SAVI for SLAAC update

draft-ietf-savi-fcfs-04

IETF78 - Maastricht

Changes from 03 version

- Reflected last WG decisions
  - SHOULD trigger the binding creation process upon the reception of a data packet for which there is no binding
    - Included the arguments for qualifying the SHOULD in an appendix
  - Added a new section for discovering prefixes based on Router Advertisements
    - Security based on accepting them only from trusted ports

Open questions: router ports

- As defined we have trusted ports and validating ports
- We assume that routers are connected to trusted ports
- Do we need router ports?
- A router port would allow remote traffic but validate local traffic
  - Assumes that not all routers are trusted
  - How do we deal with a router forwarding local traffic (e.g. The case of a subnet with multiple routers, redirects)
  - We trust the router port to send any transit traffic anyway, so how much security this adds?

Open Issues: garbage collection

- When to delete bindings?
  - Under normal condition: When the lifetime of the binding is over
    - What should be a good default value for the lifetime?
    - Currently, we are extending the lifetime upon each data packet. How if this processing wise?
    - We could link it to the prefix lifetime when the prefix is automatically discovered. What to do with manually configured prefixes?
    - Should the SAVI device send a NUD probe before deleting in this case?
    - Other option would be to not delete unless needed (i.e. Under attack or when we create another binding for the address)

Open issues: garbage collection (2)

- Deleting bindings under attack
  - Suppose an attacker sends a bulk of DAD NSOL
  - The SAVI device does not have enough resoruces to store all bindings, which ones to delete?
    - Note that the effect of deleting a binding is NOT blocking a host, but that an attacker can steal the binding
  - Proposed solution: delete newer bindings
    - The attacker binding compete with each other and bindings prior the attack are not affected
  - Do we need to take other measures?

Open issues: rate limiting

- SAVI SLAAC generates packets
  - DAD NSOL packets
    - upon reception of NADV and data pacekts
    - When the lifetime expires to verify the binding before deletion
- How do we rate limit them?