IPv4/IPv6 Source Address Verification

draft-baker-sava-operational-00

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

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."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on December 20, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This note proposes a practical solution to Internet Layer Source Address Verification. The purpose of such verification is to prevent attacks from using spoofed addresses and to facilitate the tracking of attack datagrams to the computers that send them.
Table of Contents

1. Introduction ................................................. 3
   1.1. On attacks and attack management ....................... 3
   1.2. On Trust .............................................. 4
   1.3. Glossary ............................................... 4
2. Eliminating spoofed addresses in the Internet ........... 5
   2.1. Host to link layer neighbor or switch ................ 7
   2.2. Upstream routers ...................................... 7
   2.3. ISP edge PE Router .................................... 8
   2.4. ISP NNI Router to ISP NNI Router ..................... 8
3. Verification and Accountability ............................ 8
4. Encouraging customer use of antispooﬁng procedures ...... 9
5. Accommodating incremental deployment ...................... 9
   5.1. ISP PE Router to CPE delivery point ................. 10
   5.2. ISP ﬁltering under attack ........................... 10
6. Identiﬁed Addresses in the Internet ....................... 10
   6.1. Identiﬁed addresses in edge networks ................. 11
      6.1.1. IEEE802.1X ....................................... 11
      6.1.2. IPv4 Address Resolution Protocol ............... 12
      6.1.3. IPv6 Neighbor Discovery ......................... 12
      6.1.4. IPv4 and IPv6 Dynamic Host Conﬁguration Protocol
             Access ............................................. 13
   6.2. Identiﬁed addresses in a global domain ............... 13
   6.3. On source addresses .................................... 13
7. IANA Considerations .......................................... 14
8. Security Considerations .................................... 15
9. Acknowledgements .......................................... 15
10. References .................................................. 15
    10.1. Normative References .................................. 15
    10.2. Informative References ................................ 16
Authors’ Addresses .............................................. 17
Intellectual Property and Copyright Statements ............. 18
1.  Introduction

This note proposes a practical solution to Internet Layer (which is to say IPv4 [RFC0791] and IPv6 [RFC2460]) source address verification. The purpose of such verification is to prevent attacks from using spoofed addresses and to facilitate the tracking of attack datagrams to the computers that send them. The source address verification problem is proposed and motivated in other papers on this topic [I-D.sava-problem-statement].

There are three contributions in this document. The first is a compilation of mechanisms available for source address verification at various points in the Internet, and an informal analysis of the confidence in the verification for each of those mechanisms. The second is the notion that source address verification can be negotiated between Internet entities based on this confidence in the source address verification mechanisms, and how source address verification can be used to accomplish goals such as attack avoidance and accountability for attacks. The third contribution is a way to incorporate source address verification into the Internet without requiring ubiquitous adoption of source address verification mechanisms.

1.1.  On attacks and attack management

The fundamental purpose of source address verification is the management of attacks. Attacks come in many forms, from malicious activities such as denial of service or service disruption, to more subtle forms of theft, to limiting the provision of service to one’s customers or clients. Source address verification can be used in two ways to manage attacks: to detect and reject IP datagrams with incorrect (‘spoofed’) source addresses, which cannot guide a response to a datagram to the system that sent it; and, to establish accountability for attacks using IP datagrams with valid source addresses.

The principal mode of attack in which a datagram with a spoofed source address is used is a single datagram attack; it is possible to spoof an address for the first exchange or a random exchange in a TCP session (as is done in TCP SYN and RST attacks), but given that nothing is known of how a peer replies to a datagram that was sent from a spoofed address, the further into such a session one goes the more difficult it is to maintain the illusion of coherence. Therefore, the first requirement is that the first datagram in a session have its address validated, and datagrams that fail this verification are ignored or dropped.

IT administrations want to be able to track a datagram to its source.
Reasons include isolating the zombie sources of an attack, or tracking malicious behavior to the user of a system. Removing IP datagrams with spoofed source addresses ensures that the remaining datagrams can be reliably traced back to their source.

