

Network Working Group A.
Cooper
Internet-Draft
CDT
Intended status: Informational F.
Gont
Expires: January 16, 2014 Huawei
Technologies
D.
Thaler
Microsoft
2013 July 15,

**Privacy Considerations for IPv6 Address Generation Mechanisms
draft-cooper-6man-ipv6-address-generation-privacy-00.txt**

Abstract

This document discusses privacy and security considerations for several IPv6 address generation mechanisms, both standardized and non-standardized. It evaluates how different mechanisms mitigate different threats and the trade-offs that implementors, developers, and users face in choosing different addresses or address generation mechanisms.

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 <http://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 January 16, 2014.

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with

respect

Cooper, et al.
1]

Expires January 16, 2014

[Page

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	2
2.	Terminology	4
3.	Weaknesses in IEEE-identifier-based IIDs	4
3.1.	Correlation of activities over time	4
3.2.	Location tracking	5
3.3.	Address scanning	6
3.4.	Device-specific vulnerability exploitation	6
4.	Privacy and security properties of address generation mechanisms	6
4.1.	Single-address scenarios	7
4.1.1.	Static, manually configured address only	8
4.1.2.	Cryptographically generated address only	8
4.1.3.	Temporary address only	8
4.1.4.	Persistent random address only	8
4.1.5.	Random-per-network address only	9
4.1.6.	DHCPv6 address only	9
4.2.	Multiple-address scenarios	9
4.2.1.	Temporary addresses and IEEE-identifier-based address	10
4.2.2.	Temporary addresses and persistent random address	11
4.2.3.	Temporary addresses and random-per-network addresses	11
5.	Other Privacy Issues	11
6.	Miscellaneous Issues with IPv6 addressing	12
6.1.	Network Operation	12

[12](#) [6.2.](#) Compliance

[12](#) [6.3.](#) Intellectual Property Rights (IPRs)

[12](#) [7.](#) Security Considerations

[13](#) [8.](#) IANA Considerations

[13](#) [9.](#) Acknowledgements

[13](#) [10.](#) Informative References

[15](#) Authors' Addresses

[1.](#) **Introduction**

IPv6 was designed to improve upon IPv4 in many respects, and mechanisms for address assignment were one such area for improvement.

In addition to static address assignment and DHCP, stateless autoconfiguration was developed as a less intensive, state-shared means of performing address assignment. With stateless autoconfiguration, routers advertise on-link prefixes and hosts generate their own interface identifiers (IIDs) to complete their addresses. Over the years, many interface identifier generation techniques have been defined, both standardized and non-standardized:

- o Manual configuration
 - * IPv4 address
 - * Service port
 - * Wordy
 - * Low-byte
- o Stateless Address Auto-Configuration (SLAAC)
 - * IEEE 802 48-bit MAC or IEEE EUI-64 identifier [[RFC1972](#)][RFC2464]
 - * Cryptographically generated [[RFC3972](#)]
 - * Persistent random [[Microsoft](#)]
 - * Temporary (also known as "privacy addresses") [[RFC4941](#)]
 - * Random-per-network (also known as "stable privacy addresses") [[I-D.ietf-6man-stable-privacy-addresses](#)]
- o DHCPv6-based [[RFC3315](#)]
- o Specified by transition/co-existence technologies
 - * IPv4 address and port [[RFC4380](#)]

Deriving the IID from a globally unique IEEE identifier [[RFC2462](#)] was

one of the earliest mechanisms developed. A number of privacy and security issues related to the interface IDs derived from IEEE identifiers were discovered after their standardization, and many of the mechanisms developed later aimed to mitigate some or all of these

weaknesses. This document identifies four types of threats against IEEE-identifier-based IIDs, and discusses how other existing techniques for generating IIDs do or do not mitigate those threats.

2. Terminology

This section clarifies the terminology used throughout this document.

Stable address:

An address that does not vary over time within the same network. Note that [[RFC4941](#)] refers to these as "public" addresses, but "stable" is used here for reasons explained in [Section 4.2](#).

Temporary address:

An address that varies over time within the same network.

Public address:

An address that has been published on some sort of directory service, such as the DNS [[RFC1034](#)].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [[RFC2119](#)]. These words take their normative meanings only when they are presented in ALL UPPERCASE.

