Source Address Validation Improvements – SAVI –

Monday, March 23, 2009. 15:20 – 17:20 am
Continental 4

Agenda

- Summary of design decisions so far — 15:30
  Christian Vogt
- Liaison from Broadband Forum — 15:45
  Christian Vogt
- Do we need a Binding Distribution Protocol? — 15:50
  Jun Bi, Marcelo Bagnulo
- Discussion — 16:20
  All
- SAVI Progress Report in CERNET2 — 16:50
  Jun Bi

Lightening talks on potential future work, if time permits:

- Access Node Control Protocol for SAVI — 5 min
  Frank Xia, draft-kaippallimalil-ancp-sav
- CGA Extension Header of IPv6 — 5 min
  Padmanabha Nallur, draft-dong-savi-cga-header
- SAVI with the Host Identity Protocol — 5 min
  Andrei Gurtov, draft-kuptsov-sava-hip — end at 17:20

Design Decisions Since IETF 73

1. control packets can trigger binding establishment
   - prevents attacker from creating false bindings for addresses being configured (front-running attack)

2. no First-Come-First-Serve for IP version 4
   - prevents attacker from creating false bindings for all available addresses (address exhaustion attack)

3. introduce DHCP mode for IP version 6
   - enables higher security in managed environments
   - prioritization of address configuration modes possible

4. under discussion: binding distribution protocol?

Liaison From Broadband Forum

During our last meeting we have been discussing the specific use of IPv6 in a residential broadband environment. **We believe the presence of duplicate link-local addresses may result in security issues.** We can envision a number of scenarios, both malice or vendor incompetence by which this can happen.

An additional potential complication is that contrary to the assumptions taken in the IPv6 protocol suite – in particular RFC 4861 and RFC 4862 – **a split-horizon model is employed in such environment.** This implies that different IPv6 hosts will not be able to communicate directly at the Ethernet link-layer. Instead, host-host communication needs to cross an IP Edge Router.

We also believe that in the case of Ethernet network reconfiguration (e.g. resulting in another Access Node being connected to the Edge Router)**, the Neighbor Cache of the Edge Router may be partially or fully overwritten, resulting in similar security issues.**

Given this, we would like you to provide feedback as to whether or not you believe there is indeed a security issue to be solved in such a deployment model. If there is, **we would like to ask you to consider this as part of your ongoing work plan and provide feedback** on your findings.