A SAVI Solution for WLAN

draft-bi-savi-wlan-23

Jun Bi, Jianping Wu, Tao Lin, You Wang, Lin He

MADINAS, ietf114

July 2022
Outline

• Background
• Solution Overview
• Next Step
Background
SAVI goals and framework

• Goals
  • 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 link-layer property
3. enforce binding
Solution Overview
SAVI for WLAN

User → AP → AC → Gateway DHCP Server

Address assignment snooping

Synchronize sniffed MAC and IP addresses through CAPWAP extension

Confirm the legitimacy of binding entries through CAPWAP extension protocol

DAD → DHCP Procedure
Two data structures

• **IP-MAC Mapping Table**
  • maps IP addresses to their corresponding MAC addresses
  • used in the control process
  • An IP address can have only one corresponding MAC address.
  • Different IP addresses can be mapped to the same MAC address.

• **MAC-IP Mapping Table**
  • maps MAC addresses to the corresponding IP addresses
  • used for filtering
  • A MAC address can be mapped to multiple IP addresses.

• 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 anchor

• Banding 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.
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

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

• Look up the MAC address in the MAC-IP mapping table and check if the MAC-IP pair exists.
  • If exists, forward the packet,
  • Otherwise, go the next step.

• Look up the IP address in the IP-MAC mapping table and check if the IP address exists.
  • If exists, check whether the MAC address in the entry is the same as that in the frame.
    • If so, forward the packet.
    • Otherwise, drop the packet.
  • If not, drop the packet.
Deployment scenarios (1)

• Scenario 1: Centralized WLAN (FIT Access Points and Access Controllers)
  • AP filtering
    • AC maintains IP-MAC Mapping Table while AP maintains MAC-IP Mapping Table and perform address snooping
  • 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.
Mobility Solution

User

AP

AC

Request the IP address corresponding to the MAC address

Return result

Inter-AC synchronization
Deployment scenarios (2)

- Scenario 2: Autonomous WLAN (FAT Access Points)
  - FAT AP maintains both MAC-IP and IP-MAC Mapping Table and performs both address snooping and packet filtering.
MAC address randomization and SAVI

- In WLAN, random MAC addresses are mainly used for discovering wireless networks, accessing networks and communicating.
  - **Discover wireless network**
    - Use probe request frames to discover wireless networks. This does not affect the establishment of SAVI binding anchors.
  - **Access networks and communicate**
    - 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 point of SAVI binding is stable during one access, and the SAVI function will work well.
Next Step
Next Step

• Where to promote this work?
  • madinas?
  • intarea?

• Solicit comments and refine the draft
Comments?

Thank You!

IETF114, Philadelphia