

IPv6+技术的 安全风险与安全机制

Security Risks and Mechanisms of IPv6+ Technology

佟 恬,赵 菁,庞 冉,曹 畅(中国联通研究院,北京 100048)

Tong Tian,Zhao Jing,Pang Ran,Cao Chang(China Unicom Research Institute,Beijing 100048,China)

摘 要:

IPv6/IPv6+适用于更多的场景、更多样的用户需求以及更复杂的安全环境,在全面推进IPv6商用部署和IPv6+创新研究的过程中,网络安全问题也被更加重视。然而IPv6+新技术尚在研究和试点中,其安全威胁还未充分暴露,需要结合国内外最新标准研究进展和试点应用经验来分析IPv6+新协议、新技术、新地址编码可能会带来的安全风险和问题,强化IPv6+技术安全管理和防护手段,以做到安全保护措施与IPv6网络改造同步规划、同步建设、同步使用,为构建IPv6/IPv6+下一代网络安全防护体系开展前瞻布局研究。

关键词:

IPv6+;网络安全;安全风险;安全机制

doi: 10.12045/j.issn.1007-3043.2024.04.006

文章编号:1007-3043(2024)04-0032-07

中图分类号:TP393.4

文献标识码:A

开放科学(资源服务)标识码(OSID):



Abstract:

IPv6/IPv6+ is applicable to more scenarios, diverse user needs and complex security environment, and in the process of comprehensively promoting the commercial deployment of IPv6 and the innovative research of IPv6+, network security issues are also paid more attention. However, the new IPv6+ technology is still being researched and piloted, and its security threats have not yet been fully exposed. It is necessary to combine the latest standard research progress and pilot application experience at home and abroad to analyze the security risks and problems that may be brought by the new IPv6+ protocols, technologies and address encoding, and strengthen IPv6+ technical security management and protection means in order to synchronise the planning, construction and use of security protection measures with IPv6 network transformation, and carry out forward-looking layout research for the construction of IPv6/IPv6+ next-generation network security protection system.

Keywords:

IPv6+; Network security; Security threat; Security mechanism

引用格式:佟恬,赵菁,庞冉,等. IPv6+技术的安全风险与安全机制[J]. 邮电设计技术,2024(4):32-38.

1 概述

互联网是国民经济和社会发展的基础设施,IPv6是互联网升级演进的必然趋势,是网络技术创新的重要方向。IPv6/IPv6+将适用于更多的应用场景、更多样的用户需求以及更复杂的安全环境。随着IPv6规模部署和IPv6演进技术(IPv6+)研究工作的不

断开展,产业界也更加注重IPv6网络的安全问题,然而IPv6+新技术尚在研究和试点中,其安全威胁还未充分暴露,需要由内而外的对IPv6+网络的安全风险、安全策略与措施展开研究,提升IPv6网络安全的保障能力。本文结合国内外最新研究进展,充分分析IPv6+协议的安全风险,提出IPv6+内生安全解决思路。

2 IPv6网络的安全优势

IPv6以其充足的地址空间、层次化的地址结构、简

收稿日期:2024-03-11

化的报文头格式、灵活的扩展头、增强的邻居发现机制而快速发展。相比于 IPv4 网络,IPv6 在资产管理、保护能力等方面均有明显优势,具体可以描述为以下 4 点。

a) 资产管理能力增强。IPv6 具备充足的地址编码空间,可为每个终端配置全球唯一的“身份证”,可以应用到网络资产探测、流量综合分析及流量行为异常检测、资产唯一标识等场景。

b) 保护能力增强。许多网络攻击者通过地址扫描识别用户的地理位置,发现漏洞并入侵,IPv6 海量地址空间可以避免野蛮扫描风险,有效降低被嗅探的风险,提升网站与用户终端设备的安全性。IPv6 可以更好地支持源地址验证,因为 IPv6 地址构造是可汇聚的、层次化的,其地址前缀的分配较规律,这将会使下游互联网服务提供商(Internet service provider,ISP)的地址总是落在上游 ISP 的汇总地址空间内,易于 ISP 在入口实现过滤,有效防御虚假源地址攻击,也增加了 IPv6 网络的安全性。此外,利用 IPv6 的地址规划、虚假子网、拓扑隐藏等技术,有效隐藏网络真实结构,也会增加攻击者网络侦查和嗅探的资源消耗,提高专网反侦察能力。

