Network Working Group
Internet Draft
Intended status: Standard Tracks
Expires: OCT, 2011

J. Bi
J. Wu
Y. Wang
Tsinghua University
T. Lin
Hangzhou H3C Tech. Co., Ltd.
April 6, 2011

A SAVI solution for WLAN

draft-bi-savi-wlan-00.txt

Abstract

This document describes a source address validation solution for WLAN enabling 802.11i or other security mechanisms. This mechanism snoops NDP and DHCP to bind IP address with MAC address, and relies on the security of MAC address guaranteed by 802.11i or other mechanisms to filter IP spoofing packets. It can work in the special situations described in the charter of SAVI workgroup, such as multiple MAC addresses on one interface. This document describes three different deployment scenarios, with solutions for migration of mapping entries when hosts move from one access point to another.

Status of this Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on October 6, 2011.

Table of Contents

1. Introduction

This document describes a mechanism to perform per packet IP source address validation in WLAN. This mechanism performs ND snooping or DHCP snooping to bind allocated IP address with authenticated MAC address. Static addresses are bound to the MAC addresses of corresponding stations manually. Then the mechanism can check validity of source IP address in local packets according to the binding association. The security of MAC address is assured by 802.11i or other mechanisms, thus the binding association is secure.

The situation that one interfaces with multiple MAC addresses is a special case mentioned in the charter of SAVI. And this situation is the only special case that challenges MAC-IP binding. The mechanism to handle this situation is specified in the document.

There are three deployment scenarios specified in this document. The mechanism is deployed on different devices in different scenarios. The deployment detail is described in the document.

When hosts move from one access point to another, the migration of mapping entries may be triggered according to the specific mobility scenario. The mechanism to handle host mobility is specified in the document according to different deployment scenarios.

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [RFC2119].

3. IP-MAC Binding

This section specifies the operations of binding IP addresses to MAC addresses, and the clear of binding.

3.1. Data Structures

3.1.1. IP-MAC Mapping Table

This table maps IP addresses to corresponding MAC addresses. IP address is the index of the table. One IP address can only have one corresponding MAC address, while different IP addresses can be mapped to the same MAC address.

This table is used in control process. Before creating new IP-MAC bindings, this table must first be consulted in case of conflict in binding entries. This table must be synchronized with the MAC-IP table specified in Section 3.1.2.

The address allocated by DHCP has a limited lifetime, so the related entry has a limited lifetime, too. According to [RFC4862], stateless address also has a limited lifetime, the stations set this lifetime by itself.

3.1.2. MAC-IP Mapping Table

This table maps MAC addresses to corresponding IP addresses. MAC address is the index of the table. It is a one-to-many mapping table, which means a MAC address can be mapped to multiple IP addresses. Though multiple MAC addresses may exist on one interface, these MAC addresses must be mapped to different IP addresses.

This table is used for filtering and we will specify the details in Section 4. This table must be synchronized with the IP-MAC table specified in Section 3.1.1.

3.2. Pre-conditions for binding

In the binding based mechanism, the security of IP address is based on the security of the binding anchor. In WLAN, a number of security mechanisms on link layer make MAC address a strong enough binding anchor, for instance, 802.11i, WAPI, WEP.

If MAC address has no protection, attackers can spoof MAC address to succeed in validation. However, in general cases, if MAC address is not protected, more serious attack can be launched than IP spoofing attack.

3.3. Binding IP addresses to MAC addresses

All the static IP-MAC address pairs are configured into the IP-MAC Mapping Table with the mechanism enabled.

An individual procedure handles binding DHCP addresses to MAC addresses. This procedure snoops the DHCP address assignment procedure between attached hosts and DHCP server. DHCP snooping in WLAN is the same as wired network.

An individual procedure handles binding stateless addresses to MAC addresses. This procedure snoops Duplicate Address Detection procedure. ND snooping in WLAN is the same as wired network.

3.4. Clear Binding

Three kinds of events will trigger clearing binding:

1. The lifetime of an IP address in one entry has expired. This IP entry MUST be cleared.

2. A station leaves this access point. The entries for all the related MAC addresses MUST be deleted.

3. A DHCP RELEASE message is received from the owner of corresponding IP address. This IP entry MUST be deleted.

4. Source Address Validation

This section describes on source address validation procedure on packet. In this procedure, all the frames are assumed to have passed the verifications of 802.11i or other security mechanisms.

This procedure has the following steps:

1. Extract the IP source and MAC source from the frame. Lookup the MAC address in the MAC-IP Mapping Table and check if the MAC-IP pair exists. If yes, forward the packet. Or else go to next step.

