A SAVI Solution for WLAN

draft-bi-intarea-wlan-02

Mingwei Xu, Jianping Wu, Tao Lin, Lin He, You Wang

intarea, ietf119

March 2024
Outline

• Background
• SAVI-WLAN Solution
• Next Steps
Background
Source address spoofing

Src: A  
Dst: C

A  B

C
Source address spoofing
Source address validation

• Source Address Validation Improvements (savi)

• July 2008 – October 2018

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

1. derive legitimate IP address from on-link traffic
2. bind legitimate IP address to link-layer property
3. enforce bindings on SAVI devices
Binding anchors & existing solutions

• Various binding anchors:
  • The IEEE extended unique identifier, EUI-48 or EUI-64, of a host's interface.
  • The port on an Ethernet switch to which a host attaches.
  • The combination of a host interface's link-layer address and a customer relationship in cable modem networks.
  • …

• Existing Solutions

<table>
<thead>
<tr>
<th>RFCs</th>
<th>Title</th>
<th>Scenarios</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFC6620</td>
<td>FCFS SAVI: First-Come, First-Served Source Address Validation Improvement for Locally Assigned IPv6 Addresses</td>
<td>SLAAC and Static</td>
</tr>
<tr>
<td>RFC7219</td>
<td>SEcure Neighbor Discovery (SEND) Source Address Validation Improvement (SAVI)</td>
<td>SEND</td>
</tr>
<tr>
<td>RFC7513</td>
<td>Source Address Validation Improvement (SAVI) Solution for DHCP</td>
<td>DHCP</td>
</tr>
<tr>
<td>RFC8074</td>
<td>Source Address Validation Improvement (SAVI) for Mixed Address Assignment Methods Scenario</td>
<td>Mixed</td>
</tr>
</tbody>
</table>
How about in wireless LANs?

- Lack of naturally available binding anchors in wireless LANs

Wired LAN

![Wired LAN Diagram]

Wireless LAN

![Wireless LAN Diagram]

- User mobility in wireless LANs

<table>
<thead>
<tr>
<th>AP1’s Binding table</th>
<th>Access Point 1</th>
<th>Access Point 2</th>
<th>AP2’s Binding table</th>
</tr>
</thead>
<tbody>
<tr>
<td>Binding anchor</td>
<td>A</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

AP2 cannot enforce binding without A’s entry!
SAVI-WLAN Solution
SAVI-WLAN overview

User → AP → AC → Gateway → DHCP Server

Address assignment snooping (DHCP, SLAAC)

Binding entry creation

MAC-IP Synchronization

Binding entry confirmation
Binding anchor

• Binding anchor: MAC address
  • secured by 802.11i or other mechanisms

• If the MAC address is unprotected, an attacker can spoof the MAC address to pass validation successfully.
Two data structures

- **IP-MAC Mapping Table**
  - maps an IP address to a MAC address
  - used in the control process

- **MAC-IP Mapping Table**
  - maps a MAC address an IP address
  - used for filtering

- The MAC-IP mapping table and the IP-MAC mapping table can be maintained separately on different devices.

- A synchronization mechanism must be used between these two tables to ensure the consistency of the bindings.
Binding creation

• Static:
  • All the static IP-MAC address pairs are configured into the IP-MAC mapping table with the mechanism enabled.

• DHCP [RFC7513]:
  • snoops on the DHCP address assignment process between the attached host and the DHCP server.

• SLAAC [RFC6620]:
  • snoops Duplicate Address Detection procedure or Address Resolution procedure between attached hosts and neighbors.
Binding clearing

1. A host leaves explicitly this access point.
   • All entries in the MAC-IP mapping table associated with this MAC address MUST be cleared.

2. A DHCP RELEASE message is received from the owner of the corresponding IP address.
   • This IP entry in the IP-MAC mapping table and the corresponding entries in the MAC-IP mapping table MUST be cleared.

3. A timeout message of the AC's client idle-time is received.
   • All entries in the MAC-IP mapping table related to the MAC address MUST be cleared.
Source address validation

Source <MAC, IP> extraction

<MAC, IP> in MAC-IP table?

IP in IP-MAC table?

<IP, MAC> in IP-MAC table?

Forward

Drop
The CAPWAP extension is used to synchronize binding entries between APs and ACs, while the method of synchronization between ACs can be determined independently.
Deployment scenarios

• Scenario 1: Centralized WLAN (FIT AP + AC)

• Scenario 2: Autonomous WLAN (FAT AP)
Scenario 1: Centralized WLAN

- Case 1: AP filtering
  - AC maintains IP-MAC Mapping Table
  - AP maintains MAC-IP Mapping Table and perform address snooping
Scenario 1: Centralized WLAN

• Case 2: AC filtering
  • AC maintains both MAC-IP and IP-MAC Mapping Table and performs both address snooping and packet filtering
  • All the packets must be forwarded to AC firstly

![Diagram showing the flow of packets and mappings]

**IP-MAC Mapping Table**

<table>
<thead>
<tr>
<th>IP</th>
<th>MAC</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP1</td>
<td>MAC1</td>
<td>DHCP</td>
</tr>
<tr>
<td>IP2</td>
<td>MAC2</td>
<td>SLAAC</td>
</tr>
<tr>
<td>IP3</td>
<td>MAC1</td>
<td>SLAAC</td>
</tr>
</tbody>
</table>

**MAC-IP Mapping Table**

<table>
<thead>
<tr>
<th>MAC</th>
<th>IP</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC1</td>
<td>IP1</td>
<td>DHCP</td>
</tr>
<tr>
<td>MAC2</td>
<td>IP2</td>
<td>SLAAC</td>
</tr>
</tbody>
</table>
Scenario 2: Autonomous WLAN

• AP filtering
  • FAT AP maintains both MAC-IP and IP-MAC Mapping Table and performs both address snooping and packet filtering.
MAC address randomization

• In WLAN, random MAC addresses are mainly used for discovering wireless networks, accessing networks and communicating.
  
  • **Wireless network discovery**
    • Use probe request frames to discover wireless networks. This does not affect the establishment of SAVI binding anchors.
  
  • **Network access and communication**
    • Random MAC addresses are used to send and receive packets.
    • In 802.11i wireless networks, the key used for communication is tied to the MAC address, and the random MAC address does not change during communication.
    • Usually, in the same wireless network, the random MAC address does not change when you re-access the wireless network to ensure roaming experience.
    • If the MAC address changes, the access needs to be rechecked.

• In summary, the anchor of SAVI binding is stable during one access, and the SAVI function will work well.
Next Steps
Next Steps

• Solicit comments and refine the draft.

• The authors would like to thank Bob Hinden, Erik Kline, Qinggen Wu, Xiangqing Chang, Nanzhi Su, and Lu Huang for their valuable comments.

Thank You!

*IETF119, Brisbane*