Unspoofable Source Identifiers without Global Trust
Xin Liu, Xiaowei Yang, David Whetherall, and Thomas Anderson

Motivation

Benefits:
- Providing unspoofable packet signatures for filtering
- Providing unspoofable identifiers for fair resource allocation
- Limiting reflector attack
- Useful for deterring future attacks

Solution: Packet Passport

Every packet carries a passport, and packets with invalid passports are dropped or demoted.

Key Features
- An attacker cannot forge valid passports.
- It is efficient to generate and verify passports at packet forwarding time.
- The passport system is scalable and robust against DoS attacks.
- The passport system supports incremental deployment and provides incentives for early adoption.

Previous Solutions to Packet Source Identification

Fast but weak:
- Ingress/egress filtering: Source address is not verifiable.
- Path Identifier [Yaar03] & AITF [Argyraki05]: Part of a path identifier is spoofable.
- Authenticated Marking Scheme [Song01]: The path identifier is not verifiable at packet forwarding time.

Spoofing Prevention Method [Anat05]: The secrets are transmitted in plain text, and there is no secret exchange protocol.

Strong but inefficient and unscalable:
- R.Perlman’s PhD Thesis [Perlman88]: Public key signatures are in packets to identify their sources.

Passport Processing

MAC: Message Authentication Code
MAC = MAC_{AS_i,AS_j}((AS_i,AS_j,SrcIP,DstIP,⋯))
K(X,Y): Symmetric key shared between two domains X and Y

1. Intra-domain identifier is inserted.
2. Intra-domain identifier is verified & full passport is inserted.
3. MAC_2 is verified using the key K(AS_1,AS_2).
4. MAC_3 is verified using the key K(AS_1,AS_3).

Preventing Replay Attack

Problem: Attack sources cannot be identified.
Solution: Using bloom filters to detect passport duplication
Using fast-rekeying to deal with bloom filter flushing

Key Distribution

Diffie-Hellman Key Exchange
\[ d_x = g^{r_x} \mod p \]
\[ d_y = g^{r_y} \mod p \]
\[ K(X,Y) = d_x^y \mod p = d_y^x \mod p \]

Preliminary Evaluation

Practical with today’s hardware technology
- Passport generation & verification: with UMAC, a commodity PC can generate 975K passports and verify 3.9M passports per second.
- Key distribution: computation, communication and storage costs are negligible.
- Bloom filter: 16MB SRAM can “remember” 2.5Gbps traffic for 5 seconds with a false positive rate of $5.7 \times 10^{-6}$

For details, please visit: http://nds.ics.uci.edu/pktpassport