SAVI F.Shi
Internet Draft China Telecom
Intended status: Standard Tracks K.Xu, L.Zhu, G.Hu
Expires: May 2014 Tsinghua Univ.
Nov 4, 2013

SAVI Requirements and Solutions for ISP IPv6 Access Network
draft-shi-savi-access-04.txt

Abstract

Internet is always confronted with many security threats based on IP address spoofing which can enable impersonation and malicious traffic redirection. Unfortunately, the Internet architecture fails to provide the defense mechanism. Source Address Validation Improvement (SAVI) was developed to prevent IP source address spoofing. Especially, the mechanism is essential for ISPs. However, due to the diversity of address assignment methods, SAVI solution is also different accordingly. This document describes five scenarios of ISPs'IPv6 access network, and moreover, states its SAVI requirements and tentative solutions accordingly.

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 May 4, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

This document may contain material from IETF Documents or IETF Contributions published or made publicly available before November 10 2008. The person(s) controlling the copyright in some of this material may not have granted the IETF Trust the right to allow modifications of such material outside the IETF Standards Process. Without obtaining an adequate license from the person(s) controlling the copyright in such materials, this document may not be modified outside the IETF Standards Process, and derivative works of it may not be created outside the IETF Standards Process, except to format it for publication as an RFC or to translate it into languages other than English.

Table of Contents

1. Introduction

Spoofing of IP source addresses can jeopardize people's privacy, enable malicious traffic redirection which causes the network topology and traffic information to be leaked out. Further, it will be difficult to trace the source host which has forged the packet. The Source Address Validation Improvement (SAVI) method was designed to prevent hosts attached to the same link from spoofing each other's IP address. It is developed to complement ingress filtering with finer-grained, standardized IP source address validation. It is also can be deployed easily in networks due to its modularization and extensibility.

ISPs that provide Internet access services, information services and value-added services to the customers always have to be confronted with many threats enabled by IP source address spoofing, while the Internet architecture fails to prevent IP source address spoofing [draft-ietf-savi-threat-scope]. So they have an imperative demand to apply the mechanism in order to defend the attack and ensure the security of its network and customers' privacy.

Internet Service Provider has multiple access scenarios not limited to Ethernet, and usually is deployed with DHCP. Other scenarios such as ADSL with PPP and Ethernet with PPP are also popular in the real world. Unfortunately, SAVI Switch only works in the scenarios of wire or wireless Ethernet and does not support all address assignment methods that can be used in access network. There are four address assigned methods identified in one of the SAVI documents:

1. Stateless Address Auto Configuration (SLACC) [I-D.ietf-savi-fcfs]

2. Dynamic Host Control Protocol address assignment (DHCP) [I-D.ietf-savi-dhcp]

3. Secure Neighbor Discovery (SeND) address assignment [I-D.ietf-savi-send]

4. Mix Address assignment methods

[I-D.ietf-savi-mix]

Thus, According to different access network scenarios, SAVI should adjust its deployment and make improvement to adapt to the real situation. This note analyzes five scenarios of ISPs' IPv6 access network, and on this basis, gives tentative SAVI solutions accordingly.

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].

In this document, these words will appear with that interpretation only when in ALL CAPS. Lower case uses of these words are not to be interpreted as carrying RFC-2119 significance.

3. Terminology

The following acronyms and terms are used throughout this document.

HRG: Home Residential Gateway, an intelligent gateway between network devices and external network in a family.

BRAS: Broadband Remote Access Server, a network switch that funnels traffic from DSL and/or cable modem aggregation devices to various carriers' networks based on the type of an application or that of a service required.

STB: Set Top Box, a device which can provide value-added services used to enhance or extend the function of TV.

AAA: Authentication, Authorization, Accounting. AAA server can provide verification and authority service.

C+W: CDMA (CDMA2000) + WLAN, an integrated wireless broadband network business of China telecom.

WAG: Wireless Access Gateway.

PDSN: Packet Data Serving Node, responsible for the establishment and terminating point-to-point protocol (PPP) connection and assign dynamic address for nodes.

