Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 201 (2022) 406–412

Procedia Computer Science

www.elsevier.com/locate/procedia

The 13th International Conference on Ambient Systems, Networks and Technologies (ANT)
March 22 - 25, 2022, Porto, Portugal

On SRv6 Security

David Lo Bascio[a,*], Flavio Lombardi[b,c]

[a]*Department of Information Engineering, Electronics and Telecommunications (DIET) "Sapienza" University of Rome, Italy*
[b]*Istituto per le Applicazioni del Calcolo, Consiglio Nazionale delle Ricerche (IAC-CNR), Rome, Italy*
[c]*Member of the INdAM-GNCS research group*

Abstract

SRv6 is a routing architecture that can provide hybrid cooperation between a centralized network controller and network nodes: IPv6 routers maintain the multi-hop ECMP-aware segments, whereas the controller, responsible for the Traffic Engineering policy, combines them to form a source-routed path through the network. Since the state of the flow is defined at the ingress to the network and then is contained in a specific packet header, called Segment Routing Header (SRH), the importance of such a header itself is vital. Motivated by the increasing success and widespread deployment of such approaches and technologies, this paper introduces the context and discusses some of the issues tied to possible tampering with the Segment Routing Header content. Finally, some details of an experimental testbed aimed at evaluating the above issues are provided.

Keywords: Segment Routing; Networking; Security
2008 MSC: 68M10; 68M11; 68M12; 68M25

1. Introduction

Today's pervasive networks are increasingly smart and flexible [19, 5]. This is also due to the advanced technologies, together with IPv6 support, that are deployed on network devices (both physical ones and virtual ones).

Traffic Engineering (TE) in IP carrier networks is one of the functions that can benefit from the Software Defined Networking (SDN) paradigm [17]. Nevertheless, traditional per-flow routing requires a direct interaction between the SDN controller and each node that is involved in the traffic paths. Segment Routing (SR) is one technology that can help simplify route enforcement by delegating all the configuration and per-flow state at the border of the network.

In the traditional routing approach a distributed intelligence is used: each decision on the traffic path is taken on the packet by each node of the network. In fact, conventional routers in the network determine the path incrementally

* Corresponding author. Tel.: +39-06-44585365; Fax: +39-06-44585632.
E-mail address: david.lobascio@uniroma1.it

1877-0509
10.1016/j.procs.2022.03.054

based on the packet destination. New networking paradigms such as SDN have introduced a centralized optimization but require maintaining a per-flow state on each node.

A Segment Routing (SR) architecture [9] can provide hybrid centralized/distributed cooperation between the controller and the network, where the network maintains the multi-hop ECMP-aware [1] segments while the centralized controller combines them to form a source-routed path through the network. In SR the state is removed from the network and it is only present at the ingress to the network and then in the packet header itself.

The IPv6 protocol has many features including the expanded addressing capability, auto-configuration mechanism, simplification of the header format, improved support for extensions and options (see [12] and [20]), extensions for authentication and privacy, flow labeling capability and so on.

For these reasons SR can be instantiated over the IPv6 data plane, in what is Segment Routing v6 (SRv6) [7], using a new type of Routing Extension Header called the Segment Routing Header (SRH).

The main motivation for our work is the lack of a detailed and comprehensive discussion and experimental validation and evaluation of the potential attacks SRv6 is vulnerable to. As such, this paper aims at introducing the technological context and discussing some of the most relevant issues tied to tampering with the SRH content. The present paper shows that SRv6 technology can be potentially misused and cause security and performance issues that are discussed in the following.

2. Technological Background

A **source-routing** architecture seeks the right balance between distributed intelligence and centralized optimization. Source routing allows the sender of a packet to partially or completely specify the route the packet takes through the network. Two main options exist: *Loose source routing* uses a source routing option in IP to record the set of routers a packet must visit; *Strict source routing* where every step of the route is decided in advance when the packet is sent.

