Spring
Internet-Draft
Intended status: Informational
Expires: January 9, 2020

C. Li
Z. Li
Huawei

July 8, 2019

Security Considerations for SRv6 Networks
draft-li-spring-srv6-security-consideration-01

Abstract

SRv6 inherits potential security vulnerabilities from Source Routing in general, and also from IPv6. This document describes various threats and security concerns related to SRv6 networks and existing approaches to solve these threats.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 9, 2020.

Table of Contents

1. Introduction

Segment routing (SR) [RFC8402] is a source routing paradigm that explicitly indicates the forwarding path for packets at the source node by inserting an ordered list of instructions, called segments. A segment can represent a topological or service-based instruction.

When segment routing is deployed on IPv6 [RFC8200] dataplane, called SRv6 [I-D.ietf-6man-segment-routing-header], a segment is a 128 bit value, and can the IPv6 address of a local interface but it does not have to. For supporting SR, a new type of Routing Extension Header is defined and called the Segment Routing Header (SRH). The SRH contains a list of SIDs and other information such as Segments Left. The SRH is defined in [I-D.ietf-6man-segment-routing-header]. By using the SRH, an ingress router can steer SRv6 packets into an explicit forwarding path so that many use cases like Traffic Engineering, Service Function Chaining can be deployed easily by SRv6.

However, SRv6 also brings some new security concerns. This document describes various threats to networks deploying SRv6. SRv6 inherits

potential security vulnerabilities from source routing in general, and also from IPv6.

- SRv6 makes use of the SRH which is a new type of Routing Extension Header. Therefore, the security properties of the Routing Extension Header are addressed by the SRH. See [RFC5095]and [I-D.ietf-6man-segment-routing-header] for details.

- SRv6 consists of using the SRH on the IPv6 dataplane which security properties can be understood based on previous work [RFC4301], [RFC4302], [RFC4303] and [RFC4942].

In this document, we will consider the dangers from the following kinds of threats:

- Wiretapping/eavesdropping

- Packet Falsification

- Identity Spoofing

- Packet Replay

- DOS/DDOS

- Malicious Packet Data

The rest of this document describes the above security threats in SRv6 networks and existing approaches to mitigate and avoid the threats.

2. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119] and [RFC8174].

This document uses the terminology defined in [RFC5095] and [I-D.ietf-6man-segment-routing-header].

3. Security Principles of SRv6 Networking

As with other similar source-routing architectures, an attacker may manipulate the traffic path by modifying the packet header. SPRING architecture [RFC8402] allows clear trust domain boundaries so that source-routing information is only usable within the trusted domain and never exposed to the outside world. It is expected that, by

default, explicit routing is only used within the boundaries of the administered domain. Therefore, the data plane does not expose any source-routing information when a packet leaves the trusted domain. Traffic is filtered at the domain boundaries [RFC8402].

Unless otherwise noted, the discussion in this document pertain to SR networks which can be characterized as "trusted domains", i.e., the SR routers in the domain are presumed to be operated by the same administrative entity without malicious intent and also according to specifications of the protocols that they use in the infrastructure.

This document assumes that the SR-capable routers and transit IPv6 routers within the SRv6 trusted domains are trustworthy. Hence,the SRv6 packets are treated as normal IPv6 packets in transit nodes and the SRH will not bring new security problem. The security considerations of IPv6 networks are out of scope of this document.

4. Types of Vulnerabilities in SR Networks

This section outlines in details the different types of vulnerabilities listed in Section 1. Then, for each type, an attempt to determine whether or not the vulnerability exists in a trusted domain is made.

4.1. Eavesdropping Vulnerabilities in SRv6 Networks

As with practically all kinds of networks, traffic in an SRv6 network may be vulnerable to eavesdropping.

- Threats: Eavesdropping

- Solutions: Encapsulating Security Payload (ESP, [RFC4303]) can be used in order to prevent Eavesdropping. The ESP header is either inserted between the IP header and the next layer(transport) protocol header, or before an encapsulated IP header (tunnel mode). ESP can be used in order to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and (limited) traffic flow confidentiality. The set of services provided depends on the selected options at the time of the Security Association (SA) establishment and on the location of the implementation in a network topology.(add reference to the different points explained in this paragraph).

- Conclusion: In tunnel mode of ESP, packets are encrypted and can not be eavesdropped in a trusted SRv6 domain. In transport mode of ESP, the payload of packets are encrypted and cannot be

eavesdropped in a trusted SRv6 domain, even if the IPv6 and SRH headers are not encrypted.

- Gaps: The IPv6 and SRH headers are not encrypted in transport mode of ESP which may be eavesdropped by attackers.

