

OSPF 路由协议脆弱性研究及分析

朱绪全¹, 包婉宁¹, 张进¹, 江逸茗², 马海龙²

¹网络通信与安全紫金山实验室 南京 中国 210000

²国家数字交换系统工程技术研究中心 郑州 中国 450002

摘要 互联网的高速发展带来了网络规模的持续增长以及拓扑结构的愈加复杂,同时给网络安全提出了巨大的挑战,OSPF(Open Shortest Path First)已经成为网络部署中使用最为广泛的路由协议,OSPF等路由协议的安全是网络安全的重要组成部分,没有正确的路由信息,也就没有了网络的安全与稳定。本文论述了 OSPF 路由协议内在的交互机制,挖掘了自身机制存在的漏洞,深入研究了基于 OSPF 协议脆弱性的攻击技术,通过分析协议的设计缺陷,突破协议自带的保护机制,扰乱正常协议交互达到攻击目的。本文详细描述了几种典型的攻击原理,在仿真软件中搭建网络环境证实了漏洞的存在。本文对 OSPF 安全隐患与常见漏洞做了详细的量化评估与分析,基于 OSPF 漏洞特点对 CVSS3.0 评分系统进行扩展,创新地增加攻击范围的修正系数,提高了 OSPF 协议漏洞评价的合理性,量化评估结果能为漏洞防御的研究工作提供指导,对其他路由协议的脆弱性研究分析有积极的示范作用。最后针对本文描述的漏洞提出了相应的安全防范措施,提出一个路由威胁监测预防系统用于路由协议攻击的监测和预防。总之,保护 OSPF 等路由协议的安全需要建立一个整体的安全观,从多个层面来保障网络安全。

关键词 OSPF 协议; 路由; 脆弱性; 评估; 攻击; 防范

中图分类号 TP393 DOI 号 10.19363/J.cnki.cn10-1380/tn.2023.03.04

Research and Analysis on the Vulnerability of OSPF Routing Protocol

ZHU Xuquan¹, BAO Wanning¹, ZHANG Jin¹, JIANG Yiming², MA Hailong²

¹Purple Mountain Laboratories, Nanjing 210000, China

²National Digital Switching System Engineering and Technological Research Center, Zhengzhou 450002, China

Abstract The rapid development of the Internet has brought about the continuous growth of the network scale and the increasingly complexity of the topology, and at the same time it has presented huge challenges to network security. OSPF (Open Shortest Path First) has become the most widely used routing protocol in network deployment, The security of OSPF and other routing protocols is increasingly becoming an important part of network security, there will be no network security and stability without the correct routing information. This paper discusses the internal interaction mechanism of OSPF, and digs out the loopholes in the OSPF routing protocol itself, deeply studies the attack technology based on the vulnerability of the OSPF protocol, analyzes the design flaws of the protocol, breaks through the protocol's built-in protection mechanism, and disrupts the normal protocol interaction to achieve the purpose of attack. This paper describes in detail several typical attack principles, and the establishment of a network environment in the simulation software that confirms the existence of vulnerabilities. In this paper, several typical attack principles are described in detail, and the existence of vulnerabilities is verified by constructing network environment in simulation software. Based on the characteristics of OSPF vulnerabilities, the CVSS3.0 scoring system is expanded, and the correction coefficient of the attack range is innovatively increased, which improves the rationality and quantification of OSPF protocol vulnerability evaluation. The evaluation results can provide guidance for the research work of vulnerability defense, and have a positive demonstration effect on the vulnerability research and analysis of other routing protocols. Finally, some corresponding security measures are proposed for the vulnerabilities described in this paper, and a routing threat monitoring and prevention system is proposed to monitor and prevent routing protocol attacks. In a word, to protect the security of routing protocols such as OSPF, an overall security concept should be established to ensure network security at multiple levels.

Key words OSPF; route; vulnerability; evaluation; attack; prevention

0 引言

互联网的高速发展带来了网络规模的持续增长以及拓扑结构的愈加复杂,同时给网络安全提出了巨大的挑战,OSPF(Open Shortest Path First, 开放式最短路径优先)已经成为网络部署中使用最为广泛的内部网关协议。OSPF 作为一种典型链路状态路由协议,通过 LSA(Link State Advertisement, 链路状态通告)的形式发布路由,在 OSPF 区域内依靠各设备交互 OSPF 报文以达到路由信息的统一。

OSPF 路由协议的正确运行依赖于邻居路由器信息的正确性,没有正确的路由信息 OSPF 就不能算出正确的路径到达目的地,也就没有了网络的安全与稳定,而在实际的网络环境中存在着大量恶意伪造的虚假路由信息,如果没有防范保护措施,将会面临路由信息被篡改、恶意路由信息注入并洪泛到网络中,导致流量黑洞、侦听、路由欺骗,严重时会导致网络中断。

首先,本文深入研究了 OSPF 路由协议的脆弱性,从协议自身和当前路由器版本实现的角度分析其安全机制及存在的隐患,基于 OSPF 协议脆弱性,提出了几种典型的攻击方法,并详细阐述了其攻击原理。然后,对本文总结描述的 OSPF 安全隐患与常见威胁进行了相应的漏洞评估,最后基于本文描述的所有基于 OSPF 协议脆弱性的攻击提出了相应的安全防范措施,并设计一个路由威胁监测预防系统用于 OSPF 路由协议攻击的监测和预防。

1 OSPF 协议安全机制及常见威胁

1.1 OSPF 协议安全机制分析^[1]

OSPF 协议具有多种内在的安全机制预防恶意攻击。

1) 可靠的认证机制

OSPF 协议支持空认证、明文口令和 MD5(Message-digest Algorithm 5, 信息-摘要算法 5)认证^[2]。对于前两种认证类型,在物理链路中劫持并抓取报文就能知悉内容,因此无法提供安全性保证。使用 MD5 认证时,所有接入同一网络或子网的路由器配置相同的密钥,对每个 OSPF 协议包使用该密钥进行 MD5 校验,预防恶意报文攻击,保证安全性。

2) 层次化路由

OSPF 协议将自治系统划分为一个骨干区域和多个非骨干区域,各非骨干区域通过 ABR(Area Border Router, 区域边界路由器)与骨干区域相连。每

个区域各自拥有自己的链路状态数据库,使得本区域内拓扑可对其他区域屏蔽,同时不受其他区域错误路由信息的影响。

3) 反击机制

反击机制^[3]是一种防止路由干扰破坏的有效机制。当路由器收到以自己名义发送的 LSA, 该 LSA 比当前数据库中的 LSA 实例新,并且描述信息与自身获知不一致时,将立即通告一个含有正确链路状态且更大链路序号的 LSA,以纠正错误,其示意图见图 1,反击机制使恶意用户伪造的 LSA 很难被其他路由器利用。

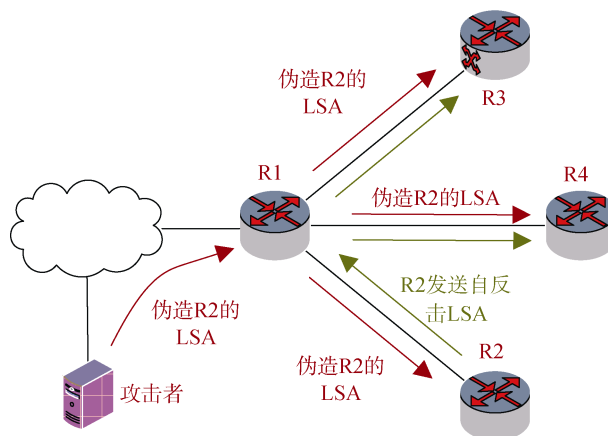


图 1 自反击机制示意图

Figure 1 Schematic diagram of self-counter attack mechanism

4) 双向链路机制

在路由表生成过程中,只有那些被两端路由器都通告的链路才会被加入计算中。如果攻击者通告一个不存在的链路到另一个路由器,而另一个路由器没有通告这条链路,那么这条链路对于路由表不会有任何影响。