c) 传输安全能力增强。IPv6 协议支持互联网安全协议(Internet Protocol Security,IPSec),为通信双方提供数据完整性保护、数据内容的机密性验证、有限的数据流机密性保证和数据起源验证,并提供了抗报文重放保护。因而,可以将用户、报文和攻击一一对应,实现对用户行为的安全监控,在网络层实现端到端数据加密传输。

d) 监控、检测与溯源能力增强。IPv6 网络可以规范地址管理策略,实现终端标识信息与位置信息的扩展、实现用户与 IP 绑定,禁止自生成地址和隐私扩展地址等。在威胁的检测和阻断方面,通过基于媒体访问控制(Media Access Control,MAC)地址或端口的阻断可以精确地识别和阻断威胁终端,通过五元组/三元组精准阻断威胁流量而不影响正常业务。IPv4 网络中由于大量私网的存在,使得恶意行为很难溯源,在 IPv6 网络中,节点采用公网地址取代私网地址,每一个地址都是真实的,易于对威胁行为溯源。

基于上述优势,IPv6 可以避免或缓解 IPv4 存在的不足和安全风险。

a) 防范网络放大攻击。ICMPv6(Internet Control Message Protocol for the Internet Protocol Version 6)在设

计上不响应组播地址和广播地址的消息,可以有效避免 IPv4 网络中利用广播地址发起的广播风暴攻击和分布式拒绝服务(Distributed Denial of Service,DDoS)攻击的风险。

b) 防止已知的碎片攻击。IPv6 不仅对碎片机制进行了严格限制,还提供了更健全的分片机制,通过发送伪造碎片报文发动攻击的方式在 IPv6 下不再有效。

c) 有效抵御基于遍历扫描的网络蠕虫攻击。IPv6 网段地址空间巨大,基于地址遍历的网络漏洞扫描不再适用。因此,病毒及网络蠕虫通过遍历扫描和随机选择 IP 地址的方式在 IPv6 网络中传播变得极为困难,有效防范了蠕虫病毒的传播。

d) 对网络关键基础设施的安全性提供扩展。DNSv6 定义了域名系统(Domain Name System,DNS)安全扩展协议,提供认证和完整性保障,避免域名被篡改。

e) 避免 NAT 使用带来的安全隐患和管理困难。NAT 通过将私有地址和公网地址进行转换,解决了 IPv4 地址不足的问题,隐藏并保护网络内部的终端,避免来自公共互联网的攻击,起到一定安全作用,但也带来了安全隐患和管理上的困难,IPv6 网络中无需 NAT 地址转换。

f) 有效防御基于 IP 地址欺骗的攻击方式。IPv6 有较为健全的认证机制,有能力在第一跳阻止恶意设备,可以最大限度预防中间人攻击。

3 IPv6 网络协议的安全风险

IPv6 协议是对 IPv4 协议的优化和改进,因此会继承 IPv4 协议的一些安全问题,也可能出现新的安全漏洞,面临原有安全机制无法应对新技术新业务下的威胁。本章将对 IPv6 网络协议面临的安全风险进行介绍。

3.1 从 IPv4 网络继承的安全风险

IPv6 相较于 IPv4 在保密性和完整性方面有较大幅度的改进,但有些安全风险并没有因为 IPv6 协议的出现而发生改变,例如:嗅探攻击、拒绝服务攻击、中间人攻击、应用层攻击等,这些攻击都可能对 IPv6 网络造成潜在的危害。

3.2 IPv6 新协议引入新的安全风险

IP 协议在设计之初几乎没有考虑安全问题,IPv6 协议在安全性的考虑上要比 IPv4 更加周全,但 IPv6/

IPv6+协议的应用依然会引入一些新的安全风险,攻击者总能找到协议交互机制上的漏洞并加以利用,出现一些专门针对IPv6新协议的攻击。本节对IPv6协议特有的安全风险进行介绍。

a) IPv6扩展头攻击。IPv6相比IPv4报文格式的一个重要变化就是引入了扩展头,协议对扩展头数量没有限制,同种类型的扩展头被允许在IPv6扩展报文中多次出现。攻击者可以通过构造异常数量扩展头的报文对防火墙或目标主机进行DoS攻击,防火墙或者目标主机在解析报文时将耗费大量资源,从而影响设备性能。逐跳选项扩展头可能导致拒绝服务攻击,因为网络中所有节点都需要检查并处理该报头。

