Security Considerations for Networks Using SRv6
draft-perkins-sr-security-00

Abstract
This document identifies various threats to networks employing segment routing over an IPv6 transport. Segment Routing inherits potential security vulnerabilities from source routing in general, and from label-switching approaches such as MPLS. The document discusses how common security vulnerabilities may be present in SRv6 networks, depending on the security policies that are imposed.

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 2, 2020.

Copyright Notice

Copyright (c) 2019 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (https://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of
This document identifies various threats to networks employing segment routing. Segment Routing inherits potential security vulnerabilities from source routing in general, and also from label-switching approaches such as MPLS. The document discusses how common
security vulnerabilities may be present in SRv6 networks, depending on the security policies that are imposed.

- SR is a descendent of IPv6 routing header, and consequently its security properties need to be understood in light of previous work [RFC5095].

- SRv6 inherits some insecurities from label-switching architecture. Some of the consequences have been outlined in [RFC8341].

SRv6 is envisioned for use in a number of important kinds of network deployments (see [RFC8354], [I-D.ietf-dmm-srv6-mobile-uplane]):

- SRv6 in the Small Office
- SRv6 in the Access Network
- SRv6 in Data Center
- SRv6 in Content Delivery Networks
- SRv6 in Core Networks
- SRv6 for user-plane in mobile networks

Segments are currently being designed and applied to exploit SRv6 for the above use cases (see [RFC8402], [I-D.ietf-dmm-srv6-mobile-uplane]). Some of these segments are as follows:

- IGP-Prefix
- IGP-Node
- IGP-Anycast
- IGP Adjacencies
- BGP-Prefix
- BGP Peering
- IGP Mirroring Context
- IGP-Prefix
- Args.Mob.Session
o  End.M.GTP6.E (GTP encapsulation)

o  End.M.GTP6.D (GTP decapsulation)

o  End.Limit

During the discussion in the following sections, the above segments may be useful for more concrete understanding of the vulnerabilities.

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

o  Loss of Confidentiality

o  Tampering with Packet Data

o  Packet data intending to cause harm

o  Denial of Origination

o  Packet Replay

o  Loss of Connectivity

o  Identity Theft

o  Hijacking

o  DoS, Distributed DoS

In the rest of this document, applicability for Segment Routing and for the details of the security observations will first be described. Then the terminology will be presented, followed by a review of threats and network vulnerabilities as recently discussed at IETF meetings. Some new mechanisms introduced by SR that can threaten network security are outlined. Then, in order to have more concrete understanding, some use cases envisioned for Segment Routing architectures will be reviewed according to the descriptions in other cited documents. Afterwards, several kinds of security policies relevant to SR network administration will be outlined. This collection of security policies is not intended to be comprehensive, but at least representative of possible SR networks. Finally, some ameliorations for some of the threats will be described as well as known gaps in an effort to motivate future work.
2. Applicability

"Segment Routing Architecture" [RFC8402] recommends that SR should be restricted to operation within a trusted domain. In other words, the SR routers in the domain are presumed to be operating without malicious intent and also to conform to specification for the protocols that they use.

A network’s vulnerability to each threat depends substantially on whether or not the network border routers accept incoming packets with segments. On the other hand, there are use cases for which an incoming source route can be quite useful (e.g., for Mobile IP [RFC6275]), and advances in SRv6 security would be beneficial to such use cases.

It also has to be specified whether or not all routers in the network (not just SR-capable) are all trusted. A network might allow intermediate routers to handle interconnections between SRv6 routers. These intermediate routers would not require any SRv6 capability, or security associations with SRv6 routers. They would be configured so that they would never insert or delete any SID.

It has been noted that AH and ESP are not directly applicable to reducing the vulnerabilities of SR routing, due to the presence of mutable fields in the SR Header. Future work to improve security in SRv6 networks will be to include a new design so that SRv6 mutable fields can be authenticated separately while still allowing use of these basic IPv6 functions.

3. 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 [RFC8402] and [RFC5095]. In addition, the following definitions are used.

trusted domain: A network in which all routers are known to be trustworthy.

closed domain: A network in which border routers reject any incoming packet that includes a SRv6 header.

ingress domain: A network in which border routers may accept certain incoming packets that include a SRv6 header.
4. Types of Vulnerabilities in SR Networks

Each vulnerability in the previous section requires particular attention and evaluation within the context of the various security policies for SRv6 considered in this document.