2. Lookup the IP address in the IP-MAC Mapping Table and check if the IP address exists. If no, insert a new entry into the IP-MAC Mapping Table and forward the packet. If yes, check whether The MAC address in the entry is the same as that in the frame. If yes, forward the packet. Else drop the packet.

5. Deployment Scenarios

This section specifies three deployment scenarios including two under centralized WLAN and one under autonomous WLAN. The deployment details and solutions for host mobility between access points are described respectively in each scenario.

5.1. Centralized WLAN

Centralized WLAN is comprised of FIT Access Points (AP) and Access Controllers (AC). In this scenario, this document proposes the following two deployment solutions.

5.1.1. Filter on AP

In this scenario, AC will maintain the IP-MAC Mapping Table in the control plane, while AP will maintain the MAC-IP Mapping Table in the data plane for filtering. Packet filtering will be performed on each AP as specified in Section 4.

5.1.1.1. Candidate Binding

AP executes the procedure specified in Section 3.3. Candidate binding is generated after snooping procedure. Candidate binding must be confirmed by AC to be valid.

After a candidate binding is generated, AP will notify AC the binding and AC determines whether the binding is valid. The validity of a candidate binding is determined by whether the binding violates any existing binding in the IP-MAC Mapping Table. If an address is not

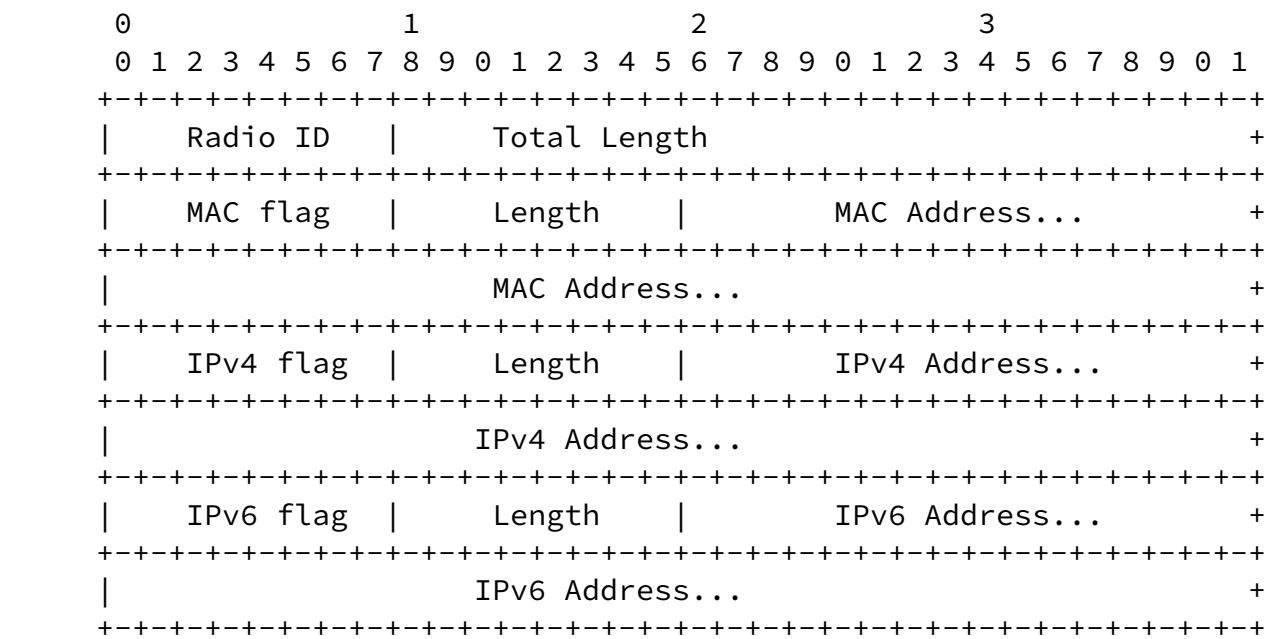
suitable for a host to use, AC will notify AP. If the candidate binding is valid, AC will add an entry into the IP-MAC Mapping Table and notify AP, and then AP will also add an entry into the local MAC-IP Mapping Table.

5.1.1.2. CAPWAP Extension

CAPWAP is used to communicate between AP and AC. A new CAPWAP protocol message element is introduced here, it extends the [CAPWAP]. The station's IP message element is used by the AC and WTP(AP) to intercommunicate Station's IP address.

The station's IP message element MAY be sent by the WTP. When WTP knows station's IP, it can report all the station's IP addresses to AC by this message, and give its suggestion of the IP's state and lifetime.