The **Segment Routing (SR)** architecture is based on the loose source routing paradigm. A node steers a packet through an ordered list of instructions, called ”segments”. The list of segments represents an SR policy instantiated at the ingress node to the SR domain. A segment is often referred to by its Segment Identifier (SID), it can represent any kind of instruction. A segment associated with a **topological** instruction can be:

- a topological *local* segment, which may instruct a node to forward the packet via a specific outgoing interface;
- a topological *global* segment, which may instruct an SR domain to forward the packet via a specific path to a destination.

A segment can also be **service-based** – e.g., the packet should be processed by a container or Virtual Machine (VM) associated with the segment – or may be associated with a QoS treatment – e.g., shape the packets received with this segment at x Mbps. The SR architecture supports any type of instruction associated with a segment.

The SR architecture supports any type of **control plane**: distributed, centralized, or hybrid. In a *distributed* control plane segments are allocated and signaled by Intermediate System to Intermediate System (IS-IS) or Open Shortest Path First (OSPF) or Border Gateway Protocol (BGP): a node individually computes the SR Policy and decides on its own to steer packets based on that policy. In a *centralized* control plane, segments are allocated and instantiated by an SR controller: the SR controller computes the source-routed policies and decides which nodes need to steer which packets on those policies. The SR architecture does not restrict how the controller programs the network. A *hybrid* scenario complements a base distributed control plane with a centralized controller.

The SR architecture can be instantiated on various **data planes**: SR over Multi Protocol Label Switching (SR-MPLS) and SR over IPv6 (SRv6). SR can be directly applied to the *MPLS* architecture with no change to the forwarding plane: a segment is encoded as an MPLS label and an SR Policy is instantiated as a stack of labels. The segment to process (the active segment) is on the top of the stack. Upon completion of a segment, the related label is popped from the stack.

[1] Equal-cost multi-path routing[11]

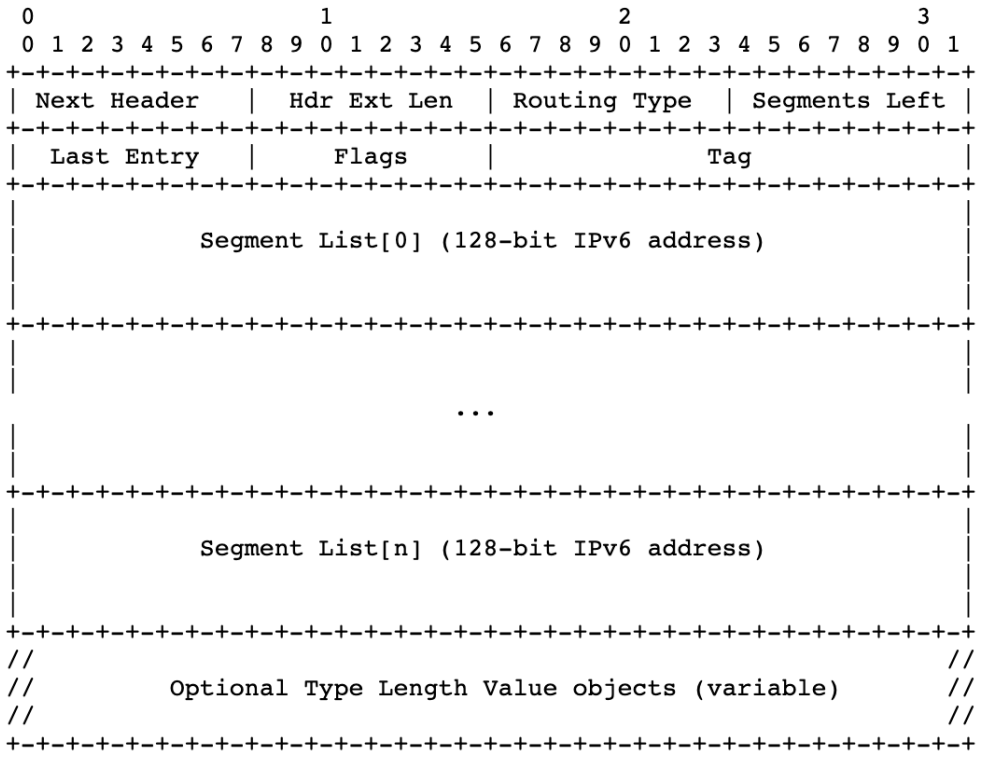

Fig. 1. SRv6 Header [7]

