How Interface ID Allocation Mechanisms are Performed in IPv6

Qinwen Hu
University of Auckland
qhu009@aucklanduni.ac.nz

Nevil Brownlee
University of Auckland
n.brownlee@auckland.ac.nz

ABSTRACT

IPv6 addresses contain a 64-bit Interface ID (IID) that is allocated by site administrators. A random IID allows them to reduce the effectiveness of IPv6 reconnaissance attacks. In this paper, we look at how IPv6 IIDs are assigned in practice. In particular, we classify the IPv6 server and client addresses from various trace files. We apply our classification method to a number of datasets to find different regions and different IID allocation schemes. The results show a difference among datasets, and imply that IID allocation differs between regions (as we expected).

Categories and Subject Descriptors

C.2.0 [**General**]: Security and protection

Keywords

IPv6; Interface Identification; Security

1. INTRODUCTION

IPv6 was proposed as a solution in 1996; its larger address space not only supports the increased number of connected devices, but also reduces some security issues. In [1], Chown describes several methods to reduce the address scans happening in an IPv6 network, such as not using sequential addresses, not using simple patterns, and using random numbers to allocate the IID field. If network administrators apply these suggestions, that would make the classic network address scans less feasible. However, our IPv6 address usage survey shows that some network administrators use customized IID allocation mechanisms to satisfy different requirements, so it is possible to launch a network reconnaissance attack in IPv6 networks by using appropriate heuristics. In [2], authors discuss security and privacy issues that related to some existing IID allocation mechanisms; also they claim that using the randomized values in the IID field will make reconnaissance attacks less effective for IPv6 networks. This paper explores a number of IID allocation mechanisms that have been used for allocating IPv6 client addresses, and summarizes changes in IID allocation during the last five years.

2. DATASETS

We collect our data from a link connecting a UoA (University of Auckland) IPv6 network with IPv6 networks outside UoA. We observed 72931 traffic flows per hour. The traffic flows are reasonably high between 9am-11pm, 105269 traffic flows are found in this period and the traffic rate drops to 30732 flows during 0am-9am. We built a high-speed flow monitoring system which is able to process and record the first nine packets of each flow into a pcap file every hour. We collected our samples from both flow directions in the period from 2014-05-09 to 2014-08-09.

3. METHOLOGY

Our study is not the first paper that presents techniques to analyse IPv6 IID usage, but we believe this is the first paper to analyse the distribution of pseudo-random numbers in the IPv6 IID field.

3.1 Distinguishing IPv6 clients and servers

Trace files do not intuitively tell us whether an address in a packet is a 'client' or 'server'. Therefore, we propose some methods to classify IPv6 servers and clients. For example, we use port numbers, SYN flags and look at the DNS reverse zones.

3.2 Grouping IPv6 clients into regions

Unlike the IPv4 protocol, IPv6 has divided addresses into two parts: the upper 64-bit network prefix gives information as to a node's location; the lower 64-bit IID field contains information about how an IPv6 node has been configured. Our 'regions' are our own university (UoA), and geographic regions covered by the Regional Internet Registries (RIR): APNIC, ARIN and RIPE [5].

3.3 Identifying randomized IPv6 IID values

We use a frequency distribution plot to examine the continuous probability function among IID values. Each bar in the plot shows the frequency of a given IID value's occurrence. In Figure 1, the x axis repents the range 0-2^{64}, while the y axis indicates the number of occurrences for groups of IID values. We observe that such distributions spread more or less evenly across the 0-2^{64} range, with no obvious gaps or significant spikes. The probability of a pseudo-random IID being misclassified as EUI-64 is less than 1 in 2^{24} and is ignored.

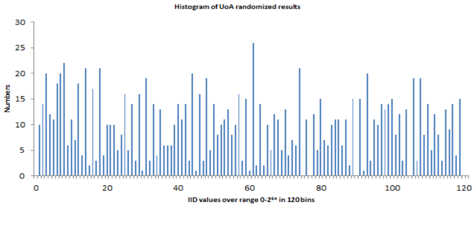

Figure 1 Histogram (Randomized IID schemes)

3.4 Identifying IID allocation schemes

We identify IID schemes as follows. EUI-64 is generated using EUI-64 algorithm based on each MAC address, the address can be recognized by observing the FF:FE bytes in the IID field. The Embedded-IPv4 scheme encodes an IPv4 address in the lowest-32 bits of the IPv6 address, for instance 2001:888::24:194:109:20:106, this scheme is easily identifiable; we verify our results by pinging those IPv4 addresses.

