

OSPF 协议 DD 报文的脆弱性分析与验证

安宁刚^{1,2}, 李国栋^{1,2}, 覃尊颖¹, 李 卫^{2,3}, 黄旭昌³

(1 西安交通大学 网络中心, 陕西 西安 710049;

2 通讯网信息传输与分发技术重点实验室, 河北 石家庄 050081;

3 西安交通大学 电子与信息工程学院, 陕西 西安 710049)

摘 要: 分析了 OSPF 协议在 EXSTART/EXCHANGE 状态下 DD(Database Description) 报文交互过程, 提出了该过程存在的脆弱性, 设计开发了验证系统, 并对两款不同厂家的路由器进行了验证和对比, 证明了该缺陷的存在。

关键词: OSPF; DD 报文; 泛洪; LSA; 脆弱性

中图分类号: TN402

文献标识码: A

文章编号: 1000-7180(2015)02-0052-04

Vulnerability Analysis and Verification of OSPF DD Packet

AN Ning-gang^{1,2}, LI Guo-dong^{1,2}, QIN Zun-ying¹, LI Wei^{2,3}, HUANG Xu-chang³

(1 Center of Network, Xi'an Jiaotong University, Xi'an 710049, China; 2 Science and Technology on Information Transmission and Dissemination in Communication Networks Laboratory, Shijiazhuang 050081, China;

3 School of Electronic and Information Engineering, Xi'an Jiaotong University, Xi'an 710049, China)

Abstract: This paper analyzes the packet interactive process of DD (Database Description) under the state of EXSTART/EXCHANGE and proposes the vulnerability of this process. It designs and develops the verification system, verifies and compares the two kinds of routers from different manufacturers, and proves the existence of the vulnerability.

Key words: OSPF; DD packet; flooding; LSA; vulnerability

1 引言

基于 IP 的信息网络经过不断的发展演化, 已经成为承载当今人类社会信息传递交流的重要基础设施, 在政治、经济、文化等各方面日益发挥着重要作用。如何保障网络安全、稳定、可靠运行, 以及确保信息安全是互联网发展面临的巨大挑战。信息网络的基础是由一系列的网络协议构成, 其中路由协议是网络最重要的基础协议之一^[1-4]。OSPF^[5] (Open Shortest Path First, 开放式最短路径优先) 协议是应用最为广泛的内部网关路由协议, 其安全性、健壮性受到人们的关注。经过国内外研究人员的不断研究, 发现了 OSPF 协议的多个脆弱性, 如报文的验证

机制安全性不足, 泛洪机制易引发 DoS 攻击, 协议报文交互过程中存在多种脆弱性, 已知的脆弱性常见的攻击有 OSPF LSR 报文伪造攻击^[6]、OSPF DR/BDR 篡改攻击^[7]、OSPF 序列号加 1 攻击、OSPF 最大序列号攻击、OSPF 最大年龄攻击^[8]等。

本文分析研究^[5-7]了 OSPF 协议在 EXSTART/EXCHANGE 状态下 DD(Database Description) 报文交互过程, 论述了该过程存在的脆弱性, 并设计开发了验证系统对两款不同厂家的路由器进行了验证, 证明了该缺陷的存在。

2 OSPF 协议及报文格式

OSPF 是目前广泛使用的一个内部网关协议,

收稿日期: 2014-03-29; 修回日期: 2014-05-18

基金项目: 通讯网信息传输与分发技术重点实验室开放课题(ITD-U11001)

用于在单一自治系统内决策路由. 与 RIP 相比 OSPF 是链路状态路由协议, 而 RIP 是距离向量路由协议. OSPF 通过路由器之间通告网络接口的状态来建立维护一张网络有向拓扑图, 利用最小生成树算法(SPF 算法)得到路由表. OSPF 协议状态包含 Down、Attempt、Init、two-way、ExStart、Exchange、Loading、Full.

OSPF 总共有 5 种类型报文, 其共同的头部格式如图 1 所示, 其中的 Type 域标识了报文类型, 分别代表如下含义: 1 为 Hello 报文, 2 为 DD 报文, 3 为 LSR 报文, 4 为 LSU 报文, 5 为 LSAck 报文.

