Privacy Addresses v2

draft-ietf-ipv6-privacy-addrs-v2-01

Suresh Krishnan
Ericsson

ipv6 working group
2004/11/11 IETF-61
Washington DC

What is new?

- Temporary address generation is disabled by default
- DAD run on all addresses not just per Interface ID
- Problem statement
- Security considerations
- Algorithm for generation no longer mandated

What is new?

- Multiple temporary interface identifiers allowed for multiple prefixes
- Clarifying text for
  - ingress filtering issues
  - means of correlation
  - implications of stable prefix
  - implications of small number of nodes
- Excluding reserved anycast (RFC2526) addresses from temporary identifier

Open Issues

- Per-prefix knobs
- Unique local addresses
  - Should we create temporary addresses for ULA?
  - Are ULAs special?
- ISATAP and RFC2526 downref
- 64-bit interface IDs only?
- Any other issues?

Wrapping up

- Questions?
- Comments?

Problem statement

- The correlation can be performed by
  - An attacker who is in the path between the node in question and the peer(s) it is communicating to, and can view the Ipv6 addresses present in the datagrams.
    - may be able to perform significant correlation based on
      - The payload contents of the packets on the wire
      - The characteristics of the packets such as packet size and timing.
      - Use of temporary addresses will not prevent such payload based correlation
  - An attacker who can access the communication logs of the peers with which the node has communicated.

Resolving downref

- OLD: Compare the generated identifier against a list of known values that should not be used. Inappropriate values include those used in reserved anycast addresses [RFC2526], those used by ISATAP [ISATAP], the value 0, and those already assigned to an address on the local device. In the event that an unacceptable identifier has been generated, the node MUST restart the process...
- NEW: Compare the generated identifier against a list of reserved interface identifiers and to those already assigned to an address on the local device. In the event that an unacceptable identifier has been generated, the node MUST restart the process...