A SAVI Solution: 
Control Packet Snooping

SAVI-CPS-01 
Jun Bi, Jianping Wu, Guang Yao, Fred Baker 
IETF75, Stockholm 
July 30, 2009
Outline

• SAVI-CPS overview
details at draft-savi-bi-cps-01
• CNGI-CERNE2 deployment report
Introduction to SAVI-CPS
SAVI-CPS

• CPS (Control Plan/Packet Snooping):
  – Set up IP/port binding (permit entry) at SAVI-switch port based on control packet snooping, to make the host attached to that port can’t spoof its source address
  – Default Dropping at the port that directly attached with the host (When src addr of incoming packet matches a permit entry then forwarding, otherwise dropping)

• Snoop
  – DHCPv6, DHCPv4
  – NDP, ARP
SAVI-CPS

- Work for both IPv6 and IPv4
  - IPv6: DHCPv6, SLAAC
  - IPv4: DHCPv4, Manually configured address

- Benefits
  - Support address assignment standards
  - No new protocol design, such as BDP
  - Initial binding based on only control packets, not data packets (important advice from vendors)
  - No client software
  - Could precisely traceback the source of host bill by source address within SAVI-area
SAVI-CPS

• Port Attributes in SAVI-Switch
  – SAVI-Host: validate src addr based on binding table
  – SAVI-Trunk-Default: verify if src addr conflicts with local binding then forward (SAVI-Legacy switch trunk)
  – SAVI-Trunk-Snooping (an option for SAVI-SAVI trunk)
  – SAVI-DHCP-Trust: validate msg from DHCP server
  – SAVI-RA-Trust: validate RA from router

• Handle cases in DHCPv6 and SLAAC (demo)
  – Multiple addresses at host
  – DHCP-only and DHCP-SLAAC mixed network
  – Host changes port
  – Host changes switch
  – SAVI-Switch changes topology
  – SAVI-switch reboots ….
SAVI-CPS State Transition Diagram
DHCPv4/v6 snooping
ND snooping

Receive unsolicited NA/NS
Source Addr in SLAAC scope?
Yes
Add an entry into BST
Send DAD probe

Receive DAD NS
Target Addr in SLAAC scope?
Yes
Add an entry into BST
Receive a NA for the Addr after timeout
Yes
End process
No
Add entry into FT
IPv4 binding

Flowchart:

1. Receive ARP Req
2. Source Addr in IPv4 scope?
   - No: End process
   - Yes: Add an entry into BST
3. Send ARP probe
4. Receive a ARP for the Addr after timeout?
   - Yes: End process
   - No: Add entry into FT
5. Receive Gratuitous ARP
6. Target Addr in IPv4 scope?
   - No: End process
   - Yes: Add an entry into BST
CNGI-CERNE2 deployment
Goals

• CNGI-CERNET2
  – CERNET: was the 2\textsuperscript{nd} Large ISP, 2000+ university campus networks, 20M+ users
  – CERNET2 is the largest IPv6 network launched in 2004

• CNGI-CERNET2 SAVI Deployment
  – 100 universities campus networks nationwide
  – 1 Million users

• Time frame: 2008-2010
Goals

• Strictly Anti-spoofing at host granularity
  – Accurately traceback a host at the switch port. When attack traffic or unwanted traffic happens in SAVI deployed area, we could traceback the precise host by source address of unwanted traffic, then take actions.
  – Accurately bill the traffic usage to the precise host in SAVI deployed area. It’s important for a operator to bill by usage not by fixed monthly rate.
  – To get precise measurement data
  – All above drive the requirement to SAVI: prevent a host in SAVI deployed area from spoofing used nor unused addresses
SAVI switches installation: 100 Univ. campus net (red dot)
Example: Tsinghua Univ. campus network is being deployed (the number of switches, hosts are real)

<table>
<thead>
<tr>
<th></th>
<th>subnets</th>
<th>switches</th>
<th>port</th>
<th>hosts</th>
<th>users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main</td>
<td>114</td>
<td>1018</td>
<td>23414</td>
<td>22644</td>
<td>20280</td>
</tr>
</tbody>
</table>

**Campus Backbone**

(IPv4/IPv6)

**SAVI-access switch**

20K users (students)
Thank You!
Q & A