Source Address Validation Improvements BoF

70th IETF meeting, Vancouver

December 5, 2007

Today's Agenda

- Problems to solve, focus for SAVI 10 min

  Danny McPherson, Christian Vogt

- IPv4 Source Guard – An existing technique for IP source address validation on the 1st hop 10 min

  Fred Baker, draft-baker-sava-cisco-ip-source-guard-00

- A Source Guard for IP version 6 15 min

  Fred Baker, draft-baker-sava-implementation-00

- Discussion 25 min

Problems to solve, focus for SAVI

Danny McPherson

<u>Christian Vogt</u>

- **General problem**
- **Existing solutions**
- **Scope of SAVI**
- **Related work**

Source Address Validation – Why Do We Need It?

- Internet fails to prevent IP source address spoofing
  - Packet delivery based on IP destination address only
  - IP source address used by receiver, network entities
    - Sender identification
    - Destination for return traffic

- Resulting threats
  - Illegitimate authorization to service
  - Circumvent accounting
  - Identity/location spoofing
  - Redirect unwanted traffic to 3rd party

Existing Solutions

- Ingress filtering
- Unicast Reverse Path Forwarding + variants
- Cisco IPv4 Source Guard

- Not sufficient
  - Too coarse (IP address prefix validation at aggregated level)
  - Not standardized (as oftentimes demanded for procurement)
  - M.I.T. Spoofer project: IP source address spoofing possible in ¼ of observed addressing space

- Need additional protection – standardized

Possible Solution Scopes

- on local link
- within administrative domain
- across administrative domains

Possible Solution Scopes

- on local link
- within administrative domain

Focus on this

(low-hanging fruit)

- across administrative domains

Do more research

Envisioned benefits in focus area

- Detect misconfigurations locally
- Trace IP spoofing attacks
- Authorization/accounting
- Localization

Proposed SAVI solutions will…

- ensure that hosts attached to the same router cannot spoof each other's IP addresses
- track IP address configuration traffic
- work for IPv4 and IPv6
- apply to hosts only (not routers)
- <u>not</u> validate user identities

Selected Related Pre-BoF Work

- Pekka Savola: Experiences with Unicast RPF
  draft-savola-bcp84-urpf-experiences
  - Deployment of feasible-paths variant
  - Finnish University and Research Network
- Jianping Wu & al.: First-Hop Source Address Validation
  draft-wu-sava-solution-firsthop-eap
  - Secure IP address assignment upon access authentication
  - Integratable with EAP, Radius/Diameter
  - IP address enforcement on switch
  - Testbed implementation in CERNET
- Jun Bi & al.: Signature-based Source Address Validation
  draft-bi-sava-solution-ipv6-edge-network-signature
  - Session key exchange during access authentication
  - IP address bound to session key
  - Per-packet signatures in extension header