1.2 OSPF 安全性隐患和常见威胁

通过研究 OSPF 协议内在的交互机制,可以得出不同的报文字段在协议运行过程中扮演着重要的角色,针对 OSPF 协议中 Hello、DD、LSR、LSU 等报文类型都存在潜在的攻击威胁。如果攻击者恶意篡改其中的一些字段,很可能导致路由器非预期的一些操作。虽然 MD5 算法可以有效的防止报文被恶意修改,但攻击者可以截取之前的一些 OSPF 报文实施重放攻击,况且 MD5 并不安全,王小云教授在 2004 年国际密码学会议上利用碰撞方法成功破解 MD5 算法。Perlman 在链路状态信息发布和公钥发布中引入非对称加密技术框架,消息的签名和认证使用不同的密钥^[4-5]。MurPhy 和 Badger 提出了一种设计方案,

该方案通过数字签名框架实现 OSPF 路由协议中链路状态信息和公钥的安全发布^[6]。数字签名框架是一个解决链路状态信息发布问题的有力候选者, 但是该方案用于生成和验证签名的开销是巨大的。在现实世界中, 维护密钥是一项比较繁重的工作, 密钥值需要双方操作员经过协商达成一致, 而操作员往往不了解密钥相关原理, 这就导致了很多自治系统中的密钥都相同, 或者不配置 MD5 认证, 从而埋下安全隐患, 密钥长时间不变也给攻击者提供足够的时间破解。进一步, 如果某台路由器被黑客攻破利用, 或者攻击者放置一台恶意的路由器接入网络, 并通过特种方式获取 MD5 键值, 利用 OSPF 协议漏洞进行内部攻击造成的后果往往更严重。

OSPF 协议内建的安全机制具有一定的保护作用, 但这些安全机制并非无懈可击, 仍具有脆弱性。攻击者通过分析 OSPF 内在的交互机制, 研究基于 OSPF 协议脆弱性的攻击技术, 挖掘协议的设计缺陷, 突破协议自带的保护机制, 扰乱正常协议交互达到攻击目的。攻击者通过网络基础设施脆弱性探测分析, 获取 ASBR、ABR、DR 等关键节点信息, 选取这些节点作为攻击目标, 使目标路由器或因扰乱无法正常进行关键路由信息的交互、或因资源耗尽致瘫, 切断局部路由传输通道, 严重影响路由交换, 能够形成更大规模的攻击, 对于网络造成的危害也更严重; 攻击者通过研究基于 LSA 的路由伪造及篡改技术, 造成局部路由计算错误, 使区域内部路由紊乱, 导致区域内部网络瘫痪; 攻击者通过篡改 LSA 协议的路由信息, 在区域内部形成路由环路, 短时间内造成数据环路风暴, 导致域内网络瘫痪。

OSPF 通过 Hello 报文建立和维护邻接关系, 通过 LSA 传递路由信息。攻击者通过伪造 Hello 报文可实现中断邻接关系, 通过伪造满足更高链路状态序列号、更大校验和、最大年龄条件(缺省为 1 小时)以及老化时间差超过 Max-Age-Diff(缺省为 15 分钟)且老化时间越小 LSA 信息包, 成功将恶意路由表项安装到目标路由器中, 能够实现攻击效果的最大化, 可导致运行 OSPF 路由协议的网络失效。常见的安全威胁如下^[7-13]。

1) 最大年龄攻击

攻击者发送携带最大年龄的 LSA 信息包, 成功将恶意 LSA 安装到其他路由器中, 使得路由器错误地清除路由表, 由于 OSPF 协议自带反击机制的滞后性, 攻击效果已经达成。持续该攻击将使得路由器数据库表项频繁地删除添加, 消耗路由器资源, 导致网络震荡和短时不可用。

2) 序列号增量攻击

攻击者向 OSPF 网络发送序列号较大的 LSA 信息包, 导致网络中其他路由器的路由被篡改、删除以及恶意路由注入, 持续该攻击的效果与最大年龄攻击类似。

3) 最大序列号攻击

攻击者向 OSPF 网络发送携带序列号为 0x7FFFFFFF 的 LSA 信息包, 成功将恶意 LSA 安装到其他路由器中。当路由器收到以自己名义发送的 LSA 时, 通过自反击机制, 重新发送序列号为 0x800000001 的修正 LSA。但是很多 OSPF 协议实现都存在缺陷, 路由器在发送正确的 LSA 之前不会冲掉此前恶意的 LSA, 所以正确的 LSA 会被当作过期的 LSA 而丢弃, 恶意的 LSA 会存活一个小时, 持续该攻击将造成路由器功能混乱, 导致网络失效。

4) 周期注入 LSA

OSPF 标准不允许路由器在 MinLSInterval(最小时间间隔, 默认为 5 秒)内生成发送同样 LSA 的两个实例。利用该实现, 攻击者通过高速持续地注入多个恶意 LSA 使得自反击机制失效, 该攻击的影响是持久的, 可扰乱正常协议功能, 导致网络失效。

5) 邻居表溢出攻击

攻击者持续不断的发送包含了许多虚假的邻居标识的 Hello 包, 导致目标路由器的邻居表溢出和震荡。

6) 邻接中断攻击

攻击者发送恶意的 Hello 包, 改变其中的指定路由器字段或者使其他路由器与指定路由器建立邻接关系, 网络中的路由器需要几十秒的时间重新建立邻接关系, 在这段时间中, 网络被通告为残余网络, 导致路由器不能正确转发数据。

7) Gabi Nakibly 单 LSA 攻击

根据文献^[14]描述, 目前 Cisco IOS 绝大多数版本在处理 LSA 头部时, 没有对链路状态标识与通告路由器的一致性进行检查, 攻击者利用该缺陷, 成功将恶意 LSA 安装到所有路由器中, 该 LSA 到达目标路由器时, 协议进程发现通告路由器不是自己, 所以不会触发自反击机制。

8) Gabi Nakibly 双 LSA 攻击

文献^[15]提出了一种双 LSA 攻击的方法, 为逃避 OSPF 自反击机制, 攻击者需要连续发送 2 条恶意 LSA。第一条 LSA 的序列号大于当前受害者 LSA 的真实序列号, 该 LSA 被称为 Trigger LSA。第二条 LSA 的序列号大于 Trigger LSA, 并且自反击 LSA 的序列号、校验和、链路状态标识与通告路由器相同,

但携带恶意路由信息, 称为 Disguise LSA。当网络中的路由器收到 Disguise LSA 后, 更新链路状态数据库, 由于自反击 LSA 可能晚于 Disguise LSA 到达, 因此被误当作副本丢弃, 从而使得自反击 LSA 失效。

9) 幻影路由器攻击

攻击者以一个不存在的幻影路由器在受害路由器所在的网段上与它建立虚假的邻接, 并以幻影路由器的身份注入虚假的路由实施恶意行为, 文献^[15]详细描述了幻影路由器与受害路由器建立双向邻接关系的方法, 但并未介绍如何构造恶意报文实施攻击的具体细节。

综上所述, OSPF 协议对于邻居设备的安全检查并不完备, 攻击者可通过恶意替换网络设备或者放置一台网络设备接入网络实施攻击, 如幻影路由器攻击。通过研究分析 OSPF 不同报文类型的交互机制, 可实施 Hello 攻击、DD 攻击、LSA 攻击以及 LSR 攻击。通过研究 LSA 的更新、老化以及生成机制, 可实施最大年龄攻击、序列号增量攻击、最大序列号攻击、周期性注入 LSA、单 LSA 攻击以及双 LSA 攻击。通过获取 OSPF 网络拓扑, 可有针对性地对 DR、BR、ABR、ASBR 进行攻击, 使得攻击造成的影响范围更广。研究基于 OSPF 协议防环机制, 通过攻击造成网络环路, 可导致网络级联式致瘫。

