Source Address Validation Improvements – SAVI –

Monday, November 17, 2008. 9:00 – 11:30 am
Salon AB
Agenda

- Summary of design decisions so far
  Christian Vogt
  9:10 am

- First-come-first-serve SAVI for IPv4 + IPv6
  Marcelo Bagnulo
  9:30 am

- SAVI for IPv6 Secure Neighbor Discovery
  Marcelo Bagnulo
  10:00 am

- Thoughts about SAVI in Ethernet-based broadband
  David Miles and Wojciech Dec
  10:30 am

- SAVI scenarios and solution space
  Jun Bi
  11:00 am

end at 11:30 am
Recent Design Decisions of the SAVI working group

draft-vogt-savi-rationale

Christian Vogt

SAVI working group meeting at IETF 73. November 2008
Framework for SAVI Solutions

ensure that hosts don’t spoof each other’s IP addresses
1. derive legitimate IP address from on-link traffic
2. bind legitimate IP address to lower-layer binding anchor
3. enforce binding
Initial Design Questions

tradeoff between strength of security vs. ease of deployment
- conclusions encourage wide deployment

1. which IP address ownership proof?
   - conclusion: weak proof OK; stronger proof where possible

2. which binding anchor?
   - conclusion: support all, provide recommendations/defaults

3. complement or substitute ingress filtering?
   - conclusion: complement
     ingress filtering costs little extra, but simplifies SAVI solution
Initial Design Questions

tradeoff between strength of security vs. ease of deployment
  ▪ conclusions encourage wide deployment

1. which IP address ownership proof?
  ▪ **conclusion**: weak proof OK; stronger proof where possible

2. which binding anchor?
  ▪ **conclusion**: support all, provide recommendations/defaults

3. complement or substitute ingress filtering?
  ▪ **conclusion**: complement
  ingress filtering costs little extra, but simplifies SAVI solution

4. how to distinguish 1-hop vs. forwarded packets?
Distinguishing 1\textsuperscript{st}-Hop/Forwarded Packets

two techniques

<table>
<thead>
<tr>
<th>configuration options</th>
<th>potential errors</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>false negatives</td>
</tr>
<tr>
<td>true</td>
<td>false drops</td>
</tr>
</tbody>
</table>

| learn routers          | Secure ND manual | possible | never |
| learn on-link prefixes | DHCP, ND manual  | never    | possible |
Distinguishing Two Forwarded Packets

Two techniques for learning routers and prefixes with on-link prefixes:

- DHCP, ND
- Manual

False positives never possible

Disguising two techniques with on-link prefixes:

- Wrong source IP address with on-link prefix
- False drops

Possible source and destination

ERICKSON
Distinguishing 1\textsuperscript{st}-Hop/Forwarded Packets

two techniques

<table>
<thead>
<tr>
<th>auto-configurability</th>
<th>potential errors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>false negatives</td>
</tr>
<tr>
<td></td>
<td>false drops</td>
</tr>
</tbody>
</table>

| learn routers       | Secure ND manual  | possible | never |
|                     |                   |          |       |
| learn on-link prefixes | DHCP, ND manual | never    | possible |

possible conclusion: use at least one, both if possible
Working Group Deliverables

- problem statement
draft-mcpherson-savi-threat-scope

- design rationale (new)
draft-vogt-savi-rationale

- IPv4 solution
draft-bagnulo-savi-fcfs

- IPv6 solution
draft-bagnulo-savi-fcfs

- IPv6 solution extension for SeND (new)
draft-bagnulo-savi-send

- solution for Ethernet-based broadband