

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: 16 August 2022

K. Xu  
J. Wu  
X. Wang  
Y. Guo  
Tsinghua University  
12 February 2022

Practical Inter-Domain Source Address Validation  
draft-xu-psav-00

## Abstract

Because the Internet forwards packets according to the IP destination address, packet forwarding typically takes place without inspection of the source address and malicious attacks have been launched using spoofed source addresses. The inter-domain source address validation architecture is an effort to enhance the Internet by using state machine to generate consistent tags. When communicating between two end hosts at different ASes, tags will be added to the packets to identify the authenticity of the IP source address.

This memo introduces PSAV, an Inter-AS source address validation mechanism.

## 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 <https://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 16 August 2022.

## Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

Internet-Draft

PSAV

February 2022

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://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 Revised BSD License text as described in Section 4.e of the [Trust Legal Provisions](#) and are provided without warranty as described in the Revised BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Terminology and Abbreviation . . . . .	<a href="#">3</a>
<a href="#">3.</a>	PSAV Framework . . . . .	<a href="#">3</a>
<a href="#">4.</a>	Control Plane . . . . .	<a href="#">5</a>
<a href="#">5.</a>	Data Plane . . . . .	<a href="#">6</a>
<a href="#">6.</a>	Consistency . . . . .	<a href="#">7</a>
<a href="#">7.</a>	Scalability . . . . .	<a href="#">7</a>
<a href="#">7.1.</a>	Compatibility . . . . .	<a href="#">7</a>
<a href="#">7.2.</a>	Expansion Management . . . . .	<a href="#">7</a>
<a href="#">8.</a>	Security Consideration . . . . .	<a href="#">7</a>
<a href="#">8.1.</a>	Attack towards community information . . . . .	<a href="#">8</a>
<a href="#">8.2.</a>	Attacks towards Initial Status Negotiation . . . . .	<a href="#">8</a>
<a href="#">8.3.</a>	Tag Guessing and Key Cracking . . . . .	<a href="#">8</a>
<a href="#">9.</a>	IANA Consideration . . . . .	<a href="#">8</a>
<a href="#">10.</a>	Acknowledgements . . . . .	<a href="#">8</a>
<a href="#">11.</a>	Normative References . . . . .	<a href="#">8</a>
	Authors' Addresses . . . . .	<a href="#">9</a>

## [1.](#) Introduction

IP spoofing has been a long-recognized threat to Internet security for decades. Inter-domain source address validation (SAV) has long served as the primary defense mechanism due to its better cost-effectiveness. However, over years of effort, the deployment of inter-domain source address validation is still not optimistic. An important reason for this is the difficulty of balancing the clear security benefits of partial deployments with the scalability of large-scale deployments. uRPF [[RFC5635](#)], for example, routing-based schemes to filter spoofed traffic, which may result in a lack of security benefits due to the dynamic nature of routing or incomplete information caused by partial deployments. And while cryptography-based schemes such as IPsec [[RFC4301](#)] can provide clear security

gains, the additional end-to-end overhead will present new challenges in scalability.

This document provides a framework of practical inter-domain SAV (PSAV). PSAV is a cryptography-based SAV to guarantee consistent security benefits. Key maintenance is performed between the source and destination ASes, and the key is used to generate packet tags to validate the authenticity of the source address. Meanwhile, in PSAV, ASes are organized as a hierarchical structure to provide scalability, in which only fully-connected key maintenance is performed between ASes on the same layer, and ASes between different layers achieve end-to-end source address validation through cross-layer validation and tag replacement.

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](#), [BCP 14](#) [[RFC2119](#)] and indicate requirement layers for compliant CoAP implementations.

## [2.](#) Terminology and Abbreviation

+=====+=====+	
Abbreviation	Description
+=====+=====+	
TA	Trust Alliance, the IPv6 network
	that uses the SAVA-X mechanism.
+-----+-----+	
ACS	AD Control Server, the server that
	maintains state machine with other ACS
	and distribute information to AER.
+-----+-----+	
ABR	AS or AS community border router,
	which is placed at the boundary of
	an AS of trust alliance.
+-----+-----+	
Tag	The authentic identification of
	source address of a packet.
+-----+-----+	

Table 1

### 3. PSAV Framework

PSAV is a cryptography-based end-to-end inter-domain source address verification method that guarantees security benefits at partial deployment. PSAV implements inter-AS tag maintenance by establishing a hierarchical community structure that utilizes border nodes on the forwarding path for tag replacement and validation. This mainly includes the following components.

