Backbone Infrastructure Attacks and Protections

draft-savola-rtgwg-backbone-attacks-03.txt

Pekka Savola
CSC/FUNET

Introduction & Background

- Background: originated in 2006
  - ICMP and TCP-RST attacks, ingress filtering etc. were a hot topic
  - Understanding in IETF lacking wrt attack/protection applicability
  - Last discussed at IETF66 at OPSEC & RPSEC WGs, no clear resolution

- An ops view of ISP backbone network attacks
  - Assumes certain degree of ingress/egress filtering in the network
  - Could apply in ~all Tier3+ and enterprise networks

- Target audience
  - IETF people working on standardization of protections
  - Ops people in applicable deployments

Some related work

- RFC 4778 (i.e. draft-ietf-opsec-current-practises)
  - More generic, did not analyze attack/protection big picture
- draft-ietf-opsec-infrastructure-security (halted)
  - A set of "tools", but not the big picture
- draft-zinin-rtg-dos-02 (May 2005, expired)
  - Implementation approaches for control plane protection
- Non-IETF: Team Cymru, secure router templates
  - Offers quite a few tips but no big picture

- Observation: attempts at protection listings
  - But no analysis of attacks/protections
  - Ops view of a big picture missing so far
  - Is IETF the wrong forum or ..?

Next steps?

- Is this useful enough to be published as an RFC?
  - If yes, is the scope of the document appropriate?
    - If not, how should it be changed?
- Is OPSEC the right place to work on this?
- How many have read the document?
  - How many think this is essentially ready?