3. Weaknesses in IEEE-identifier-based IIDs

There are a number of privacy and security implications that exist for hosts that use IEEE-identifier-based IIDs. This section discusses four generic attack types: correlation of activities over time, location tracking, device-specific vulnerability exploitation, and address scanning. The first three of these rely on the attacker first gaining knowledge of the target host's IID. This can be achieved by a number of different attackers: the operator of a server

to which the host connects, such as a web server or a peer-to-peer server; an entity that connects to the same network as the target (such as a conference network or any public network); or an entity that is on-path to the destinations with which the host communicates, such as a network operator.

3.1. Correlation of activities over time

As with other identifiers, an IPv6 address can be used to correlate the activities of a host for at least as long as the lifetime of the address. The correlation made possible by IEEE-identifier-based IIDs

is of particular concern because MAC addresses are much more permanent than, say, DHCP leases. MAC addresses tend to last roughly

the lifetime of a device's network interface, allowing correlation on

the order of years, compared to days for DHCP.

As [[RFC4941](#)] explains,

Cooper, et al.
4]

Expires January 16, 2014

[Page

"[t]he use of a non-changing interface identifier to form addresses is a specific instance of the more general case where a constant identifier is reused over an extended period of time and in multiple independent activities. Anytime the same identifier is used in multiple contexts, it becomes possible for that identifier to be used to correlate seemingly unrelated activity. ... The use of a constant identifier within an address is of special concern because addresses are a fundamental requirement

of

communication and cannot easily be hidden from eavesdroppers and other parties. Even when higher layers encrypt their payloads, addresses in packet headers appear in the clear."

IP addresses are just one example of information that can be used to correlate activities over time. DNS names, cookies [[RFC6265](#)], browser fingerprints [[Panopticlick](#)], and application-layer usernames can all be used to link a host's activities together. Although

IEEE-

identifier-based IIDs are likely to last at least as long or longer than these other identifiers, IIDs generated in other ways may have shorter or longer lifetimes than these identifiers depending on how they are generated. Therefore, the extent to which a host's activities can be correlated depends on whether the host uses multiple identifiers together and the lifetimes of all of those identifiers. Frequently refreshing an IPv6 address may not mitigate correlation if an attacker has access to other longer lived identifiers for a particular host. This is an important caveat to keep in mind throughout the discussion of correlation in this document. For further discussion of correlation, see Section 5.2.1 of [[I-D.iab-privacy-considerations](#)].

3.2. Location tracking

Because the IPv6 address structure is divided between a topological portion and an interface identifier portion, an interface identifier that remains constant when a host connects to different networks (as an IEEE-identifier-based IID does) provides a way for observers to track the movements of that host. In a passive attack on a mobile host, a server that receives connections from the same host over

time

would be able to determine the host's movements as its prefix changes.

Active attacks are also possible. An attacker that first learns the host's interface identifier by being connected to the same network segment, running a server that the host connects to, or being on-path to the host's communications could subsequently probe other networks for the presence of the same interface identifier by sending a probe packet (ICMPv6 Echo Request, or any other probe packet). Even if the host does not respond, the first hop router will usually respond with an ICMP Address Unreachable when the host is not present, and be silent when the host is present.

3.3. Address scanning

The structure of IEEE-based identifiers used for address generation can be leveraged by an attacker to reduce the target search space [[I-D.ietf-opsec-ipv6-host-scanning](#)]. The 24-bit Organizationally Unique Identifier (OUI) of MAC addresses, together with the fixed value (0xff, 0xfe) used to form a Modified EUI-64 Interface Identifier, greatly help to reduce the search space, making it easier for an attacker to scan for individual addresses using widely-known popular OUIs.

3.4. Device-specific vulnerability exploitation

IPv6 addresses that embed IEEE identifiers leak information about the device (Network Interface Card vendor, or even Operating System and/or software type), which could be leveraged by an attacker with knowledge of device/software-specific vulnerabilities to quickly find possible targets. Attackers can exploit vulnerabilities in hosts whose IIDs they have previously obtained, or scan an address space to find potential targets.

4. Privacy and security properties of address generation mechanisms

Analysis of the extent to which a particular host is protected against the threats described in [Section 3](#) depends on how each of a host's IIDs is generated and used. In some scenarios, a host configures a single global address and uses it for all communications. In other scenarios, a host configures multiple addresses using different mechanisms and may use any or all of them. This section compares the privacy and security properties of a variety of IID generation/use scenarios. The scenarios are grouped according to whether one or more addresses are configured. The table below provides a summary of the analysis.

