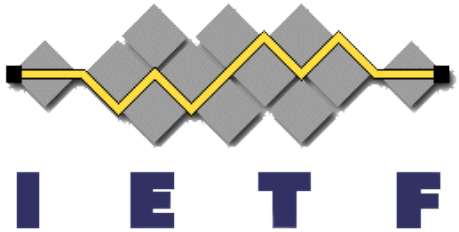


Hasso Plattner Institut

IT Systems Engineering | Universität Potsdam

A Simple Secure Address generation Scheme for IPv6 Autoconfiguration (SSAS)

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

Hosnieh Rafiee, Christoph Meinel

Hasso Plattner Institute, Germany

IETF86

6man WG

Orlando, FL

March 2013

Motivation – purpose of this draft

response to discussions in mailing list

- Privacy and Security issues - IID generation algorithms
  - Cryptographically Generated Addresses (CGA) - RFC 3972
    - Large computational costs
    - Verification : Need to re-generate CGA along with signature verification

    Verification occurs:

    - During Duplicate Address Detection
    - When verifying the other nodes in the cache (reachability checking) section 3 RFC 4861
  - Privacy Extension – RFC 4941
    - ND threats – RFC 3756 (Lack of security) when CGA isn't used

- ND widely used in different applications such as
  - Mobile networks for Care of Address generation- RFC 6543, 6275
  - Sensor networks, 6LoWPAN – RFC 6775
  - Vehicular networks

Comparison of
A Simple Secure Address generation Scheme (SSAS) to CGA

1. Much faster and easier to use than the CGA algorithm (generated in less than 250 milliseconds along with public key generation)
   - Good for nodes with limited resources
   - Mobile IPv6 uses CGA - RFC 4866
     - This cost efficient algorithm can be used in place of CGA

2. Good to use when nodes need to observe privacy
   - Integrates privacy and security when administrators want to observe both
     - The main purpose of CGA is not for providing privacy but for providing security

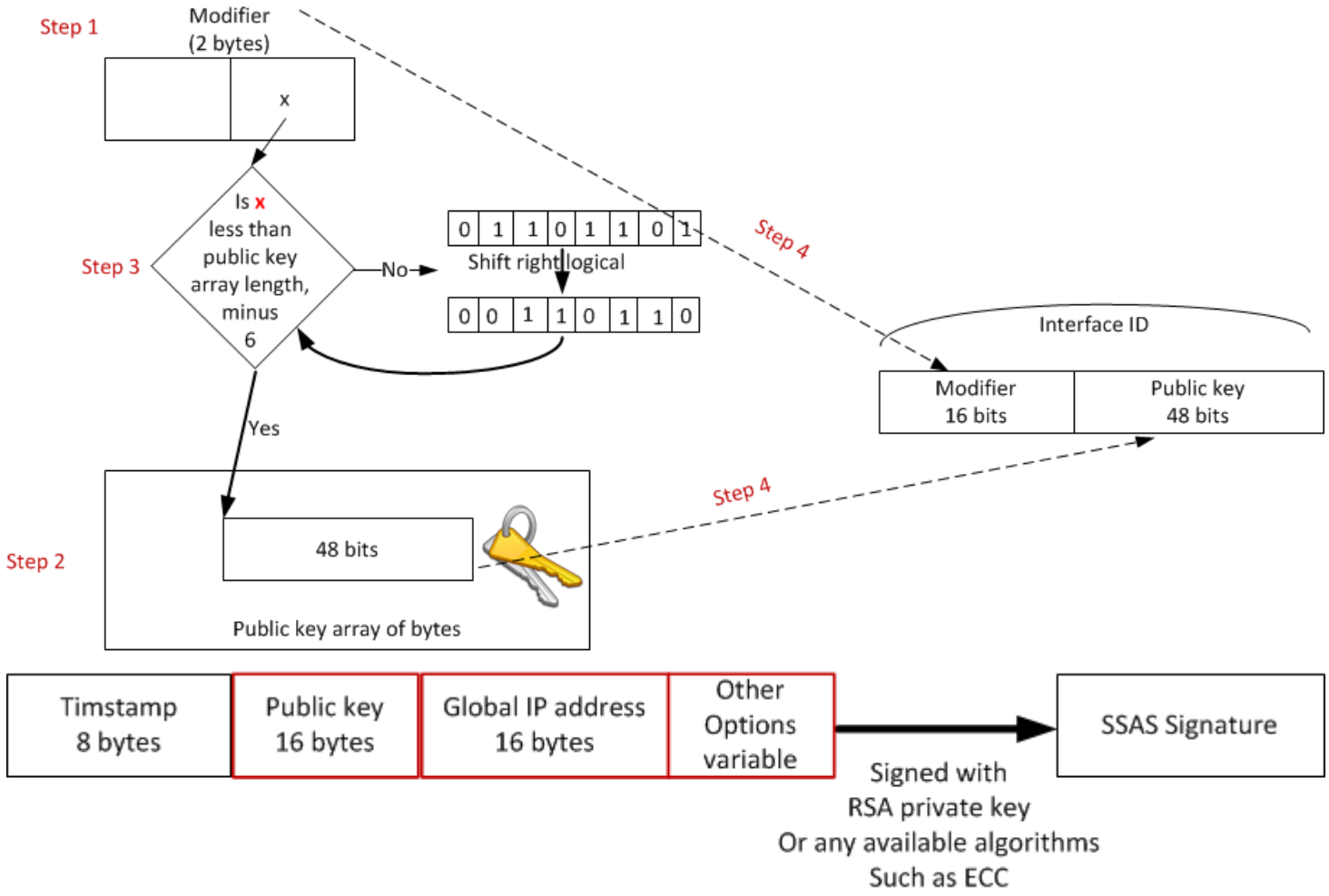
Comparison of
A Simple Secure Address generation Scheme (SSAS) to CGA