4. Scenarios for ISPs'IPv6 Access Network

There are various access methods for ISPs'IPv6 access network. To facilitate the deployment of the SAVI method in networks of various kinds, the SAVI method is designed to support different IP address assignment methods [I-D.ietf-savi-framework]. However, there are still some mixed address assignment methods which cannot be supported. It is important to note that the deployment of SAVI device has been

impacted greatly by access network scenarios and its address assignment methods. In order to meet different IP Source Address Validation requirements, SAVI solutions may need to be improved to adapt to the real situation.

From the perspective of SAVI deployment, there are five typical scenarios of ISPs'IPv6 access network:

1. Home Residential gateway (HRG) acts as DHCPv6 proxy.

2. Set Top-box (STB) gets an IP address via DHCPv6.

3. Host gets IP address via PPPoE & RA.

4. Laptop accesses Internet via WLAN.

5. Laptop accesses Internet via C+W.

We will discuss the SAVI solution for each scenario in detail in the next section.

4.1. Scenario 1: Home Residential gateway (HRG) acts as DHCPv6 proxy

```
                    +--------+
                    |  BRAS  |
                    +-------,+
```

```
                (PPPoE/ND/RA)|| (DHCPv6-PD)
                                     ||
                                 +---||---+
                                 |   HRG  |
                                 +--/----/+
                           (DHCPv6)|     |(DHCPv6)
                              +----\-+  +\-----+
                              |  PC  |  |  STB |
                              +------+  +------+
```

Figure 1: Scenario 1

Figure 1 shows the main elements in scenario 1. PC and STB connect to the Internet via HRG. Its address assignment mechanism can be described as follows: First, HRG gets a link-local IPv6-IPv6 address from BRAS via PPPoE and ND/RA. Then, HRG gets an IPv6 address from BRAS via DHCPv6-PD. At last, PC and STB get IPv6 addresses from HRG

via DHCPv6. Of course, PC and STB can also get IPv6 addresses via ND/RA, but the DHCPv6 is much more popular.

According to the SAVI mechanism, in order to achieve Source Address Validation, the SAVI device must snoop the whole procedure of Address assignment. In addition, the preferred location of SAVI instances is close to hosts, such as in access switches that directly attach to the hosts where host IP addresses are being validated [I-D.ietf-savi-framework]. So we can deploy the SAVI device in places close to the HRG, such as the first hop access device. It can be illustrated in figure 2.

```
                                 +--------+
                                 |  BRAS  |
                                 +-------,+
                        (PPPoE/ND/RA)|| (DHCPv6-PD)
                                     ||
                          . . . . . .|| . . . . . . .
                          .          ||    Protection.
                          .       +-------+ Perimeter.
                          .       | SAVI  |          .
                          .       | Device|          .
                          .       +-------+          .
```

```
.          ||              .
. . . . . .|| . . . . . . .
       +---||---+
       |   HRG  |
       +--/----/+
 (DHCPv6) |    |(DHCPv6)
   +----\-+   +\-----+
   |  PC  |   |  STB |
   |      |   |      |
   +------+   +------+
```

Figure 2: SAVI solution for Scenario 1

Figure 2 shows the deployment of SAVI device. It also allows multiple SAVI devices and non-SAVI devices co-existing on a link. In addition, for this solution, the SAVI mechanism needs to improve to snoop the procedure of DHCPv6-PD, so as to bind the relationship <HRG/PC/STB's IP address, port, MAC>.

4.2. Scenario 2: STB gets an IP address via DHCPv6

The difference between scenario 1 and scenario 2 is the absence of HG which acts as DHCPv6 proxy. In scenario 2, STB, having its internal account and password gets IPv6 prefix by DHCPv6. The general scene workflow includes the following steps: STB sends requests to all routers on a local link by using a link-local address based on its MAC address. The BRAS gives a message to STB to adopt DHCPv6 address assignment method as a response. STB initiates the DHCPv6 procedure and BRAS acts as a DHCP Relay to add some authorities' messages. An AAA server decides whether assign address parameters depend on the result of authentication. At last, BRAS receives IPv6 parameters from AAA server, and then, informs STB via DHCPv6 protocol. It can be illustrated in figure 3.

```
+--------+  +-----------+
|   AAA  |  |DHCP server|
+--------+  +-----------+
         \ /
```

```
                      ||
                      ||
                   +--||--+
                   | BRAS |
                   +-------+
                       |
                    (DHCPv6)
                       |
                   +--------+
                   |  STB   |
                   +--------+
```

