IP反向追踪技术综述

冉晓旻

摘 要 拒绝服务攻击(DoS)给政府部门和商业机构造成了严重的经济损失和社会威胁。IP追踪技术能够反向追踪IP数据包到它们的源头,所以是识别和阻止DoS攻击的重要一步。本文针对DoS攻击,对比分析了各个IP反向追踪方法的基本原理和优缺点。
关键词 DoS攻击 主动追踪 反应追踪

随着Internet在商业活动中的重要性不断增长,网络攻击特别是拒绝服务(DoS)攻击也在不断增加。IP追踪技术能够使受害主机的网络管理员识别发起DoS攻击的大量数据包的真正源头,对于尽快恢复正常的网络功能、阻止再次发生攻击以及最终让攻击者为此负责非常重要。仅仅识别产生攻击业务的计算机和网络似乎是一个有限目标,但是它所提供的重要线索有助于识别实际的攻击者。本文针对DoS,对比分析了现有各个IP反向追踪技术的基本原理、优缺点和局限性。

一、DoS攻击

DoS攻击一般都默认地使用IP欺骗方式实施攻击,使网络服务器充斥大量要求回复的信息,消耗网络带宽或系统资源,导致网络或系统不胜负荷以至于瘫痪而停止为合法用户提供正常的网络服务。大部分DDoS攻击都是间接地通过其他主机系统攻击它们的目标。一旦攻击者知道无辜用户的账号,他就能伪装成那个人实施犯罪。攻击者还可以通过获得管理特权,在任何一台计算机上创建新账号。攻击者利用窃取来的账号清洗攻击数据包:被窃取账号的主机(以下称清洗主机)接收和处理攻击主机的数据包,然后再将数据包发送给受害主机。因此,攻击者就利用清洗主机伪装了它们的身份。在DDoS攻击中,为了提高攻击的成功率,攻击者会同时控制成百上千台清洗主机,每台清洗主机根据攻击命令向目标主机发送大量的DoS数据包,使目标主机瘫痪。

必须采取相应的措施来阻止或者减轻DoS/DDoS攻击,并对攻击做出反应。阻止或者减轻攻击效果的方法称为预防性措施,包括优化软件参数、输入过滤和速率限制。而要对攻击做出反应,则必须采用各种IP反向追踪技术:不仅能识别攻击主机的真正IP地址,而且还可以获得产生攻击的机构信息,例如它的名称和网络管理员的E-mail地址等。

二、IP追踪方法

根据IP追踪的主动程度,可以将现有的IP追踪技术分为两大类:主动追踪和反应追踪。主动追踪技术为了追踪IP源地址,需要在传输数据包时准备一些信息,并利用这些信息识别攻击源。主动追踪方法在数据包通过网络时记录追踪信息,受害主机可以使用产生的追踪数据重建攻击路径,并最终识别攻击者。主动追踪包括数据包记录、消息传递和数据包标记。而反应追踪却是在检测到攻击之后,才开始利用各种技术从攻击目标反向追踪到攻击的发起点。必须在攻击还在实施时完成它们,否则,一旦攻击停止,反应追踪技术就会无效。输入调试和可控涌塞属于反应追踪措施。大部分反应追踪需要很大程度的ISP合作,这样会造成大量的管理负担以及困难的法律和政策问题,因此有效的IP追踪方法应该需要最少的或者根本不需要ISP合作。

IP追踪技术的关键需求包括:

与现有网络协议的兼容;网络业务开销可以忽略;支持新增的实现;

与现有的路由器和网络结构兼容;

对付DDoS攻击的有效性;

在时间和资源方面的最小开销;

应该不需要ISP合作;追踪的成功不应该取决于攻击的持续时间。

1、链路测试

顾名思义,链路测试(有时也称为逐段追踪)法通过测试路由器之间的网络链路来确定攻击业务源头。大部分技术从最接近受害主机的路由器开始,测试它的输入(上行)链路以确定携带业务的路由器。如果检测到了有电子欺骗的数据包(通过比较数据包的源IP地址和它的路由表信息),那么它就会登录到上一级路由器,并继续监控数据包。如果仍然检测到有电子欺骗的扩散攻击,就会登录到再上一级路由器上再次检测电子欺骗的数据包。重复执行这一过程,直到到

达实际的攻击源。链路测试是反应追踪方法，要求攻击在完成追踪之前都一直存在。输入调试和受控淹没是链路测试方法的两种实现方法。

许多路由器都存在这种特性：管理员能够确定特定数据包的输入网络链路。如果路由器操作人员知道攻击业务的特定特性（称为攻击特征），那就有可能在路由器上确定输入网络链路。然后，ISP必须对连接到网络链路的上游路由器执行相同的处理过程，依次类推直到找到业务源、或者直到踪迹离开了当前ISP的界线。在后一种情况中，管理员必须联系上游ISP继续追踪过程。