b) ICMPv6协议攻击。ICMPv6是IPv6协议簇中的一个基础协议,合并了IPv4中的因特网控制报文协议(Internet Control Message Protocol, ICMP)、地址解析协议(Address Resolution Protocol, ARP)、反向地址解析协议(Reverse Address Resolution Protocol, RARP)等多个协议的功能。ICMPv6协议控制着IPv6网络中的地址生成、地址解析、差错控制、组播控制等关键环节,因此攻击者可能利用ICMPv6协议的漏洞和机制达到攻击目标。

c) NDP协议攻击。IPv6网络采用NDP协议实现了IPv4网络中的ARP协议的功能,二者虽然协议层次不同但实现机制大同小异,所以针对ARP协议的攻击如ARP欺骗、ARP泛洪攻击、中间人攻击等在IPv6网络中仍然存在。

d) 重复地址监测(Duplicate Address Detection, DAD)攻击和前缀欺骗攻击。攻击者在某个主机的IP地址自动分配过程中监听DAD过程,在侦听到邻居请求(Neighbor Solicitation, NS)报文时,通过发送非法的邻居通告(Neighbor Advertisement, NA)报文来宣称占用该地址,破坏主机的地址分配的过程,造成该主机无法完成网络地址配置从而无法联网。DAD攻击产生的根本原因,是无法对NA报文的合法性进行验证。攻击者还可能把DAD攻击和前缀欺骗攻击结合起来,首先通过DAD攻击使新入网设备不能获得正确的IP地址,同时发布自己的前缀,并且开启本机路由转发功能,这样攻击者将能成为本链路所有主机的默认路由器,实施中间人攻击。

4 IPv6+网络安全风险与安全策略

IPv6+是以IPv6为基础,通过扩展报文头来支持

一系列新的网络应用,包括SRv6、业务链(Service Function Chain, SFC)、网络切片、随流检测、IPv6封装的比特位索引显式复制(Bit Index Explicit Replication IPv6 encapsulation, BIERv6)、应用感知网络等一系列协议创新。

IPv6+可以升级网络导航能力、为业务提供专属通道、提升运维能力和安全防御能力。

针对IPv6网络运维中的安全问题,在国际标准方面,IETF RFC9099分析了对IPv6网络运营安全的考虑,RFC9098分析了IPv6扩展头在运营中存在的问题。在国内标准方面,CCSA行业标准《IPv6安全标准化关键问题研究》对IPv6安全标准化现状与趋势、IPv6安全能够标准化的领域和技术、IPv6安全标准等内容进行了梳理。

在IPv6+创新技术方面,国内外标准组织近年来积极开展了IPv6+的研究与标准化工作,但IPv6+安全方面,目前只有IETF的SRv6 Security Considerations个人草案和CCSA的《SRv6网络安全技术研究》对SRv6的安全威胁进行了分析。

4.1 SRv6的安全风险与安全策略

基于IPv6转发平面的段路由(Segment Routing IPv6, SRv6)是指采用IPv6数据平面的段路由(Segment Routing, SR)技术,利用一种新型的IPv6路由扩展报头(Segment Routing Header, SRH)来施加一个有序的路径列表来控制数据包的转发。为保障SRv6网络安全可靠运行,需要注意或解决一些安全问题,本节分析了SRv6网络中常见的安全威胁,并提出避免或减轻这些安全威胁的方法。

4.1.1 SRv6安全风险分析

在SRv6网络中,攻击者可以通过监听SRH来窃取网络拓扑,篡改SRH发起源路由攻击等,具体如下。

a) 侦听攻击窃取SRv6相关信息。SRv6的段列表中保存着报文转发路径中经过的多个网元或服务的地址信息,SRv6网络中的沿途攻击者通过各种探测手段获取IPv6头部和SRH扩展头中携带的节点信息、SR策略等SRv6相关信息,以获取网络拓扑及推断出路由策略。虽然侦听攻击收集的信息不会损害用户数据的机密性,但攻击者利用收集的信息可发动其他攻击。攻击者还可能窃取报文payload信息,但这并不是SRv6特有的风险。