Figure 3: Scenario2

Figure 3 shows the main elements in scenario 2. Due to the pure DHCPv6 address assignment method in this scenario, we can deploy SAVI device in places close to STB directly and SAVI mechanism need not make any improvement. It just needs to bind relationship <STB's IP Address, port, STB's MAC Address> which is supported in the existing SAVI function. The solution can be illustrated in figure 4.


```
            +---------+  +------------+
            |   AAA   |  |DHCP server|
            +---------+  +------------+
                     \ /
                   +--||---+
                   |  BRAS |
                   +-------+
                       |
                    (DHCPv6)
                       |
             . . . . . . . . . . .  .
             .  +---------------+ .
             .  |  SAVI device  | .
             .  +---------------+ .
             . . . . . . . . . . .  .
```

```
             |
         +--------+
         |  STB   |
         +--------+
```

Figure 4: SAVI solution for Scenario 2

4.3. Scenario 3: PC gets an IP address via PPPoE & RA

In this scenario, first of all, PC gets a link-local address from BRAS via PPPoE. BRAS broadcasts IPv6 prefix via RA. Finally, PC configures its address automatically and gets some additional messages from BRAS.

```
          +---------+
          |   AAA   |
          +---------+
              \
               |
          +---|---+
          | BRAS   |
          +--------+
               |(ND)
          +--------+
          |   PC   |
          +--------+
```

Figure 5: Scenario3

Figure 5 shows the main elements in scenario 3. As the function of ND snooping has already been designed, we only take PPPoE snooping into

account. Thus, the solution to this scenario which is illustrated in figure 6 is to deploy the SAVI device directly and binding relationship <PC's IP Address, port, PC's MAC>. In this scenario, SAVI needs to improve in order to realize PPPoE snooping.

```
         +---------+
         |   AAA   |
         +---------+
              \
           +-- |---+
```

```
                      | BRAS   |
                      +--------+
                      (ND)|
                 . . . . . . . . . . .  .
                 .  +---------------+ .
                 .  |  SAVI device  | .
                 .  +---------------+ .
                 . . . . . . . . . . .  .
                          |
                      +--------+
                      |  PC    |
                      +--------+
```

Figure 6: SAVI solution for Scenario 3

4.4. Scenario 4: Laptop accesses Internet via public WLAN

The interaction in this scenario is relatively simple. The laptop gets an IPv6 address via DHCPv6. Then, users are enforced to be certified by submitting a password on a portal page.


```
                 +---------+  +------------+
                 |   AAA   |  |DHCP server|
                 +---------+  +------------+
                          \/
                    +--||---+
                    | BRAS   |
```

```
                 +--------+
                     |(DHCPv6)
                 +--------+
                 |LAPTOP  |
                 +--------+
```

Figure 7: Scenario 4

Figure 7 shows the main elements in scenario 4. We can deploy the SAVI device directly and bind relationship <LAPTOP's IP Address, port, LAPTOP's MAC>. The solution can be illustrated in figure 8.

```
            +---------+  +------------+
            |   AAA   |  |DHCP server|
            +---------+  +------------+
                     \ /
                      ||
                  +--||---+
                 | BRAS   |
                 +--------+
                      |(DHCPv6)
                      |
             . . . . . . . . . .  .
             .  +----------------+ .
             .  |  SAVI device   | .
             .  +----------------+ .
             . . . . . . . . . .  .
                      |
                 +--------+
                 |LAPTOP  |
                 +--------+
```

