·综述 ·评论 ·争鸣 ·

拒绝服务攻击防范技术研究

张娅莉[1,2*],张彬彬[3],李 淼[4]

(1.华中师范大学,湖北 武汉 430079; 2.信阳职业技术学院,河南 信阳 464000;
3.公安部第一研究所,北京 100044; 4.中国信息安全产品测评认证中心,北京 100089)

摘 要:拒绝服务攻击对网络构成了巨大的安全威胁.由于网络协议本身并不安全,所以处理拒绝服务攻击是非常困难的.从分析拒绝服务攻击的起因入手,揭示拒绝服务攻击的机制和过程,并对拒绝服务攻击进行归类,总结了防范拒绝服务攻击的措施.

关键词:拒绝服务;缓解;集中;速率限制;追踪
中图分类号: TP393.08 **文献标识码**: A **文章编号**: 1003-0972(2008)04-0626-04

Survey on Countermeasure Against Denial-of-Service Attacks

ZHANG Ya-li[1,2], ZHANG Bin-bin[3], LI Miao[4]

(1. Huazhong Normal University, Wuhan 430079, China; 2. Xinyang Vocational & Technical College, Xinyang 464000, China;
3. The First Research Institute of Ministry of Public Security, Beijing 100044, China;
4. The Information Technology Security Certification Center, Beijing 100089, China)

Abstract: Denial-of-Service (DoS) attacks present a considerable security threat to the internet. It is increasingly difficult to treat the Denial of Service attacks, because internet protocol is inherently not secure. In this paper we analyze the causes of DoS attacks, exposes their various mechanisms and proceduresand and summarize the countermeasure of keeping away DoS attacks.

Key words: denial-of-service; mitigation; aggregates; rate-limiting; trace-back

0 引言

信息安全包括机密性、完整性、可用性、不可否认性等几个方面的基本属性.拒绝服务(Denial of Service, DoS)攻击是一种破坏可用性的攻击行为,它主要通过发送过量的数据包请求,消耗网络带宽或系统资源,使网络或系统服务负载过重,导致服务质量下降,甚至瘫痪或停止. DoS攻击易于实施、难以防范,目前已经成为信息安全领域的研究热点之一.目前的网络产品及安全产品,只能解决终端用户上恶意攻击流量的部分问题,这是远远不够的.一些研究者针对伪造攻击 IP地址,提出了不保存连接信息来避免资源滥用的方法[1];而对真 IP地址,由于追溯成本非常高,可以考虑建立一种成本相对较低的手段,但这需要运营商积极发挥应有作用,而不是简单地将用户网站路由设为"黑洞路由",使恶意流量无法访问;针对攻击源头,一些研究者提出通过研究蜜网技术发现攻击者,以及分析网上广泛散播的攻击工具特征来识别特定攻击并实现有针对性的防护[2-3].

1 DoS攻击

DoS攻击是一种恶意地拒绝向合法用户提供服务的攻击方式.由于其发生的频率、攻击强度、造成的危害程度愈演愈烈,对今天的互联网已经构成了巨大的威胁. 2002年 10月, DoS攻击对全球 13个根 DNS服务器中的 8个造成了严重的影响,以后的几年内也连续发生了许多 DoS攻击事件. Moore的研究表明,全球每周可能发生 4000起 DoS攻击事件[4].

1.1 DoS的起因

回顾 Internet的演化历史,可以看出过去的努

收稿日期: 2008-06-20;**修订日期**: 2008-08-04; *.**通讯联系人**, E-mail: wwzyl6@126.com
基金项目:国家 863计划项目(2005AA142150)
作者简介:张娅莉(1977-),女,河南信阳人,讲师,硕士,主要从事应用数学研究.

力集中于 Internet协议的性能和可扩展性上,而对协议的安全性不够重视甚至完全忽略,这就导致恶意的攻击者可能利用协议本身的安全漏洞(vulnerability)进行破坏活动. DoS攻击通常会利用 Internet协议的下面这些特性:

1) 依据目的地址进行路由. Internet路由器的主要任务是转发数据包,一旦其接收到数据包,会依据数据包的目的地址进行转发,而不考虑数据包的源地址.

2) Internet的无状态性. 路由器不维护它所转发数据包的任何状态信息,从而导致计算机事件的事后调查非常困难.

3) Internet身份鉴别机制的缺失. 由于缺乏身份鉴别机制,恶意用户可以假冒(spoofing)其他用户身份从事破坏活动,而检测和定位恶意用户的难度较大.