This note will not go on to generalized attack management. Other papers, notably [I-D.ietf-idr-bgp-prefix-orf], and [RFC4778] address this; the matter will be left with them.

1.2. On Trust

Trust, in the Internet, is very much about relationships. Two companies or two parties that do not know each other may provide minimal services, such as access to a web page, but do not rely on each other. However, if a satisfactory relationship can be established, limited levels of trust are extended. For example, an ISP that contracts with its customer or another ISP to exchange BGP routing will open the session and advertise and accept routes. The ISP will also limit the routes it accepts (and therefore the trust it extends) to those specified in the agreement. Similarly, the group that administers an enterprise network is often different from the group that manages the company’s end systems. The level of trust between an enterprise network and the end systems it services is often similarly limited; the end systems are viewed as liabilities as much as they are clients.

This document is about the management of trust, and the level of trust that can be extended to a system that originates IP datagrams at the network layer. This trust differs from session trust, in which a user logs in to a remote system or service, but the two can be used together to accomplish useful things. Section 2.4 describes a method through which parties in the Internet such as service providers can negotiate the level of trust they are willing to assume in their exchange of Internet traffic. This method provides a practical way in which source address verification can be deployed and used in the Internet.

1.3. Glossary

The following acronyms are used in this document:

BGP: The Border Gateway Protocol, used to manage routing policy between large networks.

CPE Router: Customer Premises Equipment Router. The router on the customer premises, whether owned by the customer or the provider. Also called the Customer Endpoint, or CE, Router.
IP Address: An Internet Protocol Address, whether IPv4 or IPv6.

ISP: Internet Service Provider. Any person or company that delivers Internet service to another.

MAC Address: An Ethernet Address.

NNI Router: Network to Network Interface Router. This router interface faces a similar system operated by another ISP or other large network.

PE Router: Provider Endpoint Router. This router faces a customer of an ISP.

TCP: The Transmission Control Protocol, used on end systems to manage data exchange.

uRPF: Unicast Reverse Path Forwarding. A procedure in which the route table, which is usually used to look up destination addresses and route towards them, is used to look up the source address and ensure that one is routing away from it. When this test fails, the event may be logged, and the traffic is commonly dropped.

2. Eliminating spoofed addresses in the Internet

The first requirement is to eliminate datagrams with spoofed addresses from the Internet. Identifying and dropping datagrams whose source address is incompatible with the Internet topology at sites where the relationship between the source address and topology can be checked can eliminate such datagrams. For example, Internet devices can confirm that:

- The IP source address is appropriate for the lower layer address (they both identify the same system)
- The IP source address is appropriate for the device at the layer 2 switch port (the address was assigned to a, and perhaps the, system that uses that port)
- The prefix to which the IP source address belongs is appropriate for the part of the network topology from which the IP datagram was received (while the individual system may be unknown, it is reasonable to believe that the system is located in that part of the network).

Filtering points farther away from the source of the datagram can
make decreasingly authoritative assertions about the validity of the source address in the datagram. Nonetheless, there is value in dropping traffic that is clearly inappropriate, and in maintaining knowledge of the level of trust one can place in an address.

Figure 1: Points where an address can be validated

Figure 1 illustrates five places where a source address can be validated:

- Host to host or host to switch,
- Host to enterprise CPE Router,
- Enterprise CPE Router to ISP edge PE Router,
- ISP NNI Router to ISP NNI Router, and the
- ISP edge PE Router facing the destination CPE Router.

In general, datagrams with spoofed addresses can be detected and discarded by devices that have an authoritative mapping between IP addresses and the network topology. For example, a device that has an authoritative table between layer 2 and IP addresses on a link can discard any datagrams in which the IP address is not associated with (and is therefore assumed to be spoofed) the layer 2 address in the datagram. The degree of confidence in the source address depends on
where the spoofing detection is performed and the prefix aggregation in place between the spoofing detection and the source of the datagram. The means of building such an authoritative mapping is discussed further in Section 6.1.

