IP Router-Alert Considerations and usage

draft-rahman-rtg-router-alert-considerations-02

Reshad Rahman
David Ward
Francois Le Faucheur
Ashok Narayanan
Cisco

Adrian Farrel
Old Dog Consulting

Tony Li
Redback

Francois Le Faucheur
flefauch@cisco.com

What is this all about?

- RAO security concerns & solutions not documented well
- Some feel careful router implementation & careful deployment address the RAO security concerns
- Most feel concerns are far from addressed
- Practical questions remain unanswered:
  - Should IETF discourage definition of new protocols using RAO?
  - Should IETF block extensions to existing protocols using RAO?
  - Should an operator block e2e RAO packets to protect itself?
  - Should RAO definition be enhanced?
- Objective: documents concerns/solutions and answer above questions

History

- Work started in Routing Area
- Recently moved to Internet-Area

IP Router Alert Documents

draft-rahman-rtg-router-alert-considerations-02

- Based on current RAO definition
- BCP Track
- Concerns & Recommendations

draft-narayanan-rtg-router-alert-extensions-00

- Explores enhanced RAO definition

The Fundamental RAO Concern

- Basic RAO semantic → punt to slow path
- No mechanism specified to facilitate triage between desired & undesired RAO packets

→Potential RAO-based DOS attack

Use of RAO by New Protocols ?

- e2e delivery of RAO packets cannot be relied upon today
  - Some ISPs simply drop received RAO packets
- new Apps are likely to be muxed over shared transport protocol (which prevents per-PID triage)

→ **"it is RECOMMENDED that new end to end applications or protocols be developed without using IP Router Alert"** *(*)*

(*) assuming current definition of RAO

Use of RAO by Existing Protocols in Controlled Environments ?

- RAO can be used safely in isolated environments
  - e.g. Enterprise network
- RAO can also be used safely in more sophisticated controlled environments, (e.g. Enterprise + SP, provided the SP protects himself efficiently):
  - By Implementing efficient triage & rate-limiting of “undesired RAO” at every hop, or
  - By Tunneling “undesired RAO” (draft-dasmith-mpls-ip-options)

→Existing protocols are used and are OK in Controlled Environments

→extensions to existing protocols that use RAO in Controlled Environments are OK

Router Alert Protection Approaches for Service Providers

→ it is RECOMMENDED that a SP implements strong protection against RAO attack

→ it is RECOMMENDED that an SP uses mechanisms that avoid dropping of e2e RAO

→ SP may:

- → Turn-off RAO punting (if does not depend on RAO)
- → Use selective filtering and rate-limiting (e.g. to protect RSVP-TE)
- → "Tunnel RAO" via mechanisms such as discussed in [I-D.dasmith-mpls-ip-options]
- → As the very last resort, drop RAO packet

Guidelines for Router Implementation

- → It is RECOMMENDED that RAO implementations include protection mechanisms against RAO-based DOS attacks
  - → E.g ability on an edge router to "tunnel" RAO as discussed in [I-D.dasmith-mpls-ip-options]
  - → E.g. new implementations may include selective (possibly dynamic) filtering and rate-limiting of RAO packets
- → A router implementation SHOULD forward within the "fast path" a packet carrying RAO containing a payload that is not of interest

Proposed Next Steps

- Get review
- Turn into WG document,
- Issue as BCP

Back Up slides

Changes 01→02

- Adjusted structure for clarity and to provide clearer answers to the key RAO related questions:
  - we recommend new protos don't use RAO
  - it is OK for existing protos to use RAO in an umber of controlled environments
  - there are better ways for an SP to protect themselves than dropping RAO packets
  - router implementations should think about protection against RAO DOS
- In accordance with RTG WG feedback, remove the details on the various mechanisms that could be implemented by a router for RAO protection (those are implementation specific) and replace with generic recommendation (section 4)