Last-hop Threats to PIM

draft-savola-pim-lasthop-threats-01.txt

Pekka Savola, James Lingard

Last-hop threats to PIM (1/2)

- Background
  - draft-ietf-mboned-mroutesec-xx.txt (now in RFC-ed queue)
    - only described the multicast *routing infrastructure* threats
  - There has not been an analysis on "last-hop multicast threats"
    - last-hop meaning nodes (hosts) attacking other nodes on the same link, denying the service on the link, or bypassing the DR controls
  - These issues deserved to be spelled out

- Vulnerabilities
  - Nodes may send unauthorized register messages
  - Nodes may become unauthorized PIM neighbors
  - Routers may accept PIM messages from non-neighbors
    - The spec should probably be tightened here..
  - An unauthorized node may be elected as the PIM DR
  - A node may become an unauthorized asserted forwarder

Last-hop threats to PIM (2/2)

- Threats / Attacks (exploiting the vulnerabilities)
  - Denial of service attack on the link
  - DoS on the outside
  - Confidentiality, Integrity and Authorization violations

- Mitigation methods
  - PIM "passive mode"
  - Using IPsec among the valid routers on a link
  - IP filtering of PIM messages (all of proto=103)

  - Main issues are with multiple valid PIM routers on a link
    - you'll have to use IPsec between them to be secure.
    - with just one router, filtering PIM messages is a good method

Last-hop threats to PIM - Now what

- What's the contribution of this draft?
  - Explicit threat/vulnerability analysis and spelling out
  - More elaborate description compared to the PIM spec section 6.1
  - More extensive discussion of non-IPsec countermeasures
    - and in which cases IPsec is a must
- Now what -- options:
  - Make this an Informational RFC of its own (WG adoption)
    - Add an informative reference from the PIM spec?
  - Merge it with the PIM-SM spec's security considerations section
  - Wait until the IESG evaluates the PIM spec, ask/see how they react
    - If necessary, then merge/refer
  - Make this dormant until the PIM-SM spec is revised (for DS)
  - Drop the project completely