2 典型 OSPF 协议脆弱性攻击原理

在现实世界中, 攻击者往往会利用虚假的 LSA 生成恶意路由实施中间人攻击或者拒绝服务攻击。攻击者通过发送链路状态标识不存在的 LSA, 不断的向网络中的路由器添加 LSA, 导致路由器链路状态数据库溢出, 不能处理正常的 LSA。攻击者通过研究序列号机制, 利用序列号的溢出和各厂家路由器的实现机制缺陷, 逃避自反击机制, 篡改路由表, 导致 OSPF 协议进程异常。利用目前 OSPF 协议不具备智能化的缺陷, 随意伪造报文, 引起 OSPF 链路邻接关系以及路由表的震荡、断链或者路由表项异常。

根据 RFC2328 标准描述, OSPF 对路由信息的描述通过封装 LSA 中发布出去, LSA 是链接状态协议使用的一个分组, 它包括有关邻居和通道成本的信息, LSA 被路由器接收用于维护各自的 RIB (Routing Info Base, 路由表)。网络中运行 OSPF 协议的每台路由器根据路由器的分类产生一种或多种 LSA, 路由器把收集到的 LSA 存储在 LSDB (Link-state Database, 链路状态数据库)中, 然后运行 SPF 算法计算出路由表。所有的 LSA 都有相同的报头, 格式图 2 所示:

0	15	23	31
LS age		Options	LS type
Link State ID			
Advertising Router			
LS sequence number			
LS checksum		Length	

图 2 LSA 首部格式

Figure 2 LSA header format

- 1) LS Age: LSA 生成后经过的时间秒数;
- 2) Options:路由域的可选项;
- 3) LS type: LSA 类型, 包含 7 种类型。
- 4) Link State ID: 链路状态标识, 唯一标识一个 LSA;
- 5) Advertising Router:通告 LSA 的路由器标识;
- 6) LS sequence number: LSA 的序列号, 用于判定旧的或重复的 LSA;
- 7) LS checksum: 排除 Age 字段的校验和;
- 8) Length: LSA 的总长度;

经过的大量的理论研究和工程实践, 本文给出了三种典型的攻击方式。

2.1 链路状态标识不存在的 LSA 攻击

链路状态数据库是 OSPF 协议最关键的数据, 它储存了所有邻居的关键链接状态信息, 但该数据库的容量是有限的。攻击者通过持续发送链路状态标识不存在的 LSA, 不断的向数据库添加表项信息, 从而导致所有路由器链路状态数据库的溢出, 实现拒绝服务攻击。

攻击者通过伪造一个链路状态标识不存在的 LSA 并发送, 该恶意 LSA 到达真实产生该 LSA 的路由器时, 协议进程发现链路状态标识不是自己, 不会触发自反击机制, 并将 LSA 保存到数据库中, 导致网络中所有接收路由器的链路状态数据库信息篡改。每一条 LSA 将保存在链路状态数据库中直到过期(默认 1 个小时), 而数据库的容量是有限的, 持续攻击将导致数据库溢出, 使得受害路由器不能处理新的 LSA, 从而无法计算出正确的路由表, 造成网络通信异常, 严重者将导致网络瘫痪。

2.2 最大序列号减一攻击

在 OSPF 自反击机制中, 当路由器收到链路状态标识是自身的 LSA 时, 将收到的 LSA 序列号加一, 填充正确的数据信息后将 LSA 再发送出去, 从而达到修正数据信息的目的。然而, 序列号是有范围的, 攻击者利用自反击机制在最大序列号机制实现上的缺陷, 通过连续伪造携带最大序列号减一以及最小序列号的两个恶意 LSA, 使得 OSPF 自反击机制失效,

从而实现篡改路由表项, 导致网络中断、路由欺骗等目的。

根据 RFC2328 标准描述, LSA 的序列号字段有效范围是 $0x80000001 \sim 0x7FFFFFFF$, 循环往复。攻击者向 OSPF 网络发送序列号为 $0x7FFFFFFE$ 的 LSA, 触发目标路由器自反击机制, 目标路由器发送序列号为最大序列号 $0x7FFFFFFF$ 的 LSA, 然后, 攻击者再发送最小序列号 $0x80000001$ 的 LSA 报文, 按照标准规定, 该 LSA 应该由目标路由器生成, 由于实现机制方面的原因, 网络中的路由器以及目标路由器认为序列号小于当前序列号, 并不处理此类 LSA, 因此不会引起自反击机制, 使得目标路由器正确的 LSA 信息被网络中的其他路由器删除, 而目标路由器数据库信息中的 LSA 在 3600 秒老化后没有被冲洗, 导致整个域内的路由数据异常。

2.3 伪造数据库描述报文攻击

攻击者利用源地址欺骗的方式构造 DD (Database Description, 数据库描述) 报文, 引起两个邻接路由器之间的链接震荡, 使得网络中的路由器不断收到重新建链后的 LSU (Link State Update, 链路状态更新) 报文, 如果持续不断的构造 DD 报文, 将在网络中产生 LSU 报文风暴, 严重者将引起网络堵塞, 导致网络混乱。

攻击者利用源地址欺骗的方式构造 DD 报文并发送, 目标路由器收到该报文后, 认为邻居重新发起了邻接关系的建立流程, 因此将和真实邻居之间重新交互大量的报文, 经过 `exstart`、`exchange`、`loading`、`full` 状态重新建立邻接关系, 并更新路由域内所有关于该邻居的链路数据表项, 如果路由表项容量较大, 并且攻击者持续不断地构造恶意的 DD 报文, 将导致网络中充斥着大量 DD、LSU、LSAck (Link State Acknowledge, 链路状态确认) 报文, 严重占用网络带宽, 使得路由器不能正常处理有效报文, 造成网络中断、紊乱, 达到拒绝服务攻击的目的。

如果攻击者伪造 DD 报文, 并加入大量不存在的链路状态数据库概述信息, 与之交互的路由器将发送关于这些不存在的链路状态信息的 LSR (Link State Request, 链路状态请求) 消息, 但是由于真实路由器没有这些链路状态数据信息, 因此请求将得不到响应, 超时后会被放进重传列表, 如此将导致路由器不仅会耗竭请求列表资源, 也会耗尽重传列表资源。

3 漏洞评估

CVSS, 全称 Common Vulnerability Scoring System, 即“通用漏洞评分系统”, 是一个行业公开标

准, 其被设计用来评测漏洞的严重程度, 并帮助确定所需反应的紧急度和重量^[16]。CVSS3.0 通过基础度量、时间度量、环境度量计算分值。漏洞可利用性及漏洞影响度被用于评估该漏洞的静态分值, 作为漏洞的基础度量 V_B , 是 CVSS3.0 评估标准的基础^[17-18]。本文将从漏洞可利用性以及影响度两个方面对所描述的所有漏洞进行评估, 其中影响度评分针对 OSPF 协议漏洞的特点, 增加了攻击范围的修正项以提高评估的合理性。