3. Can mitigate DoS types of attack against verifier nodes
   - Verification time is much less than that of CGA
     - The node can verify more packets per second than when using CGA
     - For cache reachability checking the node needs to verify several packets that come from other nodes, per second
   - Just need to verify the signature to protect the node against ND attacks.

4. Provides another approach for the generation of the IID

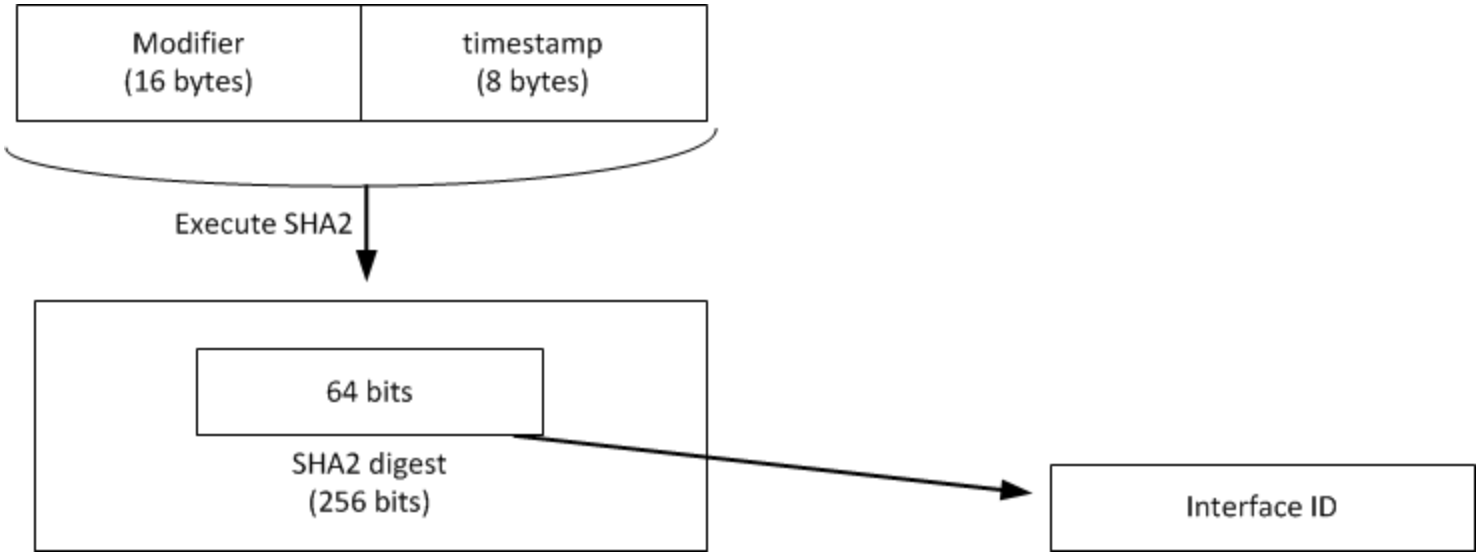
Brief description of SSAS algorithm

Considering Privacy and Security



Brief description of SSAS algorithm

Considering Privacy without Security



Using RPKI or DNS as a key management approach for Router Authorization

- Using RFC 6491, 6494 for Resource public key Infrastructure

- A possible scenario - Using DNS
  - Clients need to use the DNSKEY RR (RFC 4034) in order to authorize routers

Next steps

- Clarification of the use of RPKI

Useful document? Adoption to WG?