Figure 8: SAVI solution for Scenario 4

4.5. Scenario 5: Laptop accesses Internet via C+W

This scenario describes that the laptop accesses the Internet via CDMA and WLAN. The general scene workflow includes the following steps: The laptop gets a temporary IPv6 address from BARS via DHCPv6,

and then, obtains the WAG address from a DNS server. The laptop

establishes a UDP tunnel to WAG by sending register request. If the tunnel is established successfully, the laptop can get IPv6 prefix from PDSN via PPP and RA, whereas PDSN acts as the PPP terminal. At last, the laptop gets some additional information such as the DNS address. When the above steps are all accomplished, the laptop acquires the ability to access the Internet.

```
+---------+  +-----------+
|   AAA   |--|    PDSN   |
+---------+  +-------|----+
+---------+  +-------|----+
|AN-AAA   |--|    WAG    |
+---------+  +-----------+
               //
              // UDP tunnel
              ||
              ||
           +--||---+
           | BRAS  |
           +-------+
               |
               |(DHCPv6)
               |
           +-------+
           | LAPTOP|
           +-------+
```

Figure 9: Scenario 5

Figure 9 shows the main elements in scenario 5. in this scenario, we also can deploy the SAVI device in places close to the LAPTOP. SAVI needs to improve to support the PPPoE protocol snooping. It also binds relationship <LAPTOP's IP Address, port, LAPTOP's MAC>. The solution is described in figure 10.

```
                         +---------+  +------------+
                         |   AAA   |--|    PDSN    |
                         +---------+  +-------|----+
                         +---------+  +-------|----+
                         |AN-AAA   |--|    WAG     |
                         +---------+  +------------+
                                       //
                                      // UDP tunnel
                                      ||
                                      ||
                                  +--||---+
                                  | BRAS  |
                                  +-------+
                                      |
                                   (DHCPv6)
                                      |
                                 +---------+
                                 |  SAVI   |
                                 |  device |
                                 |         |
                                 +---------+
                                      |
                                      |
                                  +--------+
                                  |LAPTOP  |
                                  +--------+
```

Figure 10: SAVI solution for Scenario 5

5. Conclusions

For ISPs, SAVI can defend against many security attacks effectively which are based on IP address spoofing. There are various scenarios of ISPs'IPv6 Access Network. As each scenario uses a different address assignment method and protocol, there are a variety of requirements to validate the source address for ISPs' IPv6 access network. Though SAVI cannot support all protocols and methods right now, due to expansibility of SAVI, the mechanism can satisfy various demands with a small improvement. This document presents five typical scenarios of ISPs'IPv6 access network, and proposes tentative SAVI solutions.

Moreover, for functional verification, we conducted an experiment on China Telecom's access network in Hunan province. The experimental results show that source addresses can be validated effectively as we expected in most access scenarios. Next, we will deploy more SAVI

devices on a large-scale network in order to form a complete architecture.

6. References

6.1. Normative References

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

[draft-ietf-savi-threat-scope]

McPherson, D., Baker, F., and J. Halpern, "SAVI Threat Scope", draft-ietf-savi-threat-scope-05, April 2011.

[I-D.ietf-savi-dhcp] Wu, J., Yao, G., Bi, J., and F. Baker, "SAVI Solution for DHCP", draft-ietf-savi-dhcp-10 (work in progress), July 2011.

[I-D.ietf-savi-fcfs] Nordmark, E., Bagnulo, M., and E. Levy-Abegnoli, "FCFSSAVI: First-Come First-Serve Source-Address Validation for Locally Assigned IPv6 Addresses", draft-ietf-savi-fcfs-09(work in progress), April 2011.

[I-D.ietf-savi-send] Bagnulo, M. and A. Garcia-Martinez, "SEND-based Source-Address Validation Implementation", draft-ietf-savi-send-06 (work in progress), October 2011.

[I-D.ietf-savi-framework] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt, "Source Address Validation Improvement Framework",draft-ietf-savi-framework-05 (work in progress), July 2011.

7. Acknowledgments

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

Authors' Addresses

Fan Shi
China Telecom
Beijing Research Institute, China Telecom
Beijing, 100035
China
Email: shifan@ctbri.com.cn

Ke Xu
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing, 100084
China
Email: xuke@mail.tsinghua.edu.cn

Liang Zhu
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing, 100084
China
Email: tshbruce@gmail.com

Guangwu Hu
Tsinghua University
Department of Computer Science, Tsinghua University
Beijing, 100084
China
Email: hgw09@mails.tsinghua.edu.cn