4) Internet协议的可预测性(predictability). 这并不是一个设计缺陷,而是为了保证 Internet协议(例如,TCP建立连接过程和拥塞控制机制)的正常运作所必需的.

第 1-3特性为恶意用户假冒源地址提供了可乘之机,而源地址假冒正是 DoS攻击中使用最广泛的手段之一. 源地址假冒主要有两个目的:访问对请求的源地址有限制的资源,以及隐藏攻击的来源.

1.2 DoS攻击的过程

为了发起有效的 DoS攻击,攻击者必须首先通过招募傀儡来获得足够的资源. 一个攻击者可以招募成千上万的傀儡主机来实施 DoS攻击,其基本步骤为:

1) 攻击者扫描远程计算机,搜集安全漏洞;

2) 利用发现的安全漏洞入侵计算机;

3) 攻击者在被攻陷的计算机上安装攻击工具.

攻击者也可以利用病毒和 Trojan木马实施攻击招募. 这里,假设攻击者有能力招募足够数量的傀儡.

1.3 DoS攻击的分类

DoS攻击的存在形式多种多样,并且随着发展变得愈加精密复杂. 一般来说,DoS攻击通常具有某些共性,例如利用 Internet协议的可预测性和 Internet缺乏身份鉴别机制.

从攻击者的角度看,存在两类 DoS攻击:(1)蛮力 DoS攻击,蛮力 DoS攻击通过消耗资源来实现目标;(2)利用协议的攻击. 利用协议的攻击利用协议的可预测性显著降低网络的吞吐量.

1.3.1 蛮力 DoS攻击

蛮力 DoS攻击是指攻击者向受害者发送远超过其处理能力的流量、请求或者计算任务,使其部分或完全丧失服务能力. 攻击的对象是受害者的缓存区、带宽、CPU周期. SYN flooding和 SMURF属于这类攻击.

目前发生的 DoS攻击大多属于蛮力 DoS攻击,这类攻击往往比较有效,而且威力强大. 但是,大多数蛮力 DoS攻击很容易被检测到,所以从攻击者角度来看这种攻击类型并不完美. 于是,信息安全界普遍认为攻击者会寻求更加有效且不易被检测到的方法来实施 DoS攻击.

1.3.2 利用协议的 DoS攻击

攻击者可以利用 Internet协议的可预测性,调整攻击流量的动态特性和参数,从而显著降低网络的吞吐量. 在 TCP、802.11 MAC和 QoS中都能实施利用协议的攻击,不同的是它们有些发生在控制层面,有些发生在数据层面. 下面依据这两个层次进行分类.

许多 Internet协议缺乏对控制信息的鉴别,所以攻击者能用最小的花费攫取有价值的终端系统和网络资源. 为了提供服务质量(QoS)保证,专家们提出了资源预留协议(RSVP). 这个协议使用信令技术,在给定路径的每个路由器上,为某一特定流量预留带宽. 但是,RSVP并未提供鉴别功能,这使得它成为 DoS攻击的潜在目标. 攻击者可以通过发送伪造的预留信息来窃取网络带宽,这样便形成了控制层面上利用协议的 DoS攻击.

数据层面上利用协议的 DoS攻击则有所不同:TCP、802.11和 MAC都提供了相应机制,如拥塞控制机制,以适应网络异常情况. 如果用户遵守这些协议的自适应机制,那么网络带宽的使用将是稳定、有效的. 但是,攻击者能够利用协议的自适应机制,引起服务降级和吞吐量下降,其主要目的是在不使用蛮力 DoS攻击的条件下,使目标资源的服务能力大幅下降,同时逃避检测.

2 防御措施

根据不同的目标效果,可以将 DoS防御措施分为 3类:预防、缓解和追踪.

2.1 DoS预防

DoS预防大体可分为 2类:攻击避免(attack a-

voidance)方法——消除 DoS攻击发生的可能性;可生存性方法——通过增加受害者的资源(网络带宽、计算和存储资源)或者在网络交互之前实施强健的鉴别提高受害者的可存活性.

到目前为止,攻击避免方法一直没有受到太多的关注.这是因为人们普遍认为,唯一有效预防 DoS攻击的方法就是修补所有可被攻击者利用的漏洞,而实际上这是不可能的.但是,研究表明 DoS攻击通常是利用僵尸网络(botnet)来发起的,因此,如果能够及时发现和检测到僵尸网络,就可以在一定程度上阻止 DoS攻击的发生.我们正在尝试这种预防 DoS攻击的方法.