Mechanism(s)	Correlation	Location	Address	Device
		tracking	scanning	exploits

Static	For address	For	NP	Depends on
manual only	lifetime	address		generation
		lifetime		mechanism
CGA only	Within	NP	NP	NP
	single			
	network			
Temporary	NP	NP	NP	NP
only				
Persistent	For address	For	NP	NP
random only	lifetime	address		
		lifetime		
Random-per-	Within	NP	NP	NP
network only	single			
	network			
Temporary	When IEEE-	Possible	Possible	Possible
and IEEE-	based is in			
based	use, or for			
	temp			
	address			
	lifetime			

Temporary	When random	Possible	Possible	Possible
and	is in use,			
persistent	or for temp			
random	address			
	lifetime			
Temporary	Within	NP	NP	NP
and random-	single			
per-network	network, or			
	for temp			
	address			
	lifetime			
+-----+-----+-----+-----+-----				
+				

Legend: NP = Not possible

Table 1: Privacy and security properties of IPv6 address generation mechanisms

4.1. Single-address scenarios

4.1.1. Static, manually configured address only

Because static, manually configured addresses are persistent, both correlation and location tracking are possible for the life of the address.

The extent to which location tracking can be successfully performed depends, to a some extent, on the uniqueness of the employed Interface ID. For example, one would expect "low byte" Interface IDs

to be more widely reused than, for example, Interface IDs where the whole 64-bits follow some pattern that is unique to a specific organization. Widely reused Interface IDs will typically lead to false positives when performing location tracking.

Because they do not embed OUIs, manually configured addresses are not vulnerable to device-specific exploitation. Whether they are vulnerable to address scanning depends on the specifics of how they are generated.

4.1.2. Cryptographically generated address only

Cryptographically generated addresses (CGAs) [[RFC3972](#)] bind a hash of the host's public key to an IPv6 address in the SEcure Neighbor Discovery (SEND) [[RFC3971](#)] protocol. CGAs are uniquely generated for each subnet prefix, which means that correlation is possible within a single network only. A host that stays connected to the same network could therefore be tracked at length, whereas a mobile host's activities could only be correlated for the duration of each network connection. Location tracking is not possible with CGAs. CGAs also do not allow device-specific exploitation or address scanning attacks.

4.1.3. Temporary address only

A host that uses only a temporary address mitigates all four threats.

Its activities may only be correlated for the lifetime a single address.

4.1.4. Persistent random address only

Although a mechanism to generate a static, random IID has not been standardized, it has been in wide use for many years on at least one platform (Windows). Windows uses the [[RFC4941](#)] random generation mechanism in lieu of generating an IEEE-identifier-based IID. This mitigates the device-specific exploitation and address scanning

attacks, but still allows correlation and location tracking because the address is persistent across networks and time.

Cooper, et al.
8]

Expires January 16, 2014

[Page

4.1.5. Random-per-network address only

[I-D.ietf-6man-stable-privacy-addresses] specifies a mechanism that generates a unique random IID for each network. A host that stays connected to the same network could therefore be tracked at length, whereas a mobile host's activities could only be correlated for the duration of each network connection. Location tracking is not possible with these addresses. They also do not allow device-specific exploitation or address scanning attacks.

4.1.6. DHCPv6 address only

TBD

4.2. Multiple-address scenarios

[RFC3041] (later obsoleted by [RFC4941]) sought to address some of the problems described in [Section 3](#) by defining "temporary addresses"

(commonly referred to as "privacy addresses") for outbound connections. Temporary addresses are meant to supplement the other IIDs that a device might use, not to replace them. They are randomly

generated and change daily by default. The idea was for temporary addresses to be used for outgoing connections (e.g. web browsing) while maintaining the ability to use a stable address when more address stability is desired (e.g., in DNS advertisements).

[RFC3484] originally specified that stable addresses be used for outbound connections unless an application explicitly prefers temporary addresses. The default preference for stable addresses was

established to avoid applications potentially failing due to the short lifetime of temporary addresses or the possibility of a reverse

look-up failure or error. However, [RFC3484] allowed that "implementations for which privacy considerations outweigh these application compatibility concerns MAY reverse the sense of this rule" and instead prefer by default temporary addresses rather than stable addresses. Indeed most implementations (notably including Windows) chose to default to temporary addresses for outbound connections since privacy was considered more important (and few applications supported IPv6 at the time, so application compatibility

concerns were minimal). [RFC6724] then obsoleted [RFC3484] and changed the default to match what implementations actually did.