2.1. Host to link layer neighbor or switch

The first point at which a datagram with a spoofed address can be detected is on the link to which the source of the datagram is connected. At this point in the network, the source layer 2 and IP addresses are both available, and can be verified against each other. A datagram in which the IP source address does not match the corresponding lower layer address can be discarded. Of course, the trust in the filtering depends on the trust in the method through which the mappings are developed. This mechanism can be applied by neighboring hosts, or by the first hop router.

On a shared medium link, the best that can be done is to verify the layer 2 and IP addresses against the mappings. When the link is not shared, such as when the hosts are connected through a switch, the source host can be identified precisely based on the port through which the datagram is received or the MAC address if it is known to the switch. Port identification precludes transmission of malicious datagrams whose layer 2 and IP addresses are both spoofed to mimic another host.

2.2. Upstream routers

After the first hop router, which can use the mechanism described in Section 2.1 to filter datagrams, subsequent routers may additionally filter traffic from downstream networks. Because these routers do not have access to the layer 2 address of the device from which the datagram was sent, they are limited to confirming that the source IP address is within a prefix that is appropriate for downstream router from which the datagram was received.

Options include the use of simple access lists or the use of unicast reverse path filtering (uRPF). Access lists are generally appropriate only for the simplest cases, as management can be difficult. Unicast RPF accepts the source address on a datagram if and only if it comes from a direction that would be rational to send a datagram directed to the address, which means that the filter is derived from routing. These filtering procedures are discussed in more detail in [RFC3704].
2.3. ISP edge PE Router

An obvious special case of the discussion in Section 2.2 is an ISP PE router, where it provides its customer with access. [RFC2827] specifically encourages ISPs to use ingress filtering to limit the incidence of spoofed addresses in the network.

The question that the ISP must answer for itself is the degree to which it trusts its downstream network. Appropriate answers include ‘not at all’ and ‘enough to only need to verify compliance’. A contract might be written between an ISP and its customer requiring that the customer apply the procedures of Section 2.1 the customer’s own network. ISPs might, for example, mark datagrams from customers that do not sign such a contract or demonstrably do not behave in accordance with it as ‘untrusted’. Alternatively, the ISP might place untrusted prefixes into a separate BGP community and use that to advertise the level of trust to its BGP peers.

2.4. ISP NNI Router to ISP NNI Router

The considerations of Section 2.3, which are explicitly related to customer networks, can also be applied to neighboring ISPs. A contract might be written between the companies that the companies will require the procedures of Section 2.1 of their customers and apply them within their own network. ISPs might, for example, mark datagrams from neighboring ISPs that do not sign such a contract or demonstrably do not behave in accordance with it as ‘untrusted’. Alternatively, the ISP might place untrusted prefixes into a separate BGP community and use that to advertise the level of trust to its BGP peers.

In this case, uRPF is less effective as a verification tool, due to asymmetric routing. However, when it can be shown that spoofed addresses are present, the procedure can be applied.

3. Verification and Accountability

Assuming filtering as above has been implemented, the origin of malicious IP datagrams can be determined. Within an organization or administrative domain, the details of where and how filtering is applied provide accountability and can be used to trace the origin of malicious datagrams back to the ultimate source or some region of the network. Between organizations or administrative domains, the agreement in place between organizations allows an entity that detects malicious traffic to assign responsibility for the origin of that traffic.
The use of formal agreements between organizations is discussed in more detail in Section 4.

4. Encouraging customer use of antispoofing procedures

As discussed in Section 1.2, the only operational circumstance in which an ISP can be said to trust its downstream is if it has an understanding (usually formalized in a contract) with the downstream regarding a matter. For example, an ISP that opens a BGP session with a downstream trusts the routes that the downstream presents it. The ISP may limit this trust, however, by verifying that the prefixes advertised by the downstream are appropriate for it to advertise. One might characterize this kind of relationship as ‘trust but verify’.

In the case of anti-spoofing procedures, an ISP might include in its service contract a provision that the customer agrees to use the procedures in Section 2.1, and where appropriate Section 2.2, to eliminate address spoofing. In this example of a contractual arrangement, the type of source address verification is specified in the service contract, and the customer implements those source address verification mechanisms. The ISP then verifies compliance using uRPF or other audits, and applies a penalty when the procedure results in the ISP dropping traffic. The penalty could be monetary, operational, or both.