4.1. Loss of Confidentiality

As with practically all except the simplest networks, intermediate routers and transit points might be able to eavesdrop on traffic in an SR network unless measures are taken to hide the data in the packet.

However, in the case of SR networks, the segments in the segment stack are often used to express and carry out routing policies, which can be tailored to the needs of individual flows. Allowing inspection of the segments might allow a malicious party to infer policy information which is not intended for distribution to unauthorized parties.

4.2. Tampering with Packet Data

Packet data in an SR network is vulnerable to tampering unless all intermediate routers and transit points are trustworthy.

4.3. Loss of Connectivity

SRv6 networks that make use of a centralized control plane may be threatened by loss of connectivity (whether accidental or malicious) between the central controller and the network nodes. This is important since such networks depend on centralized controllers (PCE, etc.) to calculate flow paths and resulting SID lists, and the installation of the SID lists in edge/border routers.

4.4. Identity Theft

Does SRv6 create new vulnerability to Identity Theft in the network?

4.5. Hijacking

One of the main dangers from a compromised SR network router is that data in the network can be hijacked and sent to an unintended destination. Or, equally, selected data can be prevented from reaching an intended destination, or may be sent along a path that was not originally intended.
4.6. Denial of Origination

In many situations, it is important to prove whether or not the apparent source of a packet in fact originated that packet. Otherwise, for example, the true source may claim that the packet was forged and decline responsibility for a completed transaction. The segments used in an SRv6 deployment should be analyzed to see if this vulnerability is introduced.

4.7. Packet/Segment Replay

Replaying packets, to deceive the destination into thinking that the source has repeated a transaction, is an ever-present danger. In SR networks, there is the further danger of "replaying" segments from previous packets without otherwise modifying the payload of the new packet.

4.8. Distributed DoS

Distributed denial of service (DDoS) attacks take many forms and can effectively crash an entire network, or any part of the network. If malicious segments could be configured into the SR routers, say for a sensitive destination, then all such configured routers could be triggered with instructions to repeatedly bombard that destination while at the same time causing other network traffic to cease.

4.9. Malicious Packet Data in SR Networks

Suppose that an SRv6 network’s infrastructure is known to be vulnerable to particular sequences of network elements -- say, because an adversary has discovered that the release of the SRv6 router’s operating system has certain bugs, or poor configuration. In this case, the SR network may be vulnerable to insertion of segments tailored to trigger bugs in a nonlocal SRv6 router.

5. Mechanisms for Misuse of Source Routed Networks

As a packet traverses a SRv6 network, it visits a path of SRv6 routers. The path is determined by the placement of SRv6 segments on the segment stack in the IPv6 SRv6 header. The following malicious behaviors are related to the operation of SRv6 networks:

- SR deletion: defeats traffic management
- SR swapping: defeats traffic management
Address modification: DoS, otherwise same threats as insertion

5.1. SR insertion

By inserting an unauthorized segment in the segment stack, an attacker could cause the packet to be routed for processing by an unaware or compromised router. If the spurious segment were placed farther down in the segment stack, the effect of the insertion would be non-local, and thus detection of the malicious node would be more difficult. Since the SID also determines the processing steps that are taken by an SRv6 router, an attacker that is aware of the meaning of the SIDs at any particular point along the segment path, could insert particular unwanted processing steps for the packet. For instance, unauthorized traffic handling or charging could be applied to the packet.

5.2. SR deletion

By deleting a segment in the segment stack, an attacker could cause the packet to avoid various processing steps including inspection or accounting. If the deleted segment was placed farther down in the segment stack, the effect of the deletion would be non-local, and thus detection of the malicious node would be more difficult.

5.3. SR swapping

Segment swapping can be accomplished by deletion and subsequent reinsertion, possibly done twice. Such swapping would not be detectable by any non-cryptographic checksum mechanism.