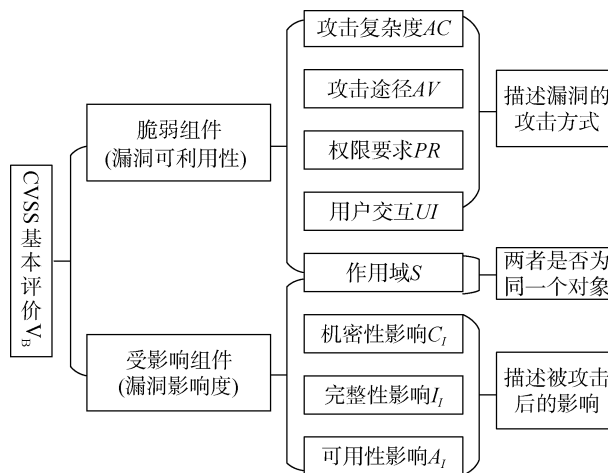


图3 CVSS 基本评价指标
Figure 3 CVSS basic evaluation

CVSS3.0 漏洞可利用性及漏洞影响度中包含的指标^[19-20]如图 3 所示, 漏洞可利用性中有攻击复杂度 AC 、攻击途径 AV 、权限要求 PR 、用户交互 UI 、作用域 S 五个指标组成, 漏洞影响度中有作用域 S 、机密性影响 C_I 、完整性影响 I_I 、可用性影响 A_I 四个指标。各个指标的分级和取值见附录 A。其中作用域是 CVSS3.0 版本计算的新属性, 反映软件组件中的漏洞会否影响其以外的资源获得其以外的权限, 当脆弱组件和受影响组件是同一个时, 被利用的漏洞只能影响由同一当局管理的资源, 此时作用域 S 为固定的(Unchange, U); 反之, 被利用的漏洞可能会影响超出脆弱组件预期授权权限的资源, 那么作用域 S 为可变的(Change, C)。

本文将对常见 OSPF 漏洞进行量化评估, 本文评估方法基于 OSPF 漏洞特点对 CVSS3.0 评分系统进行扩展, 创新地增加攻击范围的修正系数, 提高了 OSPF 协议漏洞评价的合理性。本文研究的 OSPF 漏洞可能造成整个网络拓扑中多台路由器的路由表项篡改, 因此在 OSPF 协议攻击的影响性评价中攻击范围(Modified Scope, MS)是一个重要指标, 它表示网络中受影响的路由器占比。本文使用的评估模型在

CVSS3.0 的基础上增加了攻击范围的修正系数 (*ModifiedScope Coefficient, MC*), 它是网络中受影响的路由器占比在 $[0.9, 11]$ 范围的归一化系数。在作用域为固定时, 漏洞影响的是脆弱组件自身, 所以不考虑攻击范围的影响; 在作用域为可变的时, 则需要考虑攻击范围的影响, 具体计算方式见公式(3)。

漏洞的基础度量 V_B 由漏洞可利用分值(E)和影响度分值(I)组成, 计算公式如下:

$$V_B = \begin{cases} 0 & E \leq 0 \\ \text{Roundup}(\min[(I + E), 10]) & 0 < I + E < 10 \\ & \& S = U \\ \text{Roundup}(\min[1.08 \times (I + E), 10]) & 0 < I + E < 10 \\ & \& S = C \\ 10 & I + E \geq 10 \end{cases} \quad (1)$$

漏洞可利用分值(E)的计算公式如下:

$$E = 8.22 \times AV \times AC \times PR \times UI \quad (2)$$

影响度分值(I)的计算公式如下

$$I = \begin{cases} 6.42 \times ISS & S = U \\ 7.52 \times (ISS - 0.029) \times MC & \\ -3.25 \times (ISS - 0.02)^{15} & S = C \end{cases} \quad (3)$$

其中,

$$ISS = 1 - [(1 - C_I) \times (1 - I_I) \times (1 - A_I)]$$

$$MC = 0.9 + 0.2MS$$

本文描述了多种作用域可变的攻击方式, 对于这一类攻击方式我们首先对攻击范围进行比较。本文在 EVE-NG 环境中搭建了一个有 50 个路由器的网络拓扑。实验分别对每一个位置的路由器进行攻击, 测量攻击范围为攻击者成功侵入的路由器数量占网络中路由器总数的百分比, 其中成功侵入指路由器的 LSA 被篡改。

图 4 统计了各种攻击方法攻击范围的累积分布, 其中横坐标表示攻击范围, 纵坐标表示攻击位置的累积分布。从实验结果可以看出链路状态标识不存在的 LSA 攻击的攻击范围主要集中在 90% 以上, 这是因为它不会触发自反击机制, 所以攻击范围最广。Nakibly 单 LSA 攻击方法的攻击范围最小, 虽然这种方法也不会触发自反击机制, 但这种方法有一定的局限性, 只有满足“单路径”的条件的路由器才会被

攻击。其他的攻击方法的平均攻击范围比较接近, 在 60% 左右。

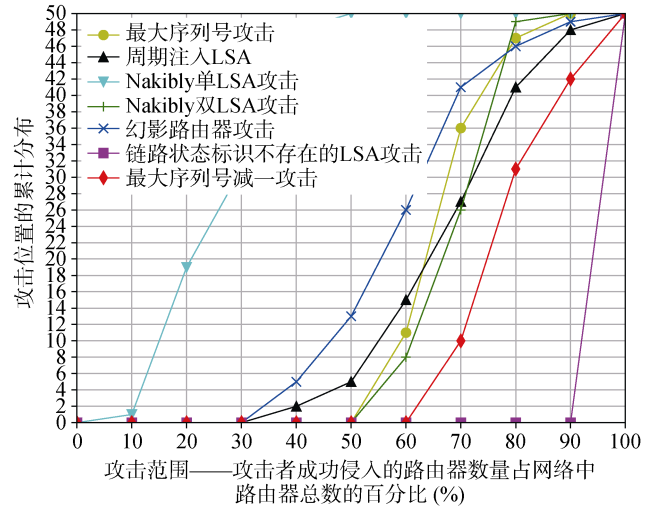


图 4 各种攻击方法攻击范围的累积分布

Figure 4 Cumulative distribution of attack range of various attack methods

根据上述漏洞评估方法, 本文对多种攻击手段进行对比, 量化评估 OSPF 协议漏洞的严重程度。本文提出的量化评估方法考虑到漏洞的可利用性和影响性, 同时考虑到攻击范围的影响, 能够较合理地评价 OSPF 协议漏洞的严重程度。量化评估结果可以使得网络管理者关注严重程度更高的漏洞, 同时为漏洞防御的研究工作提供指导, 对其他路由协议的脆弱性研究分析有积极的示范作用。

量化评估中 MS 值是上述实验中攻击范围的加权平均, 评估结果见表 1。可以看出作用范围固定的攻击方法危险性普遍稍低。作用范围可变的攻击方式可能会造成网络中大量路由器被攻击, 影响范围更广, 它们的评估得分相对更高。因此路由威胁监测预防中需要对范围可变的漏洞做出更积极的防御措施。

4 典型 OSPF 协议脆弱性攻击危害性测试

根据 2.1 以及 2.2 两个章节的描述, 本文在仿真网络环境下复现了该漏洞场景, 对漏洞危害性进行了测试。

测试网络环境在 EVE-NG 仿真软件上搭建。EVE-NG 全称 Emulated Virtual Environment - Next Generation, 能够运行任何虚拟镜像, 理论上, 只要能将虚拟机的虚拟磁盘格式转换为 qcow2, 就可以在 EVE-NG 上运行^[21]。测试网络拓扑如图 5 所示。

表 1 OSPF 攻击方式对比评估

Table 1 Comparison of OSPF attack methods

漏洞类型	AV	AC	PR	UI	S	C _I	I _I	A _I	MS	得分
最大年龄攻击	L	A	N	N	U	N	N	H	/	6.5
序列号增量攻击	L	A	N	N	U	N	N	H	/	6.5
最大序列号攻击	L	A	N	N	C	N	N	H	0.61	7.4
周期注入 LSA	H	A	N	N	C	N	N	H	0.67	6.2
邻居表溢出攻击	L	A	N	N	U	N	N	H	/	6.5
邻接中断攻击	L	A	N	N	U	N	L	H	/	7.1
Nakibly 单 LSA 攻击	L	A	N	N	C	H	N	L	0.27	8.1
Nakibly 双 LSA 攻击	L	N	N	N	C	H	N	N	0.66	8.6
幻影路由器攻击	L	N	N	N	C	H	N	N	0.56	8.6
链路状态标识不存在的 LSA 攻击	L	A	N	N	C	N	N	H	0.93	7.6
最大序列号减一攻击	L	N	N	N	C	H	N	N	0.78	8.7
伪造 DD 报文攻击	L	A	N	N	U	N	N	H	/	6.5