0	7	15	31
Version		Type	Packet length
Router ID			
Area ID			
Checksum		AuType	
Authentication			
Authentication			

图 1 OSPF 报文头部

OSPF 还定义了信息描述格式: LSA (Link-State Advertisement) 为链路状态通告, OSPF 路由器以此来维护路由表. 链路状态(LSA)就是 OSPF 接口上的描述信息, 例如接口上的 IP 地址、子网掩码、网络类型、Cost 值等等, OSPF 路由器之间交换的并不是路由表, 而是链路状态(LSA), OSPF 通过获得网络中所有的链路状态信息, 计算出到达每个目标精确的网络路径. OSPF 路由器会将自己所有的链路状态毫不保留地全部发给邻居, 邻居将收到的链路状态全部放入链路状态数据库(Link-State Database), 邻居再发给自己的所有邻居, 并且在传递过程中, 不会有任何更改. 通过这样的过程, 最终, 网络中所有的 OSPF 路由器都拥有网络中所有的链路状态, 并且所有路由器的链路状态应该能描绘出相同的网络拓扑. LSA 格式如图 2 所示, 其中的 LS age^[9] 字段表示该 LSA 自产生所经历的时间, 在路由器的链路状态数据库中其值每秒加 1, 但是在通过报文传输的过程中不变. LS age 的最大值为 3 600, 表示该 LSA 已失效, 这是最大年龄攻击的原理. LS sequence number 用于标示每一条 LSA, 值越大表示越新, 即具有大 LS sequence number 的 LSA 将替换较小值的 LSA. 该字段以有符号数值类型表示, 起始值为 0x80000001, 最大值为 0x7FFFFFFF. Link State ID 字段表示该路由的目的 IP 地址, Advertising Router 表示始发该 LSA 的路由器 ID, 以 IP 地址形式表示. LSA 附着于 DD 和

LSU 报文中发送, 不过在 DD 报文中只有 LSA 头部, LSU 报文拥有完整 LSA.

0	7	15	31
LS age		Options	LS type
Link state ID			
Advertising Router			
LS sequence number			
LS checksum		length	

图 2 LSA 头部

两台运行 OSPF 协议的路由器在建立连接时, 首先向组播地址 224. 0. 0. 5 发送 Hello 报文用于发现邻居, 然后发送 DD 报文用于同步链路状态数据库. 在一个 OSPF 自治域内, 需要达到所有路由器的链路状态数据库相一致的状态, 因此 OSPF 路由器通过 DD 报文确定本地缺失的 LSA, 然后发送 LSR 报文向邻居请求更新, 邻居发送 LSU 报文做应答. 链路状态数据库同步完成后建立连接的过程也即完成.

3 DD 报文交互过程及 DD 报文交互脆弱性分析

DD 报文(Database Description packet)在路由器发送 Hello 报文, 发现邻居后用于与邻居同步链路状态数据库. 两个 OSPF 路由器建立邻接关系时, 在 EXSTART/EXCHANGE 状态下交换 DD 报文.

当一台路由器 A 收到邻居路由器 B 发送的 DD 报文时, 路由器 A 需要查找本地链路状态数据库, 如果本地没有 B 发送的 DD 报文中携带的链路状态数据(LSA), 则需生成一个 LSR 报文向 B 请求相应的链路状态数据, 否则不需向 B 发送请求. OSPF 协议中, 没有对 DD 报文交互总量、频率和信息的可靠性做限制和验证. 如果 B 异常(设备重启)或恶意地以高频率向 A 发送 DD 报文, 并且这些 DD 报文中携带的都是 A 的链路状态数据库中不存在的数据, 当 A 的本地链路状态数据库较大(几百条, 上千条, 而在一些大型网络中可能超过万条), 在收到 B 的 DD 报文后, 路由器 A 将花费大量计算资源查找本地链路状态数据库, 并缓存收到的 LSA 报文, 导致 A 的计算资源和存储资源被大量消耗, 从而造成路由器 A 相应速度、处理性能下降, 严重时将会导致路由器 A 的不可用.

4 验证系统设计

验证系统采用伪造实体路由器方式构造一个攻击路由器, 通过伪造 DD 报文进行攻击验证所述缺陷是否存在. 伪造实体路由器方式改造了开源虚拟

路由软件 Quagga, Quagga 原名 Zebra, 由思科公司资助开发, 并以 GNU 版权方式发布. 该项目从 1996 年开始, 至今发布了多个版本, 截至本文书写时最新的版本是 0.99.22, 本系统使用 0.99.21 版本. 当前, 国内一些路由设备厂商和科研机构主要使用 Quagga 进行路由器模拟, 因此从兼容性来说, 使用 Quagga 模拟的路由器接入大多数品牌厂商的实体路由器组成的网络时不会存在大的问题.

DD 报文伪造攻击的逻辑图如图 3 所示, A 与 B 之间建立正常的 OSPF 连接, 攻击者与 A 也建立 OSPF 连接, 当攻击者的状态达到 Exstart 时发送伪造的 DD 报文. DD 报文伪造攻击处理流程如图 4 所示.

