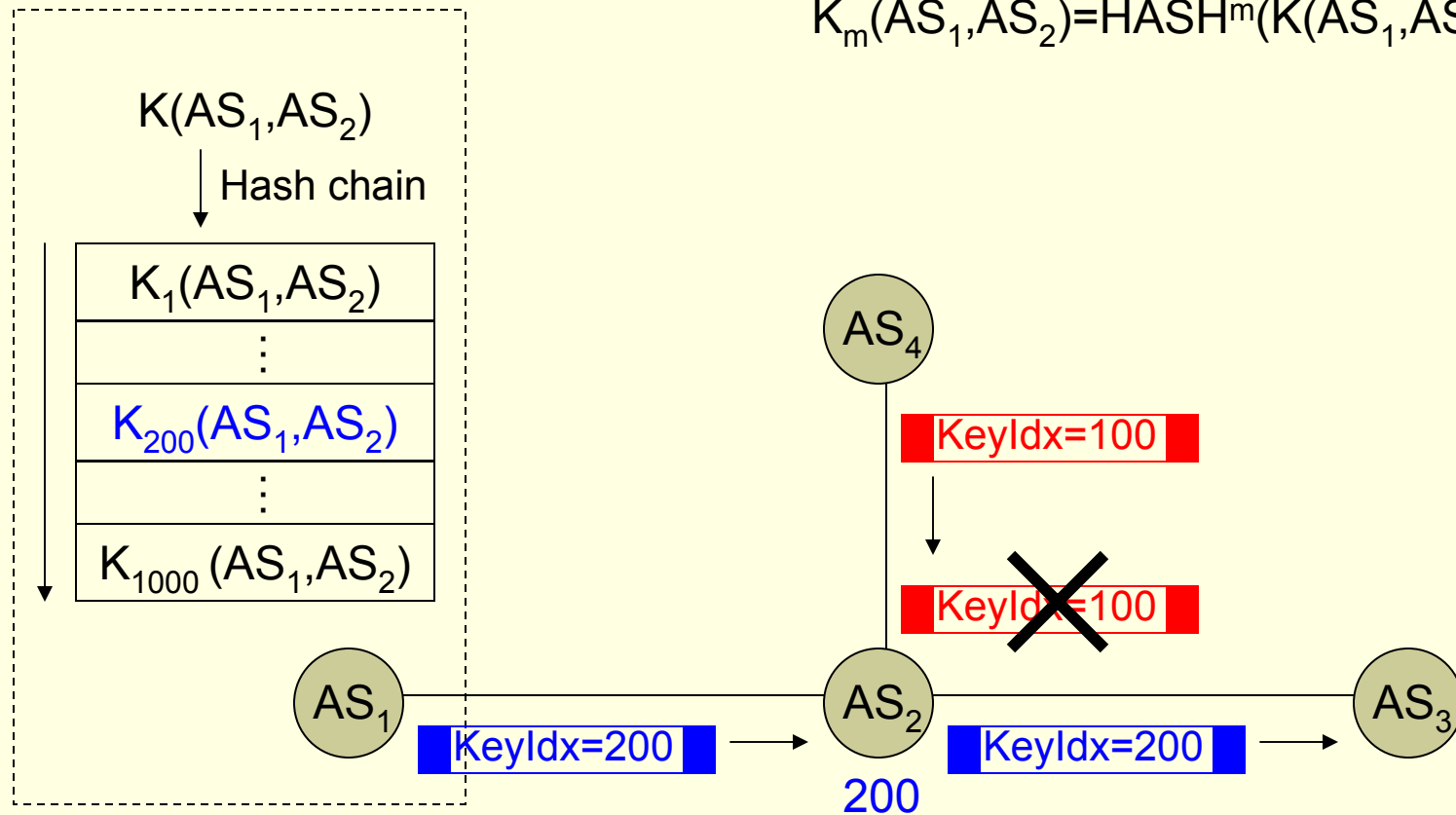
- Allowing key distribution to bootstrap
 - eBGP session between adjacent domains can be authenticated without passports [RFC3682]
- Robust against DoS flooding attack
 - BGP is a closed system: BGP traffic can get higher priority
- Supporting incremental deployment
 - d_{AS_i} can be carried in optional and transitive path attribute

Securing Key Distribution

- d_{AS_i} is signed with AS_i 's private key
- AS_i 's public key is distributed like d_{AS_i}
- AS_i 's public key is bound to AS_i using the same mechanism that binds a prefix to a domain
 - Reuse the PKI that secures routing: public key certification by CAs
 - Bind AS number to prefixes to prevent reflector attacks