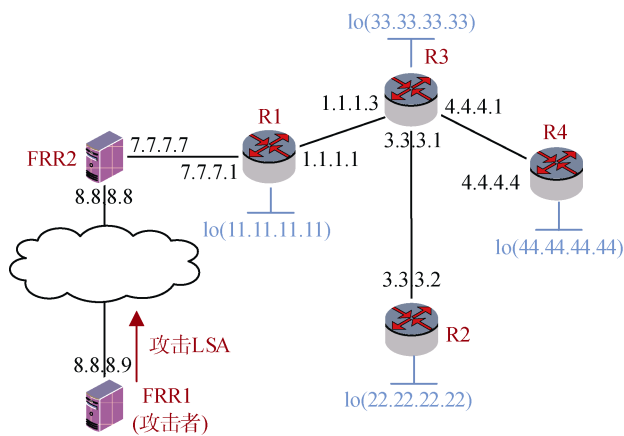


图 5 测试网络拓扑

Figure 5 Network topology of test

其中, FRR1、FRR2 为 Ubuntu18.04 系统上安装了 FRRouting 7.5.1 版本, FRRouting^[22]是一个免费的开源网络路由协议套件, 支持 linux 和 unix 平台, 实现了 BGP, OSPF, RIP, IS-IS, PIM, LDP, BFD, Babel, PBR 等功能, 最新的版本为 8.0.0。R1-R4 使用了 Cisco 3700 系列路由器的 IOS software, 版本号为 12.4 (25d)。

4.1 链路状态标识不存在的 LSA 攻击测试

1) 分别在 FRR1、FRR2、R1-R4 配置 OSPF, 配置完成后, 在 R3 上看到的链路状态数据库如图 6 所示:

```
R3#show ip ospf database
```

OSPF Router with ID (33.33.33.33) (Process ID 1)

Router Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum	Link count
8.8.8.8	8.8.8.8	297	0x80000060	0x00BC6D	2
8.8.8.9	8.8.8.9	1361	0x8000005D	0x005D15	1
11.11.11.11	11.11.11.11	1832	0x80000039D	0x002A75	3
22.22.22.22	22.22.22.22	1793	0x800000399	0x007AE4	2
33.33.33.33	33.33.33.33	155	0x8000003A3	0x008BF6	4
44.44.44.44	44.44.44.44	151	0x800000003	0x00C91E	2

Net Link States (Area 0)

Link ID	ADV Router	Age	Seq#	Checksum
1.1.1.3	33.33.33.33	1785	0x800000397	0x00D391
3.3.3.1	33.33.33.33	1785	0x800000397	0x00C76D
4.4.4.1	33.33.33.33	155	0x80000000F	0x000E57
7.7.7.7	8.8.8.8	337	0x800000011	0x00368B
8.8.8.9	8.8.8.9	1581	0x800000059	0x000F6F

图 6 R3 链路状态数据库(攻击前)

Figure 6 link state database of R3(before)

2) 在 FRR1 所在主机上构造并发送一条恶意 Router LSA, 将以下两项设置为一个不存在的路由器标识 10.10.10.10, 并设置 2 条任意的链接信息, 如表 2 所示:

表 2 恶意 LSA 报文字段

Table 2 Malicious LSA message fields

位置	字段	值
IP Header	Source Address	8.8.8.9
	Destination Address	8.8.8.8
	Protocol Number	89
OSPF Header	TTL	6
	Type	1(Link State Update)
	Router ID	8.8.8.9
LSU Header	LSA number	1
	Link State Type	1(Router LSA)
	Link State ID	10.10.10.10
LSA Header	Advertising Router	10.10.10.10
	Sequence Number	0x80000001
	Link ID	12.12.12.12
Router LSA	Link Data	255.255.255.255
	Link Type	3
	Metric	1
	Link ID	4.4.4.1
	Link Data	4.4.4.4
	Link Type	2
	Metric	1

3) 当该 LSA 到达网络中的路由器后, 协议进程认为是新的 LSA, 并添加到链路状态数据库中。如图 7 所示, 在 R3 的链路数据库中增加了一条 Link ID=10.10.10.10 的数据条目。

基于以上实验结果, 可以推断, 如果攻击者通过不断发送 Link State ID 不存在的 LSA, 将导致网络中所有接收路由器链路状态数据库表项溢出, 使

```
R3#show ip os database

OSPF Router with ID (33.33.33.33) (Process ID 1)

Router Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum Link count
8.8.8.8      8.8.8.8      1594        0x8000006D  0x00A27A  2
8.8.8.9      8.8.8.9      878         0x8000006B  0x004123  1
10.10.10.10  10.10.10.10  14          0x80000001  0x00ABCF  2
11.11.11.11  11.11.11.11  1187        0x800003A9  0x001281  3
22.22.22.22  22.22.22.22  1477        0x800003A5  0x0062F0  2
33.33.33.33  33.33.33.33  202         0x800003B1  0x006F05  4
44.44.44.44  44.44.44.44  198         0x80000003  0x00C91E  2

Net Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum
1.1.1.3      33.33.33.33  1268        0x800003A3  0x00BB9D
3.3.3.1      33.33.33.33  1268        0x800003A3  0x00AF79
4.4.4.1      33.33.33.33  202         0x8000001D  0x00F165
7.7.7.7      8.8.8.8      1644        0x8000001E  0x001C98
8.8.8.9      8.8.8.9      1030        0x80000067  0x00F27D
```

图 7 R3 链路状态数据库(攻击后)
Figure 7 link state database of R3(after)

得路由器不能处理正常的路由消息，导致拒绝服务攻击。

4.2 最大序列号减一攻击测试

1) 在这里，我们将 R4 作为攻击目标。分别在 FRR1、FRR2、R1-R4 配置 OSPF，配置完成后，选取网络中任何一台除 R4 以外的路由器，图 8 展示了 R3 的 OSPF 路由表：

```
R3#show ip route ospf
22.0.0.0/32 is subnetted, 1 subnets
O 22.22.22.22 [110/11] via 3.3.3.2, 00:04:12, FastEthernet0/0
7.0.0.0/24 is subnetted, 1 subnets
O 7.7.7.0 [110/20] via 1.1.1.1, 00:04:12, FastEthernet0/1
8.0.0.0/24 is subnetted, 1 subnets
O 8.8.8.0 [110/21] via 1.1.1.1, 00:04:12, FastEthernet0/1
11.0.0.0/32 is subnetted, 1 subnets
O 11.11.11.11 [110/11] via 1.1.1.1, 00:04:12, FastEthernet0/1
44.0.0.0/32 is subnetted, 1 subnets
O 44.44.44.44 [110/2] via 4.4.4.4, 00:04:12, FastEthernet1/0
```

图 8 R3 OSPF 路由表
Figure 8 OSPF routing table of R3

2) 在 FRR1 所在主机上构造并发送一条恶意 Router LSA，攻击目标为 R4，并设置如下字段，见表 3：

该 LSA 到达目标路由器后，触发自反击机制，目标路由器将发送 LSA 的序列号为最大序列号 0x7FFFFFFF 的 LSA。

3) 在 FRR1 所在主机上再构造发送一条恶意 Router LSA，攻击目标为 R4，将序列号设置为最小值，设置如下字段，见表 4：

由于实现机制的原因，R4 并未发送自反击 LSA，如图 9 所示，R4 上关于 Link ID = 44.44.44.44 标识的 LSA 的序列号仍然为 0x7FFFFFFF。

4) 当步骤 3 中的 LSA 到网络中的其他路由器后，由于实现机制的原因，协议进程将会删除该 LSA 的信息。如图 10 所示，R3 的路由表中关于 R4 的路由信息 44.44.44.44 已经不存在了。