b) 报文的重放、插入、删除、修改等。报文重放是指攻击者记录数据包进行报文重放攻击;报文插入是

指攻击者恶意生成包含虚假信息的报文并将报文注入网络;报文修改是指攻击者在报文传输过程中对报文进行修改,典型的如修改段路由直接影响报文的SR策略;报文删除是指攻击者通过拦截和删除网络中的数据包,阻止数据包到达目的地,其中选择性丢包可能比随机丢包造成更严重的损失;报文修改是将流量转移到攻击者可以访问且拥有更多处理资源的另一个节点,从而为更复杂的在途攻击提供便利。上述攻击一般是由对传输报文具有访问权限的沿途攻击者实施的。

c) 段路由的安全威胁。攻击者可通过篡改SRv6段列表实现任意定义流量转发路径,致使数据包路由到不同的路径上,而不是通过预期的路径路由。对SRH的修改包括将1个或多个段标识(Segment Identifiers, SIDs)添加到段列表中,删除1个或多个SIDs,或将替换掉其中一些SIDs;另一种可能的修改类型是通过添加、删除或修改SRH中的TLV字段,SR修改攻击可以通过以下1种或多种方式篡改转发路径,影响报文的转发行为(见图1)。

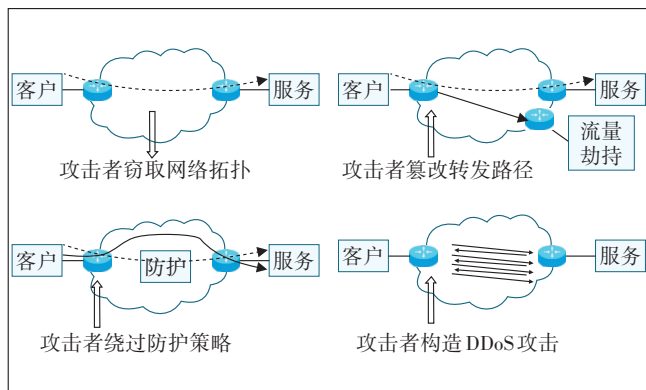


图1 SRv6源路由威胁示意

(a) 定制特定路径/服务。攻击者通过在SRv6段列表中增加某些地址,获取未经授权的服务,例如流量加速等。

(b) 避开特定节点或路径。攻击者可以操纵目的IP地址或SRH来避开特定的节点或路径,使报文避免各种处理步骤。比如绕过计费服务、避免访问控制、绕过安全防护策略以实现对内部网络的非法访问、流量攻击等。

(c) 发起DoS攻击。攻击者利用SRv6作为损害网络性能或导致DoS的手段。通过在SRv6段列表中插入重复SRv6地址,控制流量在网络中重复转发以放大

流量,发起大带宽DoS攻击,或将数据引流到非预期的目的地,降低网络性能和目的端服务器性能。

d) 对SRv6控制和管理平面的攻击。当SRv6控制平面和管理平面被入侵,会对网络造成不可预估的影响,内部攻击者可以通过发布SIDs来操纵网络中使用的SR策略,从而实施一系列攻击,包括非法注入控制平面信息、选择性删除合法报文、报文重放和被动监听等。其中,非法注入控制面信息可以由非路径攻击者执行,而报文删除、重放和监听则由沿途攻击者执行。

e) 对安全设备的影响。SRv6是运营商网络中常用的隧道技术,入口PE将负载封装在一个外部IPv6首部中,其中SRH携带SR策略段列表以及VPN业务SID。SRv6网络中的安全设备需要处理SRv6数据包,这可能会影响网络的安全设备。一是网络中较旧的安全设备不知道SRv6附加首部和隧道机制,可能会丢弃或以其他方式阻碍SRv6报文转发;二是SRv6报文在SRv6域内转发时,其目的地址不断变化,且常使用入口PE设备的loopback地址作为源IP地址,网络安全设备无法学习到真正的目的地址和源地址,难以对某些SRv6流量进行访问控制。例如,在SRv6报文转发路径上,SR-aware防火墙会检查双向VPN流量报文的关联关系,当PE1到PE2的报文的<source, destination>为<PE1-IP-ADDR, PE2-VPN-SID>,反方向报文为<PE2-IP-ADDR, PE1-VPN-SID>时,往返报文的源、目的IP地址信息是非对称的,安全设备会因为正向VPN流量和反向VPN流量的源地址和目的地址不同,认为是不同的流,导致合法流量被防火墙阻断过滤,影响安全设备的有效性。

