# Reviewing Technological Solutions of Source Address Validation

## (Submit to Bright Internet Global Summit - BIGS)

**Jongbok Byun**[1]
Business School, Sungkyunkwan University
Seoul, Korea

**Christopher P. Paolini**
College of Engineering, San Diego State University
San Diego, CA, USA

**Bongsik Shin**
Fowler College of Business, San Diego State University
San Diego, CA, USA

## ABSTRACT

It is essential to know the source IP address of a packet to prevent the IP spoofing attack which masquerades the sender's true identity. If there is a way to trace back the origin of the massive DDoS attacks, we could find the responsible parties of the incidents and prevent future attacks by blocking them. Unfortunately, the original TCP/IP stacks don't require the real source IP address to forward the packets to the destination. Malicious attackers can modify the source IP address to hide its true identity and able to send the fraudulent packets to the victim.

One of the critical features of the next generation Internet is having a secure Internet which provides trust between participants and protects the privacy of the individuals. In this paper, we review the various approach to provide the source address validation (SAV) schemes. There are many new methods have been proposed, no single way is providing the comprehensive solution to this issue. Privacy is a critical issue to consider when the true identity is available on the network as well.

[1] Corresponding author. jbyun@skku.edu +82 2 760 0481

**Keywords:** Source Address Validation, Source Address Validation Architecture, SAVA, Authenticated Source IP Address, Software Defined Networking, SDN, Internet Protocol, IPv6, Spoofing, SAVI

## INTRODUCTION

A well-known and frequently-exploited vulnerability in version 4 of the network layer *Internet Protocol* consists of an attacking host fraudulently substituting the 32-bit *Source IP Address* field with the address of a trusted host. Known as *address masquerading* or *address spoofing*, an attacking host exploits a pre-existing trust relationship that exists between two hosts and impersonates one of the trusted hosts to gain unauthorized access to the other. Many application layer services make authorization decisions based exclusively on the value of a source address. In a typical connection-oriented client-server scenario involving a client station *Alice* and a server station *Bob*, Alice initiates a TCP connection to Bob by first sending a *synchronization* datagram to Bob that contains an initial 32-bit *sequence number*. This initial synchronization datagram is acknowledged by Bob by sending a *synchronization with acknowledgment* datagram back to Alice with another sequence number chosen by Bob. Finally, a connection is established when Alice sends Bob an *acknowledgment* datagram that acknowledges Bob's sequence number. If a prior trust relationship exists between Alice and Bob wherein, for example, a user with an account on Alice is permitted to log in to Bob without requiring a password remotely. An attacker could fool Bob by constructing a TCP datagram with a properly guessed sequence number and the IP address of Alice in the 32-bit Source IP Address field shown in Figure 1. To defend against address masquerading exploits, several techniques have been proposed in the literature which aims to confirm the identity of a source address

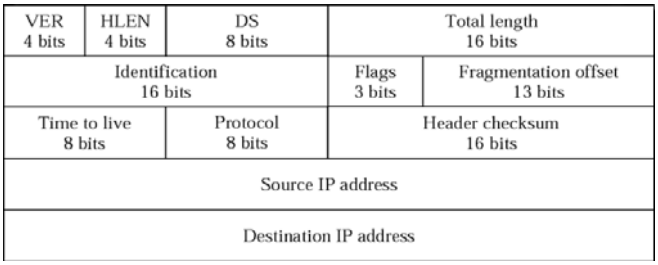


**Figure 1. Structure of the IPv4 datagram header.**

within an IP datagram. Known as *source address validation* ("SAV"), these approaches employ mechanisms within network devices to authenticate the identity of a source address as a datagram progresses from an originating local LAN to another destination LAN through intermediary switches, gateways, and routers. In this research-in-progress, we review and characterize current literature relevant to SAV to lay an initial groundwork for future research, which ultimately aims to conceive a scheme to significantly discourage cyber-attacks of various types in a non-invasive and cost-effective manner while maintaining the privacy of ordinary people.

