Workgroup: opsec
Internet-Draft:
draft-gont-opsec-ipv6-addressing-00
Published: 2 February 2023
Intended Status: Informational
Expires: 6 August 2023
Authors: F. Gont
SI6 Networks

G. Gont
SI6 Networks

Implications of IPv6 Addressing on Security Operations

Abstract

The increased address availability provided by IPv6 has concrete implications on security operations. This document discusses such implications, and sheds some light on how existing security operations techniques and procedures might need to be modified accommodate the increased IPv6 address availability.

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 6 August 2023.

Table of Contents

1. Introduction

The main driver for the adoption of the IPv6 protocol suite is its increased address space, which can provide a virtually unlimited number of public addresses for every device attached to the public Internet.

IPv6 addresses [RFC4291] can differ in a number of properties, such as address scope (e.g. link-local vs. global), stability (e.g. stable addresses vs. temporary addresses), and intended usage type (outgoing communications vs. incoming communications).

IPv6 hosts may configure and use multiple addresses with different combinations of the aforementioned properties, depending on the local host policy and the local network policy. For example, in network where SLAAC is employed for address configuration, host will typically configure one stable address and one (or more) temporary addresses per network interface, for each prefix advertised advertised for address configuration. On the other hand, for networks that employ stateful configuration, it is quite common for hosts to configure one address per network interface.

Section 2 discusses the semantics of IPv6 addresses in terms of the entity or entities the identify, according to the deployed Internet. Section 3 discusses the usage of IPv6 addresses in security operations. Section 4 discusses the implications of IPv6 addressing on security operations.

2. The Semantics of IPv6 Addresses and IPv6 Prefixes

As noted in Section 1, IPv6 hosts typically configure multiple addresses with different properties. One of the most common deployment scenarios is that in which the subnet employs SLAAC

[RFC4862] for address configuration, and where hosts configure both stable [RFC8064] [RFC7217] and temporary [RFC8981] addresses. From this perspective, it is clear that multiple addresses may correspond to the same IPv6 host.

While rather uncommon for legitimate use cases, an IPv6 host may actually employ a larger address block. For example, it is common for ISPs to lease a /56 or /48 to each subscriber, and thus a skilled user could readily employ the leased prefix in a single or multiple IPv6 hosts (whether virtual or not).

On the other hand, while one might assume an IPv6 address would correspond to at most one host (strictly speaking, to one network interface of a host), this is not necessarily the case in the deployed Internet since e.g. deployments that employ "Network Address Port Translation + Protocol Translation" (NAPT-PT) [RFC2766] for IPv6 are not uncommon, whether along with technologies such as Kubernetes, or in IPv6-enabled VPNs. Thus, a single IPv6 address may actually correspond to or identify multiple IPv6 systems.

3. Security Operations

3.1. Access Control Lists (ACLs)

It is common for network deployments to implement any of these types of ACLs:

- *Allow-lists

- *Block-lists

Allow-lists are typically employed as part of a defense-in-depth strategy, where access to specific resources is allowed only when requests originate from specific IP addresses or prefixes. For example, an organization may employ a Virtual Private Network (VPN), and require that certain resources be accessed via the VPN, by enforcing that requests originate from the IP address (or addresses) of the VPN concentrator.

On the other hand, block-lists are typically implemented to mitigate threats. For example, a network firewall might be fed with an IP reputation block-list that is dynamically updated to reflect the IP address (or addresses) of known or suspected attackers.

Both types of ACLs have a similar challenge in common: identifying the minimum set of addresses that should be employed in the ACLs definition such that the ACLs can successfully enforce the controls they are expected to enforce. For example, in the case of allow-lists, the corresponding ACLs should encompass possible legitimate changes in the set of "valid"/allowed addresses, thus avoiding false

negatives (i.e., incorrectly preventing access to legitimate users). On the other hand, in the case of block-lists, the ACLs should encompass the attacker's ability to use different addresses (or vantage points), while minimizing false positives (i.e., incorrectly blocking legitimate users).

3.2. Network Activity Correlation

Another fundamental aspect of security operations is that of network activity correlation (at times with the goal of attribution). That is, an analyst may want or need to infer the relationship among different network activities, and possibly assess whether they can be attributed to the same entity or attacker. This may be necessary for security investigations, but also to e.g. subsequently mitigate a threat by enforcing ACLs that block the alleged attacker.

4. Implications of IPv6 Addressing on Security Operations

4.1. Access-Control Lists

When implementing an allow-list, it may be necessary to specify it with a granularity of /64 -- that is, an entire /64 might need to be "allowed", since the target host(s) might employ multiple addresses from the same /64 over time (e.g., as a result of temporary addresses [RFC8981]). However, since sunch IPv6 prefix would be shared by other hosts in the same subnet, this would mean that the ACL would have coarse-granularity (i.e., all hosts (or none) would be part of the allow-list -- which is probably unacceptable in many cases.