4.1.2 SRv6安全机制

传统源路由威胁防护一般采用直接丢弃源路由报文、关闭源路由转发功能,而SRv6网络需要在正常转发SRv6报文的同时防护SRv6源路由攻击,无法直接采用丢弃源路由报文的方法进行安全防护,这对网络安全防护提出了新的挑战。IETF的RFC 7855和RFC 8799等标准文稿定义了SRv6网络需要规定网络边缘,即明确网络可信域,可信域内的设备将被认为是安全的。

a) 边界过滤。在可信域边界通过部署访问控制列表(Access Control List, ACL)策略对从可信域外进入的报文进行流量过滤,丢弃从外部非法访问内部信息的流量,包括如下3个方面。

(a) 在可信域边缘设备的对外接口上配置 ACL 规则。如果 SRv6 报文从非 SRv6 可信域进入 SRv6 可信域,若收到的 SRv6 报文的源地址来自本域可分配 SID 地址块,则丢弃报文;如果 SRv6 报文从一个 SRv6 可信域进入另一个 SRv6 可信域,若 SRv6 报文的源地址以及 SRH 中 SID List 的后续 SID 来自本域可分配 SID 地址块,则丢弃报文。这是因为正常情况下不应该将内部 SID 泄露到域外,若被域外用户获取和使用,则认定携带该地址的报文为攻击报文。

(b) 对外接口和对内接口上配置 ACL 规则。当 SRv6 报文的源地址为本地 SID 时,且源地址不是内部 SID 或内部接口地址,或者源地址不在 SID 空间范围内时,则将报文丢弃。这是由于只有内部的设备才能进行 SRv6 报文封装,所以当目的地址为本地 SID 时,源地址必须是内部 SID 或者内部接口地址。

(c) SRv6 只对显式发布为 SID 的本地 IPv6 接口地址进行 End 操作。即未声明成 SID 的本地 IPv6 接口地址如果被插入段列表,将匹配到接口地址路由,而不会触发 SID 的处理操作。如果本地 IPv6 接口地址插入最后一个 SID,即 SL=0 时,节点需跳过 SRH 的处理。如果该地址被插入 Segment List 中间,即 SL>0,则它被当作错误处理,将会被丢弃。

b) SRH 扩展头校验。SRv6 路由扩展首部的安全性由 SRH 解决。基于 HMAC 对通信源进行身份验证和 SRv6 报文头校验,防止报文被篡改带来的攻击。

c) 管控面安全。SRv6 可信域边界过滤可用于抵御外部攻击者对控制平面和管理平面的攻击,但无法抵御内部攻击者对其的攻击。现有的控制平面或管理平面协议中,对段路由没有定义任何特定的安全机制,建议采用认证和安全机制来验证信息的真实性。

4.2 SFC 的安全风险与安全策略

SRv6 SFC 在 SRv6 SDN 架构基础上增加了服务功能(Service Function, SF),SF 可能是传统的防火墙、TCP 加速等网络服务,也可能是各种应用服务,SRv6 SFC 为用户提供定制化服务能力。

4.2.1 SRv6 SFC 的安全风险分析

攻击者可窃取网络和服务等相关信息,通过仿冒、篡改服务功能链获取非授权服务功能(如 TCP 加速),绕过已定制的服务功能(如计费服务、安全检测服务等)造成网络/服务提供商损失、实现网络攻击。此外,服务功能的安全防护能力不一,容易成为黑客攻击的突破口,进而将威胁扩散到整个 SRv6 SFC 网

络。

4.2.2 SFC 安全机制

SRv6 SFC 的安全防护需要在 SRv6 网络安全防护基础上,防止非授权用户接入到 SRv6 SFC 网络,防止 SF 的威胁扩散到 SRv6 SFC 网络,防止篡改 SRv6 段列表获取非授权服务或绕过已定制的服务,防止 SRv6 SFC 多租户之间威胁扩散等。

SRv6 SFC 网络安全机制应包括 SRv6 SDN 网络安全防护、SRv6 SFC 接入认证、SRv6 SFC 路径校验、SF 安全加固、多用户隔离措施等,具体如下。

a) SRv6 信任域防御。定义 SRv6 SFC 信任域,将流分类器、业务功能转发器、业务功能划分到信任域内,开启 SRv6 信任域相关防护措施,避免源路由威胁进入 SRv6 SFC 网络,避免攻击者任意定义 SRv6 SFC 服务。