## LITERATURE REVIEW

One of the original implementations of SAV is the source address validation architecture ("SAVA") proposed and deployed by Wu et al. (Wu et al. 2007) on the China Education and Research Network (CERNET). Part of the China Next Generation Internet (CNGI) effort, CERNET supports an experimental all-IPv6 network that researchers can use to deploy and evaluate experimental protocols. SAVA employs three mechanisms to authenticate a source address. First, a source address is authenticated at the local LAN by a subnet gateway that contains an internal table which provides a mapping between MAC addresses of devices on the subnet and their authorized IP address. Received packets that contain a mismatch between IP source address and Ethernet MAC address are dropped and not forwarded. Second, a source address is authenticated within an autonomous system (AS) by routers that maintain internal tables that relate a prefix to an interface on which packets with specified prefixes may only

arrive. Datagrams that arrive on a router interface containing a prefix that is not matched by a table entry are dropped and not forwarded. Third, source addresses are authenticated between ASs using an inter-AS address validation scheme that separately handles routing between two neighboring SAVA-compliant ASs, two SAVA-compliant ASs separated by one or more non-compliant ASs, and one compliant and one non-compliant AS. Six different protocols are needed to handle these three cases, making SAVA somewhat involved to deploy. SAVA is designed to operate only with IPv6 and does not support IPv4, because SAVA requires that each device have a globally unique IP address and thus IPv4 with network address translation (NAT) cannot be supported. Also, SAVA requires centralized IP address management to be effective, and will not cope well in decentralized IT environments, where different, independent groups maintain portions of an AS address space. SAVA also requires network devices maintain tables that map IP addresses to devices and routing interfaces, something that can be implemented using software defined networking (SDN) where switches and routers can pass datagrams from a data plane (DP) to a control plane (CP) where SAVA protocols are implemented in software. Nevertheless, SAVA has been successfully implemented, in an incremental fashion, on a CNGI IPv6 test-bed connecting 12 universities in China (Bi et al. 2008; Hu and Wu 2012), although additional research is needed to evaluate if SAVA can be deployed at the scale of the global Internet.

He et al. (2010) has developed a routing protocol, *Minimum Hop to First SAVA* (MHFS) node that enables incremental deployment of SAVA. MHFS will guarantee that at least one SAVA-compliant device will process the route of datagrams (He et al. 2010). SAVA was designed at Tsinghua University; researchers at Nanchang University have proposed improvements to SAVA, *Source Address Validation Improvements* (SAVI) (Yan et al. 2011), as

an IETF working group. More recently, source address validation in IPv6 networks based on SAVI design principles has been investigated by Hu and Wu at South China University of Technology in Guangzhou (Hu and Wu 2012) who have successfully implemented SAVI address validation and forwarding rules in Ethernet switches. Although SAVA provides the individual level traceability for the source identity, it requires additional devices which have a SAVA compatible. The costs of implementation and maintenance of such devices are problems to deploy the SAVA systems over the multi-AS networks because the implementation costs and benefits are not equally shared between the senders and the receivers of the packets.

We classified the various source address validation schemes as the Table 1. In this table, the schemes are classified by the place that they are applied.

**Table 1: Source Address Validation Classification**

| | Source Hosts | Intermediate Routers | Destination Hosts |
|---|---|---|---|
| Validation Scheme | Packet Authentication<br>Digital Signature | Filtering<br>Marking<br>Smart Network | IP traceback |
| Mechanism | Packets are authenticated with the unique identifiers with or without encryption | Packet information are shared.<br>Packet are marked for additional monitoring.<br>Additional devices and protocols are applied. | Passive or active IP traceback |
| Examples | SAVA, SAVI | SDN<br>CenterTrack<br>OpenFlow<br>FloodShield | PIT<br>SPIE |

Although SAVA and SAVI have all three levels validation mechanisms, they are mainly creating the source address validity at the source host level. The intermediate Routers can generate ICMP (Internet Control Message Protocol) messages to share the hop information,

timestamp, and MAC address of each packet and share it with neighbor routers (Bellovin et al. 2003). BGP (Border Gateway Protocol) messages also can be used at the border gate routers to exchange the packet information (Duan et al. 2007; Singh et al. 2016). Using these messages, the tracking of the sources is possible. Marking the packet itself is another way to trace back to the origin. Using PPM (Probabilistic Packet Marking) and DPM (Deterministic Packet Marking) mechanisms, one can mark packets (Bellovin et al. 2003). When routers inspect the incoming and outgoing packets regularly for these marks, it is possible to know the source information. Routers can hold the IP header information that it transfers in its storage for future references. SPIE (Source Path Isolation Engine) uses specific filtering mechanism to keep the data it the router's storage (Snoeren et al. 2001). CenterTrack is an approach to provide a special inspection when there are flooding attacks in the network (Stone and others 2000). In a normal situation, special routers do not intervene, but when there are abnormal traffic attacks, the traffic is redirected to specific servers which can inspect the traffic and examine the traceback information. This approach can identify the attackers accurately. SDN (Software Defined Network) and other intelligent network architectures can provide the source identification correctly also (Zhang et al. 2018).