If SR uses an *IPv6* data plane, each instruction is associated with a segment and encoded as an IPv6 address. An SRv6 segment is also called an SRv6 SID. An SR Policy is instantiated as an ordered list of SRv6 SIDs in a new type of routing header called the SR Header (SRH); so, when a packet is steered on an SR Policy, the related SRH is added to the packet by a headend node – the Source SR node – that is a SR-capable router. SR Header (SRH) is created with Segment list in reversed order of the path; the active segment is indicated by the Destination Address (DA) of the packet and it is set to the first segment. The packet is sent according to the IP DA, through a normal IPv6 forwarding. The next active segment is indicated by the Segments Left (SL) pointer in the SRH. When a SRv6 SID is completed, the SL is decremented and the next segment is copied to the DA. The SRH is shown in Figure 1.

A Transit node forwards the packet containing the SR header as a normal IPv6 packet, so the Transit nodes do not need to be SRv6-aware. A transit node executes plain IPv6 forwarding, solely based on IPv6 DA; it doesn't inspect or update the SRH.

SR Endpoints are SR-capable nodes whose address is in the IP DA. They inspect the SRH and update the DA in the IPv6 Header according to the Segment Left and the Segment List specified by the SRH. After processing, the packet is forwarded according to the new IP DA. A a useful survey to better delve into Segment Routing can be found here [22].

3. Discussing Segment Routing v6 Issues

Some IPv6-related security issues are reported in [21]. The Segment Routing Header is an extension header of IPv6 used by an IPv6 source to list one or more intermediate nodes to be passed through by the packet on the path to a destination. One security issue comes from the fact that an attacker can detour the access list of security system, for example firewalls, and then he can access the protected internal system by using SRH. An interesting article on LWN [14] mentions HMAC as a mitigating approach to the Segment Routing header tampering problem.

Using a SRH is a form of source routing, therefore it has some well-known security issues as described in RFC4942 [13] and RFC5095 [1] as explained in [23]:

- *amplification attacks*: where a packet is forged in such a way as to introduce loops among a set of SR-enabled routers, yielding unnecessary traffic, hence a Denial of Service (DoS) [6] against bandwidth;
- *reflection attack*: where an attacker forces an intermediate node to appear as the immediate attacker, hence hiding the real attacker from naive forensic;
- *bypass attack*: where an intermediate node is used as a step stone (for example in a De-Militarized Zone) to attack another host (for example in the data center or any back-end server).

RFC2460 [10] defines an IPv6 extension header called Routing Header, in particular a Routing Header subtype denoted as Type 0 a.k.a. RH0 is defined that may contain multiple intermediate node addresses, including repetitions. This allows a packet to be constructed such that it will oscillate between two RH0-processing hosts or routers many times. This property can be used to cause congestion and DoSes [4]. This attack is particularly serious in that it affects the entire path between the two exploited nodes, not only the nodes themselves or their local networks. Analogous functionality can be found in the IPv4 source route option, but the opportunities for abuse are greater with RH0 due to the ability to specify more intermediate node addresses in each packet. The severity of this threat was considered to be sufficient to warrant deprecation of RH0 entirely.

In Segment Router v6 it is possible to consider two kind of nodes (routers and hosts):

- nodes belonging to a single SR domain where all nodes are trusted;
- nodes outside of the SR domain, that cannot be trusted.

SRv6 is quite protected in a single administrative domain with trusted nodes, but its potentialities are limited. Further, SRv6 nodes ignore SRH created by external nodes, making the RFC 5095 attacks far more complex to perform.

In is worth noting that the security-related fields in SRH feature are:

- a HMAC Key-id, 8 bits wide;
- a HMAC, 256 bits wide (optional, exists only if HMAC Key-id is not 0).

The HMAC field is used to verify the validity of the SRH. Nevertheless, some tampering is still possible due to the limited key length.