这个技术的最大缺点是多个网络边界和ISP之间的通信和协作努力上的巨大管理开销，它在受害主机和ISP方面都需要时间和人力。这些问题在DDoS攻击中变得更加复杂，因为攻击业务可以来自属于许多不同ISP的计算机。表1说明了输入调试的优缺点。

表1　输入调试的优缺点

优点	缺点
与现有协议兼容	时间和人力开销
网络业务开销可以忽略	必须建立攻击路径沿途ISP的通信和协作
支持新增的实现	要成功追踪，攻击时间必须足够长
与现有的路由器和网络基础结构兼容	不太适合DDoS

受控淹没技术是从受害网络向上游网络段产生一个网络业务突发，并且观察这个故意产生的业务涌塞是如何影响攻击业务强度的。受害主机使用周围已知的Internet拓扑结构图，选择最接近自己的那个路由器的上游链路中的主机，对这个路由器的每个输入网络链路分别进行强行淹没。由于这些数据包同攻击者发起的数据包同时共享了路由器，因此增加了路由器丢包的可能性。

受控淹没的最大问题是技术本身是一类DoS攻击，这可能会破坏信任的上游路由器和网络上的有效业务。当然，这不适合Internet上的普遍常规应用。表2说明了受控淹没的优缺点。

表2　受控淹没技术的优缺点

优点	缺点
与现有协议兼容	本身是一类拒绝服务攻击
支持新增的实现	需要正确的网络拓扑图
与现有的路由器和网络基础结构兼容	要成功追踪，攻击时间必须足够长
	不太适合DDoS
	可能需要ISP合作

2、数据包记录

确定侵犯Internet业务的真正起源的显而易见的方法是在通过Internet的关键路由器上记录数据包，然后使用数据钻取技术提取有关攻击业务源的信息。尽管这个解决方法似乎很显然，并且可以对攻击业务做出准确分析（即使在攻击已经停止之后），但是它的最大缺点是保存记录所需要的大量处理和存储能力，且保存和在ISP之间共享这个信息的需求还存在法律及保密问题。

Alex Snoeren等提出了一个新的数据包记录和IP追踪方法，称为SPIE(Source Path Isolation Engine)。他们不是存储整个数据包，而是只在称为Bloom Filter的有效存储结构中存储它的相应固定部分的Hash摘要。为了完成IP追踪请求，数据搜集网络和遍布不同网络的分析代理可以使用这个方法提取重要的数据包数据，并且产生合适的攻击图，从而识别攻击业务的源头。

当前基于数据包记录的追踪方法使用滑动时间窗来存储记录的数据，从而避免了在攻击正在进行时或者攻击发生后不久捕获攻击时需要过多的存储和分析需求（因此，所需的记录数据仍然可以使用）。表3说明了数据包记录的优缺点。

表3　数据包记录法的优缺点

优点	缺点
与现有协议兼容	在处理和存储需求方面是资源密集性的
支持新增的实现	在多个ISP之间共享记录信息存在法律和保密问题
与现有的路由器和网络基础结构兼容	不太适合DDoS
允许在攻击之后分析	
网络业务开销可以忽略	
可以追踪单个数据包	

3、消息传递

2000年7月，Internet工程任务组(IETF)成立了一个工作组来开发基于iTrace方法的ICMP追踪消息。这个方法利用加载了跟踪机制的路由器（称为iTrace路由器）以很低的概率发送一种特殊定义的ICMP数据包。

这个数据包包含局部路径信息：发送它的路由器的IP地址、前一跳和后一跳路由器的IP地址以及它的身份验证信息。

可以通过查找相应的ICMP追踪消息，并检查它的源IP地址，来识别经过的路由器。但是，由于为每个分组创建一个ICMP追踪消息增加了网络业务，所以每个路由器以1/20,000的概率为要经过它传输的分组创建ICMP追踪消息。如果攻击者发送了许多分组（例如，在扩散类型的攻击中），那么目标网络就可以收集足够的ICMP追踪消息来识别它的攻击路径。该算法的缺陷在于产生ICMP追踪消息数据包的概率不能太高，否则带宽耗用太高，所以该算法在攻击数据包数量很多时才比较有效。

iTrace机制的缺点在DDoS攻击中变得更加明显。在这类

情况下,选择攻击数据包的可能性比使用的抽样速率小得多。受害主机可能会从最近的路由器获得许多ICMP追踪消息,但是很少是由接近僵尸主机的路由器产生的。

为了克服这个缺点,研究人员对iTrace提出了一种改进方法,称为Intension驱动的ICMP追踪。这个技术分开了判决模块和iTrace产生模块之间的消息传递功能。接收网络为路由表提供了特定的信息以指出它需要ICMP追踪消息。在路由表中提供的特定信息的基础上,判决模块将选择接着使用哪类数据包来产生iTrace消息。然后,iTrace产生模块处理这个选中数据包,并且发送一个新的iTrace消息。

