SRv6 Operational Security Considerations

<draft-bdmgct-spring-srv6-security>

Nick Buraglio (*Esnet*), Tal Mizrahi (*Huawei*)
Tian Tong (*China Unicom*), Luis M. Contreras (*Telefónica*)

IETF 119, Brisbane, March 2024

Goals

- Provide comprehensive, unbiased view of what running SRv6 looks like from a risk perspective.
- Outline the practical security considerations for operating a production SRv6 based network.
- Create a referenceable draft useful to get folks started, and fill in operational gaps.

Where we are

- Version -01 released before IETF 119
- Progress of the document with several addition / fixes
  - Technical (details on next slides)
  - Added terminology
  - Open points moved to section on “Topics for Further Discussion”
  - Added Luis to the draft

Technical progress
New section on attacks

- Reformulation of previous chapter on security considerations
- Attacks structured in the form Overview / Scope / Impact
- Attacks considered
  - SR modification attack
  - Reconnaissance
  - Packet insertion
  - Control and Management plane attacks
  - Others

Technical progress
Expansion of section on mitigation methods

- Methods to mitigate the previous attacks
- Methods considered
  - Filtering (both for SRH and address range)
  - Encapsulation of packets

Technical progress

New section on implications on existing equipment

- Previous sub-section transformed in new section with focus on impacts in existing equipment
- Implications considered
  - Limitations in filtering capabilities
  - Middlebox filtering issues
  - Emerging technology growing pains

More details

- Current repo: https://github.com/buraglio/draft-bdmgct-spring-srv6-security
- Pull requests and reviewers welcomes (and encouraged)
- https://buraglio.github.io/draft-bdmgct-spring-srv6-security/draft-bdmgct-spring-srv6-security.html

Next steps

- Authors believe the draft is ready for WG adoption
- Collect comments and feedback from the WG
- Work on surveying existing security considerations across WG documents / RFCs