January 2019 – Version 1.0

IPv6 Security

Frequently Asked Questions (FAQ)

Author
Fernando Gont

Internet Society

Executive Summary

The Internet Society recognises that global deployment of the IPv6 protocol is paramount to accommodate the present and future growth of the Internet. Given the scale at which IPv6 must be deployed, it is important that the possible security implications of IPv6 are well understood and considered during the design and deployment of IPv6 networks, rather than as an afterthought. This document is organized as a list of frequently asked questions about IPv6 security, providing answers and highlighting the most important aspects of IPv6 security.

1. General Aspects of IPv6 Security

1.1. Is IPv6 more secure than IPv4?

No, but the question (as such) is probably irrelevant and rather imprecise since it may refer to at least two very different things:

- Whether the IPv6 protocols are (specifications wise) more secure than their IPv4 counterparts, or,
- Whether IPv6 deployments are more secure than their IPv4 counterparts

If one compares IPv6 and IPv4 at the protocol level, one may probably conclude that the increased complexity of IPv6 results in an increased number of attack vectors – that is, more possible ways to perform different types attacks. However, a more interesting and practical question is how IPv6 deployments compare to IPv4 deployments in terms of security. In that sense, there are a number of aspects to consider:

- Maturity of protocol specifications
- Maturity of implementations
- Confidence/experience with the protocols
- Support in security devices and tools

Most security vulnerabilities related to network protocols are based on implementation flaws, such as the so called “buffer overflows” or the failure to graciously process specially-crafted packets. Typically, security researchers find vulnerabilities in protocol implementations, which eventually are “patched” to mitigate such vulnerabilities. Over time, this process of finding and patching vulnerabilities results in more robust implementations. For obvious reasons, the IPv4 protocols have benefited from the work of security researchers for much longer, and thus IPv4 implementations are generally more robust than their IPv6 counterparts.

In some cases, vulnerabilities are based on flaws in the actual protocol specifications -- whether because the standards specify vulnerable mechanisms, or because they lack appropriate advice to prevent vulnerable implementation approaches. Whilst there has recently been significant work to mitigate vulnerabilities in the IPv6 protocol specifications, they have not yet received the same level of scrutiny than their IPv4 counterparts -- hence there might still be protocol design flaws to be addressed.

Besides the intrinsic properties of the protocols, the security level of the resulting deployments is closely related to the level of expertise of network and security engineers. In that sense, there is obviously much more experience and confidence with deploying and operating IPv4 networks than

with deploying and operating IPv6 networks -- and this has a concrete impact on the security properties of the resulting deployments.

Finally, implementation of IPv6 security controls obviously depends on the availability of features in security devices and tools. Whilst there have been improvements in this area, it is normally still the case that there is a lack of parity in terms of features and/or performance when considering IPv4 and IPv6 support in security devices and tools. Where such lack of parity exists, the ability to produce secure/resilient deployments is hindered.

1.2. My network is IPv4-only. Should I worry about IPv6 security?

Your network is, most likely, dual-stack and **not** IPv4-only. Therefore, regardless of whether your network has global IPv6 connectivity or not, most nodes on your network probably support IPv6. This means that nodes in your network may already employ IPv6 for local traffic, and they might also inadvertently employ IPv6 for non-local traffic if an attacker enables global IPv6 connectivity on your network. IPv6 might also lead to VPN traffic leakages if VPN implementations without appropriate IPv6 support are employed. Please check [RFC7123] and [RFC7359] for further details.

1.3. Should I expect increased usage of IPsec with IPv6?

No. Former IPv6 specifications ([RFC4294]) required all nodes to include support for IPsec. This, together with the expected ability to employ native IPsec in IPv6 networks (typically prevented in the IPv4 world by NATs), possibly led to the expectation that IPsec usage would become widespread.

However,

- The IETF eventually standardized the tunneling of IPsec over UDP (see [RFC3948]), removing the barrier of IPsec deployment on IPv4 networks.
- The requirement to support IPsec did not imply a requirement to actually use it. And, in any case, such requirement was formally removed in subsequent revisions of the IPv6 specifications (see [RFC6434]).
- IPsec employs Extension Headers, which typically result in packet drops when employed on the public Internet (see [RFC7872]).