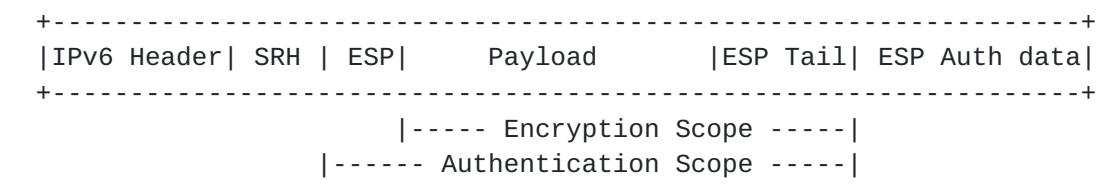

Figure 1: Transport Mode ESP for SRv6 packets

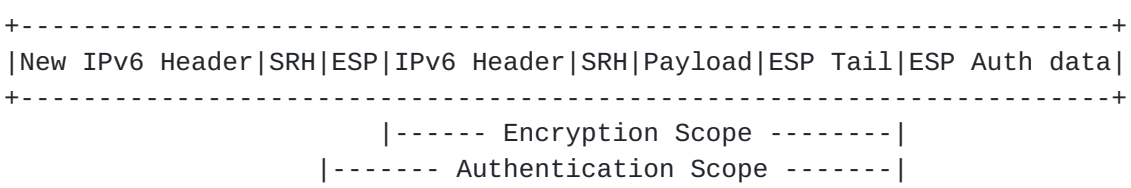

Figure 2: Tunnel Mode ESP for SRv6 packets

4.2. Packet Falsification in SRv6 Networks

As SRv6 domain is a trusted domain, there is no Packet Falsification within the SRv6 domain.

As the packets from outside of SRv6 domain cannot be trusted, an Integrity Verification policy is typically deployed at the external interfaces of the ingress SRv6 routers in order to verify the incoming packets (i.e., from outside of SRv6 domain [I-D.ietf-spring-srv6-network-programming]). Also, the packets with SRH sent form hosts within the SRv6 domain should be verified in order to prevent the falsification between the host and the ingress router. [I-D.ietf-spring-srv6-network-programming].

- Threats: Packet Falsification

- Solutions: The packets from outside can not be trusted, so Integrity Verification policy should be deployed at the external interfaces by using , e.g., IPSec [RFC4301] (AH [RFC4302], ESP [RFC4303]) or HMAC [RFC2401]. AH [RFC4302], ESP [RFC4303] and HMAC [RFC2401] can provide Integrity Verification for packets, while the ESP can encrypt the payload in order to provide higher security. However, it has been noted that the AH and ESP are not directly applicable in order to reduce the vulnerabilities of SRv6

due to the presence of mutable fields in the SRH. In order to solve this problem, [I-D.ietf-6man-segment-routing-header] defines a mechanism in order to carry HMAC TLV in the SRH so to verify the integrity of packets including the SRH fields. The HMAC TLV is usually processed based on the local policy, only at the ingress router. Within the SRv6 domain, the packets are trusted, so HMAC TLV is typically ignored. In other words, the segment list is mutable within the SRv6 domain but cannot be changed before processing the HMAC TLV.

- o Conclusions: There is no Packet Falsification within a trusted SRv6 domain. Integrity Verification policy like HMAC processing should be deployed at the external interfaces of the ingress SRv6 routers filtering SRH packets from outside the trusted domain and SRH packets from hosts within the SRv6 domain.

- o Gaps: IPsec cannot provide verification for SRH.

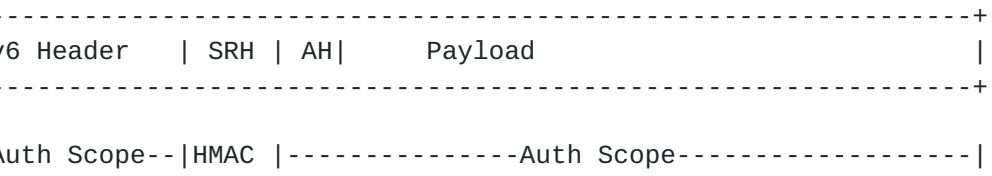

Figure 3: Transport Mode AH and HMAC for SRv6 packets

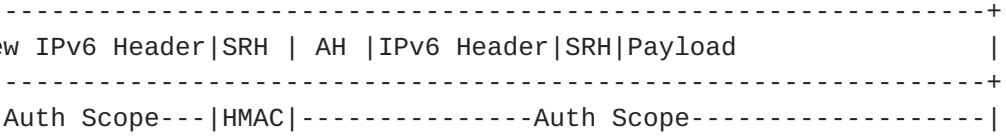

Figure 4: Tunnel Mode AH and HMAC for SRv6 packets

4.3. Identity Spoofing in SRv6 Networks

The same as for Packet Falsification, there is no Identity Spoofing possible within the boundaries of a SRv6 trusted domain where all nodes are under control of the same administrative organization.

