Charter and Goals of the SAVI Working Group

Christian Vogt, Bill Fenner

Opsec working group meeting @ IETF 72, Dublin

July 30, 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 — scope of SAVI
- 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

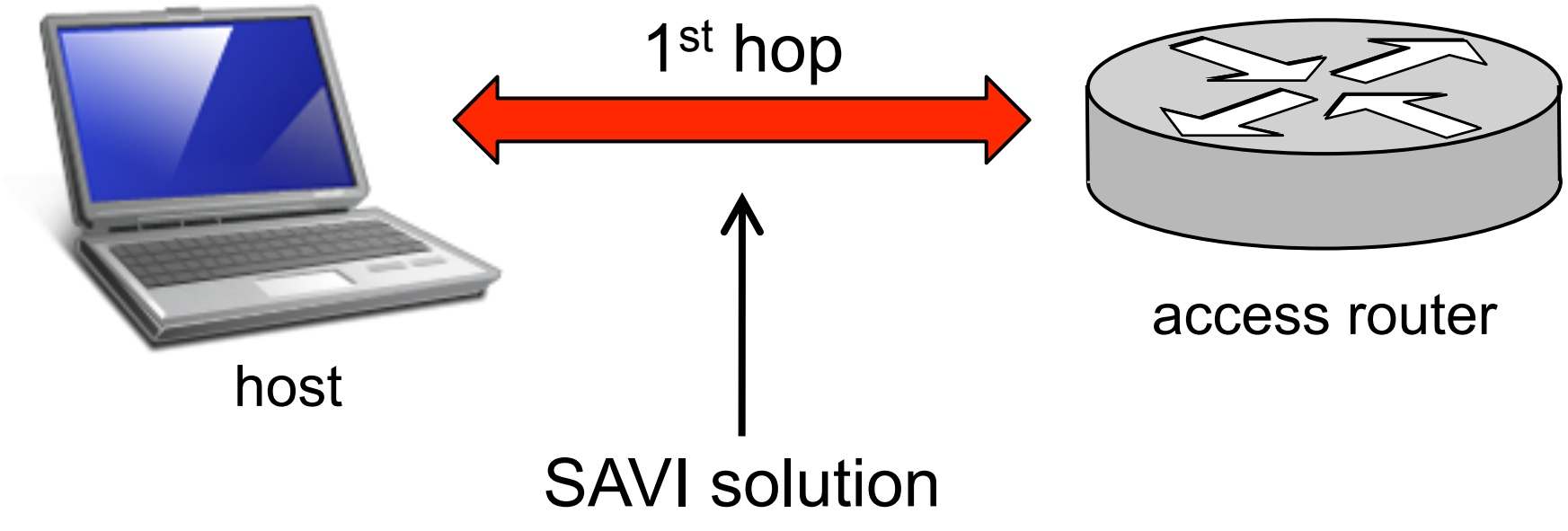
ensure that hosts attached to the same IP link cannot spoof each other's IP addresses without disrupting legitimate traffic

- 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

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**

Framework for SAVI Solutions



IP address → lower-layer entity **binding**

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

Functional Components

binding

association between IP source address and lower-layer entity

binding anchor

lower-layer entity in a binding

binding verification

method for verifying a binding

binding cache

memory that stores verified bindings to avoid repeated binding verification

binding conflict

when a packet's IP source address is in binding cache, but with different binding anchor

binding conflict resolution

method for handling a binding conflict

Degrees of Freedom

which binding anchor?

- switch port
- link layer address

which binding verification?

- check sending host (direct)
- ask other hosts (indirect)

which binding conflict resolution?

- drop packets that cause a binding conflict
- re-verify on binding conflict

Analysis

binding verification	binding conflict resolution	multiple IP addresses: address translator	multiple link layer addresses	mobility at link layer	multiple interfaces on same link: anycast addressing	routers
check sending host (direct)	drop packet	yes	yes (switch port) no (L2 address)	no (switch port) yes (L2 address)	no	no
	re-verify binding	yes	yes	yes	yes	no
ask other hosts (indirect)	drop packet	yes	yes (switch port) no (L2 address)	no (switch port) yes (L2 address)	no	yes
	re-verify binding	yes	yes (switch port) no (L2 address)	yes	no	yes

binding anchor

Next Steps

follow up on mailing list…

- Which challenges must/can be addressed?
- Where in the taxonomy should SAVI aim?