Thus, the motivations and barriers for employing IPsec are essentially the same in IPv4 and IPv6, and there is nothing suggesting that IPsec usage will increase as a result of IPv6 deployment.

2. IPv6 Security Assessment

2.1. What security assessment tools may I use to assess my networks and devices?

There are at least three free and open source IPv6 toolkits:

- SI6 Networks' IPv6 Toolkit [SI6-Toolkit]
- The Hacker's Choice IPv6 Attack Toolkit [THC-IPv6]
- Chiron [Chiron]

2.2. Is it possible to address scan IPv6 networks?

It depends. IPv4 address scanning is typically done by brute force, since the search space is rather small (256 addresses in a /24, 65536 addresses in a /16, etc.). On the other hand, standard IPv6 subnets are /64s, resulting in an address space that is so large that becomes unfeasible to scan by brute force. However, there is empirical evidence that the addresses of IPv6 nodes may follow specific patterns:

- Infrastructure nodes (routers, servers, etc.) typically employ predictable addresses, such as "low-byte" addresses (2001:db8::1, 2001:db8::2, etc.)
- Client nodes (laptops, workstations, etc.) typically employ randomized addresses

Thus, infrastructure nodes can be easily discovered by means of "targeted" address scans, where scanning tools target specific address patterns. It is generally unfeasible though to address scan a network for client devices, since their addresses are randomized over a very large address space.

2.3. How should I perform IPv6 network reconnaissance?

If the target is a local subnet, the following techniques have been found to be effective:

- Multicasted probes (ICMPv6 echo, and crafted probe packets that elicit ICMPv6 error messages)
- Multicast DNS (mDNS) queries.

On the other hand, if the target is a remote network, the following techniques may be used:

- Pattern-based address scans
- DNS zone transfers
- DNS reverse mappings
- Certificate transparency framework
- Search engines

You can find more information about these and other techniques in [RFC7707] and [IPV6-RECON].

2.4. Is it possible to perform host-tracking attacks in IPv6?

It depends. Host tracking refers to the correlation of network activity as of hosts move across networks. Traditional SLAAC addresses required nodes to embed their MAC address in the IPv6 Interface Identifier, thus making IPv6 host tracking very trivial. Temporary addresses (see [RFC4941]) have mitigated part of the problem by providing randomized addresses that can be used for (client-like) outgoing communications, while stable-privacy addresses ([RFC7217]) replace traditional SLAAC addresses such that the problem is eliminated (please see [RFC8064]).

Over time, implementations have been moving towards the implementation of both temporary (RFC4941) and stable-privacy (RFC7217) addresses. However, you should check support for these standards in your operating system. Please check [RFC7721] for further discussion about the privacy implications of IPv6 addressing.

2.5. Does it make sense to employ unpredictable addresses (such as RFC7217) for servers?

There is an implicit trade-off between easy-to-remember predictable addresses, and hard-to-scan unpredictable addresses. It is normally up to the administrator to analyze the associated tradeoffs and convenience for each network scenario.

We note that it is frequently (and incorrectly) argued that unpredictable addresses are of no value for servers, since their addresses are published on the DNS. However, this is incorrect, since an attacker meaning to "target all servers in a given prefix" would have no easy way to achieve that goal if unpredictable addresses were employed (assuming other network reconnaissance techniques are mitigated).

2.6. How can I mitigate network reconnaissance based on DNS reverse mappings?

One option is to configure DNS reverse mapping only for systems that required it - mostly mail transfer agents (MTAs). Another option - if your DNS software supports it - is to configure wildcard reverse mappings, so that every possible domain name for the reverse mappings contains a valid PTR record.