5.4. SID tampering

Every router along the routing path of a packet in an SRv6 network has the opportunity to tamper with the segments that are present in the segment stack. This is possible even for routers that are not SRv6 routers, because each such router could inspect the IPv6 packet header to determine whether or not the SR header is present.

By tampering with the Segment ID or the data associated with the Segment ID, each such router along the path could cause unwanted processing steps, or defeat traffic management for the packet.

6. Effects of the above on SR Use Cases

In the following sections we describe the effects of the above-mentioned threats in terms of applicability statement and the use cases given in [RFC8354] and [I-D.ietf-dmm-srv6-mobile-uplane].
Almost by the very nature of Segment Routing, hijacking of traffic flows is possible by inserting an unauthorized segment into an existing segment stack, or by modifying the destination address of one of the segments already on the stack. This threat has to be considered for each one of these use cases. In fact, almost all networks are vulnerable to hijacking attacks if one of the routers is compromised. What is new with SRv6 networks, is that the actual hijacking can occur at a point in the routing path that is arbitrarily distant from the point at which the unauthorized segment was inserted. This could complicate attempts to identify the source of the attack.

6.1. Threats to SRv6 in the Small Office

According to [RFC8354], "A SPRING-enabled SOHO provides the ability to steer traffic into a specific path from end hosts in the SOHO or from a customer edge router in the SOHO".

A malicious node might be able to steer particular traffic flows into a more favorable or less favorable path. This could include sending packets originated by an end host within the SOHO out through an unauthorized edge router.

6.2. Threats to SRv6 in the Access Network

Access networks are typically required to provide efficient service to a wide variety of traffic flows. Some flows may consume only a small amount of network capacity, but require very low latency for packet delivery. Other flows may be resilient against packet loss but have requirement for high capacity. There may be regulatory requirements in place, and sometimes the nature of traffic between two endpoints can change, requiring a dynamic readjustment for handling by the service provider.

A malicious node might be able to disrupt the orderly classification or modify the segment path through the access network. This could
enable particular flows to evade regulatory requirements, or to avoid proper billing for use of resources.

6.3. Threats to SRv6 in Data Center

SRv6 is attractive for use by data center operators in order to provide a scalable platform for multiple (or many) tenants. The path taken by information through the data center interconnection can be closely controlled by segment routing and tailored to the needs of specific tenants.

A malicious node might be able to divert traffic from one tenant network into a different routing space. It would also be possible to divert traffic to take advantage of resources that are paid for by some other tenant, and have the next segment on the segment stack restore the packet to its original path after making unauthorized use of the other tenant’s resources.

6.4. Threats to SRv6 in Content Delivery Networks

Content Delivery Networks (CDNs) have placed new requirements for supplying video traffic to consumers across operator networks and infrastructure. Some of the traffic is real time; for example, television programming, news, and sports events. Other traffic may require higher bandwidth but also allow more buffering for resilience against temporary bottlenecks, such as high definition movies. In the future, the requirements for special handling of video content will only increase, especially as virtual and augmented reality applications become more popular.

Caching is an important technique for delivering video content to many customers at the same time. The caches can be provisioned hierarchically. In such a system, segment routing can be designed for beneficial use to proceed along a path of cached data in the hierarchy until a cache hit provides the desired content.

A malicious node might be able to cause major disruption and service outage to many paying customers by misdirection of cache requests along the service hierarchy. Other threats are similar to those listed against SRv6 deployment in access networks.

6.5. Threats to SRv6 in Core Networks

In order to meet the divergent demands for different kinds of service, network operators have been buying more specialized equipment for deployment within their core infrastructure. Some of the equipment has extremely high bandwidth compared to existing equipment, so that the network as a whole supports network paths with
widely varying capacities. Some lower-bandwidth paths through the core infrastructure may be connected to allow very low-latency communications. Some portions of the network may be set up to handle very predictable traffic in a more efficient manner. Detnet [RFC8557], [RFC8558] is likely to create new requirements for diversity, resilience, and low latency.

A malicious node that could make changes to a segment path through a core network would be able to cause major damage to the network and to perhaps millions of customers. By inserting unauthorized segments, diversion to a hostile node could be accomplished for traffic analysis, delay, hijacking, or almost arbitrary disruption to the customers' network communications. By the nature of segment handling, this disruption could occur in places of the network not immediately traceable to the malicious device inserting the unauthorized segment.