Xu, et al.

Expires 16 August 2022

[Page 3]

Internet-Draft

PSAV

February 2022

1. Tag generation. In PSAV, the packet tag is generated by maintaining the key between ASes and using the generation algorithm. The destination AS will validate the source address by the packet tag. The above process requires a mapping relationship between AS-IP\_Prfix-Key, which will be provided based on existing Internet infrastructure, e.g., such as RPKI, ROVER, etc.
2. Hierarchical structure. In PSAV, AS is organized into hierarchical AS communities, which can provide good scalability by reducing the tag maintenance overhead in large-scale deployments, managing the validation responsibilities corresponding to address allocation, and shielding external community changes. To implement tag validation in AS communities, PSAV will provide corresponding tag cross-layer validation and replacement methods.
3. Membership configuration. AS sends join, exit, or update to all participating nodes through a specific message format, and the participating nodes further complete membership configuration by verifying the authenticity of the messages to form a distributed consensus.

A typical workflow of PSAV is shown in Figure 1. AS1 joins the PSAV trust alliance with the signed join information, maintains the packet tag with AS2. After that, AS1 sends out the packet with Tag <AS1, AS2>, and AS2 validates it and replaces the Tag with <AS2, AS3>. Then AS3 validates and replaces the tag with <AS3, AS4>. After AS4 validation, confirm that the packet source address is true.

