一种基于回溯的Web上应用层DDOS检测防范机制

王 睿
(中山大学信息科学与技术学院 广州 510006)

摘 要 分布式拒绝服务攻击(Distributed Denial of Service)是一种攻击者使用各种方法,试图将攻击目标的网络资源和系统资源消耗殆尽,使之无法向真正的合法用户提供服务的攻击。随着技术的进一步发展,基于网络层上的DDOS攻击得到了很大程度上的削弱。然而,越来越多的攻击出现在了应用层,攻击的形式更加多样和复杂。从下层协议的角度来看,攻击中涉及的流量可能是合法的,使得检测和防范工作愈发困难。文中以实例为基础,解释基于应用层的攻击原理和方法,结合现有的技术,总结出检测和防范的机制并进行改进。

关键词 分布式拒绝服务攻击,攻击检测,攻击防范,网络安全
中图法分类号 TP393 **文献标识码** A

Mechanism of Detecting and Preventing Application Layer DDOS Attack Based on Traceback

WANG Rui
(School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510006, China)

Abstract Distributed Denial of Service is an attempt to make a machine or network resource unavailable to its intended users. With the further development of technology, DDOS attacks on the network layer have been largely weakened. However, more and more attacks occur in the application layer with various and more complicated forms. Attack traffic may be legitimate from the view of the lower layer protocol, which makes the detection and prevention more difficult. This article explained the discipline and measures of application DDOS attack by instances, summarizes and improves the mechanism of detection and prevention with present technology.

Keywords DDOS, Attack detection, Attack prevention, Network security

当今社会,信息技术在经济、军事、文化的发展中扮演着重要的作用。通过网络,人们可以获取、共享信息,自由地交流。然而,在网络中的许多安全问题也随之而来,出现了多种类型的攻击,造成了严重经济损失。其中一个危害很大的攻击就是DDOS。它可以在没有任何征兆的情况下,消耗掉攻击目标的资源。DDOS攻击的目标是降低服务器性能,直至瘫痪,导致合法的用户无法访问网络服务。如今的DDOS攻击已经从网络层逐渐发展到了应用层。由于高层协议的多样性和复杂性,应用层的DDOS攻击很难被检测到,而且高层协议通常具有较强的功能,可以实现多种复杂的功能,因此应用层的DDOS攻击的破坏性更加巨大。下面将首先讨论应用层攻击的原理和一些具体的实现方法,接着讨论基于DDOS攻击的一些相关的检测防范机制,最后讨论结合多种技术的新型检测防范机制。

1 Web应用层DDOS攻击

1.1 攻击原理

应用层的DDOS攻击不仅仅是基于泛洪,还可以通过发送很少量的数据包就使得服务器系统资源大量被占用。具体可以分为3种[1]:

(1)请求泛洪攻击。在一次应用层会话中向目标主机和网络发送大量超过正常数量的请求。

(2)不对称攻击。向目标主机发送一个能引发攻击目标巨大工作负载的请求。例如,攻击者发送针对数据的大量处理的操作,使得攻击目标消耗掉大量的自身资源。

(3)重复的单次攻击。在一次会话中只发送一个请求,但是却以高于正常情况的速率建立多个会话。

1.2 攻击实例

下面以Web服务器为例,介绍和分析4种应用层的DDOS攻击。

(1)Slowloris:每个HTTP请求都是以空行结尾,即以两个(\r\n)结尾。若将空行去掉,即以一个(\r\n)结尾,则服务器会一直等待直到超时。在等待过程中占用线程,服务器线程数量达到极限,则无法处理新的合法的HTTP请求,达到DOS目的。

(2)HTTP POST DOS:攻击者向服务器发送POST请求,告诉服务器它将要POST的数据为n,服务器将分配长度为n的空间来等待接收数据。当n足够大,POST的请求足够多的时候,这种攻击会占用服务器的大量内存,从而降低服务器性能,甚至导致瘫痪。

(3)HTTP RANGE DOS:属于不对称攻击。只需要发送一个数据包就可以消耗服务器大量内存(针对Apache服务器)。在HTTP请求的RANGE HEADER中包含大量字段,使得服务器在服务端将一个很小的文件分割成大量的更小的片段再压缩。分段压缩过程消耗大量的服务器资源,导致DOS。