The envisioned relationship in [RFC3484] between stability of an address and its use in "public" can be misleading when conducting privacy analysis. The stability of an address and the extent to which it is linkable to some other public identifier are independent of one another. For example, there is nothing that prevents a host

from publishing a temporary address in a public place, such as the

Cooper, et al.
9]

Expires January 16, 2014

[Page

DNS. Publishing both a stable address and a temporary address in the DNS or elsewhere where they can be linked together by a public identifier allows the host's activities when using either address to be correlated together.

Moreover, because temporary addresses were designed to supplement other addresses generated by a host, the host may still configure a more stable address even if it only ever intentionally uses temporary addresses (as source addresses) for communication to off-link destinations. An attacker can probe for the stable address even if it is never used as such a source address or advertised (e.g., in DNS or SIP) outside the link.

The scenarios in this section describe the privacy and security properties in cases where a host configures both a temporary address and an address generated via another mechanism. The analysis distinguishes between cases when both addresses are used as source addresses or are advertised off-link and cases where only the temporary address is used in those manners.

[TO DO: Add in Temporary + manual, Temporary + DHCP, Temporary + other link-layer-derived, Temporary + CGA, and perhaps re-arrange this section to avoid repetition.]

4.2.1. Temporary addresses and IEEE-identifier-based address

By using an IEEE-identifier-based IID and temporary addresses, a host can be vulnerable to the same attacks as if temporary addresses were not in use, although the viability of some of them depends on how the host uses each address. An attacker can correlate all of the host's activities for which it uses its IEEE-identifier-based IID. Once an attacker has obtained the IEEE-identifier-based IID, location tracking becomes possible on other networks even if the host only makes use of temporary addresses on those other networks; the attacker can actively probe the other networks for the presence of the IEEE-identifier-based IID. Device-specific vulnerabilities can still be exploited. Address scanning is also still possible because the IEEE-identifier-based address can be probed.

A host that configures but does not use an IEEE-identifier-based IID is vulnerable to address scanning because the address can be probed even if the IEEE-identifier-based address is otherwise never used. Once an attacker has received such a response, it can exploit device-specific vulnerabilities or probe other networks over time to track the location of the host. Correlation over time, however, is significantly mitigated, since the temporary addresses that the host

routinely uses on the network refresh often.

Cooper, et al.
10]

Expires January 16, 2014

[Page

4.2.2. Temporary addresses and persistent random address

Using a persistent, random address as a stable address for server-like connections together with temporary addresses for outbound connections presents some improvements over the previous scenario. The address scanning and device-specific exploitation attacks are no longer possible because the OUI is no longer embedded in any of the host's addresses. However, correlation of some activities across time and location tracking are both still possible because the random

IID is persistent. As in [Section 4.2.1](#), once an attacker has obtained the host's random IID, location tracking is possible on any network by probing for that IID, even if the host only uses temporary addresses on those networks.

A host that configures but does not use a persistent random address mitigates all four threats. Correlation is only possible for the lifetime of a temporary address. The persistent random address cannot be easily discovered in an address scan (although it is available to an on-link adversary), which prevents an attacker from using it for location tracking or device-specific exploitation.

4.2.3. Temporary addresses and random-per-network addresses

When used together with temporary addresses, the random-per-network mechanism [[I-D.ietf-6man-stable-privacy-addresses](#)] improves upon the previous scenario by limiting the potential for correlation to the lifetime of the random-per-network address (which may still be lengthy for hosts that are not mobile) and eliminating the possibility for location tracking (since a different IID is generated for each subnet prefix).

As in the previous scenario, a host that configures but does not use a random-per-network address mitigates all four threats.

5. Other Privacy Issues

Since IPv6 subnets have unique prefixes, they reveal some information about the location of the subnet, just as IPv4 addresses do. Hiding this information is one motivation for using NAT in IPv6 (see [RFC 5902 section 2.4](#)).

Teredo [[RFC4380](#)] specifies a means to generate an IPv6 address from the underlying IPv4 address and port, leaving many other bits set to zero. This makes it relatively easy for an attacker to scan for

IPv6

addresses by guessing the Teredo client's IPv4 address and port (which for many NATs is not randomized). For this reason, popular implementations (e.g., Windows), began deviating from the standard

by

including 12 random bits in place of zero bits. This modification was later standardized in [[RFC5991](#)].

6. Miscellaneous Issues with IPv6 addressing

6.1. Network Operation

It is generally agreed that IPv6 addresses that vary over time in a specific network tend to increase the complexity of event logging, trouble-shooting, enforcement of access controls and quality of service, etc. As a result, some organizations disable the use of temporary addresses [[RFC4941](#)] even at the expense of reduced privacy [[Broersma](#)].

