Spells out "last-hop" Vulnerabilities

- Nodes may send unauthorized register messages
- Nodes may become unauthorized PIM neighbors
- Routers may accept PIM messages from non-neighbors
  - The PIM spec could probably be tightened here..
- An unauthorized node may be elected as the PIM DR
- A node may become an unauthorized asserted forwarder
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 (deals with off-link register messages as well)
Last-hop threats to PIM (3/3)

- **Status**
  - Only reference/edit. updates since draft-savola-..-02
  - PIM-SM spec referencing this has been published
  - PIM "Passive mode" implemented by at least one vendor (JunOS)

- **What next?**
  - Not much review lately. Is the doc perfect? :-)
  - Time for WGLC or solicit explicit reviews?