Peer ISPs can develop a somewhat different form of service contract, in which each ISP guarantees that it will identify traffic or the source prefixes of customers have not implemented source address verification, and that the ISPs have implemented the appropriate checks to confirm that verification.

5. Accommodating incremental deployment

In the Internet, new technologies are inevitably deployed incrementally. Source address verification is no exception. This incremental deployment is problematic in the case of source address verification, in that aggregated traffic flows include both verified and unverified traffic. But simply dropping unverified traffic is unacceptable, as it prevents any form of incremental deployment. What is needed is a way to aggregate and deliver verified and unverified traffic, while retaining the ability to differentiate between those two types of traffic.
5.1. ISP PE Router to CPE delivery point

A simple operational differentiation that can be applied to traffic from untrusted downstream networks (those who have not signed a contract such as described in Section 4, or who are demonstrably not in compliance with it) is to mark traffic from them as ‘untrusted’. A simple approach would use a DSCP value [RFC2474] indicating that the datagram is from an untrusted source and therefore potentially contains a spoofed source address.

The ultimate use of the ‘Untrusted’ DSCP value is at choke points in the infrastructure, usually at network egress. Denial of Service attacks using spoofed addresses often target choke points. By classifying untrusted traffic and running it through a queue of lower priority or rate, one can preserve the services of trusted senders, and squeeze out potentially-spoofed traffic.

Thus, the use of the ‘Untrusted’ DSCP value both denies the untrusted user the enjoyment of network services end to end and permits prejudicial classification to give them distinctly poor service when they are potentially part of an attack. This, along with monetary incentives, incents them both to become trusted and trustworthy communication partners.

5.2. ISP filtering under attack

Another approach, if the prefixes of untrusted sources are advertised between ISPs using an appropriate BGP community, would be for a network under attack (or whose customers are under attack) to temporarily block untrusted prefixes and then add them back piecemeal. If the attack is sourced from an untrusted prefix, dropping the traffic will protect against the attack, and upon restoration of the prefix the attack should again be observable. This obviously only works as described with continuous attacks, but it can be helpful in isolating punctuated attacks as well.

6. Identified Addresses in the Internet

The document Internet Architectural Guidelines [RFC3439] focuses on a number of principles that have been used to beneficial effect in the design of the Internet. An important one is the Simplicity Principle, which asserts that complexity is the primary factor that limits the ability of a system to scale to large populations. Another is the Coupling Principle, which is borrowed from Information Theory and asserts that as systems get larger, they often exhibit increased interdependence (coupling) between components.
The design principle that has fostered the economic vitality of the Internet is the localization of information on a ‘need to know’ basis, with a view to limiting unnecessary complexity and interaction. In this context, making the Internet scale to large numbers of users calls on us to limit knowledge of individual users to the organizations they are part of, and to limit knowledge of individual systems to the networks in which they reside. In other networks within the Internet system, we scale the Internet by carrying knowledge of the networks, or of important characteristics of relationships such as whether a user or system is trusted or not.

As such, we divide the problem of address identification into two parts: identification of a user within the network that provides him service, whether that is an enterprise network, residential ISP, or other network, and the identification of other networks.

6.1. Identified addresses in edge networks

A common IT requirement is for an enterprise or residential ISP to restrict service to its authorized users or customers. Numerous procedures have been used for this, such as DHCP Authentication and the definition of names in carried in DHCP requests. While any adequate user management system could be used by the enterprise, at this point the state of the art appears to be the use of IEEE 802.1X access control, which associates a user with a MAC address and can be used with IPv4 or IPv6.

6.1.1. IEEE802.1X

IEEE 802.1X [IEEE802.1X] is an IEEE standard for port-based Network Access Control; it is part of the IEEE 802 (802.1) group of protocols. It provides authentication to devices attached to a LAN port or wireless access point, establishing a point-to-point connection or preventing access from that port if authentication fails.