Fast Re-keying to prevent replays

$$K_m(AS_1, AS_2) = \text{HASH}^m(K(AS_1, AS_2))$$



- Only on-path replays are possible

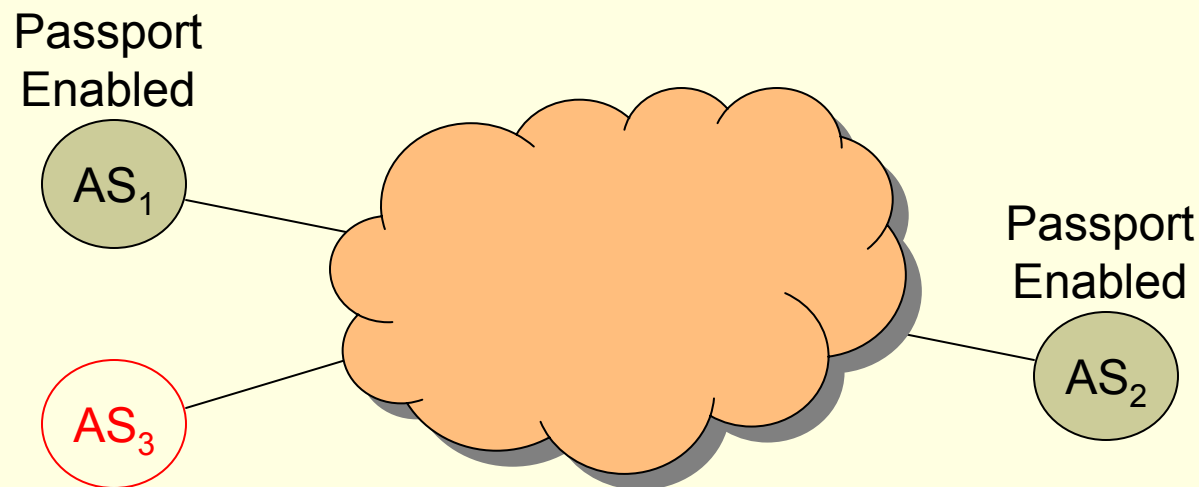
Applications

- Prevent reflector attacks
 - Routers verify source AS identifiers
 - Use BGP to bind source Id to source address
- DoS filtering
 - Cannot evade filers
- Resource allocation
 - Per-AS, or per host, no need for per-IP
- Verifiable paths
 - AS on the path insert MACs with keys shared with a destination after verification

Supporting Incremental Deployment

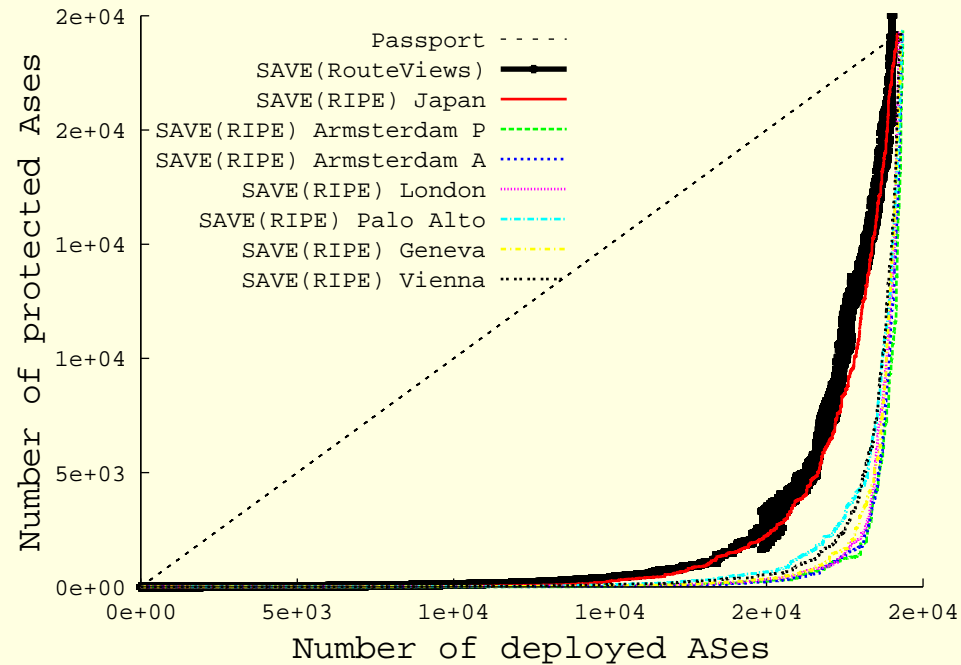
- Key distribution messages are wrapped in optional and transitive path attributes in prefix announcements
- Passport can be implemented as a shim layer
- AS path in a passport only includes those that have deployed packet passport system