SRv6 security has been addressed in several works, we mention just a few here below.

Li and Xie [15] describe various threats and security concerns related to SRv6, but unfortunately do not consider some relevant security issues as they consider SR networks as “trusted domains”. 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 question here is how strong and realistic the assumption of having trusted domains is.

Barton and Henry [3] show how a path computation element of a network configured for segment routing receives, from a plurality of path computation clients in the network, segment identifiers identifying a destination segment. They show how the above element also receives fatigue states for segments of the network to allow rerouting to proactively mitigate overloaded segments in the network.

Filsfils and Garvia [8] show how Segment Routing network nodes protect IPv6 Segment Routing (SRv6) using Security Segment Identifiers providing origin authentication, integrity of information and antireplay protection. Nevertheless, this is a patented approach with limited applicability.

Vyncke, Previdi and Lebrun [24] propose SR-TPP, a mechanism based on SRv6 to support network path verification while hiding both-end and path information. SR-TPP approach is distributed and this opens up some issues related to state transmission and potential further attacks to the distributed system.

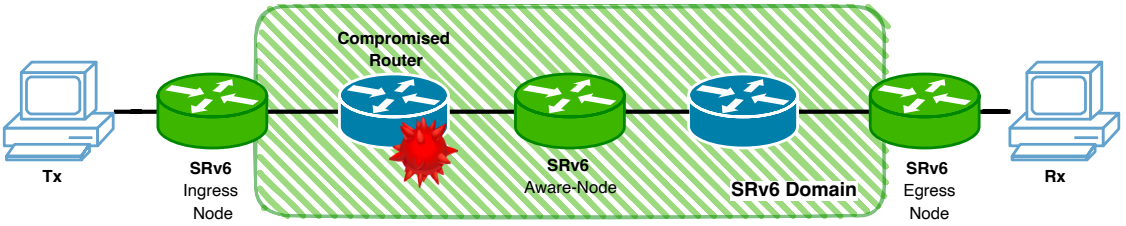

Fig. 2. Transit Node Attack Scenario

4. Most Relevant Segment Routing v6 Attacks

The most relevant attack scenarios for segment routing v6 can be summarized as follows:

- **Ingress SRv6 Node Attack**: the router at the beginning of the SR domain, which is responsible of SRH encapsulation is compromised. It would be interesting to abuse HMAC computation so that it becomes so costly as to possibly determine a DoS by surpassing the computation capabilities of routers who have to check/verify integrity. Here breaking HMAC cost and feasibility are key issues [18].
- **Transit Node Attack**: a SR-unaware router, which is passed through by a packet in the plain forwarding operation, is compromised. This node, which should not inspect or update the SRH, could try to alter IPv6 DA with a rogue SID, manipulating the SR policy;
- **SR Endpoint Attack**: this node, which is a SR-capable router, is compromised. This SR-aware node is responsible for inspecting SRH, updating Segment Left field in SRH, updating DA in IPv6 Header and in case processing the payload. Malicious actions on this node have a great impact on SR policy and traffic redirecting.

5. Implementing a Simulation Testbed

It would be really useful to implement a testbed in order to fully simulate and evaluate multiple scenarios using a strategy similar to what provided in [2] and Rose [2]. We believe that leveraging a Network Testbed emulator such as EVE-NG [3] would be the right choice to allow a real world evaluation of the feasibility and cost of the above mentioned attacks. The main motivation for choosing EVE-NG comes from its scalability, flexibility and support for real world router and network node images that allow performing complex network activities in a fully controlled realistic environment.

The starting feasibility tests should be performed on the basic topology shown in Figure 2. This will allow verifying first of all the feasibility, and then the consequences of the attacks depicted above, in particular with respect to packet dropping and/or tampering. We believe that leveraging a user/kernel space real time packet header tampering application would be particularly useful to the proposed evaluation strategy. Of course, this would require making use of existing functionality from state-of-the-art network tools. Some relevant candidates tools include the following:

- Netmap [16] i.e. a framework for very fast packet I/O from userspace, implemented as a single kernel module for FreeBSD and Linux. It can handle tens of millions of packets per second, matching the speed of 10G and 40G ports.
- Netfilter,[4] i.e. the leading open source project for Linux networking enabling packet filtering, network address and port translation (NA[P]T), packet logging, userspace packet queueing and most importantly, packet mangling. In particular, netfilter hooks inside the Linux kernel that would allow kernel modules to register callback functions allowing mangling strategies to be applied per packet.