802.1X is available on network switches, and can be configured to authenticate hosts that are equipped with supplicant software, denying unauthorized access to the network at the data link layer.

On wireless access points, 802.1X can be used in certain situations where an access point needs to be operated as a closed access point. The authentication is usually done by a third-party entity, such as a RADIUS server. This provides for client-only authentication, or more appropriately, strong mutual authentication using protocols such as EAP-TLS [RFC3748].

Upon detection of the new client (supplicant), the port on the switch
(authenticator) will be enabled and set to the ‘unauthorized’ state. In this state, only 802.1X traffic will be allowed; other traffic, such as DHCP and HTTP, will be blocked at the data link layer. The authenticator sends the EAP-Request identity to the supplicant, to which the supplicant replies using the EAP-Response datagram that the authenticator will forward to the authenticating server. The authenticating server can accept or reject the EAP-Request; if it accepts the request, the authenticator will set the port to the ‘authorized’ state and normal traffic will be allowed. The supplicant logs off by sending an EAP-Logoff message to the authenticator. The authenticator will then set the port to the ‘unauthorized’ state, once again blocking all non-EAP traffic.

The effect of such mutual authentication is two-fold. First, the network (wired or wireless) can determine whether a person that is seeking attachment of his system is authorized to do so. Also, the person’s computer can determine whether the point of attachment is a rogue access point or is in fact the network it intends to enter. As a side-effect of such authentication and authorization, server logs can be scanned at any time to determine what user was associated with any given system or MAC address and what IP (version 4 or 6) addresses are in use by those same MAC addresses, or such information can be logged in a search database for forensic purposes.

6.1.2. IPv4 Address Resolution Protocol

ARP [RFC0826] carries mappings between layer 2 and IP addresses, which can be used by nodes to construct a table of associations between layer 2 and IP addresses for other nodes on the same link. A switch can intercept and examine ARP traffic as well to determine the layer 2 and IP addresses of nodes attached to its ports.

However, as ARP is not secured in any way, the associations learned through ARP are not highly trustable. It is easy to construct ARP messages that can alter the ARP tables in nodes so the source addresses in a datagram appear to be valid.

6.1.3. IPv6 Neighbor Discovery

The Neighbor Discovery protocol [RFC2461] (ND), which is part of the IPv6 protocol suite, provides address resolution functions and supports address assignment. In much the same way as ARP can be used to learn associations between layer 2 and IPv4 addresses, the contents of ND messages can be used to learn associations between layer 2 and IPv6 addresses.

SEcure Neighbor Discovery [RFC3971] (SEND) can be used to authenticate the associations between layer 2 and IPv6 addresses.
6.1.4. IPv4 and IPv6 Dynamic Host Configuration Protocol

DHCP [RFC2131][RFC3315] can also be used to learn associations between layer 2 and IPv4 or IPv6 addresses. In this method, network elements that actively transmit DHCP messages (‘DHCP relay agents’; typically a router) or forward DHCP messages (switches) between a DHCP server and hosts examine the contents of the DHCP messages and extract the associations between the layer 2 and IPv4 or IPv6 for hosts. The layer 2 and IP addresses are contained in or can be deduced from the forwarded DHCP messages. In many situations, the network path between the router/switch and the DHCP server is secure, so the information extracted from the DHCP messages is considered more reliable than information taken from ARP or ND.

6.1.5. Protocol for Carrying Authentication for Network Access

PANA [I-D.ietf-pana-pana] is related to IEEE802.1X, in that it authenticates the identity of a user and uses that authenticated identity to authenticate the association between a layer 2 address and an IP address. PANA differs from IEEE802.1X in that it is carried as a layer 4 protocol, and can be used across intermediate network elements to an authenticating device. As a side effect of PANA authentication, the authenticating device can derive a layer 2 to IP address association for later use in detecting spoofed traffic.

6.2. Identified addresses in a global domain

In accordance with the design principles of the Internet, users in one network are generally not visible to other network administrations. Rather, the administration of one network will refer questions of identity to the administration serving a user or system.

