Charter and Goals of the SAVI Working Group

Christian Vogt, Bill Fenner
SAVI working group meeting @ IETF 72, Dublin
July 28, 2008
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 provides evidence
  - spoofing possible in ¼ of observed IP address space

- need additional protection – standardized
Possible Solution Scopes

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

envisioned benefits in focus area
- detect misconfigurations locally
- trace IP spoofing attacks
- IP-address-based authorization/accounting
- location identification
SAVI Goals and Requirements

- for Ethernet or Ethernet-based broadband
- observe/use existing protocols
- no host changes
- for IPv4 and IPv6
- for all address configuration methods
- preferably auto-configuring

Ensure that hosts attached to the same IP link cannot spoof each other's IP addresses without disrupting legitimate traffic.
Framework for SAVI Solutions

1. derive legitimate IP address from on-link traffic
2. bind legitimate IP address to lower-layer entity
3. enforce binding
Challenges

- multiple IP addresses per interface
- multiple link layer addresses per interface
- host mobility at link layer
- hosts with multiple interfaces on same link
- routers
- address translators
- anycast addressing

SAVI solution can be “default-on” only if it never disrupts legitimate traffic despite these challenges
Deliverables

Aug 08  first working group draft on threats document
Oct 08  first working group draft on IPv4 solution
Oct 08  first working group draft on IPv6 solution
Oct 08  submit document on threats to IESG for Informational RFC
Feb 09  first working group draft on solution for Ethernet-based broadband access network
Mar 09  submit IPv4 solution to IESG for Proposed Standard
May 09  submit IPv6 solution to IESG for Proposed Standard
Oct 09  submit Ethernet-based broadband access network solution to IESG for Proposed Standard