Intention驱动的追踪还允许无论接收网络是否想接收iTrace数据包,都可以发信号,这就增加了对接收网络有用的消息比例。如果特定网络怀疑或者检测到它正遭到攻击,那么这种方法也很有用:它可以向上游路由器请求iTrace数据包,以识别攻击业务的源头。表4列出了消息传递方法的优缺点。

表4 消息传递技术的优缺点

优点	缺点
与现有协议兼容	即使对追踪消息使用非常低的概率,也产生了额外的网络业务
支持新增的实现	除非还有实现了密钥分配的加密机制,否则攻击者可以在数据包流中插入假的ICMP追踪消息,以
	掩饰攻击业务的真正来源
与现有的路由器和网络基础结构兼容	由于会在多个常见攻击情况中使用ICMP业务,所以公司会越来越多地过滤ICMP业务
如果用加密和密钥分配机制实现,为对付拒绝服务攻击提供了一个非常有前景和可扩展的技术	在DDoS机制中,只有非常少的ICMP追踪消息来自远端路由器(但是会通过intension驱动的ICMP追踪解决这个问题)
不需要ISP合作 允许在攻击之后分析	攻击路径重建需要较长的时间,例如30分钟

4、数据包标记

数据包标记方法是在被追踪的IP数据包中插入追踪数据,从而在到目标主机的网络上的各个路由器上标记数据包。数据包标记的最简单的实现是使用记录路由选项(在RFC 791中指定的)在IP头的选项字段中存储路由器地址。但是,这个方法增加了每个路由器处的数据包长度,并且可能导致额外的分段。而且,攻击者可能试图用假数据来填充为路由保留的字段,从而逃避追踪。

Stefan Savage等人在2001年提出了利用随机业务抽样和压缩的数据包标记算法。依赖随机数据包标记(PPM)的追踪机制使用概率为1/25的随机抽样,从而避免了路由器数据包标记的过多开销。此外,每个数据包只存储它的路由信息的一部分,而不是整条路径的信息。而且如果攻击数据包足够多,就可以保证受害主机重构攻击路径上的每一个路由器。

压缩的边缘分段抽样技术(CEFS)已经成为最著名的IP追踪机制之一。要执行一次成功的追踪,受害者必须搜集足够的数据包来重建攻击路径的每个边缘和完整的攻击图。但是这在DDoS攻击中非常困难,因为正确地将分段和编码的路径边缘组织在一起很困难。

Dawn Song和Adrian Perrig对Savages的基于边缘识别PPM的方法提出了改进,通过存储每个IP地址的Hash值(而不是地址本身)进一步减少了存储需求。这种方法假设受害主机拥有所有上游路由器的完整网络图。在重新组装边缘分段之后,该方法将产生的IP地址Hash值与从网络图得到的路由器IP地址Hash值相比较(以便于重建攻击路径)。这个改进方法比以前的方法对于DDoS攻击更加有效。

表5列出了数据包标记的优缺点。

表5 数据包标记的优缺点

优点	缺点
使用逐渐增多,并且是低成本的	需要改进协议
适用于现有的路由器和网络基础结构	产生假阳性路径(不是路径攻击的一部分)
对DDoS很有效	不能处理分段
不需要ISP合作 允许在攻击之后分析	不能用于IPv6,并且与IPSec不兼容

三、应用前景

随着Internet的发展,越来越多的服务都是通过网络为大众提供的,但是与此同时,针对互联网服务的攻击手段也越来越多。目前提出的所有IP追踪机制都有它们自己特定的优点和缺点。没有一种解决方案可以实现有效追踪方法所规定的所有需求。要使其中任何一个IP追踪方案有效,必须在大部分Internet基础结构中的公司和行政边界都使用它们。这本身似乎就是统一IP追踪方法的最大障碍之一。而且,一些方法对于DDoS攻击不太有效、是资源密集的、会引起网络开销,或者不能在攻击之后进行分析。因此,除非在整个Internet上使用IP追踪方法,否则它们只对受控网络而不是整个Internet有效。

而且,即使使用这种追踪系统,也还需要人类的干预。特别是,人们必须解决追踪的管理屏障,并且提供自动处理无法获取的信息,例如工作记录、电话记录等。要求系统管理员保持日志、记录以及追踪系统工作所需要的其他信息;要求行业内部、服务提供商、网络管理员、网络用户和法律执行部门的有效协作。(作者单位 解放军信息工程大学信息工程学院)