b) 控制面安全。包括控制器自身安全、控制器北向接口和南向接口安全、网元控制面和数据面安全等。

c) 业务功能 SF 安全加固。为 SF 制定统一的安全防护基线,提升业务功能安全性,避免 SF 成为网络攻击突破口。

d) 接入认证。用户流量进入 SRv6 SFC 时,首先对用户身份进行校验;认证成功后,为用户流量提供 SRv6 SFC 功能,避免攻击流量进入 SRv6 SFC 网络,避免非授权用户获取业务服务。

e) SRv6 SFC 路径校验。在 SRv6 SFC 转发过程中对 SRv6 段列表路径进行校验,可采用 SRv6 HMAC、SID 加密校验等技术,为用户提供安全可靠的定制化服务。

f) SRv6 用户隔离。为不同用户提供独立的业务和网络服务,为不同用户提供独立的校验密钥,避免用户间威胁的扩散。

综上所述,如图 2 所示,当用户流量进入 SRv6 SFC 网络时,首先根据 SRv6 信任域过滤,丢弃目的地址是信任域内 SRv6 地址的报文,避免 SRv6 源路由威胁进入到 SRv6 SFC 信任域;然后边界网关对用户进行接入认证,认证通过后为用户提供 SRv6 SFC 服务;报文转发过程中,开启 SRv6 路径校验技术,丢弃校验失败报文,防止攻击者篡改路径获取非授权服务或绕过已定制的服务。

4.3 APN 的安全风险与安全策略

4.3.1 APN 安全风险分析

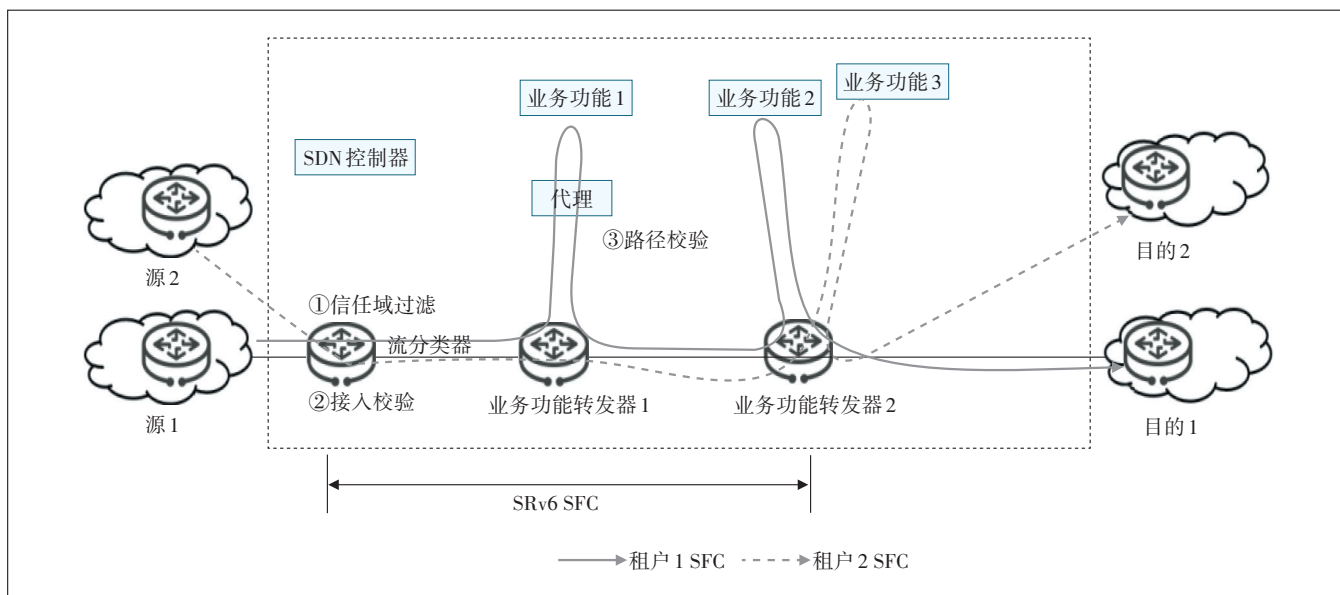


图2 SRv6 SFC安全防护

APN的标准尚在推进中,国内外标准对其安全风险和安全机制的研究较少。APN分为网络侧APN方案和主机侧APN方案,网络侧APN是在网络侧的头节点和边缘节点感知应用,为用户流量添加应用标记,APN ID的添加在ISP内部可信网络中,因此安全风险较小可以忽略。应用侧APN是应用侧/云侧设备直接将应用标识信息和需求信息封装进IPv6数据报文扩展头中,APN ID是在ISP网络信任域外添加的,可能会带来安全问题。APN的可信域如图3所示,这里假设设备操作系统可信,APN头节点之后的ISP内部网络是可信的,业务感知节点及其之后的链路是ISP的核心网,并连接到APP服务器的数据中心,链路安全性较高。APN的相关安全问题可以分为4类。