Authentication policy should be deployed at the external interfaces of the ingress SRv6 routers in order to validate the packets from outside of SRv6 domain [I-D.ietf-spring-srv6-network-programming]. Also, the packets with SRH sent form hosts inside the SRv6 domain should be validated in order to prevent the Identity Spoofing [I-D.ietf-spring-srv6-network-programming].

- Threats: Identity Spoofing

- Solutions: IPSec [RFC4301] (AH [RFC4302], ESP [RFC4303]) or HMAC [RFC2401] can be used for Authentication. AH, ESP and HMAC can provide Authentication of source node, while the ESP can encrypt the payload in order to provide higher security. Same as section 3.2.

- Conclusion: There is no Identity Spoofing within a trusted SRv6 domain. Identity Spoofing policy should be deployed on the external interfaces of the ingress SRv6 routers for the packets from outside and the packets with SRH from hosts within the SRv6 domain.

- Gaps: TBA

4.4. Packet Replay in SRv6 Networks

There are no new Packet Replay threat brought by SRH. ESP can be applied to SRv6 in order to prevent Packet replay attacks.

- Threats: Packet Replay

- Solutions: ESP [RFC4303]) can be used to prevent Replay Attacks.

- Conclusion: There are no new Packet Replay threat brought by SRH. ESP can be applied to SRv6 in order to prevent Packet replay attacks.

- Gaps: TBD

4.5. DOS/DDOS in SRv6 Networks

The generation of ICMPv6 error messages may be used in order to attempt DOS(Denial-Of-Service)/DDOS(Distributed Denial-Of-Service) attacks by sending an error-causing destination address or SRH in back-to-back packets [I-D.ietf-6man-segment-routing-header]. An implementation that correctly follows Section 2.4 of [RFC4443] would be protected by the ICMPv6 rate-limiting mechanism also in the case of packets with an SRH.

- Threats: DOS/DDOS

- Solutions: ICMPv6 rate-limiting mechanism as defined in [RFC4443]

- Conclusions: There are no DOS/DDOS threats within SRv6 domain, the threats come from outside of the domain, and can be prevented by ICMPv6 rate-limiting mechanism.

- Gaps: TBD

4.6. Malicious Packet Data in SRv6 Networks

TBA

5. Effects of the above on SRv6 Use Cases

This section describes the effects of the above-mentioned vulnerabilities in terms of applicability statement and the use cases given in citation.

TBA.

6. Security Policy Design

The basic security for intra-domain deployment is described in [I-D.ietf-spring-srv6-network-programming] and the enhanced security mechanism is defined in [I-D.ietf-6man-segment-routing-header].

In [I-D.ietf-spring-srv6-network-programming], additional basic security mechanisms are defined. For easier understanding, a easy example is shown in Figure 5.

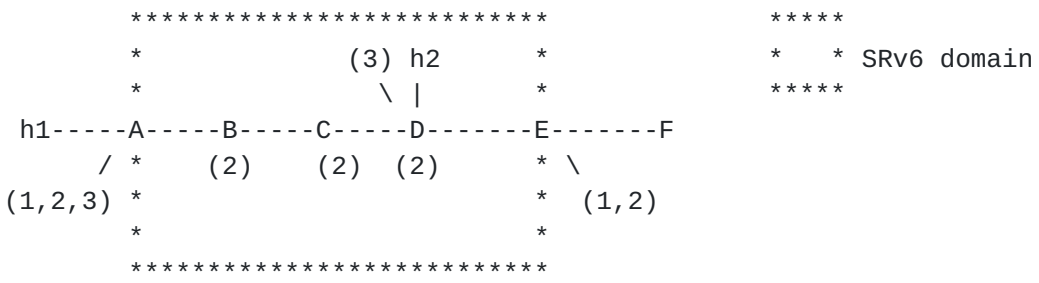

Figure 5: SRv6 Security Policy Design

- A-E: SRv6 Routers inside the SRv6 domain, A and E are the edge router, can be called Ingress router instead.

- F: Router F outside the SRv6 domain.

- h1: A host outside the SRv6 domain connects to router Router A.

- h2: A host within SRv6 domain, which connects to the Router D.

- (1): Security policy 1: ACL for External Interface.

- (2): Security policy 2: ACL for Internal Interfaces.

- (3): Security policy 3: Policy for processing HMAC, should be deployed at the ingress nodes.

