Security Considerations for SRv6 Networks

draft-li-spring-srv6-security-consideration-10

C. Li, **N. Geng**, C. Xie, H. Tian, T. Tian, Z. Li, J. Mao

March 2023

Introduction

- This document describes various threats to networks deploying SRv6. SRv6 inherits potential security vulnerabilities from source routing in general, and also from IPv6 [RFC9099].
- Main content
  - Describe various threats and security concerns related to SRv6 networks and existing approaches to solve these threats
  - Provide some security policies
- The document can provide some guidance to SRv6 network operations. It can also be used as a reference for other SRv6 documents.

Threats and Solutions

- □ Eavesdropping
  - ◆Solutions: ESP can be used in order to prevent Eavesdropping.
- □ Packet Falsification
  - ◆Solutions: HMAC
- □ Identity Spoofing
  - ◆Solutions: AH, ESP or HMAC; SAV BCP 84 [RFC3704]
- □ Packet Replay
  - ◆Solutions: ESP can be used to prevent Replay Attacks.
- □ DoS/DDoS
  - ◆Solutions: ICMPv6 rate-limiting; DoS/DDoS mitigation tools; SAV

Update History

□ Previous Main Updates (v00-v09, from2019 to 2022)

- ◆More details in threat analysis and solution
- ◆Add some figures for illustrating solutions

□ Recent Updates (v10, 2023)

- ◆Add some descriptions on source address validation in sec. 4.3 (ID spoofing);
- ◆Add some descriptions on DoS which attacks the target SIDs and some descriptions on DoS mitigation tools;
- ◆Remove sec. 5. The effects of the threats will be incorporated into sec. 4;
- ◆Update the sections of security considerations and IANA considerations.

□ Next steps

- ◆Solicit comments and refine the draft

Thanks!