王 睿(1993—),男,主要研究方向为网络与信息安全、逆向工程。

(4)HTTP Slow Read DOS:向 Web 服务器发送正常合法的 read 请求,将 TCP 滑动窗口 size 设置很小如 1 或 2,服务器就会以非常缓慢的速度发送文件,文件将长期滞留在服务器内存中,消耗资源,造成 DOS。

1.3 攻击特点

DDOS 攻击一般具有以下特点:

(1)若是基于泛洪的攻击,则 DDOS 攻击的会话请求频率高,时间间隔短,并且数据量大。

(2)若是基于不对称的攻击,以很少的数据包来实施攻击,则种类繁多,但是共同点是利用高层协议的漏洞进行攻击,使得服务器的资源被耗尽。

此外,与下层(网络层、传输层)DDOS 攻击相比,应用层的 DDOS 攻击具有以下特点:

(3)以高层协议实现,但是以正常的 TCP 连接和 IP 分组为前提,因此不具备传统 DDOS 攻击的特征(Smurf、ICMP flooding、TCP flooding、UDP flooding)。

(4)由于高层的协议和服务差异很大,应用层攻击的形式有很多,而且一个简单的数据包就可能造成服务器一系列的复杂操作。

2 相关检测防范机制

2.1 检测回溯机制

这是 Khamruddin 提出的一种基于 Smurf、ICMP flooding、TCP flooding、UDP flooding 攻击的检测防范机制[2]。我们同样可以将其应用到应用层。

这种方法依然使用传统的攻击检测方法。首先在最靠近受攻击服务器的路由器上持续地检测数据包,分析数据包的头部,获取源/目的地址、源/目的端口号、传输层协议。并且定义流速率(Flow rate = ReceivedBytes/s)和数据包数量(Packet Count=总共收到的数据包的数量)的阈值。当服务器受到攻击时(流速率和数据包数量超过阈值),首先使用 NAT 进行负载匀衡,确保网络服务的可用,接着从最接近受攻击服务器的路由器开始,向上游路由器发送攻击特征信息并同时减少攻击流量,上流路由器同时也向上游路由器发送攻击特征信息减少攻击流量。最终整个网络中的攻击流量都会减少,减轻了整个网络的带宽负担。在之后会详细介绍如何将这种回溯的方法运用到应用层。

2.2 Puzzle

这是 Kandula 等提出的基于"Puzzle"的检测和防御方法[3]。当服务器的网络资源或系统资源消耗超过预设的阈值时,可以怀疑是否受到攻击。由于攻击由程序生成,不具有人的智能性,因此可以产生一些简单的问题来检验连接是否是攻击源,若返回不正确则可以确定攻击源。这种方法的好处是,可以很简便且有效地分辨出攻击源和正常用户。但是,这种方法最大的问题就是会影响合法用户的体验,对用户正常访问造成干扰。同时,生成问题、等待回答以及验证问题答案仍然会消耗自身的资源。

2.3 基于访问行为的检测防御

Web 挖掘的研究指出:通过对 Web 用户的访问页面进行内容监控和分析,可以挖掘出用户的兴趣,而且其他一些研究也指出一个 Web 网站仅有 10%的内容被客户高频访问,而且文件被访问的概率呈 Zipf 分布。这说明尽管访问者各不相同,但是在一定的时期内他们对给定的 Web 服务器的访问兴趣和访问行为是非常近似的。所以高层的 Web 用户访问行为特征可以作为应用层 DDOS 攻击检测的有效信号。检测方法如图 1 所示。

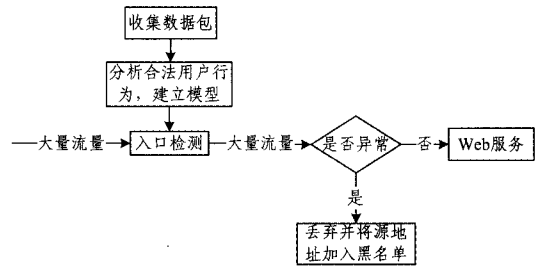

图 1 基于访问行为的检测流程

基于用户访问行为的检测防御方法有很多,文献[4]使用隐半马尔可夫模型,首先对正常用户的行为进行建模,再根据收集到的数据包判断流量是否为攻击流量。文献[5]提出了 ANRC 检测方法,通过建立监控列表动态增加、删除列表中的保护对象,根据用户访问的目的服务器是否在监控列表中进行过滤,然后实时统计单位时间内请求次数和 IP 个数,计算 ANRC 值判断是否受到攻击。文献[6]结合 Agent 和信息熵算法提出新的模型进行 DDOS 攻击检测。