That said, once source address spoofing has been eliminated, the source address of a datagram can be used to identify the domain from which it originated, and as a result what network administration must be contacted if it appears to be misbehaving. This is the proper use of WHOIS service; IANA and the relevant RIR, or in some cases the NIR or LIR or local ISP, can identify the administration a prefix has been assigned to and provide contact information.

6.3. On source addresses

It is seductive to think of this as providing the ability to use this technology to trace a datagram to the person who originated it. For several reasons, the technology can be used to derive circumstantial evidence, but does not actually solve that problem.
In the network layer, the source address of a datagram is the address of the system that originated it and to which any reply is expected to come. But systems fall into several broad categories. Many are single user systems, such as laptops and PDAs. Multi-user systems are commonly used in industry, and a wide variety of middleware systems and application servers have no user at all, but by design relay messages or perform services on behalf of users of other systems.

Two simple examples middleware relays are SMTP (Electronic Mail) and peer-to-peer file sharing. In SMTP, an email sent by a user is generally presented to a succession of intermediaries, which are called Mail Transfer Agents or MTAs. While the email was originated by a person, the network address used on each successive MTA-MTA transfer is that of the MTA. BitTorrent File Sharing may determine that a number of requests for a given file are coming from a given topological region in the network and push the file to a system it happens to know is located near there – without the knowledge of the originator of the file, the user whose system it was pushed from, the user whose system it was pushed to, or any potential future requester of the file. In both cases, the network layer address has no relationship to the application layer user, and in the latter case the presence of the file on a given system does not imply that the user of the system knows it is there or has any intent to use it.

Any association of an Internet address with a user is at best circumstantial; it may identify a set of obvious suspects, but it does not identify the user, and in many applications does not limit the set of suspects to the obvious ones. Examples of personal identifications in Internet messages may be found in DKIM [I-D.ietf-dkim-base], SMIME [RFC1847], and Open PGP [RFC2440], among others.

7. IANA Considerations

This memo adds no new IANA considerations. That said, one could imagine a future specification requesting a common DSCP identifying datagrams from untrusted sources based on an appropriate description of the relevant PHB.

Note to RFC Editor: This section will have served its purpose if it correctly tells IANA that no new assignments or registries are required, or if those assignments or registries are created during the RFC publication process. From the author’s perspective, it may therefore be removed upon publication as an RFC at the RFC Editor’s discretion.
8. Security Considerations

The security issues this document imposes are not worse than existing security behavior. The use of ARP, and DHCP are not currently secured, which may be an open attack vector. Neighbor Discovery is similarly unsecured, but Secure Neighbor Discovery is usable in the context. The mechanics of securing address assignment and announcement is considered a separate issue from the subject matter of this paper, but is material to its usefulness.

The security considerations of RFCs 2474 and 2475 apply, as this uses the Differentiated Services Architecture.

In any discussion of identity, an important issue is the chain of trust and the anchor of that chain. In this context, the chain of trust is Internet routing, and the anchor of that chain is the system that verifies the source address used by its downstream peer. As such, the first step - the verification of the source address by the immediate neighbor of an end system - is of paramount importance, and any check after that point is of lower efficacy. That said, the first system that can be said to be trusted by any administrative entity is the ingress system under its control. As such, each enterprise and ISP en route is responsible for its own security and must implement a verification procedure to ensure its own compliance.

9. Acknowledgements

The discussion of contracts and DSCP markings was first proposed by Steve Crocker in [Crocker].

The discussion of BGP Communities derives from discussions with Barry Greene.

The description of IEEE 802.1X was adapted from the Wikipedia article on the topic. Paul Gleichauf added comments on trust and trust management. Pekka Savola performed a detailed review.

10. References

10.1. Normative References


[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering:
Defeating Denial of Service Attacks which employ IP Source Address Spoofing”, BCP 38, RFC 2827, May 2000.

10.2. Informative References


Authors’ Addresses

Fred Baker  
Cisco Systems  
Email: fred@cisco.com

Ralph Droms  
Cisco Systems  
Email: rdroms@cisco.com