3. First-Hop Security

3.1. Should I worry about Address Resolution and automatic-configuration attacks?

It depends. In principle, these attacks should be as much of a concern (or not) as ARP and DHCP attacks from the IPv4 world – that is, Neighbor Discovery and automatic-configuration attacks are the IPv6-equivalent of ARP-based and DHCP-based attacks from the IPv4 world. If ARP/DHCP attacks are a concern for your IPv4 network, then their IPv6 counterparts should also be a concern for your IPv6 networks.

Typical mitigations for Neighbor Discovery and automatic-configuration attacks are similar to the existing mitigations for the IPv4 version of these attacks. For example, RA-Guard [RFC6104][RFC6105] and DHCPv6-Shield/DHCPv6-Guard [RFC7610] are the IPv6-equivalent of DHCP-snooping.

3.2. What are the differences between SLAAC and DHCPv6 in terms of address logging?

When DHCPv6 is employed for address configuration, the DHCPv6 server typically maintains a log of IPv6 address leases. This means that in the event a host is compromised (e.g. by malware) and such behavior is detected, it is trivial to correlate the malicious activity to the infected node.

When SLAAC is employed though, there is no centralized log of IPv6 addresses since addresses are "auto-configured". If an address log is required, it must be implemented by means of additional software or some ad-hoc mechanism.

It is important to note that DHCPv6 does not prevent hosts from configuring addresses on their own (instead of requesting the address via DHCPv6). As a result, DHCPv6 logs should only be relied upon

for scenarios where nodes can be expected to cooperate with the network, and not for scenarios where an attacker may intentionally configure IPv6 addresses unilaterally to avoid logging.

3.3. Are RA-Guard and DHCPv6-Guard/Shield effective to protect against automatic-configuration attacks?

It depends. Many implementations of these mechanisms can be easily circumvented by means of IPv6 extension headers (see [RFC7113]. In some cases, evasion can be mitigated by dropping packets that contain an "undetermined transport" (in Cisco-speak).

Please check [SI6-RA6] for information of how to assess your RA-Guard implementation, and [CISCO-FHS] for details regarding how to avoid evasion of Cisco's implementation of RA-Guard.

3.4. Should I consider deploying Secure Neighbor Discovery (SEND) on my network?

No. At the time of this writing, there is virtually no support for SEND in any popular host operating system. Thus, regardless of other considerations (such as the possible "return of investment" of deploying SEND), it is currently unfeasible to deploy SEND.

3.5. What are Neighbor Cache Exhaustion (NCE) attacks, and how can they be mitigated?

NCE attacks aim at creating an arbitrarily large number of entries in the Neighbor Cache, such that that it is no longer possible to create new legitimate entries and therefore leading to a Denial of Service (DoS). NCE may also result as a side effect of an address scanning remote network, where the last-hop router creates one entry for each of the target addresses, thus eventually exhausting the Neighbor Cache. Depending on each specific implementation, NCE may cause the target device to become unresponsive, crash, or reboot.

One implementation-based mitigation is to limit the number of Neighbor Cache entries in the "INCOMPLETE" state. On the other hand, an operational mitigation for NCE attacks against nodes connected by point-to-point links is to enforce an artificial limit on the maximum number of entries in the Neighbor Cache by employing long prefixes (e.g., /127s) for the point-to-point link [RFC6164].

Please check [RFC6583] and [ND-INDEF] for further information.

4. Firewalling and Security Architectures

4.1. Will IPv6 cause a shift from a network-centric security paradigm to a host-centric security paradigm?

No, although the question is rather bogus. The security paradigm of IPv4 networks is not really "network-centric": for example, host-based firewalls are common-place, and they are typically employed along with network-based firewalls. IPv6 networks are will likely follow the same hybrid paradigm.

4.2. Will all my systems become exposed on the public IPv6 Internet if I deploy IPv6?

Not necessarily.

While virtually all IPv6 networks are likely to employ global address space, this need not imply any-to-any global-reachability. For example, IPv6 firewalls may be deployed at the same point of the network topology where IPv4 networks currently employ a NAT device. Such IPv6 firewall may enforce a filtering policy of "only allowing outgoing communications", thus resulting in similar host exposure as in IPv4 networks.