3 检测防范机制的结合

3.1 攻击检测

Web 上的应用层的攻击检测不能单纯地通过分析 IP 分组和 TCP 连接来判断,而应用层的负载信息也是需要考虑的重要特征。当然,孤立地分析每一个 HTTP 请求也无法完全检测应用层攻击。2.3 节介绍的基于访问行为的检测防御方法是非常有效的。

这种检测方法的简化过程如下。首先,利用大量用户的历史访问记录建立正常用户行为模型。接着,对比用户访问行为和预先建立的模型,得出偏离值。偏离值较低的优先得到响应,偏离值超过阈值的丢弃。尽管攻击者可以模仿浏览器发送 HTTP 请求,并通过仿真工具重新整合攻击流的流特性,使其接近客户的流特性,但是它始终无法实时、动态地跟踪和模仿正常用户的访问行为,因为只有 Web 服务器记录了所有访问者的访问记录,而这些分析结果是攻击者无法获取的。本文将以该检测方法为基础进行讨论。

3.2 回溯攻击特征信息

因为应用层攻击是建立在正常的 TCP 连接上的,若在异常检测处查出异常流量,只是丢弃并且过滤是不够的,傀儡机器会不停地向服务器发送 TCP 连接请求,依然消耗服务器资源,而且和受攻击服务器相近的网络中,都充斥着攻击的流量,大大占用了网络带宽,造成网络拥塞。因此,在整个流量流经的网络中,屏蔽攻击的 IP 分组和 TCP 连接可以很好地解决这个问题。具体方法如下:

定义攻击特征信息。可以仿照 Khamruddin 的方法,将攻击特征信息描述如表 1 所列。

表 1 攻击特征信息

攻击特征信息
1. 源 IP 地址列表
2. 源端口号
3. 传输层协议
4. 流速率
5. 数据包数量
6. 攻击类型

其中，源 IP 地址列表是指在异常检测过程中，收集的攻击源的 IP 地址。与之前不同的为第 6 项攻击类型，这里特征信息里的攻击类型不仅仅是网络层和传输层的攻击，具体的攻击类型可以参照第 2 节，而攻击类型的判断依赖于基于正常用户行为的异常检测。

攻击特征信息是为了在下层让路由器识别攻击流量进行屏蔽并回溯，从而达到降低整个网络拥塞的目的。当异常检测得出攻击特征信息以后，从距离受攻击服务器最近的路由器开始发送攻击特征信息。路由器收到攻击特征信息之后，屏蔽源 IP 地址列表中的流量，同时向上游（攻击流量来的方向）路由器发送攻击特征信息，以此类推。接下来，在整个网络中的攻击流量都被屏蔽，大大降低了网络拥塞，同时保证了服务器的性能，避免了拒绝服务。

3.3 一种改进的应用层 DDOS 防范机制

DDOS 攻击是利用攻陷的电脑作为“丧尸”组建僵尸网络，向服务器发起密集式的 DOS 攻击。而异常检测得出的攻击源 IP 地址列表被加入黑名单之后，来自该地址列表内的任何流量都被屏蔽，即使是正常的流量。当“丧尸”没有被操纵，正常的用户想要访问网络服务的时候却被屏蔽。

为了解决这个问题，要区分恶意攻击源和被攻陷的“丧尸”，并且还要恢复部分被攻陷主机访问网络服务器的权限。对源 IP 地址定义以下参数 SourceType、AttackCount、Threshold、Timer，其含义如下：

1）ST(SourceType)：表示此 IP 地址的主机类型。分为恶意攻击源 A(attacker)和被攻陷主机 B(bot)两种。

2）AC(AttackCount)：表示此源地址对服务器攻击的次数。

3）T(Threshold)：表示被攻陷主机攻击次数的最大值。

4）Timer：恢复访问计时器，源 IP 地址每被拉黑一次，计时器开始计时，记录距离恢复访问权限还有多久。随着 AttackCount 的增加，恢复访问时间呈指数倍增加。

改进后机制对攻击流量的处理过程：

攻击流量中，对于每个源地址的 SourceType 初始为 bot，AttackCount 初始为 1。Threshold 为设定的常量。Timer 的值与 AttackCount 正相关。