Table 3 Malicious LSA message fields		
位置	字段	值
IP Header	Source Address	8.8.8.9
	Destination Address	8.8.8.8
	Protocol Number	89
	TTL	6
OSPF Header	Type	1(Link State Update)
	Router ID	8.8.8.9
LSU Header	LSA number	1
	Link State Type	1(Router LSA)
LSA Header	Link State ID	44.44.44.44
	Advertising Router	44.44.44.44
	Sequence Number	0x7FFFFFFF
	Link ID	44.44.44.44
	Link Data	255.255.255.255
	Link Type	3
Router LSA	Metric	1
	Link ID	4.4.4.1
	Link Data	4.4.4.4
	Link Type	2
	Metric	1

Table 4 Malicious LSA message fields		
位置	字段	值
IP Header	Source Address	8.8.8.9
	Destination Address	8.8.8.8
	Protocol Number	89
	TTL	6
OSPF Header	Type	1(Link State Update)
	Router ID	8.8.8.9
LSU Header	LSA number	1
	Link State Type	1(Router LSA)
LSA Header	Link State ID	44.44.44.44
	Advertising Router	44.44.44.44
	Sequence Number	0x80000001
	Link ID	44.44.44.44
	Link Data	255.255.255.255
	Link Type	3
Router LSA	Metric	1
	Link ID	4.4.4.1
	Link Data	4.4.4.4
	Link Type	2
	Metric	1

5) 基于以上实验结果，我们可以推断，该方法成功逃避了 OSPF 协议的自反击机制，如果攻击者持续发送采用这种方式发起攻击，网络的大量正常路


```

R4#show ip ospf database

        OSPF Router with ID (44.44.44.44) (Process ID 1)

        Router Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum Link count
8.8.8.8      8.8.8.8       1102        0x80000060  0x00BC6D 2
8.8.8.9      8.8.8.9       457         0x8000005E  0x005B16 1
11.11.11.11  11.11.11.11   654         0x8000039E  0x002876 3
22.22.22.22  22.22.22.22   606         0x8000039A  0x0078E5 2
33.33.33.33  33.33.33.33   575         0x800003A4  0x0089F7 4
44.44.44.44  44.44.44.44   4165        0x7FFFFFFF  0x00D417 2

        Net Link States (Area 0)

Link ID      ADV Router   Age         Seq#         Checksum
1.1.1.3      33.33.33.33  575         0x80000398  0x00D192
3.3.3.1      33.33.33.33  575         0x80000398  0x00C56E
4.4.4.1      33.33.33.33  575         0x80000010  0x000C58
7.7.7.7      8.8.8.8       1142        0x80000011  0x00368B
8.8.8.9      8.8.8.9       687         0x8000005A  0x000D70

R4#show ip route ospf
 1.0.0.0/24 is subnetted, 1 subnets
O   1.1.1.0 [110/20] via 4.4.4.1, 00:15:54, FastEthernet0/0
 33.0.0.0/32 is subnetted, 1 subnets
O   33.33.33.33 [110/11] via 4.4.4.1, 00:15:54, FastEthernet0/0
 3.0.0.0/24 is subnetted, 1 subnets
O   3.3.3.0 [110/20] via 4.4.4.1, 00:15:54, FastEthernet0/0
 22.0.0.0/32 is subnetted, 1 subnets
O   22.22.22.22 [110/21] via 4.4.4.1, 00:15:54, FastEthernet0/0
 7.0.0.0/24 is subnetted, 1 subnets
O   7.7.7.0 [110/30] via 4.4.4.1, 00:15:54, FastEthernet0/0
 8.0.0.0/24 is subnetted, 1 subnets
O   8.8.8.0 [110/31] via 4.4.4.1, 00:15:54, FastEthernet0/0
 11.0.0.0/32 is subnetted, 1 subnets
O   11.11.11.11 [110/21] via 4.4.4.1, 00:15:54, FastEthernet0/0

```

图 9 R4 链路状态数据库和 OSPF 路由表

Figure 9 link state database and OSPF routing table of R4

```

R3#show ip route ospf
 22.0.0.0/32 is subnetted, 1 subnets
O   22.22.22.22 [110/11] via 3.3.3.2, 00:00:48, FastEthernet0/0
 7.0.0.0/24 is subnetted, 1 subnets
O   7.7.7.0 [110/20] via 1.1.1.1, 00:00:48, FastEthernet0/1
 8.0.0.0/24 is subnetted, 1 subnets
O   8.8.8.0 [110/21] via 1.1.1.1, 00:00:48, FastEthernet0/1
 11.0.0.0/32 is subnetted, 1 subnets
O   11.11.11.11 [110/11] via 1.1.1.1, 00:00:48, FastEthernet0/1

```

图 10 R3 OSPF 路由表

Figure 10 OSPF routing table of R3

由将被恶意删除, 导致网络异常和混乱。

5 安全防范措施

一个具备严格安全防范措施的路由器不但可以抵御外部攻击, 同时也能抵御内部攻击, 本文将设计一个路由威胁监测预防系统用于路由协议攻击的监测和预防。根据本文第 3 节对多种 OSPF 协议攻击方法的量化评估, 路由威胁监测预防系统对于严重程度不同的漏洞会区别处理, 对于高分的严重漏洞系统会给出更积极的处理态度, 对于低分的漏洞则给出提示性信息以供网络管理者参考。另外, 本文将系统性描述对于上述攻击的安全防范措施, 针对上述攻击分别提出检测和防御方法。

1) 最大年龄攻击的防范措施, 攻击者通常伪装成网络中的一台或者几台路由器发起最大年龄攻击, 路由威胁监测预防系统在处理该类型攻击时, 需要主动记录攻击路由器的标识信息、攻击类型为最大年龄攻击到威胁数据库中, 缓存该报文, 暂不发送给路由协议处理进程, 同时启用超时机。依赖于

OSPF 自反击机制, 真实路由器收到该攻击报文并发现路由器标识是自身时会发送正确的 LSA 携带正确的年龄信息, 路由威胁监测预防系统收到后将判定之前缓存的报文为攻击报文, 做丢弃处理。对于真实的链路状态更新报文, 并不会触发自反击机制, 因此超时后, 将原报文发送给路由协议进程处理, 流程图见图 11。通过该方式能够大大降低路由器的数据表信息被篡改又被修正的概率, 避免造成网络的不稳定和震荡。

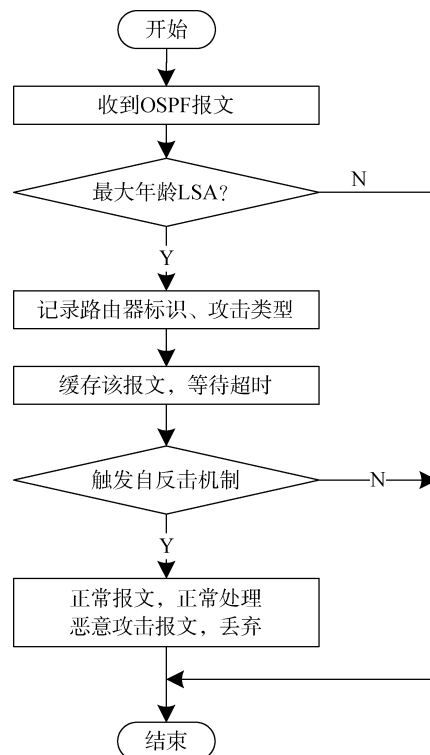


图 11 最大年龄攻击防御工作流程图

Figure 11 Work flow chart of maximum age attack defense

2) 序列号增量攻击的防范措施, 同最大年龄攻击类似, 正常路由器不会在短时间内重复增加序列号发起路由更新。路由威胁监测预防系统通过记录路由器标识、攻击类型为序列号增量攻击到威胁数据库中, 缓存该报文, 暂不发送给路由协议处理进程, 同时启用超时机。对于真实的链路状态更新报文, 并不会触发自反击机制, 超时后将原报文发送给路由协议进程处理。对于恶意的攻击报文, 将触发自反击机制发送修正报文, 路由威胁监测预防系统收到后认定之前的缓存报文为攻击报文, 做丢弃处理。因此路由器的路由表不会遭到污染, 防止路由表震荡。

