Router Advertisement Based Privacy Extension In IPv6 Autoconfiguration

http://tools.ietf.org/html/draft-rafiee-6man-ra-privacy

Hosnieh Rafiee, Prof. Dr. Christoph Meinel
Hasso Plattner Institute, Germany

IETF87
6man WG
Berlin
July 29, 2013

Definitions

- What is Privacy on Internet?
  - □ Privacy is a term that is concerned with a user’s information whether it belongs to individuals, governments or companies. So it is related to someone’s private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address.

- Differences between Privacy, Security and Anonymity
  - □ Privacy gives one the ability to choose which data one might want to expose to others
  - □ Security gives one the ability to protect one’s data or to make or keep one’s data confidential
  - □ Anonymity is the act of hiding ones real identity

Definitions - II

- Privacy and Security can actually conflict with each other
  - The gathering of location information for security reasons might prove detrimental to privacy
- Privacy and Security might be moving in the same direction
  - Using cryptographic approaches for security reasons also helps to increase privacy
- The IETF’s first attempt at protecting privacy is defined in RFC 4941.

Deficiencies with the use of Privacy Extension RFC (RFC 4941) - I

- RFC 4941 promotes the use of IIDs generated by a MAC address as a public address for the node
- The node cuts his connections with other nodes if the lifetime of the temporary IIDs has expired.
- The node might not generate a new IID when it receives a new RA message if the option in the router advertisement tells the node to extend the lifetime of its address, and if the maximum lifetime of that address has not been reached. The node will then will keep its current IID without generating a new one.

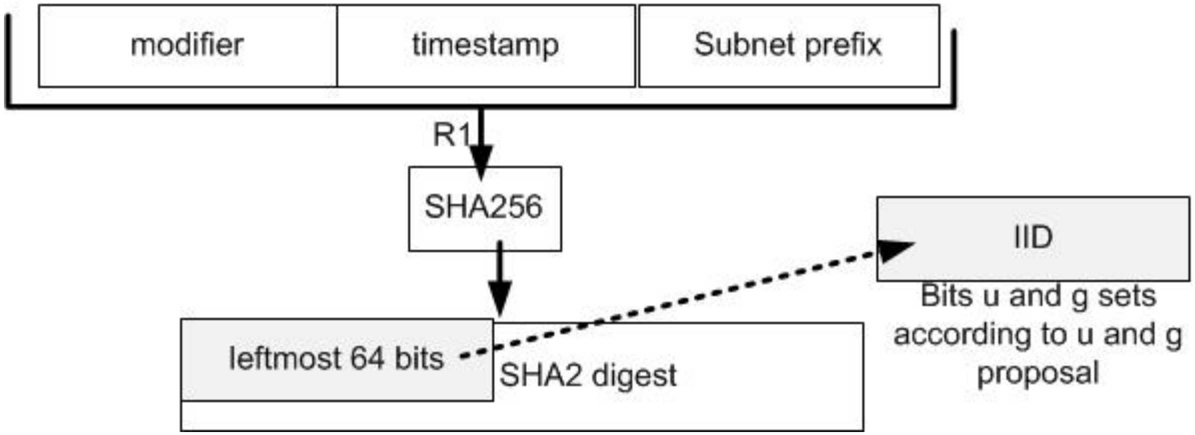
Deficiencies with the use of Privacy Extension RFC (RFC 4941) - II

- A node may determine a need for the use of a large and stable storage area in which to store each newly generated IID. This needs to be done in order to provide a database to be used in preventing the generation of another currently "in use" value.
- When there is no stable storage available the node may not be able to make use of a greatly randomized IID because, according to section 3.2.2 of RFC 4941, there is nothing to force the use RFC 4086.