At the destination host level, traceback approach is common. Use ICMP messages and other network administration messages; the destination host can initiate the passive or active traceback to the source hosts. When there is no valid response from the hosts with random probing, the destination hosts can block the incoming packets from the unresponsive sources (Bi et al. 2015; Strayer et al. 2004). Although the traceback could be applied global scale without any significant costs, it is a limited and reactive approach, and it could add more stress to the destination network devices which are already stressed out.

## CONCLUSION

In this paper, we briefly reviewed the current source IP address validation efforts. Currently, there are practical hurdles of the source address validation. For instance, although ISPs are in an excellent position to deter much of the cyber threats and attacks and although ISPs are increasingly realizing that their networks are not immune from the cyber threats, their counter efforts are hampered by such practical issues as their legal implications and necessary infrastructure investment and subsequent transference of the implementation costs to service users. As a result, ISPs may lack incentives to implement such scheme as source address validation. Nonetheless, we feel that we have reached the tipping point where a fundamental solution is necessary to discourage cybercriminals from wreaking havoc on individuals, businesses, and governments.

## REFERENCES

Bellovin, S. M., Leech, M., and Taylor, T. 2003. *ICMP Traceback Messages*, Internet Engineering Task Force.

Bi, J., Wu, J., Li, X., and Cheng, X. 2008. "An IPv6 Test-Bed Implementation for a Future Source Address Validation Architecture," in *Next Generation Internet Networks, 2008. NGI 2008*, pp. 108–114.

Bi, J., Wu, J., Yao, G., and Baker, F. 2015. "Source Address Validation Improvement (SAVI) Solution for DHCP," *RFC* (7513), pp. 1–54.

Duan, Z., Dong, Y., and Gopalan, K. 2007. "DMTP: Controlling Spam through Message Delivery Differentiation," *Computer Networks* (51:10), Elsevier, pp. 2616–2630.

He, R., Song, L., Wang, X., and Lin, B. 2010. "Routing in Trustworthy Networks with SAVA Nodes," in *Advanced Computer Control (ICACC), 2010 2nd International Conference On* (Vol. 4), pp. 402–406.

Hu, J., and Wu, Y. 2012. "Source Address Validation Based Ethernet Switches for IPv6 Network," in *Computer Science and Automation Engineering (CSAE), 2012 IEEE International Conference On* (Vol. 3), pp. 84–87.

Singh, K., Singh, P., and Kumar, K. 2016. "A Systematic Review of IP Traceback Schemes for Denial of Service Attacks," *Computers & Security* (56), Elsevier, pp. 111–139.

Snoeren, A. C., Partridge, C., Sanchez, L. A., Jones, C. E., Tchakountio, F., Kent, S. T., and Strayer, W. T. 2001. "Hash-Based IP Traceback," in *ACM SIGCOMM Computer Communication Review* (Vol. 31), pp. 3–14.

Stone, R., and others. 2000. "CenterTrack: An IP Overlay Network for Tracking DoS Floods.," in *USENIX Security Symposium* (Vol. 21), p. 114.

Strayer, W. T., Jones, C. E., Tchakountio, F., and Hain, R. R. 2004. "SPIE-IPv6: Single IPv6 Packet Traceback," in *Local Computer Networks, 2004. 29th Annual IEEE International Conference On*, pp. 118–125.

Wu, J., Ren, G., and Li, X. 2007. "Source Address Validation: Architecture and Protocol Design," in *2007 IEEE International Conference on Network Protocols*, pp. 276–283.

Yan, Z., Deng, G., and Wu, J. 2011. "SAVI-Based IPv6 Source Address Validation Implementation of the Access Network," in *Computer Science and Service System (CSSS), 2011 International Conference On*, pp. 2530–2533.

Zhang, C., Hu, G., Chen, G., Sangaiah, A. K., Zhang, P., Yan, X., and Jiang, W. 2018. "Towards a SDN-Based Integrated Architecture for Mitigating IP Spoofing Attack," *IEEE Access* (6), IEEE, pp. 22764–22777.