Please see [RFC6092] for recommended default security policies for residential CPEs.

4.3. In the IPv4 world, I normally black-list IPv4 addresses in response to malicious activity. What granularity should I use when blacklisting IPv6 addresses?

IPv6 hosts are generally able to configure any arbitrary number of IPv6 addresses within their /64 local subnet. In the event of malicious activity you should black-list at least the /64 from which you have detected malicious activity.

Depending on the specific upstream ISP, the attacker might have control of prefixes of any length between /48 and /64 (e.g., if the attacker gets a prefix delegated via DHCPv6-PD). Therefore, to the extent that is possible, if malicious activity persists after blacklisting the offending /64, you may want to block shorter prefixes (larger blocks of addresses) - e.g., start blocking a /64, and subsequently resort to blocking a /56 or /48 if necessary.

4.4. My systems/networks block IPv6 fragments for security reasons. Is this a safe practice?

It depends. Dropping IPv6 fragments is only safe when two conditions are met:

- You are only employing protocols that can avoid fragmentation -- e.g. TCP with Path-MTU Discovery
- You also block ICMPv6 "Packet Too Big" (PTB) error messages that advertise MTUs smaller than 1280 bytes

UDP-based protocols may rely on fragmentation, and thus it is generally not advisable to block fragmented traffic when such protocols are employed. Other protocols, such as TCP, may completely avoid the use of fragmentation by means of mechanisms such as Path-MTU discovery (see [RFC1981]).

ICMPv6 "Packet Too Big" error messages may trigger the use of fragmentation when they advertise an MTU smaller than 1280 bytes. Therefore, if IPv6 fragments are dropped, but ICMPv6 Packet Too Big error messages advertising an MTU smaller than 1280 bytes are not dropped, an attacker might leverage such ICMPv6 error messages to trigger fragmentation such that the resulting fragments get dropped, leading to a Denial of Service (DoS) condition.

Generation of IPv6 fragments in response to ICMPv6 PTB messages has been deprecated in the revised IPv6 specification [RFC8200], and thus eventually all implementations will eliminate this

feature and the associated vulnerability. However, you might be employing a legacy implementation that still implements the vulnerable behavior. Please see [RFC8021] for further details.

Note: the aforementioned mitigation implies the ability to filter ICMPv6 PTB error messages based their "MTU" field. Filtering packets at such granularity may or may not be possible.

4.5. I read about possible security issues associated with IPv6 extension headers. Should I drop packets containing IPv6 extension headers?

The recommended filtering policy for packets containing IPv6 extension headers depends on where in the network the filtering policy is to be enforced.

For example, if enforced on transit routers, to the extent that is possible you should refrain from dropping packets and only employ a blacklisting approach (to drop packets that are well-known to be problematic). On the other hand, if enforced on an enterprise network, you may want to allow only traffic that you are expecting to receive and hence employ a whitelisting approach.

[IPV6-EHS-F] contains advice on the filtering of IPv6 packets containing Extension Headers at transit routers. Additionally, it contains a security assessment of all standardized IPv6 extension headers and options, along with an analysis of any potential interoperability problems arising from the filtering of such packets.

4.6. How should I assess my networks and devices with respect to the use of extension headers to circumvent security controls?

Most IPv6 security toolkits provide support to craft attack packets with arbitrary IPv6 extension headers. For example, [SI6-RA6] explains the use of extension headers with Router Advertisement packets.

4.7. I run a dual-stack network. Which considerations should I have for the packet filtering policies?

In general, the security policies for the IPv6 protocols should match those of the IPv4 protocols. Unfortunately, many networks fail in this respect. Please see [IPV6-POL] for further discussion.

4.8. My systems employ both temporary (RFC4941) and stable (RFC7217) addresses. How should I implement IPv6 firewalling?

Allow outgoing connections from any address but incoming connections only to stable (E.G. [RFC7217]) addresses. Thus, addresses that become exposed as a result of client-like activities (such as web browsing) will not be usable for external systems to connect back or address scan to your internal nodes.