DoS预防方法的典型例子是 Ingress过滤,DWARD和 IP Easy-pass Ingress过滤的主要目的是过滤假冒源地址的 IP数据包,其工作原理是通过配置客户网络和 ISP网络之间的边界路由器,来过滤那些源地址的前缀与客户网络地址不匹配的数据包.DWARD主动识别和过滤进出网络的可疑流量,其工作原理是在边界路由器上监视 TCP、UDP、ICMP数据包的流入率和流出率,以及双向流量的异常行为. IP Easy-pass则采用了轻量级的鉴别方法,以防止针对 DiffServ体系架构下实时应用程序的 DoS攻击.

2.2 DoS缓解

DoS缓解是一种被动的防御措施.受害者通常会在检测到攻击后启动该措施.DoS缓解面临的主要挑战是如何准确地识别攻击数据包,以及如何在不影响合法流量的前提下过滤攻击数据包.DoS缓解主要分为 2类:基于限速的方法和基于统计的方法.

基于限速的方法是把 DoS攻击当作拥塞控制问题或者资源管理问题处理,其主要设计思想是识别攻击流量,并且对攻击流量进行限速.这种方法是被动的,不需要大范围配置,适用于任何类型的 flooding攻击,但是同时也将不可避免地影响合法流量.典型例子就是自动拥塞控制[5](ACC)和 pushback[6].ACC为核心路由器增加了新功能,它对流量的带宽集中进行速率限制,以此检测由 DDoS攻击引起的拥塞.但是 ACC并不能很好地区分合法流量和恶意流量,它在丢弃恶意流量的同时也丢弃了合法流量,这是 ACC的一个弱点.所以有必要研究识别合法流量的方法,以使合法流量得到优先的处理.邻近的 ACC路由器最好能协同工作,把本地的 ACC方法转化为分布式的方法:不能处理流量集中的拥塞路由器通过 pushback机制向邻近的 ACC路由器发布速率限制请求.

基于统计的方法假定攻击流量可能拥有一些很少见的属性.这种假设的依据是攻击者通常使用随机的假冒源地址、TTL值、ToS和其他属性.利用合法流量的最新轮廓,可以执行数据包级别的过滤.如果数据包的属性在正常的流量轮廓中很少见到,那么这些数据包将被丢弃,基于历史的过滤方法和 Packetscore[7]采用了这种策略.在遭受攻击期间,基于历史的过滤方法依据数据包与目标系统的交互历史,来决定丢弃该数据包或允许其通过. Packetscore利用数据包所携带的属性值,使用贝叶斯理论,为每个可疑数据包"评分",估计可疑数据包是攻击数据包的可能性.基于统计的方法有几个缺点:(1)攻击者在发动攻击以前可能首先破坏受害者端或边缘路由器所维护的流量轮廓.(2)攻击者可能利用各种方法产生与流量轮廓相匹配的攻击数据包.

2.3 DoS追踪

DoS追踪是确认 IP数据包真正来源的过程,它通常依靠 Internet路由器对攻击者进行定位,是应对使用假冒源地址实施 DoS攻击的一个重要方法.DoS追踪方法主要有 2类:数据包标记(packet-marking)方法和数据包日志(packet-logged)方法.

数据包标记方法的工作原理:当 IP数据包经过 Internet路由器时,路由器为数据包添加追踪信息;一旦受害者检测到攻击,就可以从攻击数据包中提取追踪信息,并且使用这些信息重建攻击数据包所经过的路径.因此,数据包标记方法通常由 2个算法组成:一个是运行在 Internet路由器上的包标记算法;另一个是受害者启动的追踪算法.

随机包标记方案[8](PPM)最先采用了包标记方法.在 PPM方案中,路由器对转发的数据包执行随机标记,一旦受害者检测到攻击,它就使用攻击数据包里的标记信息重建攻击路径或者攻击树(如果多个攻击者参与攻击).PPM存在一些问题:(1)为了重建攻击路径或攻击树,需要大量的攻击数据包;(2)在重建攻击树的过程中,可能给受害者带来巨大的开销负担;(3)如果多个攻击者参与攻击,就会产生较高的误报率.为了提升 PPM的性能和效果,研究人员围绕在大量攻击者参与攻击时追踪的可靠性和健壮性问题,提出了一些改进方案,但是仍然无法克服 PPM方案遗留下来的问题.