The station's IP message element MAY be sent by the AC, after AC check this message of the station by some mechanism, and reply the same format message to inform WTP which IP is valid and its state and lifetime.



Type: TBD for Station's IP

Length: >= 8

Radio ID: An 8-bit value representing the radio, whose value is between one (1) and 31.

Total Length: The length of the latter's length.

MAC flag: An 8-bit value representing the sub-field's type is MAC address, whose value is 1.

Length: The length of the MAC Address field. The formats and lengths specified in [EUI-48] and [EUI-64] are supported.

MAC Address: The station's MAC address.

IPv4 flag: An 8-bit value representing the sub-field's type is IPv4 address, whose value is 2.

Length: The length of the IPv4 Address field.

IPv4 Address: The station's IPv4 address. There may exist many entries, and each entry is comprised of one IPv4 address, 8-bit value

of address state (now, it only one value 1 for valid, and it can extended in further), and 32-bit value lifetime (second).

IPv6 flag: An 8-bit value representing the sub-field's type is IPv6 address, whose value is 3.

Length: The length of the IPv6 Address field.

IPv6 Address: The station's IPv6 address. There may exist many entries, and each entry is comprised of one IPv6 address, 8-bit value of address state (now, it only one value 1 for valid, and it can extended in further), and 32-bit value lifetime (second).

5.1.1.3. Mobility Solution

When a host moves from one AP to another AP, layer-2 association will

happen before IP packet transfer. Home AP will delete the binding when mobile host is disconnected, and foreign AP will immediately request the bound addresses with the associated MAC from AC. After AC tells AP the addresses should be bound, the binding migration is completed.

In WLAN, a host can move from an AC to another AC while keeping using the same IP address. To be compatible with such scenario, ACs must communicate to perform the binding migration.

TBD

5.1.2. Filter on AC

In this scenario, AC will maintain both MAC-IP and IP-MAC Mapping Table and perform the packet filtering. So, all the packets must go through AC before forwarding. AC executes the procedure specified in Section 3.3.

Mobility in one AC will not trigger any binding migration. Mobility between different ACs will trigger binding migration and the procedure is the same as that in Section 5.1.1.3.

5.2. Autonomous WLAN

Autonomous WLAN is comprised of FAT Access Points. In this scenario, FAT AP will maintain both MAC-IP and IP-MAC Mapping Table and perform the packet filtering, and executes the procedure specified in Section 3.3.

Mobility between different FAT APs will trigger binding migration and the procedure is the same as that in Section 5.1.1.3.

6. Security Considerations

The security of address allocation methods matters the security of this mechanism. Thus it is necessary to improve the security of stateless auto-configuration and DHCP firstly.

7. IANA Considerations

There is no IANA Consideration currently.

8. Conclusions

This solution can satisfy the requirements of SAVI charter in WLAN enabling 802.11i or other security mechanisms.

9. Contributors

Guang Yao
Tsinghua University
Network Research Center, Tsinghua University
Beijing 100084
China
EMail: yaog@netarchlab.tsinghua.edu.cn

Yang Shi
Hangzhou H3C Tech. Co., Ltd.
Beijing 100085
China
EMail: rishyang@gmail.com

Hao Wang
Hangzhou H3C Tech. Co., Ltd.
Beijing 100085
China
EMail: hwang@h3c.com

10. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

11. References

11.1. Normative References

[1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[2] Crocker, D. and Overell, P.(Editors), "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, Internet Mail Consortium and Demon Internet Ltd., November 1997.

[3] IEEE 802.11i-2004: Amendment 6: Medium Access Control (MAC) Security Enhancements

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC4862] Thomson, S., Narten, T. and Jinmei, T., "IPv6 Stateless Autoconfiguration", RFC4862, September, 2007.

[RFC3315] R. Droms, Ed., J. Bound, B. Volz, T. Lemon, C. Perkins, and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC3315, July, 2003.

[RFC5415] Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification

11.2. Informative References

Authors' Addresses

Jun Bi
Tsinghua University
Network Research Center, Tsinghua University
Beijing 100084
China
EMail: junbi@cernet.edu.cn

Jianping Wu
Tsinghua University
Computer Science, Tsinghua University
Beijing 100084
China
EMail: jianping@cernet.edu.cn

You Wang
Tsinghua University
Network Research Center, Tsinghua University
Beijing 100084
China
EMail: wangyou@netarchlab.tsinghua.edu.cn

Tao Lin
Hangzhou H3C Tech. Co., Ltd.
Beijing 100085
China
EMail: lintaog@gmail.com