4.9. How can temporary addresses affect my ACLs?

Temporary addresses change over time. As a result, ACLs meant for nodes that employ temporary addresses will typically fail if specified as a single IPv6 address or group of addresses.

If such ACLs are to be enforced, some of the possible options include:

- Specify ACLs on a per-prefix basis (e.g., /64)
- Disable temporary addresses on the affected nodes
- Enforce the ACLs on the stable addresses, and configure nodes such that stable addresses are preferred over temporary addresses for the accessing the service/application described in the ACL

5. Resources

5.1. Are there any operational security guidelines for IPv6?

[OPSEC-V6] contains general IPv6 operational security considerations, whilst [RFC7381] contains Enterprise deployment guidelines.

5.2. Which forums may I use for discussing IPv6 security?

The following mailing-lists can be used to discuss IPv6 security topics:

- IPv6 Hackers [IPV6-HACKERS]
- IPv6 Operators Forum [IPV6-OPS]
- IETF OPSEC WG [OPSEC-WG]
- IETF V6OPS WG [V6OPS-WG]

Additionally, most Regional Internet Registries (RIRs) operate mailing lists that focus on IPv6 and/or network security.

6. Acknowledgements

Kevin Meynell and Jan Žorž provided valuable comments on a preliminary version of this document.

7. References

[Chiron] "Chiron - An IPv6 Security Assessment framework with advanced IPv6 Extension Headers manipulation capabilities".
https://github.com/aatlasis/Chiron

[CISCO-FHS] "FHS".
http://docwiki.cisco.com/wiki/FHS

[IPV6-EHS-F] Gont, F., Liu, W., "Recommendations on the Filtering of IPv6 Packets Containing IPv6 Extension Headers", IETF Internet-Draft (draft-ietf-opsec-ipv6-eh-filtering), work in progress.
https://tools.ietf.org/html/draft-ietf-opsec-ipv6-eh-filtering

[IPV6-RECON] Gont, F., "How to perform IPv6 network reconnaissance", TechTarget article, July 2015.
https://searchsecurity.techtarget.com/tip/How-to-perform-IPv6-network-reconnaissance

[IPV6-OPS] IPv6 Operators Forum Mailing List
http://lists.cluenet.de/mailman/listinfo/ipv6-ops/

[IPV6-POL] Gont, F., "What to do when IPv4 and IPv6 policies disagree", TechTarget article, August 2018.
https://searchsecurity.techtarget.com/tip/What-to-do-when-IPV4-and-IPv6-policies-disagree

[ND-INDEF] Jaeggli, J., "Indefensible Neighbors", IEPG Meeting - July 2018 @ IETF 102.
http://www.iepg.org/2018-07-15-ietf102/indefensible-neighbors.pdf

[OPSEC-V6] Vyncke, E., Chittimaneni, K., Kaeo, M., Rey, E., "Operational Security Considerations for IPv6 Networks", IETF Internet-Draft (draft-ietf-opsec-v6), work in progress, October 2018.
https://tools.ietf.org/html/draft-ietf-opsec-v6

[OPSEC-WG] Operational Security Capabilities for IP Network Infrastructure (OPSEC) Working Group Mailing List
https://www.ietf.org/mailman/listinfo/opsec

[RFC3948] Huttunen, A., Swander, B., Volpe, V., DiBurro, L., and M. Stenberg, "UDP Encapsulation of IPsec ESP Packets", RFC 3948, DOI 10.17487/RFC3948, January 2005.
http://www.rfc-editor.org/info/rfc3948

[RFC4294] Loughney, J., Ed., "IPv6 Node Requirements", RFC 4294, April 2006.
https://www.rfc-editor.org/info/rfc4294

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007.
https://www.rfc-editor.org/info/rfc4941

[RFC6092] Woodyatt, J., Ed., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", RFC 6092, DOI 10.17487/RFC6092, January 2011.
http://www.rfc-editor.org/info/rfc6092