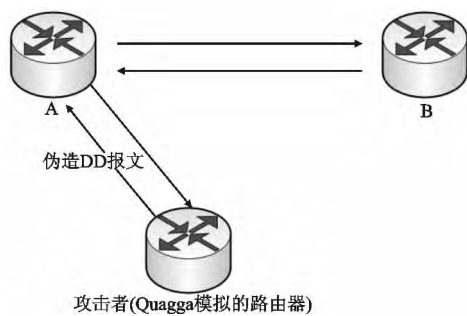


图 3 DD 报文伪造攻击示意图

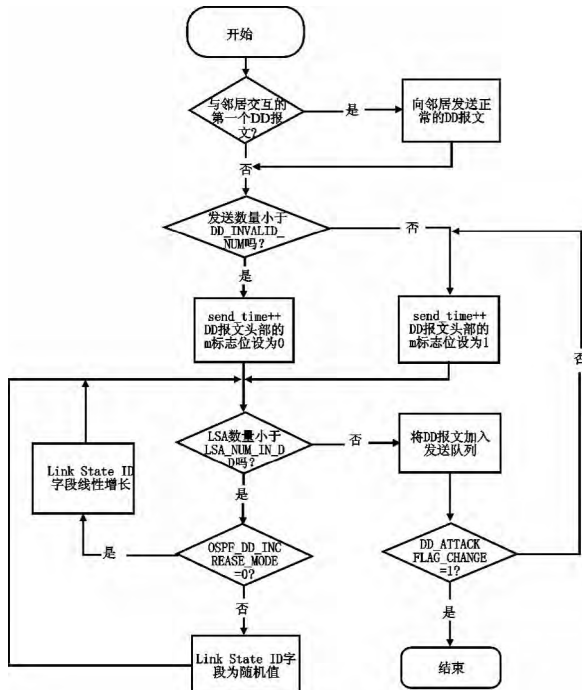


图 4 DD 报文伪造攻击处理流程

5 验证结果

验证环境如图 5 所示, 整个验证网络由三台实

体路由器 A, B, C, 伪造实体路由器 (攻击与监控服务器) 组成. 本文分别对思科和锐捷的路由器进行了测试.

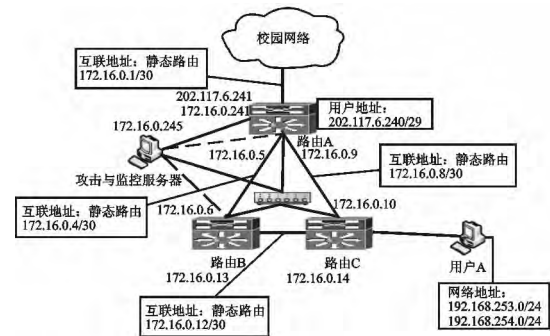


图 5 DD 报文交互脆弱性验证环境

DD 报文伪造攻击的预期效果为引起被攻击的路由器的 CPU 占用率提高, 每个 DD 报文中 LSA 数量, LSA 头部的 Link State ID 字段值, 以及路由器的链路状态数据库的大小 (以 LSA 数量表示) 这些因素将影响 CPU 的占用率. 下面将针对这三个因素分别测试, 力求发现其中的规律. 设定 Link State ID 字段值线性变化的规律为 $S + D * 80 + I$, 其中 S 为一个固定值, D 为已经发送的 DD 报文的数量, I 为 LSA 在 DD 报文中的编号.

测试的网络环境中链路 MTU 值为 1500, DD 报文除去以太网头部, IP 包头部, OSPF 包头部和 DD 报文头部的 66 字节, LSA 可占用的最大长度为 1434 字节, 而每个 LSA 头部长为 20 字节 (DD 报文中只包含 LSA 头部, 而不是完整数据), 每个 DD 报文中 LSA 的数量可以为 1~71 之间的任意值. 将链路状态数据库大小固定为 8, Link State ID 字段值线性变化, 测试 CPU 占用率与 DD 报文中 LSA 的数量变化的情况. 未进行攻击的情况下, 锐捷路由器的 CPU 占用率稳定在 6% 左右, 思科路由器 CPU 占用率稳定在 1% 左右. 通过测试, 不管是锐捷的路由器还是思科的路由器, CPU 占用率与 DD 报文中 LSA 的数量关系都不大. 不管 DD 报文中 LSA 的数量是多少, 攻击后, 锐捷路由器 CPU 占用率提高 15% 左右, 如图 6 所示, 思科路由器提高 8% 左右.

将 DD 报文中 LSA 的数量固定为 71, 链路状态数据库的大小固定为 8, 测试 CPU 占用率与 Link State ID 字段值的关系. 经过测试发现随机值比线性增长值方式 CPU 占用率高出 2~3 个百分点, 但是对于整个模型的攻击效果来说, 影响不大.