与在数据包里直接记录标记信息不同,Bellov-

in提出一种在 ICMP数据包里记录标记信息的方法,又称作 ICMP追踪. 在 ICMP追踪方案中,每个路由器以一定概率向目的地发送带有所转发数据包标记信息的 ICMP数据包. 这个方案的主要问题是它引入了额外的通信开销,即使在没有 DoS攻击的情况下,网络流量也会增加. 为了解决这个问题,Mankin提出了意向驱动 (intention-driven)的 ICMP追踪 (iTrace). 在这个方案中,只有在目的系统表明愿意接收标记信息后,路由器才会发送.

数据包日志方案是在路由器的内存中记录数据包的信息 (摘要、签名或者数据包本身). 一旦受害者检测到攻击就访问上游 (upstream)路由器,查询它们的内存中是否存在攻击数据包的信息[9]. 如果在某个路由器中发现攻击数据包的信息,那么就可以认为该路由器是攻击路径的一部分. 显而易见,数据包日志方案所面临的主要挑战是路由器的存储能力、个人隐私问题和查询路由器中数据包日志信息的方法.

哈希追踪[10]采用了数据包日志方法,通过使用 Bloom过滤器来存储数据包的哈希摘要,显著地降低了对路由器的存储要求. 由于摘要隐藏了数据包的内容,所以这个方法也维护了个人隐私. 但是,哈希追踪也存在一些明显的缺点: (1)路由器的处理和存储开销相对较大; (2)从路由器收集数据包日志信息的方法效率较低,并且需要增加特殊资源; (3)短时间内成功追踪数据包的难度较大.

3 结论

综合应用 DoS的三种防御措施 (预防、缓解和追踪),来建立一套全局的防御机制,能够产生更好的效果. 当然,接入互联网的主机应该及时地更新补丁,通过网络路由器实施过滤也可以消除一部分攻击数据包,但是,恶意流量的早期检测和清除要比任何追踪或是缓解机制的效果更好. 尽管研究人员在 DoS缓解和追踪领域已经做了大量的研究工作,但是现有成果还不尽如人意,研究更有效的 DoS缓解和追踪方法是十分必要的.

参考文献:

[1] 徐 恪,徐明伟,吴建平. 分布式拒绝服务攻击研究综述[J]. 小型微型计算机系统, 2004, 25(3): 337-346.

[2] 林梅琴,李志蜀,袁小铃,等. 分布式拒绝服务攻击及防范研究[J]. 计算机应用研究, 2006, 23(8): 136-138, 151.

[3] 赵 英,倪 铮,张莹莹. TCP SYN分布式拒绝服务攻击分析[J]. 微计算机信息, 2006 (8): 64-66, 235.

[4] David M, Geoffrey M V, Stefan S. *Inferring Internet Denial-of-Service Activity*[C]//Proceedings of 10th USENIX Security Symposium. Washington D C: USENIX Association, 2001: 9-22.

[5] Stefan S, David W, Anna K, et al. *Practical Network Support for IP Traceback*[C]//Proceedings of ACM SIGCOMM 2000 Conference, Stockholm. Sweden: ACM SIGCOMM Computer Communication Review, 2000: 295-306.

[6] Haining W, Kang G S. *Transport-Aware IP Routers: a Built-In Protection Mechanism to Counter DDoS Attacks*[J]. IEEE Transactions on Parallel and Distributed Systems (S1045-9219), 2003, 14(9): 873-884.

[7] Yoohwan K, Wing C L, Mooi C C, et al. *Packet Score: a Statistical-Based Overload Control against DDoS Attacks*[C]//Proceedings of IEEE INFOCOM 2004. Hong Kong: IEEE Computer and Communications Societies, 2004: 2594-2604.

[8] Ratul M, Steven M B, Sally Floyd V, et al. *Controlling High Bandwidth Aggregates in the Network*[J]. ACM SIGCOMM Computer Communication Review (S0146-4833), 2002, 32(3): 62-73.

[9] John I, Steven M B. *Pushback: Router-Based Defense against DDoS Attacks*[C]//Proceedings of ISOC Network and Distributed System Security Symposium. San Diego: NDSS, 2002: 6-8.

[10] Alex C S, Craig P, Luis A S, et al. *Hash-Based IP TraceBack*[C]// Proceedings of ACM SIGCOMM 2001 Conference. San Diego, CA: ACM SIGCOMM Computer Communication Review, 2001: 3-14.

责任编辑:任长江