3) 最大序列号攻击防范措施, 根据 OSPF 标准

规定, 序列号每次增加 1, 并且到达 2^{32} 后序列号重新从 0 开始回绕。因此当路由器接收到序列号为最大序列号的链路状态更新报文后, 首先判断当前序列号, 如果当前序列号与最大序列号的差值为 1, 那么将该报文缓存, 并记录路由器标识、攻击类型为序列号增量攻击到威胁数据库中, 参考序列号增量攻击的防范措施。如果序列号与最大序列号的差值不为 1 并且为最大序列号, 则认定为攻击报文, 做丢弃处理。

4) 周期注入 LSA 攻击防范措施, OSPF 标准规定不允许路由器在 MinLSInterval 时间间隔内发送同样 LSA 的两个实例(默认为 5 秒), 因此攻击者必须以很高的速率泛洪恶意的 LSA 进行攻击。路由威胁监测预防系统对该种类型的报文做入侵检测, 当检测到相同链路状态标识的 LSA 每次更新速率超过设定 MinLSInterval , 将其做阻断处理。

5) 邻居表溢出攻击以及邻接中断攻击属于 Hello 攻击, 正常 Hello 报文按照设置的报文发送间隔进行发送, 攻击者通过篡改 Hello 报文中的字段实施攻击, 因此路由威胁监测预防系统在处理 Hello 报文时, 需要记录上次收到的 Hello 报文的时间戳, 在设置的时间间隔内, 收到 Hello 报文, 缓存该报文, 暂不发送给路由协议处理进程, 在设置的时间间隔超时后, 对接收到的相同的邻居的 Hello 报文做判别处理, 如果收到了该邻居的多个报文, 则认为遭受到了攻击。通常情况下, 攻击者发送的 Hello 报文携带的邻居是不可达的, 路由监测保护系统通过发送 ICMP 报文确认邻居的可达性, 如果不可达, 则认为含有该条邻居表项的 Hello 报文为攻击报文并丢弃, 否则将正确的报文发送路由协议进程, 处理流程图见图 12。

6) Gabi Nakibly 单 LSA 攻击的防范措施, 在路由协议处理进程中通过增加链路状态标识与通告路由器的一致性进行检查, 如果链路状态标识与通告路由器的不一致则认定为攻击报文并丢弃, 可有效预防该攻击。

7) Gabi Nakibly 双 LSA 攻击的防范措施, 由于 LSA 校验和的可预测性, 使得自反击的 LSA 可能也是攻击报文。本文借鉴 Gabi Nakibly 的建议, 通过存储已安装的 LSA 的加密散列(例如 SHA-256)来扩展 LSA 数据库。散列是在整个 LSA 上计算的, 包括广告中的链接, 但不包括 Age 字段。路由器通过首先检查年龄、序列号、校验和以及散列来确定两个 LSA 是否相同, 如此就能区分伪装的 LSA 和反击的 LSA。

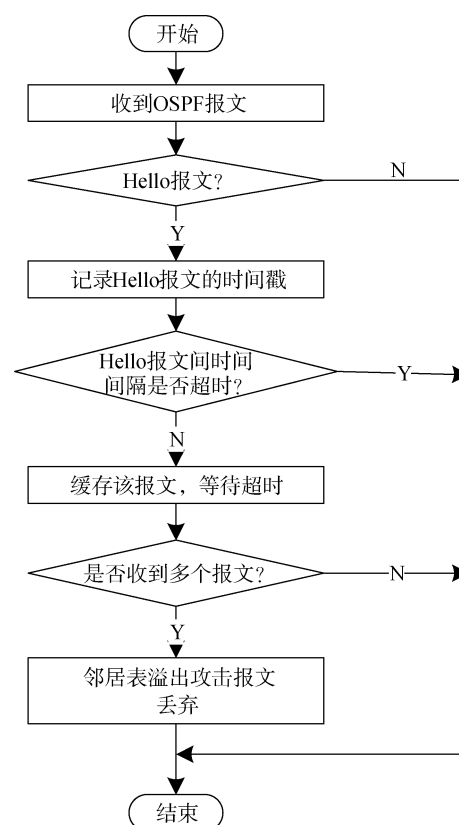


图 12 邻居表溢出攻击防御工作流程图

Figure 12 Work flow chart for preventing neighbor table overflow attacks

8) 幻影路由器攻击的防范措施, 对于幻影路由器来说, 攻击者在实施该类型攻击时, 发送的 DD 报文并不包含对于幻影路由器的数据描述信息, 也不支持对于链路状态请求消息的回复, 确认对方是真实路由器还是幻影路由器可以通过判断 DD 报文是否携带链路概要, 并且通过发送链路状态请求报文来确认是否能够得到相应的链路状态更新报文进行区别, 对从幻影路由器发出的所有报文做丢弃处理。

9) 链路状态标识不存在的 LSA 攻击防范措施, OSPF 协议进程在接收到全部的 LSU 报文后生成链路状态数据库, 等待一段指定的时间, 直至链路状态数据库收敛至稳定, 针对生成的 OSPF 路由, 遍历路由器的链路状态数据库, 如果没有发现与之关联的表项, 说明该表项被恶意插入, 及时将其从数据库中删除。

10) 最大序列号减一攻击防范措施, 首先判断当前序列号, 如果当前序列号与报文携带的序列号差值连续, 那么将该报文缓存, 并记录路由器标识、攻击类型为序列号增量攻击到威胁数据库中, 参考序列号增量攻击的防范措施。当数据库 LSA 已经为最大序列号时, 及时冲洗该 LSA, 生成并发送新的

LSA。另外对于序列号类型的攻击, 路由威胁监测预防系统需要判断收到报文的序列号与当前链路状态信息的序列号是否连续, 如果不连续, 则大概率收到恶意的 LSA, 对于此类报文应尽量不予处理。

11) 伪造 DD 报文攻击防范措施, 按照正常的报文交互流程, 两个路由器将会在 Hello 报文选取出 DR(Designated Router, 指定路由器)、BDR(Backup Designated Router, 备份指定路由器)后, 进行 DD 报文的交互。因此路由威胁监测预防系统对于接收的 DD 报文, 需要判断该 DD 报文前是否经历邻居关系的掉线和重建, 即: 之前是否有相关的多条 Hello 报文的交互, 如果没有则认为是攻击报文, 做丢弃处理, 无须触发重新建立邻接关系的处理流程, 这就要求 OSPF 协议进程对于报文的处理不仅仅是根据收到的报文做简单的应答及处理, 还需要综合 OSPF 协议状态机、链路状态数据库等进行智能化处理, 避免遭受恶意报文攻击。

总之, OSPF 协议在实现过程中, 既要引入 MD5 认证或者非对称加密技术框架, 防止外部攻击, 也要引入路由威胁监测预防系统用于内部路由协议攻击的监测和预防, 针对报文中的关键字段的上限和下限, 缓存的链路状态数据表, 链路状态机, 收到报文的上下文等关键信息综合分析和处理, 并有针对性的采取相应的保护措施。