6.6. Threats to SRv6 in Mobile User Plane

It has been proposed to use Segment Routing to gain tenant isolation and support traffic management for user plane architectures designed for 5G mobile networks [I-D.ietf-dmm-srv6-mobile-uplane]). In particular, segments have been defined to allow re-use of existing user-plane equipment by instructing the segment router to perform GTP encapsulation and decapsulation steps. Other mobility-related activities are possible to support rapid handover. Moreover, even within an IPv6-only mobile infrastructure, there will be a long-standing need for support of IPv4 GTP tunneling.

A malicious node might be able to change the endpoint for decapsulation of GTP traffic, or target particular mobile devices for eavesdropping or mismanagement. Since many people use their mobile devices for financial transactions and personal data, this would represent a major loss of privacy and financial risk for all such customers.

7. Some Trust Models

Depending upon the trust model enforced by the administration of the SRv6 network, the previously mentioned threats may be largely countered and/or prevented. In this section, some observations will be offered about specific effects of the trust model. Some recommendations will be made about work that might be undertaken to further diminish the dangers from those threats.
7.1. Trusted Domain

Many of the threats to a trusted domain Section 3 are effectively nullified by the tight administration required to configure and maintain the security associations between all the routing elements in the domain.

Since all of the routing elements are presumed to not be malicious, none of them will attempt to hijack the traffic.

Also, since the routing elements are presumed to not be malicious, there is no danger that the routers would tamper with the packet data or the segment stack in the SR header.

There might still be a danger of loss of confidentiality, if packets are visible to other nodes on the subnets upon which the routers reside.

7.2. Closed Domain

In a closed domain Section 3 all of the known Segment Routers are presumed not to be malicious, but some of the other routers may have a lesser level of assurance against compromise.

Unfortunately, a non-SR router might misperform by pretending to be an SR-router. In that case, the compromised router could attempt to modify the contents of the segment stack in some arbitrary manner. This could leave the closed domain vulnerable to most of the threats described in Section 4.

In particular there are the dangers of hijacking, packet replay, and loss of confidentiality. The first two can be triggered "remotely", so that none of the routers adjacent to the malicious action can be identified as responsible for executing the threat.

7.3. Ingress Domain

In an ingress domain Section 3 some of the border routers are configured to accept incoming packets that already contain an IPv6 SR header.

In such domains, it is important to exert tight control over the types of segments that may be included in the incoming packet. The syntax and semantics of any such incoming segment has to be well specified and conformant with the routing policy of the ingress domain. For example, source routes used for the purposes of Mobile IP [RFC6275] have very specific restrictions and are not intended to be forwarded past the target of the incoming source route. The
destinations reachable by way of the SR header in the incoming packet should also be tightly controlled so that random internal targets are not visible except by careful prearrangement.

If sufficient control is not exerted over the type or the intended destination of a source route, then many of the threats in Section 4 might become viable and, even worse, established by malicious agents external to the domain. Such external agents are typically not at all under the control of the SR network administrator.

8. Security Considerations

The subject of this draft is to improve understanding of the security model and vulnerabilities associated with Segment Routing.

9. Acknowledgements

Thanks to Andy Malis for his early review of this document.

10. References

10.1. Normative References

[I-D.ietf-dmm-srv6-mobile-uplane]
Matsushima, S., Filsfils, C., Kohno, M., Camarillo, P.,


10.2. Informative References

[I-D.ietf-spring-segment-routing-policy]

Appendix A. Ameliorations

This section lists ameliorations for the previously mentioned list of threats. It is likely to be deleted prior to publication. The purpose is simply to open up discussion about known approaches to minimize the threats listed in this document.

- Ameliorations in core networks.
- Ameliorations in RAN.
o Ameliorations in transit networks.

o The use of ACLs.

o How many security associations are needed if the SR network is not a "trusted domain"?

o Classes of security associations.

o Danger of segment stack exhaustion.

Author’s Address

Charles E. Perkins
Futurewei
2330 Central Expressway
Santa Clara 95050
Unites States

Email: charlie.perkins@futurewei.com