A Possible Solution to RFC 4941 RA-Privacy Draft - I

This draft intends to address some deficiencies with RFC 4941 and to update some sections of RFC 4941 such as:

- Section 3.2.3 in order to explain the use of CGA when security is not the issue.
  - Make use of the CGA algorithm, skipping the security step, for the purpose of generating a more highly randomized IID



A Possible Solution to RFC 4941 RA-Privacy Draft - II

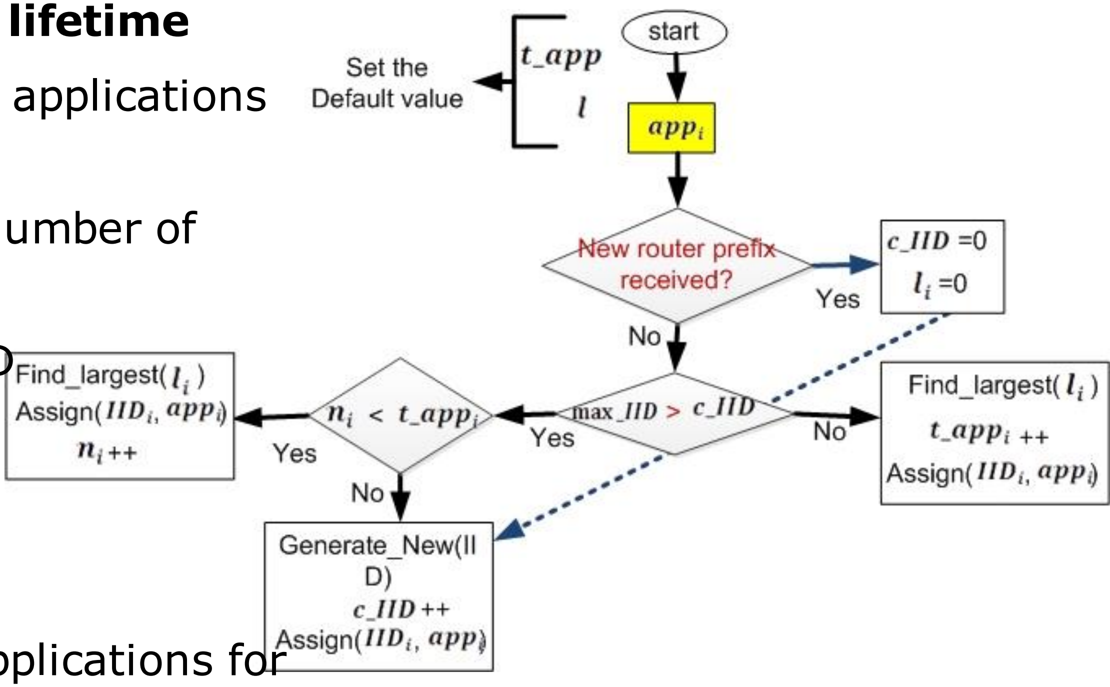
- An additional update to this RFC will explain how to maintain the lifetime of the IP address when the router prefix changes or the lifetime of the IID changes.

IID Application layer based lifetime

- t_app: maximum number of applications per IID
- max_IID: is the maximum number of valid IIDs
- c_IID: current number of IID
- IID_i : is a specific IID
- t_app_i : the total number

of applications per specific IID

- n_i : the current number of applications for a specific IID
- l: the maximum lifetime per IID



l_i The current lifetime of an specific IID

A Possible Solution to RFC 4941 RA-Privacy Draft - III

- There should be an update made to step 4, Section 3.2.1, clarifying which IIDs should be kept in stable storage.
- Modification to section 3.2.2 of RFC 4941, to use the word “should” or “must” instead of "might‟ in order to force the node to use a good randomization approach
- Automate the process for setting the lifetime
  - □ All the default values can be included in the optional section of Router advertisements message

A Possible Solution to RFC 4941 RA-Privacy Draft - IV

- The node Should not use public addresses
  - it has a negative effect on a user’s privacy. In cases where it wants to use them, the node Must not use an IID whose generation is based on a MAC address
- the node Should change its IID
  - if a user visited a website that caused harm to his privacy, then configuring a new IID decreases the chance of a node’s being tracked and the leakage of a user’s private data
- Our Reason (Implementation by a group of our master students):
  - Scanned domains: ~200k
  - Open for axfr request: 3772 => 1.8%
  - ~136000 RRs found

Thank you

- Any Question

- Does 6man wants to adopt this draft?