6.2. Compliance

Major IPv6 compliance testing suites required (and still require) implementations to support MAC-derived suffixes in order to be approved as compliant. Implementations that fail to support MAC-derived suffixes are therefore largely not eligible to receive the benefits of compliance certification (e.g., use of the IPv6 logo, eligibility for government contracts, etc.). This document recommends that these be relaxed to allow other forms of address generation that are more amenable to privacy.

6.3. Intellectual Property Rights (IPRs)

Some IPv6 addressing techniques might be covered by Intellectual Property rights, which might limit their implementation in different Operating Systems. [[CGA-IPR](#)] and [[KAME-CGA](#)] discuss the IPRs on CGAs.

7. Security Considerations

This whole document concerns the privacy and security properties of different IPv6 address generation mechanisms.

8. IANA Considerations

This document does not require actions by IANA.

9. Acknowledgements

The authors would like to thank Bernard Aboba and Rich Draves.

10. Informative References

[Broersma]

Broersma, R., "IPv6 Everywhere: Living with a Fully IPv6-enabled environment", Australian IPv6 Summit 2010, Melbourne, VIC Australia, October 2010, October 2010, <http://www.ipv6.org.au/10ipv6summit/talks/Ron_Broersma.pdf>.

[CGA-IPR] IETF, "Intellectual Property Rights on [RFC 3972](#)", 2005.

[I-D.iab-privacy-considerations]

Cooper, A., Tschofenig, H., Aboba, B., Peterson, J., Morris, J., Hansen, M., and R. Smith, "Privacy Considerations for Internet Protocols", [draft-iab-](#)

[privacy-](#)

[considerations-03](#) (work in progress), July 2012.

[I-D.ietf-6man-stable-privacy-addresses]

Enhanced

Gont, F., "A method for Generating Stable Privacy-

Addresses with IPv6 Stateless Address Autoconfiguration (SLAAC)", [draft-ietf-6man-stable-privacy-addresses-10](#) (work in progress), June 2013.

[I-D.ietf-opsec-ipv6-host-scanning]

in

Gont, F. and T. Chown, "Network Reconnaissance in IPv6 Networks", [draft-ietf-opsec-ipv6-host-scanning-01](#) (work

progress), April 2013.

[KAME-CGA]

KAME, "The KAME IPR policy and concerns of some technologies which have IPR claims", 2005.

[Microsoft]

Microsoft, "IPv6 interface identifiers", 2013.

[Panopticlick]

Electronic Frontier Foundation, "Panopticlick", 2011.

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities",

STD 13, [RFC 1034](#), November 1987.

- [RFC1972] Crawford, M., "A Method for the Transmission of IPv6 Packets over Ethernet Networks", [RFC 1972](#), August 1996.
- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC2462] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", [RFC 2462](#), December 1998.
- [RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", [RFC 2464](#), December 1998.
- [RFC3041] Narten, T. and R. Draves, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", [RFC 3041](#), January 2001.
- [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), July 2003.
- [RFC3484] Draves, R., "Default Address Selection for Internet Protocol version 6 (IPv6)", [RFC 3484](#), February 2003.
- [RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "Secure Neighbor Discovery (SEND)", [RFC 3971](#), March 2005.
- [RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", [RFC 3972](#), March 2005.
- [RFC4380] Huitema, C., "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", [RFC 4380](#), February 2006.
- [RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", [RFC 4941](#), September 2007.
- [RFC5991] Thaler, D., Krishnan, S., and J. Hoagland, "Teredo Security Updates", [RFC 5991](#), September 2010.
- [RFC6265] Barth, A., "HTTP State Management Mechanism", [RFC 6265](#), April 2011.
- [RFC6724] Thaler, D., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version (IPv6)", [RFC 6724](#), September 2012.

Authors' Addresses

Alissa Cooper
CDT
1634 Eye St. NW, Suite 1100
Washington, DC 20006
US

Phone: +1-202-637-9800
Email: acooper@cdt.org
URI: <http://www.cdt.org/>

Fernando Gont
Huawei Technologies
Evaristo Carriego 2644
Haedo, Provincia de Buenos Aires 1706
Argentina

Phone: +54 11 4650 8472
Email: fgont@si6networks.com
URI: <http://www.si6networks.com>

Dave Thaler
Microsoft
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

Phone: +1 425 703 8835
Email: dthaler@microsoft.com