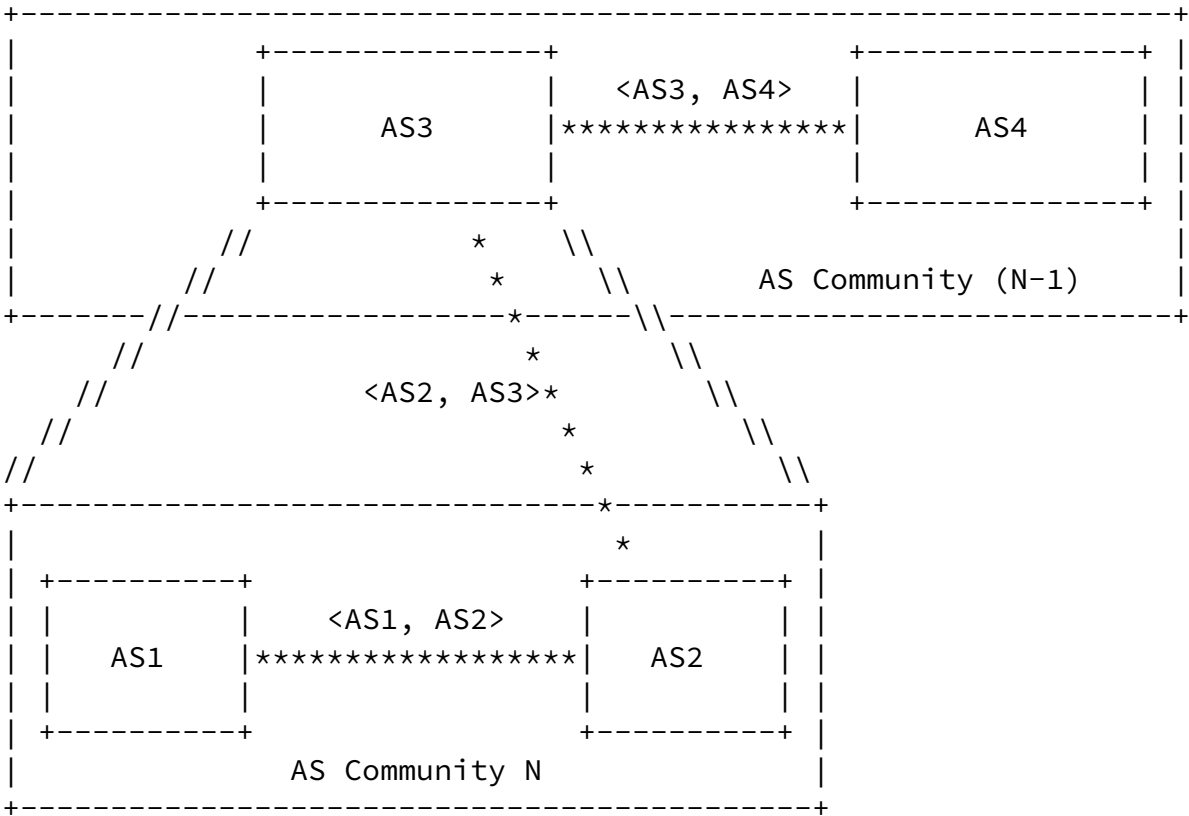


Figure 1: PSAV workflow example.

#### [4.](#) Control Plane

The functions of control plane of PSAV includes AS community information management, ACS-ACS communication, and ACS-ABR communication.

To eliminate the impact of routing dynamic caused by BGP or other routing protocols, PSAV requires its own AS community information management. These information of one AS includes AS Number (ASN), AS Community Number (ASCN), IP Prefix and Public Key. PSAV does not bind any methods of inter-domain mapping information, and it can both use centralized or distributed methods to maintain AS community information independently. When an AS or AS community wants to join or exit the Trust Alliance constructed by all the member ASes and AS communities, it SHOULD submit a certificate signing request message containing its own information. It also needs to submit such CSR message for updating its information recorded by all members in trust alliance.

The communication among ACSes is to maintain the tags used in packets in network. PSAV provides a tag generation mechanism on one-to-one state machine. In this mechanism, each AS or AS community needs one ACS. ACS negotiates initial state of the state machine with its

relevant ACS. The state transfers to the next state triggered by time flies. For crossing different layer of AS communities, it is used the tag generated by the state machine maintained by AS or AS community with its direct paternal AS community in PSAV. The communication between ACS and ABR is to deliver the AS community information and tags.

PSAV requires a heart-beat mechanism for service availability implemented in ACS-ACS communication and ACS-ABR communication. When it detects that one ACS or ABR has 'died', the other end WOULD remove its tag generation mechanism maintained with this 'died' end and sends a request message to force execute the exit trust alliance process of the other end.

#### [5.](#) Data Plane

The functions of data plane of PSAV includes prefix checking and tag processing.

The tag delivered from the control plane indicates the source address of one packet is not tampered. As the tag in use is generated by one-to-one state machine pair, it MUST be completely consistent at the same time.

It needs to divide the role of different interfaces of an ABR for functioning properly. In ABR, the interface takes the role of INGRESS, EGRESS, or TRUST. The INGRESS port links to the devices inside the AS or AS community, the EGRESS port links to the devices outside the AS or AS community, and the TRUST port links to the ABR inside the same AS or AS community. The INGRESS port validates and removes the tag in use. The EGRESS port adds or replaces the tag in the packet. The TRUST port does nothing to the packet.

When a packet arrives at the ABR, it SHOULD be checked its source address and destination address first. If it originates and destines the trust alliance, it MUST be tagged with a tag at the first hop and removed tag at the last hop. When this packet forwards crossing different layers of AS communities, it SHOULD be replaced with relevant tags maintained by its ACS with direct paternal ACS. In ABR, it maintains two mapping tables to record the AS community information and tags in use. The AS-Prefix mapping table preserves the ASN or ASCN and IP address prefix relationships. The AS-Tag mapping table holds the ASN or ASCN and relevant tags. When a packet is needed to add, replace, or remove tag, the ABR WOULD get the ASN or ASCN which the packet belongs to first via the source address of the packet from the AS-Prefix mapping table. The ABR WOULD obtain the tag should be used by the ASN or ASCN from the AS-Tag mapping table.

## [6.](#) Consistency

PSAV is a cryptography-based source address validation mechanism to guarantee consistent security benefits and provide scalability for different deployment scales and validation granularity. PSAV uses the hierarchical structure to reduce the size of the secret symmetric keys to cut down the maintenance overhead. Hierarchy validation filters malicious traffic as early as possible to avoid wasting

network resources. PSAV also provides clear security responsibilities corresponding to IP address allocation authority.