Process	SSus	1Min	5Min	Process
0	0%	0%	0%	HISB INT
1	0%	0%	0%	ktimer
2	0%	0%	0%	atimer
3	0%	0%	0%	perioctask
4	0%	0%	0%	waitqueue_process
5	0%	0%	0%	tasklet_task
6	0%	0%	0%	events
7	0%	0%	0%	snmpd
8	0%	0%	0%	snmp_trapd
9	0%	0%	0%	netblock
10	0%	0%	0%	gc_task
11	0%	0%	0%	Contest
12	0%	0%	0%	basepd
13	0%	0%	0%	hdf flush
14	0%	0%	0%	hupdate
15	0%	0%	0%	ll_nt
16	0%	0%	0%	ll main process

图6 DD报文伪造攻击效果图

将 DD 报文中 LSA 的数量固定为 71, Link State ID 字段值采用线性增加,测试 CPU 占用率与链路状态数据库大小的关系。经过测试发现 CPU 占用率随着链路状态数据库的增大而提高。

通过上面的测试可以发现路由器查找 LSA 的算法对需要查找的 LSA 的数量以及 LSA 的 Link State ID 值不敏感,但是查找的容量大小对算法效率有影响,同时验证了 DD 报文伪造攻击模型对于思科 3900 和锐捷 5750 交换机有效。另外在测试的过程中发现思科和锐捷的路由器在 DD 报文交互流程方面的一点差异。思科路由器要求收到的第一个 DD 报文中必须有一个 LSA 的 Link State ID 值为接收者本身,锐捷的路由器没有这个要求。

6 结束语

OSPF 路由协议由于其自身的复杂性,虽经多次改进(V2/V3),但仍然存在一些脆弱性,单纯依靠协议本身较难以防范各类攻击给网络带来的安全隐患,因此本文建议采用积极的方式主动防护和检测机制来增加网络安全管理^[10]。

参考文献:

- [1] Hartman S, Zhang D. Analysis of OSPF security according to KARP design guide[S]. IETF: draft-ietf-karp-ospf-analysis-02, 2011.
- [2] JAVVIN. TCP/IP network vulnerability and security [EB/OL]. [2014-05-15]. <http://www.javvin.com/networksecurity/tcpipnetwork.html>.
- [3] Jones E, Moigne O. OSPF security vulnerabilities analysis[S]. IETF: draft-ietf-rpsec-ospf-vuln-02 (work in progress), 2006.
- [4] Barbir A, Murphy S, Yang Y. Threats to routing protocols [S]. IETF: RFC 4593, 2006.
- [5] Moy J. OSPF Version 2[S]. IETF: RFC2328, 1998.
- [6] 陈海燕,季仲梅,李鸥,等. OSPF 路由协议安全性分析及其攻击检测[J]. 微计算机信息, 2005(5): 234-235.
- [7] 蔡朝权. OSPF 路由协议的攻击分析与安全防范[J]. 计算机工程与技术, 2007, 28(23): 5618-5620.
- [8] 高峰,李林涛. OSPF 协议安全性分析[J]. 黑龙江科技信息, 2011(11): 78.
- [9] Vetter B, Wang Feiyi, Wu S F. An experimental study of insider attacks for OSPF routing protocol[C] // IEEE 1997 International Conference on Network Protocols. Atlanta, Georgia, 1997.
- [10] 孔伟桐,杨家海. 基于 OSPF 的实时网络监控[J]. 微电子学与计算机, 2006, 23(9): 10-12.

作者简介:

安宁刚 男, (1977-), 硕士, 工程师. 研究方向为计算机网络管理. E-mail: annng@mail. xjtu. edu. cn.

李国栋 男, (1975-), 硕士, 高级工程师. 研究方向为计算机网络安全.

覃尊颖 女, (1984-), 硕士, 工程师. 研究方向为计算机网络管理.

李卫 男, (1968-), 博士, 副教授, 博士生导师. 研究方向为计算机网络安全、网络管理.

(上接第 51 页)

- [10] 李抒音, 姚崇怀. 基于增量式更新带权差别集合的属性约简算法[J]. 微电子学与计算机, 2008, 25(11): 68-71.
- [11] 刘清. Rough set 及 Rough 理[M]. 北京: 科学出版社, 2001: 7-16.
- [12] Zhang J, Li T, Ruan D, et al. Rough sets based matrix approaches with dynamic attribute variation in set-valued information systems[J]. International Journal

of Approximate Reasoning, 2012, 53(4): 620-635.

- [13] 景运革, 李天瑞. 一种基于关系矩阵的决策表正域约简算法[J]. 计算机科学, 2013, 40(11): 261-264.

作者简介:

景运革 男, (1970-), 博士研究生, 讲师. 研究方向粗糙集理论. E-mail: jyg701022@163. com.