[RFC6104] Chown, T. and S. Venaas, "Rogue IPv6 Router Advertisement Problem Statement", RFC 6104, February 2011.
http://www.rfc-editor.org/info/rfc6104

[RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., Mohacsi, J., "IPv6 Router Advertisement Guard", RFC 6105, February 2011.
http://www.rfc-editor.org/info/rfc6105

[RFC6164] Kohno, M., Nitzan, B., Bush, R., Matsuzaki, Y., Colitti, L., and T. Narten, "Using 127-Bit IPv6 Prefixes on Inter-Router Links", IETF RFC 6164, April 2011.
http://www.rfc-editor.org/info/rfc6164

[RFC6434] Jankiewicz, E., Loughney, J., and T. Narten, "IPv6 Node Requirements", RFC 6434, DOI 10.17487/RFC6434, December 2011.
https://www.rfc-editor.org/info/rfc6434

[RFC6583] Gashinsky, I., Jaeggli, J., Kumari, W. "Operational Neighbor Discovery Problems", RFC 6583, March 2012.
http://www.rfc-editor.org/info/rfc6583

[RFC7113] Gont, F., "Implementation Advice for IPv6 Router Advertisement Guard (RA-Guard)", RFC 7113, DOI 10.17487/RFC7113, February 2014.
http://www.rfc-editor.org/info/rfc7113

[RFC7123] Gont, F. and W. Liu, "Security Implications of IPv6 on IPv4 Networks", RFC 7123, February 2014.
http://www.rfc-editor.org/info/rfc7123

[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.
http://www.rfc-editor.org/info/rfc7217

[RFC7359] Gont, F., "Layer 3 Virtual Private Network (VPN) Tunnel Traffic Leakages in Dual-Stack Hosts/Networks", RFC 7359, August 2014.
http://www.rfc-editor.org/info/rfc7359

[RFC7381] Chittimaneni, K., Chown, T., Howard, L., Kuarsingh, V., Pouffary, Y., and E. Vyncke, "Enterprise IPv6 Deployment Guidelines", RFC 7381, DOI 10.17487/RFC7381, October 2014.
https://www.rfc-editor.org/info/rfc7381

[RFC7610] Gont, F., Liu, W., and G. Van de Velde, "DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers", BCP 199, RFC 7610, DOI 10.17487/RFC7610, August 2015.
https://www.rfc-editor.org/info/rfc7610

[RFC7707] Gont, F. and T. Chown, "Network Reconnaissance in IPv6 Networks", RFC 7707, DOI 10.17487/RFC7707, March 2016.
https://www.rfc-editor.org/info/rfc7707

[RFC7721] Cooper, A., Gont, F., and D. Thaler, "Security and Privacy Considerations for IPv6 Address Generation Mechanisms", RFC 7721, DOI 10.17487/RFC7721, March 2016.
https://www.rfc-editor.org/info/rfc7721

[RFC7872] Gont, F., Linkova, J., Chown, T., and W. Liu, "Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World", RFC 7872, DOI 10.17487/RFC7872, June 2016.
https://www.rfc-editor.org/info/rfc7872

[RFC8021] Gont, F., Liu, W., and T. Anderson, "Generation of IPv6 Atomic Fragments Considered Harmful", RFC 8021, DOI 10.17487/RFC8021, January 2017.
https://www.rfc-editor.org/info/rfc8021

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

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017.
https://www.rfc-editor.org/info/rfc8200

[SI6-RA6] "ra6 - A security assessment tool for attack vectors based on ICMPv6 Router Advertisement messages". ra(1) manual page.
https://manpages.debian.org/jessie/ipv6toolkit/ra6.1.en.html

[SI6-Toolkit] "SI6 Networks' IPv6 Toolkit".
https://www.si6networks.com/tools/ipv6toolkit

[THC-IPv6] "The Hackers' Choice IPv6 Attack Toolkit".
https://github.com/vanhauser-thc/thc-ipv6

[V6OPS-WG] IPv6 Operations (V6OPS) Working Group Mailing List.
https://www.ietf.org/mailman/listinfo/v6ops

CC BY SA