## [7.](#) Scalability

### [7.1.](#) Compatibility

Hierarchy effectively blocks external changes and provides scalability in large-scale deployments. AS the forwarding path is independent of the tag validation by using a mechanism for crossing different layers, PSAV is a segmented end-to-end cryptography scheme essentially. So it does not need to obtain the routing information and has nothing influence on existing routing infrastructure. Meanwhile, PSAV supports that packets can pass through networks where PSAV has not yet been deployed without affecting validation as it is end-to-end validation in nature, which is guaranteeing a definite security benefit for the deployer without requiring a deployment rate.

### [7.2.](#) Expansion Management

On one hand, PSAV effectively isolates structural changes outside the community from internal nodes, as the hierarchical community design minimizes the impact of changes on the rest of the system. On the other hand, PSAV can be implemented with any existing distributed consensus algorithm for inter-AS consensus infrastructure. It should be noted that PSAV has no special requirements for the efficiency of this process based on the assumption that AS community information does not change frequently. Therefore, the decentralized maintenance approach can further reduce the management complexity of the expansion process.

## [8.](#) Security Consideration

### [8.1.](#) Attack towards community information



The distributed method to maintain the AS community information MAY suffer from the consistency challenges, such as witch attacks and eclipse attacks. However, the situation in PSAV is different from the normal distributed consensus scenario. Due to the hierarchical structure of PSAV, the failure of consensus on local community information does not affect other non-adjacent communities in the system. At the same time, the updated community information only needs the signature confirmation of its parent, brother and child communities, which means that the attack on the special node needs to hold specific resources, which further increases the difficulty of the attack.

### [8.2.](#) Attacks towards Initial Status Negotiation

This is the problem posed in the PSAV implementation. As the clock-synchronized state machine will run locally after the initial status negotiation stage, the attacker can only attack on this negotiation. However, when the ACS-ACS pair or ACS-ABR pair is going to connect, the SSL/TLS will be used to guarantee security in communication. Therefore PSAV can ensure that attackers cannot obtain the initial status even if it can eavesdrop the negotiation packet online.

### [8.3.](#) Tag Guessing and Key Cracking

For resisting reply attack, the eventual tag used in a packet is generated by the ABR with hashing a five-tuple including the signature generated from the state machine, the source address, the destination address, the first 8-bit of payload and source address prefix length. The attacker could guess the tag and crack that key using brute force. Nevertheless, it depends on the irreversibility of a Hash function to prevent backstepping the key from the tag. Furthermore, to decrease such probability, the signature generated from the state machine will be updated periodically.

## [9.](#) IANA Consideration

TBD.

## [10.](#) Acknowledgements

TBD.

## [11.](#) Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", [RFC 4301](#), DOI 10.17487/RFC4301, December 2005, <<https://www.rfc-editor.org/info/rfc4301>>.
- [RFC5210] Wu, J., Bi, J., Li, X., Ren, G., Xu, K., and M. Williams, "A Source Address Validation Architecture (SAVA) Testbed and Deployment Experience", [RFC 5210](#), DOI 10.17487/RFC5210, June 2008, <<https://www.rfc-editor.org/info/rfc5210>>.
- [RFC5635] Kumari, W. and D. McPherson, "Remote Triggered Black Hole Filtering with Unicast Reverse Path Forwarding (uRPF)", [RFC 5635](#), DOI 10.17487/RFC5635, August 2009, <<https://www.rfc-editor.org/info/rfc5635>>.

#### Authors' Addresses

Ke Xu  
Computer Science, Tsinghua University  
Qinghuayuan street, Haidian District  
Beijing  
100084  
China

Email: [xuke@tsinghua.edu.cn](mailto:xuke@tsinghua.edu.cn)

Jianping Wu  
Computer Science, Tsinghua University  
Qinghuayuan street, Haidian District  
Beijing  
100084  
China

Email: [jianping@cernet.edu.cn](mailto:jianping@cernet.edu.cn)

Internet-Draft

PSAV

February 2022

Xiaoliang Wang  
Computer Science, Tsinghua University  
Qinghuayuan street, Haidian District  
Beijing  
100084  
China

Email: wangxiaoliang0623@foxmail.com

Yangfei Guo  
Institute for Network Sciences and Cyberspace, Tsinghua University  
Qinghuayuan street, Haidian District  
Beijing  
100084  
China

Email: guoyangf19@mails.tsinghua.edu.cn