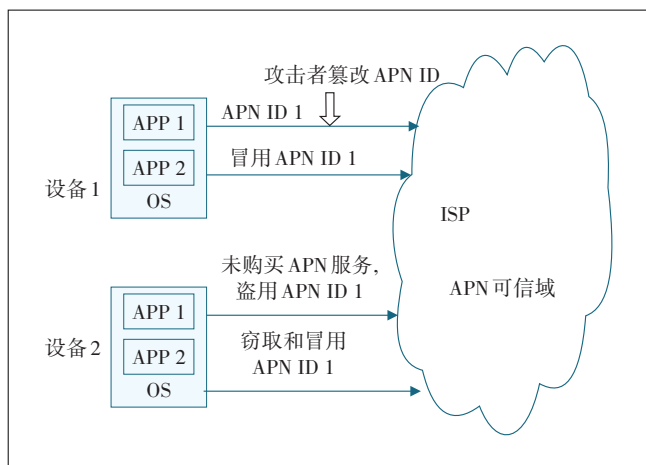


图3 APN的可信域及安全风险示意

a) 应用侧(端侧/服务器侧)内,一个恶意应用盗取了其他应用的APN ID,比如邮件APP获取了视频会议APP的APN ID,从而获得了高优先级的网络服务。

b) 应用侧(端侧/服务器侧)之间,不同应用侧设备上的相同应用,没有购买APN服务的应用窃取购买APN服务的应用的APN ID。

c) 应用侧设备打上APN ID之后,到APN头节点经过不可信路径,可能被窃取和篡改。

d) 恶意用户可能会申请许多APN ID。

4.3.2 APN安全机制分析

APN的安全也分为应用侧的安全可信和网络侧的安全可信。应用侧内的可信,需要通过端侧/服务器内的安全机制来保证,不同APP之间不能互相抢占和使用不属于自己的APN ID。在应用侧外的可信,即报文一旦发出,需要由网络侧的安全机制来保证报文内携带的APN ID可信无篡改。

APN ID的可信与安全:由于APN ID本身携带了应用层的信息和用户的信息,如果使用不当,可能会涉及隐私泄露问题。因此建议以一种轻量的方式来保证应用侧打上的APN ID在网络侧是可以被信任的,没有被篡改和仿冒。网络中业务感知边缘节点接收到报文后,通过HMAC、数字签名、IPSec等技术进行校验,如果身份认证通过,则映射进入相应网络资源(如SRv6路径、切片等);如果身份认证不通过,则流量过滤或者进入普通等级路径。接入认证有效防止单设备内的不同应用之间相互伪装/盗用应用信息、不同设

备的相同应用之间相互伪装/盗用应用信息、不同设备的不同应用之间相互伪装/盗用应用信息、应用信息发送后在到达接收方之前被篡改。

4.4 网络切片的安全风险与安全策略

基于IPv6的网络切片在网络基础物理架构上,通过扩展IGP多拓扑结构实现切片的划分与管理。OSPF、ISIS等IGP路由协议为每个切片域管理SRv6 SID空间,基于切片内的SRv6 SID进行切片业务转发,SRv6在进行切片封装转发时封装切片定制的切片参数。此外通过分配不同的切片Slice-ID实现切片资源的区分,业务转发时,在IPv6头中进行扩展,封装切片Slice-ID以及相应的切片参数。