[2] https://netgroup.github.io/rose/
[3] https://www.eve-ng.net/
[4] https://www.netfilter.org

- NFQsed [5] i.e. a tool to transparently modify network traffic using a predefined set of substitution rules, running on Linux and using the netfilter_queue library.

We expect the implementation of the proposed attack scenarios in the experimental testbed will prove the feasibility and impact of the above-described attacks. It will also serve as the basis for measuring and evaluating the impact of of the attacks on the functionality and performance of the network. Further, it will allow evaluating and comparing different mitigation approaches.

6. Conclusion

This paper has introduced the context of Segment Routing and in particular the SRv6 architecture in IP networks. It has discussed some of the issues, in particular tied to possible tampering with the Segment Routing Header in different scenarios. The main outcome is that SRv6 technology can actually be abused to produce security and performance issues. Existing tools and open-source codebase can be used to implement such attacks in practice on a simulation testbed such as the powerful EVE-NG. Nevertheless, full implementation and testing of the described security and DoS issues are under study and experimental results will be presented in future work.

References

[1] Abley Afilias, J., Savola, P., Neville-Neil, G., 2005. Deprecation of Type 0 Routing Headers in IPv6. RFC 5095. URL: https://rfc-editor.org/rfc/rfc5095.txt.

[2] Ali, W.N.A.W., Taib, A.H.M., Hussin, N.M., Othman, J., 2012. IPv6 attack scenarios testbed, in: 2012 IEEE Symposium on Humanities, Science and Engineering Research, pp. 927–932. doi:10.1109/SHUSER.2012.6269008.

[3] Barton, R.E., Henry, J., 2019. Fatigue - based segment routing. Patent H04L 29/06 (20060101); H04L 12/707 (20060101), Jul. 2019 https://patents.justia.com/patent/20190230115.

[4] Biondi, P., Ebalard, A., 2007. IPv6 Routing Header Security, in: CanSecWest Security Conference 2007, pp. 1–61. URL: http://www.secdev.org/conf/IPv6_RH_security-csw07.pdf.

[5] Caprolu, M., Di Pietro, R., Lombardi, F., Raponi, S., 2019. Edge computing perspectives: Architectures, technologies, and open security issues, in: 2019 IEEE International Conference on Edge Computing (EDGE), pp. 116–123. doi:10.1109/EDGE.2019.00035.

[6] Eliyan, L.F., Di Pietro, R., 2021. DoS and DDoS attacks in Software Defined Networks: A survey of existing solutions and research challenges. Future Generation Computer Systems 122, 149–171. URL: https://www.sciencedirect.com/science/article/pii/S0167739X21000911, doi:https://doi.org/10.1016/j.future.2021.03.011.

[7] Filsfils, C., Dukes, D., Previdi, S., Leddy, J., Matsushima, S., Voyer, D., 2020. IPv6 Segment Routing Header (SRH). RFC 8754. URL: https://rfc-editor.org/rfc/rfc8754.txt, doi:10.17487/RFC8754.

[8] Filsfils, C., Garvia, P.C., Clad, F., U.S. Patent 11019075, May. 2021. Providing processing and network efficiencies in protecting internet protocol version 6 segment routing packets and functions using security segment identifiers. URL: https://patents.justia.com/patent/11019075.

[9] Filsfils, C., Previdi, S., Ginsberg, L., Decraene, B., Litkowski, S., Shakir, R., 2018. Segment Routing Architecture. RFC 8402. URL: https://rfc-editor.org/rfc/rfc8402.txt, doi:10.17487/RFC8402.