6.1. Basic Security Design

6.1.1. ACL for External Interfaces

Typically, in any trusted domain, ingress routers are configured with Access Control Lists (ACL) filtering out any packet externally received with SA/DA having a domain internal address. An SRv6 router typically comply with the same rule.

A provider would generally do this for its internal address space in order to prevent access to internal addresses and in order to prevent spoofing. The technique is extended to the local SID space. However, in some use cases, Binding SID can be leaked outside of SRv6 domain. Detailed ACL should be then configured in order to consider the externally advertised Binding SID.

6.1.2. ACL for Internal Interfaces

An SRv6 router MUST support an ACL with the following behavior:

```
1. IF (DA == LocalSID) && (SA != internal address or SID space) :
2.    drop
```

This prevents access to locally instantiated SIDs from outside the operator's infrastructure. Note that this ACL may not be enabled in all cases. For example, specific SIDs can be used to provide resources to devices that are outside of the operator's infrastructure.

6.1.3. SID Instantiation

As per the End definition [I-D.ietf-spring-srv6-network-programming], an SRv6 router MUST only implement the End behavior on a local IPv6 address if that address has been explicitly enabled as an SRv6 SID.

Packets received with destination address representing a local interface that has not been enabled as an SRv6 SID MUST be dropped.

6.2. Enhanced Security Design

HMAC [RFC2401] is the enhanced security mechanism for SRv6 as defined in [I-D.ietf-6man-segment-routing-header]. HMAC is used for validating the packets with SRH sent from hosts within SRv6 domain.

Since the SRH is mutable in computing the Integrity Check Value (ICV) of AH [I-D.ietf-6man-segment-routing-header], so AH can not be directly applicable to SRv6 packets. HMAC TLV in SRH is used for making sure that the SRH fields like SIDs are not changed along the path. While the intra SRv6 domain is trustworthy, so HMAC will be processed at the ingress nodes only, and could be ignore at the other nodes inside the trusted domain.

7. Security Considerations

TBA

8. Acknowledgements

Manty thanks to Charles Perkins and Stefano Previdi's valuable comments.

9. References

9.1. Normative References

[I-D.ietf-6man-segment-routing-header]
Filsfils, C., Dukes, D., Previdi, S., Leddy, J., Matsushima, S., and d. daniel.voyer@bell.ca, "IPv6 Segment Routing Header (SRH)", draft-ietf-6man-segment-routing-header-21 (work in progress), June 2019.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, DOI 10.17487/RFC5095, December 2007, <https://www.rfc-editor.org/info/rfc5095>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/info/rfc8174>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

[RFC8402] Filsfils, C., Ed., Previdi, S., Ed., Ginsberg, L., Decraene, B., Litkowski, S., and R. Shakir, "Segment Routing Architecture", RFC 8402, DOI 10.17487/RFC8402, July 2018, <https://www.rfc-editor.org/info/rfc8402>.

9.2. Informative References

[I-D.ietf-spring-segment-routing-policy]
Filsfils, C., Sivabalan, S., daniel.voyer@bell.ca, d., bogdanov@google.com, b., and P. Mattes, "Segment Routing Policy Architecture", draft-ietf-spring-segment-routing-policy-03 (work in progress), May 2019.

[I-D.ietf-spring-srv6-network-programming]
Filsfils, C., Camarillo, P., Leddy, J., daniel.voyer@bell.ca, d., Matsushima, S., and Z. Li, "SRv6 Network Programming", draft-ietf-spring-srv6-network-programming-01 (work in progress), July 2019.

[RFC2401] Kent, S. and R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, DOI 10.17487/RFC2401, November 1998, <https://www.rfc-editor.org/info/rfc2401>.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005, <https://www.rfc-editor.org/info/rfc4301>.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005, <https://www.rfc-editor.org/info/rfc4302>.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005, <https://www.rfc-editor.org/info/rfc4303>.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006, <https://www.rfc-editor.org/info/rfc4443>.

[RFC4942] Davies, E., Krishnan, S., and P. Savola, "IPv6 Transition/ Co-existence Security Considerations", RFC 4942, DOI 10.17487/RFC4942, September 2007, <https://www.rfc-editor.org/info/rfc4942>.

[RFC7855] Previdi, S., Ed., Filsfils, C., Ed., Decraene, B., Litkowski, S., Horneffer, M., and R. Shakir, "Source Packet Routing in Networking (SPRING) Problem Statement and Requirements", RFC 7855, DOI 10.17487/RFC7855, May 2016, <https://www.rfc-editor.org/info/rfc7855>.

Authors' Addresses

Cheng Li
Huawei
China

Email: ChengLi13@huawei.com

Zhenbin Li
Huawei
China

Email: lizhenbin@huawei.com