

How Interface ID Allocation Mechanisms are Performed in IPv6

Qinwen Hu

qhu009@aucklanduni.ac.nz

Nevil Brownlee

n.brownlee@auckland.ac.nz

2015

Introduction

- Use customized IID allocation mechanisms can cause a network reconnaissance attack in IPv6 networks.
- Some security and privacy issues that related to some existing IID allocation mechanisms.

Background

- Security: How easy is it to scan the value in IID field?
- Visibility: How easy is it to find the IPv6 host by looking at the IID field?
- Privacy: How easy is it to track a user's activities by monitoring the IID field?

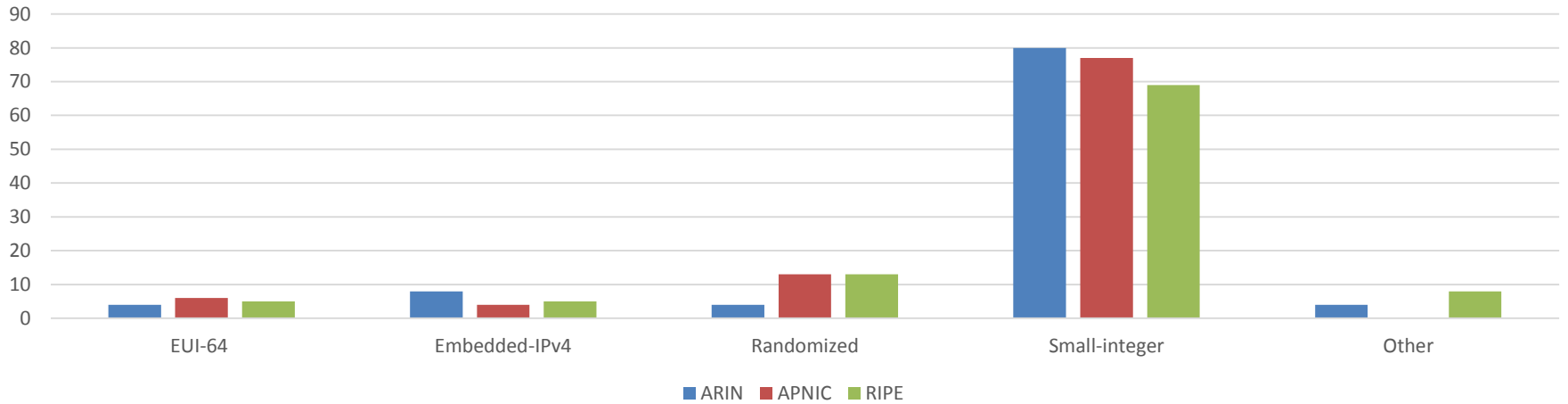
Background

Recommended IID allocation mechanisms	
EUI-64	2001:df0:0:2005:a00:27ff:fe76:eb62
Random/Privacy	2001:df0::2005:c1:e846:890a:9339
Customized IID allocation mechanisms	
Small-Integer	2001:268:fd08:6::2
Embedded-IPv4	2607:e400:1002::66:90:130:10

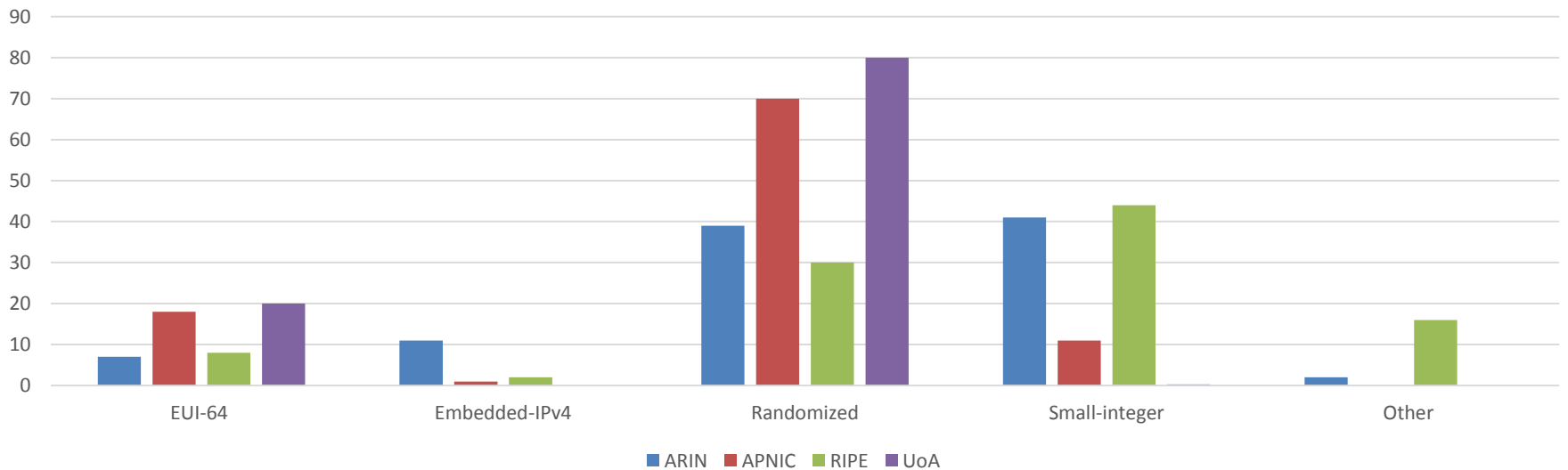
	Visibility	Privacy	Security
EUI-64	High	Low	Low
Random/Privacy	Low	High	High
Small-Integer	High	Low	High
Embedded-IPv4	High	Low	Low

Results

IPv6 server results



IPv6 client results



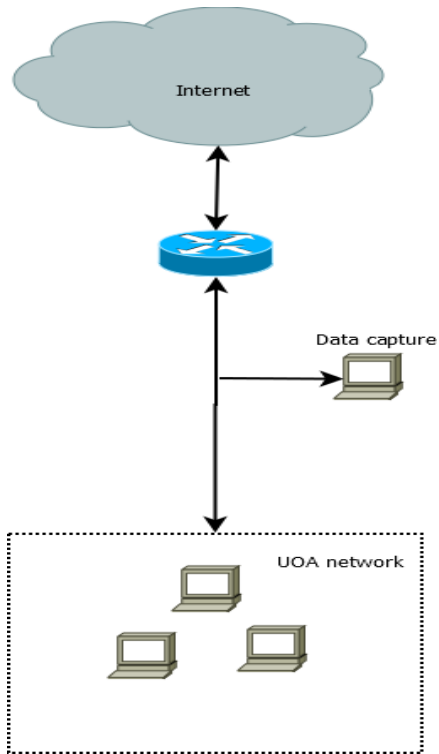
Conclusions

- Predictable patterns in the IIDs can be leveraged to reduce the IPv6 address search space.
- Randomized allocation mechanism can reduce the security and privacy implications arising from EUI-64 identifiers.
- Small integer is a popular IID scheme for allocating the IPv6 server address.
- Randomized IID scheme is becoming more common for allocating the IPv6 client address.

Questions



Datasets



- Collected the first nine packets of each flow into a pcap file every hour between May, 2014 and Aug, 2014.
- Average 72931 traffic flows per hour.

Methodology