Incentives for Early Adoption



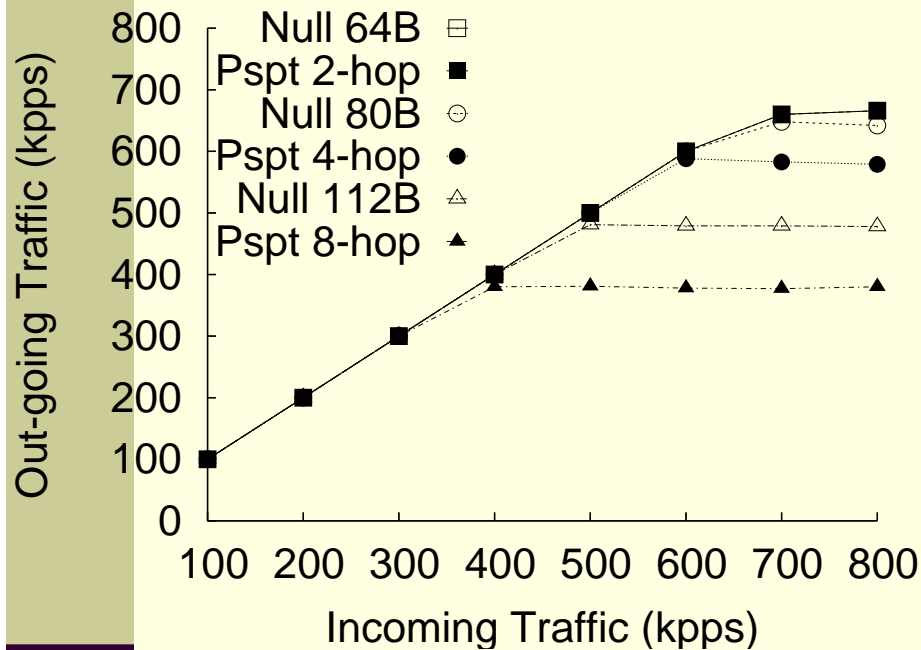
- No domains can spoof AS₁'s source identifier at AS₂
- AS₂ can filter DoS attack traffic from AS₁
- AS₁ can locate attack sources within itself

Comparison with ingress filtering

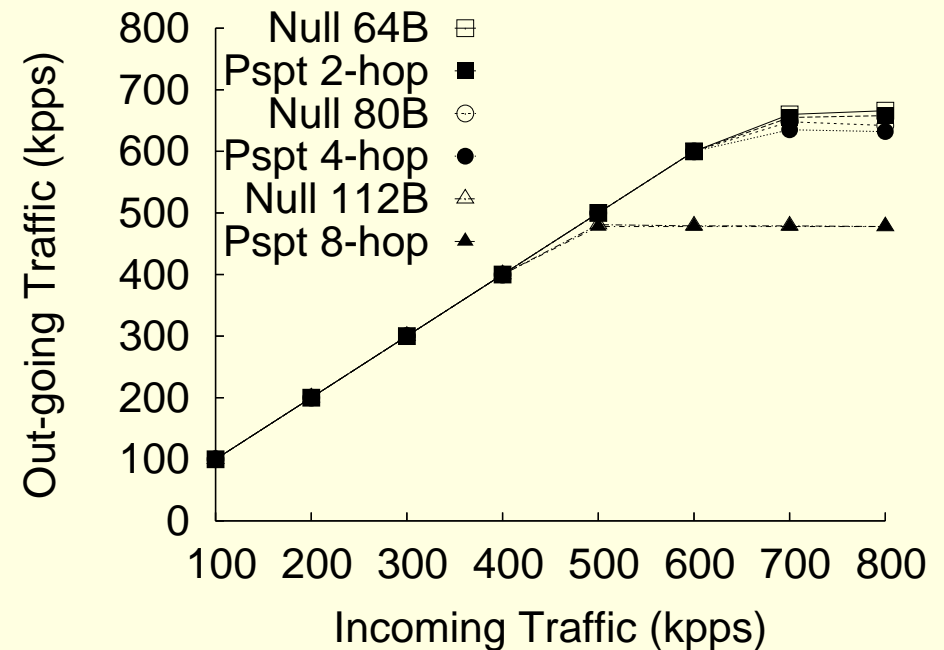


- Ingress filters installed using SAVE
- AS-level topology generated from BGP dumps

Performance



Generation



Verification

Summary

- A packet passport efficiently and securely authenticates the source of a packet.
- The system is incrementally deployable with incentives for early adoption.
- The system is practical with today's hardware technology.

Thank you!

- Questions?
- Xiaowei Yang (xwy@uci.edu)