[10] Hinden, B., Deering, D.S.E., 1998. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460. URL: https://rfc-editor.org/rfc/rfc2460.txt, doi:10.17487/RFC2460.

[11] Hopps, C., 2000. Analysis of an Equal-Cost Multi-Path Algorithm. RFC 2992. URL: https://www.rfc-editor.org/info/rfc2992, doi:10.17487/RFC2992.

[12] JaeDeok Lim, YoungKi Kim, 2006. Protection Algorithm against security holes of IPv6 routing header, in: 2006 8th International Conference Advanced Communication Technology, pp. 2004–2007. doi:10.1109/ICACT.2006.206388.

[13] Krishnan, S., Davies, E.B., Savola, P., 2007. IPv6 Transition/Co-existence Security Considerations. RFC 4942. URL: https://rfc-editor.org/rfc/rfc4942.txt, doi:10.17487/RFC4942.

[14] Lebrun, D., 2020. IPv6 segment routing. URL: https://lwn.net/Articles/722804/.

[15] Li, C., Li, Z., Xie, C., Tian, H., Mao, J., 2021. Security Considerations for SRv6 Networks. Internet-Draft draft-li-spring-srv6-security-consideration-07. Internet Engineering Task Force. URL: https://datatracker.ietf.org/doc/html/draft-li-spring-srv6-security-consideration-07.

[16] Maffione, V., Rizzo, L., Lettieri, G., 2016. Flexible virtual machine networking using netmap passthrough, in: 2016 IEEE International Symposium on Local and Metropolitan Area Networks (LANMAN), pp. 1–6. doi:10.1109/LANMAN.2016.7548852.

[17] Morreale, P.A., Anderson, J.M., 2014. Software Defined Networking: Design and Deployment. CRC Press, Inc., USA. ISBN 1482238632.

[5] https://github.com/rgerganov/nfqsed

[18] Ravilla, D., Putta, C.S.R., 2015. Implementation of HMAC-SHA256 algorithm for hybrid routing protocols in MANETs, in: 2015 International Conference on Electronic Design, Computer Networks Automated Verification (EDCAV), pp. 154–159. doi:10.1109/EDCAV.2015.7060558.

[19] Ray, P.P., Kumar, N., 2021. SDN/NFV architectures for Edge-Cloud oriented IoT: A systematic review. Computer Communications 169, 129–153. doi:https://doi.org/10.1016/j.comcom.2021.01.018.

[20] Smith, M., Kottapalli, N., 2020. In-Flight IPv6 Extension Header Insertion Considered Harmful. URL: https://tools.ietf.org/html/draft-smith-6man-in-flight-eh-insertion-harmful-02.

[21] Ullrich, J., Krombholz, K., Hobel, H., Dabrowski, A., Weippl, E., 2014. IPv6 Security: Attacks and Countermeasures in a Nutshell, in: 8th USENIX Workshop on Offensive Technologies (WOOT 14), USENIX Association, San Diego, CA. pp. 1–20. URL: https://www.usenix.org/conference/woot14/workshop-program/presentation/ullrich.

[22] Ventre, P., Salsano, S., Polverini, M., Cianfrani, A., Abdelsalam, A., Filsfils, C., Camarillo, P., Clad, F., 2020. Segment Routing: A Comprehensive Survey of Research Activities, Standardization Efforts, and Implementation Results. IEEE Communications Surveys & Tutorials PP. doi:10.1109/COMST.2020.3036826.

[23] Éric Vyncke, Previdi, S., Lebrun, D., 2015. IPv6 Segment Routing Security Considerations. Internet-Draft draft-vyncke-6man-segment-routing-security-02. Internet Engineering Task Force. URL: https://datatracker.ietf.org/doc/html/draft-vyncke-6man-segment-routing-security-02.

[24] Zhou, J., Li, H., Wu, Q., Lai, Z., Liu, J., 2020. SR-TPP: Extending IPv6 Segment Routing to enable Trusted and Private Network Paths, in: 2020 IEEE Symposium on Computers and Communications (ISCC), pp. 1–6. doi:10.1109/ISCC50000.2020.9219705.