6 结论

本文深入研究了 OSPF 路由协议的安全机制, 详细描述了 OSPF 协议存在的安全隐患及常见威胁, 提出了几种典型的基于 OSPF 协议脆弱性的攻击方法, 详细阐述其攻击原理, 并在仿真网络环境中搭建网络拓扑复现了两种攻击场景, 对其有效性及危害性进行了测试, 可以得出, OSPF 协议中 LSA 的链路状态标识和序列号等关键字段的自反击机制等方面存在安全隐患, 利用此类缺陷, 或能逃避自反击机制, 或能导致链路状态数据库溢出、OSPF 更新报文风暴, 对网络产生持续影响, 严重威胁网络正常运行。本文对 OSPF 安全隐患与常见漏洞做了详细的量化评估与分析, 基于 OSPF 漏洞特点对 CVSS3.0 评分系统进行扩展, 创新地增加攻击范围的修正系数, 提高了 OSPF 协议漏洞评价的合理性。最后, 针对本文描述的漏洞提出了相应的安全防范措施, 并引入路由威胁监测预防系统用于内部路由协议攻击的监测和预防。总之, 保护 OSPF 等协议的安全需要建立一个整体的安全观, 应该从多个层面来保障网络安全。

参考文献

- [1] Moy J. OSPF version 2[EB/OL]. <https://datatracker.ietf.org/doc/html/rfc2328>, April. 1998.
- [2] Rivest R. The MD5 Message-Digest Algorithm, Internet Request for Comments[EB/OL]. <https://datatracker.ietf.org/doc/html/rfc1321>, April. 1992.
- [3] Jones E, Moigne O L. OSPF security vulnerabilities analysis [EB/OL]. <https://datatracker.ietf.org/doc/html/draft-ietf-rpsec-ospf-vuln-02>, June. 2006.
- [4] Perlman R. Interconnections: Bridges, Routers, Switches, and Internet working Protocols[M]. China Machine Press, 2002.
- [5] Perlman R. Network layer protocols with Byzantine robustness[J]. *Massachusetts Institute of Technology*, 1988.
- [6] Murphy S L, Badger M R. Digital Signature Protection of the OSPF Routing Protocol[C]. *Proceedings of Internet Society Symposium on Network and Distributed Systems Security*, 2002: 93-102.
- [7] Cai Z Q. OSPF Routing Protocol Attacks Analysis and Security Precaution[J]. *Computer Engineering and Design*, 2007, 28(23): 5618-5620.
(蔡昭权. OSPF 路由协议的攻击分析与安全防范[J]. *计算机工程与设计*, 2007, 28(23): 5618-5620.)
- [8] Kang W. *Research and analysis of the security mechanism in OSPF*[D]. Beijing: Beijing University of Posts and Telecommunications, 2010.
(康威. OSPF 路由协议安全性分析与研究[D]. 北京: 北京邮电大学, 2010.)
- [9] Xu G T. The Research Of“Black Hole”Attacks on OSPF Routing Spoofing[J]. *Netinfo Security*, 2012(11): 10-12.
(徐国天. 基于 OSPF 路由欺骗的“黑洞”攻击及防御措施研究[J]. *信息安全*, 2012(11): 10-12.)
- [10] Chen Haiyan, Ji Zhongmei, Li Ou, et al. OSPF Routing Protocol Security Analysis and Attacks Detection[J]. *Microcomputer Information*, 2005, 21(5): 104, 230-231.
(陈海燕, 季仲梅, 李鸥, 等. OSPF 路由协议安全分析及其攻击检测[J]. *微计算机信息*, 2005, 21(5): 104, 230-231.)
- [11] Xia Y F. *Analysis of route deception based on OSPF routing protocol*[D]. Nanjing: Southeast University, 2014.
(夏云峰. 基于 OSPF 路由协议的路由欺骗分析[D]. 南京: 东南大学, 2014.)
- [12] Kasemsuwan P, Visoottiviseth V. OSV: OSPF Vulnerability Checking Tool[C]. *2017 14th International Joint Conference on Computer Science and Software Engineering*, 2017: 1-6.
- [13] Song Y B, Gao S, Hu A Q, et al. Novel Attacks in OSPF Networks to Poison Routing Table[C]. *2017 IEEE International Conference on Communications*, 2017: 1-6.
- [14] Nakibly G, Menahem E, Waizel A, et al. Owning the routing table: part II [C]. *Proceedings of Black Hat 2013*, 2013.
- [15] Nakibly G, Kirshon A, Gonikma D, et al. Persistent OSPF attacks[C]. *Proceedings of the 19th Annual Network & Distributed System Security Conference*, 2012.
- [16] Common Vulnerability Scoring System version 3.0: Specification Document, <https://www.first.org/cvss/v3.0/specification-document>,

2021.

- [17] Zhang B Y, Wang M. Research on Quantization Method of Network Attack and Defense Based on CVSS Vulnerability Score[J]. *Journal of Ordnance Equipment Engineering*, 2018, 39(4): 147-150.
(张必彦, 王孟. 基于 CVSS 漏洞评分标准的网络攻防量化方法研究[J]. *兵器装备工程学报*, 2018, 39(4): 147-150.)
- [18] Lei K N, Zhang Y Q, Wu C S, et al. A System for Scoring the Exploitability of Vulnerability Based Types[J]. *Journal of Computer Research and Development*, 2017, 54(10): 2296-2309.
(雷柯楠, 张玉清, 吴晨思, 等. 基于漏洞类型的漏洞可利用性

量化评估系统[J]. *计算机研究与发展*, 2017, 54(10): 2296-2309.)

- [19] Mell P, Scarfone K, Romanosky S. The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems[J]. *Nist Interagency/internal Report*, 2007.
- [20] Wang R Y, Gao L, Sun Q, et al. An Improved CVSS-Based Vulnerability Scoring Mechanism[C]. *2011 Third International Conference on Multimedia Information Networking and Security*, 2011: 352-355.
- [21] EVE-NG, <https://www.eve-ng.cn/doku.php>, 2017.
- [22] FRRouting Project. <https://frrouting.org/>, 2021.



朱绪全 于 2009 年在南京理工大学计算机应用专业获得硕士学位。现任网络通信与安全紫金山实验室高级工程师。研究领域为新型网络体系结构、网络空间安全防护, 研究兴趣包括: 网络空间安全防护、虚拟化、云计算、计算机系统、SDN 等。Email: zxq092@163.com



包婉宁 于 2019 年在中国矿业大学电子与通信专业获得硕士学位。现任网络通信与安全紫金山实验室工程师。研究领域为新型网络体系结构、网络空间安全防护。研究兴趣包括: 网络安全、信息编解码。Email: baowanning@pmlabs.com.cn



张进 于 2008 年在信息工程大学通信与信息系统专业获得博士学位。现任网络通信与安全紫金山实验室高级工程师, CCF 会员。研究领域为软硬件协同设计、网络安全。Email: zhangjin@pmlabs.com.cn



江逸茗 于 2014 年在信息工程大学通信与信息系统专业获得博士学位。现任信息工程大学信息技术研究所副研究员。研究领域为新型网络体系结构、网络空间安全防护。研究兴趣包括: 网络内生安全防护技术、虚拟化等。Email: j8403@163.com



马海龙 于 2011 年在信息工程大学通信与信息系统专业获得博士学位。现任信息工程大学信息技术研究所副研究员, 河南省拟态防御重点实验室副主任。研究领域为网络空间内生安全技术、网络威胁智能检测以及新型网络体系等。Email: longmanclear@163.com

附录 A: CVSS3.0 指标的分级和取值

指标	指标取值	数值
攻击途径(<i>AV</i>)	Network(N)	0.85
	Adjacent(A)	0.62
	Local(L)	0.55
	Physical(P)	0.2
攻击复杂度(<i>AC</i>)	Low(L)	0.77
	High(H)	0.44
	None(N)	0.85
权限要求(<i>PR</i>)	Low(L)	0.62 (or 0.68 if S= C)
	High(H)	0.27 (or 0.5 if S= C)
用户交互(<i>UI</i>)	None(N)	0.85
	Required(R)	0.62
机密性影响(<i>C_i</i>)	High(H)	0.56
完整性影响(<i>I_i</i>)	Low(L)	0.22
可用性影响(<i>A_i</i>)	None(N)	0