In some scenarios, a network administrator might be able to disable the use of temporary addresses [RFC8981] via e.g. group policies [GPO], or request/enforce the use of DHCPv6 [RFC8415], thus having more control on the addresses employed by local hosts. In these specific cases, it might be possible to implement an allow-list for a host by specifying a single IPv6 address (i.e., a /128).

On the other hand, implementing block-lists can be tricky. For example IP reputation lists (whether commercial or not) are commonly employed in the deployed Internet. However, these lists generally specify offending addresses as /128, as opposed to a network prefix. This means that an attacker could simply regularly change his/her IPv6 address, thus reducing the effectiveness of these lists. Additionally, a side effect of an attacker regularly changing his/her address is that the block-list might grow to such an extent that the list might have to be trimmed (as a result of implementation constraints), with the aforementioned transient addresses consuming available "slots" in the IP reputation block-list.

Similarly, tools of the kind of [fail2ban] are commonly employed by system administrators to mitigate e.g. brute-force authentication attacks by banning IP addresses after a certain number of failed authentication attempts. These tools might ban IPv6 addresses on a /128 granularity, thus meaning that an attacker could easily circumvent these controls by changing the attacking address every few attempts (e.g. before an address becomes blocked). Additionally, as with the IP reputation lists previously discussed, an attacker performing a brute force attack *and* regularly changing his/her address could make the block-list grow to an extent where it might negatively affect the system enforcing the block-list, or might cause other valid entries to be discarded in favor of the transient IPv6 addresses.

One might envision that IPv6 reputation lists might aggregate a large number of offending IPv6 addresses into a prefix that encompasses them. However, this practice is really not widespread, and might also increase the number of false positives. Thus, it is possibly a topic for further research.

4.2. Network Activity Correlation

Performing IPv6 network activity correlation can be very tricky, since the semantics of an IPv6 address in terms of what it might correspond to (see Section 2) can be complex. As discussed before, a single IPv6 address could correspond to either a single host, or multiple hosts behind an IPv6 NAPT-PT device -- in a way, this being similar to IPv4 scenarios.

However, multiple IPv6 addresses might or might not represent multiple systems. In some cases, some heuristics might help infer whether a group of addresses belonging to a /64 correspond to the same node. However, as the addresses become more sparse (e.g., a user or attacker leverages a /48), this may be more challenging. And, while some heuristics could be employed to perform network activity correlation across multiple addresses, most tools commonly used in the deployed Internet do not implement this kind of features.

5. Security Considerations

This entire document is about the implications of IPv6 addressing on Security Operations. It analyzes the impact of IPv6 addressing on a number of security operations areas, raising awareness about the associated challenges, and hopefully fostering developments in these areas.

6. Acknowledgements

The authors of this document would like to thank (in alphabetical order) [TBD] for providing valuable comments on earlier versions of this document.

This document borrows some text and analysis from [I-D.gont-v6ops-ipv6-addressing-considerations], authored by Fernando Gont and Guillermo Gont.

Fernando would also like to Nelida Garcia and Jorge Oscar Gont for their love and support.

7. References

7.1. Normative References

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006, <https://www.rfc-editor.org/info/rfc4291>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007, <https://www.rfc-editor.org/info/rfc4862>.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014, <https://www.rfc-editor.org/info/rfc7217>.

[RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/RFC8064, February 2017, <https://www.rfc-editor.org/info/rfc8064>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

[RFC8981] Gont, F., Krishnan, S., Narten, T., and R. Draves, "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6", RFC 8981, DOI 10.17487/RFC8981, February 2021, <https://www.rfc-editor.org/info/rfc8981>.

7.2. Informative References

[fail2ban] fail2ban, "fail2ban project", <https://www.fail2ban.org/>.

[GPO] Microsoft, "Windows Server 2012 R2 and Windows Server 2012", 2016, <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831791(v=ws.11)>.

[I-D.gont-v6ops-ipv6-addressing-considerations] Gont, F. and G. Gont, "IPv6 Addressing Considerations", Work in Progress, Internet-Draft, draft-gont-v6ops-ipv6-addressing-considerations-02, 1 June 2022, <https://www.ietf.org/archive/id/draft-gont-v6ops-ipv6-addressing-considerations-02.txt>.

[RFC2766] Tsirtsis, G. and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, DOI 10.17487/RFC2766, February 2000, <https://www.rfc-editor.org/info/rfc2766>.

Authors' Addresses

Fernando Gont
SI6 Networks
Evaristo Carriego 2644
1706 Haedo
Provincia de Buenos Aires
Argentina

Email: fgont@si6networks.com
URI: https://www.si6networks.com

Guillermo Gont
SI6 Networks
Evaristo Carriego 2644
1706 Haedo
Provincia de Buenos Aires
Argentina

Email: ggont@si6networks.com
URI: https://www.si6networks.com