Messaging, Malware and Mobile Anti-Abuse Working Group

M^{3}AAWG Policy Issues for Receiving Email in a World with IPv6 Hosts

September 2014

Internet mail anti-abuse efforts have often relied on the reputation associated with a sending host's IPv4 address. This reputation data provides an identifier for active agents in email handling. Although less stable and less reliable than would be preferred, IPv4 addresses have proved useful for rate limiting and reputation assessment, and most anti-abuse systems will be unable to function if the effectiveness of these mechanisms are degraded. Over the years, there has been a continuing effort to develop reputation assessment based on the more stable alternative of domain names, with or without associating an IP address. The advent of IPv6 addresses makes this essential, along with improved address-based mechanisms.

M^{3}AAWG encourages the industry's development of technologies, policies and procedures to address this concern for relaying email across administrative domains by pursuing the targeted efforts described here. These efforts will provide a solid foundation for building and operating integrated Internet mail and anti-spam systems that include IPv6 in the operational mix. The goals are: to aggregate the massive address space into more easily trackable assignments, to require operators to identify hosts intended to act as outbound mail transport agents (MTAs), and to require a valid domain authentication-based identifier for reputation assessment.

M^{3}AAWG acknowledges that work is needed to make it possible to satisfy these goals while ensuring the maintenance of a globally-integrated and seamless Internet mail service. It is our hope that standards organizations and the wider Internet community will work with us and use this document as an initial list of requirements for future services that will allow full and robust mechanisms addressing these goals.

Tracking and Actioning Aggregate IPv6 Assignments Instead of Individual /128 Addresses

Under IPv4, anti-spam mechanisms use the full /32 address by default. It is not feasible to continue using these mechanisms under IPv6 with its /128 addresses. Mechanisms attempting to track every /128 address face scaling challenges that make them impractical and the ability to send each individual email from a unique /128 address renders such mechanisms ineffective.

IP-address based anti-spam mechanisms, such as connection rate limiting or blacklisting, must aggregate a sufficiently large range of IPv6 addresses into a single entity in order to remain effective. However, selecting too large an address range will result in false positives, as the anti-spam mechanism will inappropriately act on the MTAs of unrelated actors as if they were a single entity. Ideally, ISPs will publish their aggregation sizes via a standard, open service. Anti-spam mechanisms could query this service to learn the appropriate range for aggregating IPv6 addresses within a given ISP's allocation. Alternatively, conventions for common aggregation boundaries would provide workable guidance to anti-abuse analysis efforts.

M^{3}AAWG calls on the wider Internet community to collaborate on developing and standardizing methods of determining operator address aggregation.

As an initial heuristic, M^{3}AAWG recommends using /64 as the minimum default assignment size. According to RFC 4291 (http://tools.ietf.org/search/rfc4291) the first 64 bits of an IPv6 unicast address identifies the routing prefix and subnet, and the second 64 bits identify the individual interface. It is unlikely that a single interface will contain the MTAs of multiple actors who send a significant volume of email. An anti-spam mechanism can use /64 assignments as the default minimum granularity to limit the number of entities it tracks while still taking reasonable precautions to avoid false positives. Operators are, of course, at liberty to act on larger or smaller range sizes where they feel it is appropriate, and we expect that anti-spam vendors will collect and provide data on assignment sizes as part of their services in the absence of, or in addition to, a standard assignment size query service.

Rejecting Email from Hosts Not Identified as an Outbound MTA

Malicious actors send large quantities of abusive email from networks of compromised hosts, commonly referred to as botnets. The actual owners of these compromised hosts seldom intend for them to act as outbound MTAs. If mail acceptance can be limited to sources that are explicitly authorized, it greatly reduces the value of compromised hosts. Note that implementing M^{3}AAWG recommendations on managing outbound port 25 (http://www.maawg.org/sites/maawg/files/news/MAAWG_Port25rec0511.pdf) will prevent email being sent from compromised hosts within their allocations. However, all operators are not able or willing to implement those recommendations. The number of vulnerable devices will increase dramatically as the Internet of Things becomes a reality, so an efficient defensive measure to aid inbound systems is needed.

There is currently no simple and standard method for an operator to identify the hosts that are intended to act as outbound MTAs. Sender Policy Framework (SPF) is a standard technique for a domain owner to identify authorized outbound MTAs, but it also permits malicious domain owners to identify large ranges of IP space that they do not actually own. M^{3}AAWG calls on the wider Internet technical community to collaborate on developing and standardizing a method for operators to identify outbound hosts. This method must result in a resource that can be queried in an automated manner based on only the IP address attempting to initiate an SMTP session at the time the session is initiated and which can be easily published and maintained by the owners of the address space.

Many operators configure their inbound MTAs to reject connection attempts from IP addresses without reverse DNS (PTR) records, or at least to consider email from such IP addresses highly suspicious. This technique can be an even more effective high-pass filter under IPv6. This is the case even though operators are unlikely to publish reverse DNS records for the vast majority of the IPv6 addresses in their allocation, since there is limited benefit to doing so and the process is cumbersome due to the large number of addresses. In contrast the number of hosts dedicated to relaying email across administrative boundaries is quite small by comparison, as is the number of addresses they use, and it is feasible for operators to publish and maintain reverse DNS records for this smaller set of dedicated IP addresses.

In the absence of a more appropriate mechanism for identifying hosts intended to act as outbound MTAs by their owners, M^{3}AAWG recommends rejecting email from host IPv6 addresses without reverse DNS records. This technique should be deprecated once a more suitable standard mechanism is developed.

Rejecting Email without Valid Domain Authentication

The need for more stable, more accurate reputation identifiers is even greater under IPv6 than IPv4. Even with IPv4, domain names are considerably more stable than are IP addresses.

Domain Keys Identified Mail (DKIM) (http://tools.ietf.org/html/rfc6376) and SPF (http://www.ietf.org/rfc/rfc4408.txt) are widely deployed domain authentication methods for email. They provide an authenticated domain for operational accountability. These include the 'd=' value in the case of DKIM and the envelope MAIL FROM domain (or EHLO domain for bounces) in the case of SPF that operators can use as an identifier for reputation assessment.

Large providers have already successfully implemented domain reputation as a companion to IP address reputation and enhancement to their overall email filtering systems. (See http://www.ceas.cc/2006/19.pdf).

M^{3}AAWG therefore recommends moving toward rejecting email that does not contain a valid DKIM signature or that does not pass SPF checks in order to enable consistent and reliable use of authenticated domain reputation for delivery decisions.

Accountable Domains

M^{3}AAWG also considers the accuracy of WHOIS information to be a critical component of a domain's reputation and complete WHOIS information for domains acting as SMTP clients needs to be mandatory. Operators should ensure that their records are in good order and include working abuse contact information.

Operators should also pay close attention to the output of the IETF WEIRDS working group (Web Extensible Internet Registration Data Service at https://datatracker.ietf.org/wg/weirds/charter/), which is developing a new standard to replace WHOIS.

Conclusion

This paper identifies basic IPv6 anti-spam issues and includes a few recommendations. It is intended as an initial list of requirements for further technical work to address these issues within the broader Internet technical community. Some of this can occur within M^{3}AAWG and in other Internet organizations. Those interested in pursuing IPv6 anti-abuse work in M^{3}AAWG can contact the organization through the Contact Us form at www.m3aawg.org.

M3AAWG084