CoNEXT Student Workshop'14, December 2, 2014, Sydney, Australia.
Copyright is held by the owner/author(s). Publication rights licensed to ACM.
ACM 978-1-4503-3282-8/14/12…$15.00

Table 2 Analysis of Server IIDs

Region	EUI-64	Embedded-IPv4	Randomized	Small-integer	Other
ARIN	4%	8%	4%	80%	4%
APNIC	6%	4%	13%	77%	0%
ERPI	5%	5%	13%	69%	8%

Table 3 Analysis of all client addresses by region

Region	EUI-64	Embedded-IPv4	Randomized	Small-integer	Other
ARIN	7%	11.5%	38.7%	41.1%	1.7%
APNIC	17.8%	1.4%	70%	10.6%	0.02%
ERPI	8%	2%	30%	44%	16%
UoA	20%	0%	79.7%	0.3%	0
In total	12%	4%	50%	30%	2%

The Small-integer scheme set most bytes in the IID to be 0, it can easily recognized by checking the number of zero bytes in the IID field, for instance 2001:1318:100c:1::1. We recognize the randomized scheme based on the description in [3] and [6]. A randomized address verification method is introduced in section 3.3, though other schemes exist and can be identified (e.g service-port, wordy, etc), they are quite rare in practice, so we put them under the label “Other”.

4. OBSERVATION

Table 2 provides a summary of server results in each region. The percentage in each column is the number of addressees observed in each allocation scheme divided by the total number of addresses in that region. It shows clearly that a high percentage of server addresses use specific allocation schemes (small integer).

The client results observed from our survey are similar to those in [2]. In that study 69.73% of the sample used a randomized allocation scheme and 7.72% used the EUI-64 scheme. The authors of [2] believe that network administrators should put increasing emphasis on privacy and security concerns when they allocate an IID field. However, there are still a significant number of servers IIDs using EUI-64 and embedded IPv4 strategies. Although our data are taken from a different time and location to the data in [2], our results are quite consistent with those in that study. Table 3 shows the breakdown of IID allocation schemes observed of UoA from each region. The largest proportion of IPv6 addresses seen are generated by using a random IID allocation mechanism. In order to make sure our results are correct, we apply the methodology described in section 3.3; the results imply that most network administrators do care about security and privacy and therefore use unpredictable values in the IID field. The next most common technique seems to be the small-integer mechanism. Most (30%) of these addresses allocate only a few bytes to the IID field while setting most of its bytes to zero. Some EUI-64 addresses are observed: especially, UoA contributes a large proportion of the uses of the EUI-64 mechanism. After further investigation, we find that some faculties at UoA use an EUI-64 auto-configuration mechanism to generate a global IPv6 address for a new, because this strategy can help them to manage the network more easily. When we compare the results observed in [4], there is an absence of the use of Teredo, ISATAP and 6to4 allocation techniques in our results, but we see a decrease in the use of embedded IPv4 address in the IID field, which suggest that in some areas network administrators have changed their IID allocation strategies from transition mechanisms to other solutions.

5. CONCLUSION

We observe that a number of considerations should be made when we allocate the IIDs for a new IPv6 host. Firstly, predictable patterns in the IIDs can be leveraged to reduce the IPv6 address search space. In addition, in order to reduce the security and privacy implications arising from EUI-64 identifiers, network administrators should consider generating random values for the IIDs. Although the small integer scheme is commonly used for allocating IIDs for clients and servers, it appears that the randomized IID scheme is becoming more common for allocating the IPv6 client address.

As future work, we plan to look at how hosts are allocated within an IPv6 mobile network and to provide a more detailed study of security and privacy issues in IPv6 mobile networks.

6. ACKNOWLEDGMENTS

We would like to thanks Professor Brian Carpenter for his time and effort taken to review our work.

7. REFERENCES

[1] T. Chown. IPv6 implications for network scanning. Internet RFC 5157, 2008.

[2] F. Gont and T. Chown. Network Reconnaissance in IPv6 Networks, draft-ietf-opsec-ipv6-host-scanning-04, 2014.

[3] T. Narten, R. Draves and S. Krishnan. Privacy Extensions for Stateless Address Autoconfiguration in IPv6. Internet RFC 4941, 2007.

[4] Shen W C, Chen Y J, Zhang Q L, Yang Chen, et al. “Observations of IPv6 Traffic”. International Colloquium on Computing, Communication, Control, and Management (CCCM 2009), August, 2009.

[5] Regional Internet Registries Statistics Available:http://www-public.int-evry.fr/~maigron/RIR_Stats/RIR_Delegations/World/IPv6-Alpha.html

[6] F. Gont. A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC) Available. Internet RFC 7217, April, 2014