切片攻击者可以通过伪造被攻击切片的封装信息,实现跨切片的数据访问,因此,需要将切片彼此隔离,不同网络切片的资源不应相互影响,以尽量减少对数据机密性和完整性的攻击。切片有如下安全机制。

a) 对用户进行安全认证以及授权。授权用户访问相应安全级别的网络切片,限制用户访问非授权的网络切片。

b) 安全引流。在用户接入侧,通过实施增强ACL等方式,对用户流量进行过滤,将符合IP地址规划的流量引入切片通道。

c) 切片安全隔离技术。为不同切片设置不同的安全级别,对于高级别的切片通道可以部署FlexE、时隙化小颗粒等技术,增强切片带宽隔离能力,避免当网络切片进行扩缩容时相互影响导致资源缺失。

d) 部署切片安全技术。基于网络切片组网环境以及切片隔离技术进行设计,满足切片的灵活扩展、不同切片的端到端安全特性的需求。

5 未来与展望

随着数字化进程的加速推进,网络安全已经成为社会和国家稳定发展的重要保障。作为下一代互联网技术的引领技术,IPv6+基于IPv6技术全面升级,不仅继承了IPv6技术原有的安全威胁,也导致攻击链更加智能化和多样化,危害程度更高。在国家政策、技术发展和需求的多重驱动下,IPv6+网络内生安全机制与关键技术研究也已成为未来网络发展的重要方向,此外,还应充分挖掘IPv6+赋能安全的能力,构建基于IPv6+技术体系的新安全网络,推进网络安全体系和能力建设,为下一代互联网安全可信保驾护航。

参考文献:

- [1] 李振斌,胡志波,李星. SRv6网络编程:开启IP网络新时代[M]. 北京:人民邮电出版社,2020.
- [2] 傅小兵,宗春鸿,严寒冰,等. 基于IPv6的互联网络安全探讨[J]. 中国新通信,2024,26(2):16-18.
- [3] 许国栋. IPv6网络的安全风险点与应对建议[J]. 数字技术与应用,2023,41(2):237-239.
- [4] 贺乐乐,毛云轩. 基于IPv6规模部署下的网络安全风险防范措施研究[J]. 数字通信世界,2022(11):41-43.
- [5] 李振斌,赵锋. “IPv6+”技术标准体系[J]. 电信科学,2020,36(8):11-21.
- [6] 鲁冬杰,杨凯,庄小君,等. 基于SRv6的网络安全技术研究[J]. 电信工程技术与标准化,2022,35(12):27-33.
- [7] 李树军,蔡长安. IPv6源路由机制安全性分析与攻击技术研究[J]. 成都大学学报(自然科学版),2010,29(1):60-63.
- [8] IETF. IPv6 Segment Routing Header (SRH): RFC 8754 [S/OL]. [2023-12-25]. <https://www.rfc-editor.org/rfc/rfc8754>.
- [9] IETF. Source packet routing in networking (spring) problem statement and requirements: RFC 7855 [S/OL]. [2023-12-25]. <https://www.rfc-editor.org/rfc/rfc7855>.
- [10] BURAGLIO N, MIZRAHI T, TONG T, et al. SRv6 Security Considerations: draft-bdmgct-spring-srv6-security-01 [S/OL]. [2023-12-25]. <https://datatracker.ietf.org/doc/draft-bdmgct-spring-srv6-security/>.
- [11] FILSFILS C, CAMARILLO P, LEDDY J, et al. SRv6 network programming: draft-ietf-spring-srv6-network-programming-15 [S/OL]. [2023-12-25]. <https://datatracker.ietf.org/doc/html/draft-ietf-spring-srv6-network-programming-15>.
- [12] IETF. Service Function Chaining (SFC) Architecture: RFC7665 [S/OL]. [2023-12-25]. <https://datatracker.ietf.org/doc/rfc7665/>.
- [13] 王士诚,祝鹏,何林. 基于“IPv6+”的应用感知网络(APN6)[J]. 电信科学,2020,36(8):36-42.
- [14] IETF. Operational Security Considerations for IPv6 Networks: RFC9099 [S/OL]. [2023-12-25]. <https://datatracker.ietf.org/doc/rfc9099/>.
- [15] IETF. Operational Implications of IPv6 Packets with Extension Headers: RFC9098 [S/OL]. [2023-12-25]. <https://datatracker.ietf.org/doc/rfc9098/>.
- [16] IETF. Limited Domains and Internet Protocols: RFC8799 [S/OL]. [2023-12-25]. <https://www.rfc-editor.org/rfc/rfc8799.html>.

作者简介:

佟恬,研究员,硕士,主要从事下一代互联网、IPv6网络安全、源地址验证方向的研究工作;赵菁,研究员,硕士,主要从事下一代互联网、IPv6网络安全、DNS方向的研究工作;庞冉,首席研究员,硕士,主要从事下一代互联网、算力网络方向研究工作;曹畅,高级工程师,博士,主要从事算力网络、下一代互联网等方向的研究工作。