源地址每被加入黑名单一次，AttackCount 增加 1，恢复权限时间 Timer 随之增加。同时向源地址返回消息，提醒用户自己的机器被攻陷。

当 AttackCount 大于设定的 Threshold 时，将 SourceType 改为 attack，将 Timer 设为－1，表示永久屏蔽。

改进后机制对攻击流量的处理过程如图 2 所示。

改进后机制可较好地解决以下问题：

（1）在入口检测处一旦检测到攻击流量，则立即将其源地址加入黑名单，防止了服务器受到持续的攻击，有效缓解了 DOS。

（2）根据来自源 IP 的攻击次数来判断源 IP 是否为恶意攻击者，在拉黑的同时向源 IP 发出提醒，并且使用恢复服务 Timer 来进行流量控制，Timer 计时结束则将源 IP 从黑名单除去，恢复流量通过。该种做法，首先为被攻陷的机器恢复服务访问提供途径，并且提醒源 IP，让其摆脱控制。

（3）当攻击次数超过阈值的时候，则将源 IP 判断为恶意攻击者，永久加入黑名单，这样便杜绝了攻击者的再次攻击。

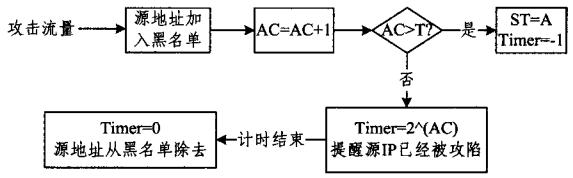

图 2 改进后机制对攻击流量的处理过程

3.4 讨论

本文给出的基于回溯的检测防范机制有两大核心功能。

首先是在整个网络中对攻击流量的特征进行回溯，并屏蔽攻击流量，缓解了网络资源消耗。该方法的优点是，可以在整个网络内减少攻击流量造成的带宽占用。

其次是通过攻击次数来判断源 IP 是否为恶意攻击者，同时提醒源 IP 已被攻陷，并且用 Timer 机制来恢复正常用户的网络访问。该方法的优点是，既兼顾了正常用户对网络服务的访问，又削弱了攻击者对傀儡机的控制。

结束语 针对 Web 上的应用层 DDOS 攻击的原理和种类进行了详细的介绍，分析了一些 DDOS 的检测和防范机制，并且结合现有的技术，设计了一种新的机制。新的机制旨在通过异常检测判断攻击流量，并且通过回溯屏蔽整个网络中的攻击流量，降低网络拥塞。改进之后的新机制还从客户端考虑，为用户脱离控制、恢复网络服务访问权限提供了途径。

参 考 文 献

[1] 肖军，张永铮，云晓春. 一种应用层分布式拒绝服务攻击过滤方法及系统[P]. 中国，2011-05-25

[2] Khamruddin M D, Rupa C. A Rule Based DDoS Detection and Mitigation[C]// Nirma University International Onfer Ence on Engineering, 2012. India, 2012

[3] Kandula S, Katabi D, Jacob M, et al. Surviving Organized DDoS Attacks that Mimic Flash Crowds[C]// NSDI'05 Proceedings of the 2nd conference on Symposium on Networked Systems Design & Implementation. CA, USA: USENIX, Association Berkeley, 2005

[4] 谢逸，余顺争. 基于 Web 用户浏览行为的统计异常检测[J]. 软件学报，2007，18(4)：967-977

[5] 赵国锋，喻守成，文晟. 基于用户行为分析的应用层 DDOS 攻击检测方法[J]. 计算机应用研究，2011，28(2)：717-719

[6] 唐鹏，张自力. 基于信息熵的多 Agent DDOS 攻击检测[J]. 计算机科学，2008，35(3)：292-295

（上接第 152 页）

[8] 黄梅珍，林斌，唐九耀，等. 不同阳极结构二维 PSD 的电流-位置输出特性[J]. 光电子·激光，2001，12(8)：795-798

[9] 黄传华，万晓明，吴魁. 一种区域降水量网格算法[J]. 人民长江，2007，38(2)：49-50

[10] 夏吉庄. 双调和样条内插方法在测井和地震资料整合中的应用[J]. 石油与天然气地质，2010，31(2)：244-249

[11] 李元金，罗立民，张鹏程，等. 基于校正靶特征与 Biharmonic 样条插值的 XRII 图像扭曲校正[J]. 东南大学学报，2011，41(6)：1213-1218

[12] 董桦. 基于 PSD 的激光位移检测中位移信号处理系统的研究[D]. 长春：长春理工大学，2010