一种可抗 TCP Flooding 攻击的网络流量监测机制①

宋春玉, 廉龙颖, 王艳涛, 高殿武

(黑龙江科技学院 计算机与信息工程学院, 哈尔滨 150027)

摘 要: DDoS 攻击是互联网的主要安全威胁之一, 而大部分 DDoS 攻击工具都使用 TCP Flooding 攻击方式, 基于大量研究相关技术的基础上, 提出了一种可用于局域网的网络流量监测机制, 可以有效的检测出 TCP Flooding 攻击, 解决当前各种网络安全设备在此方面存在的问题.

关键词: TCP Flooding; DDoS; 流量监测

Network Monitoring Machine Against TCP Flooding Attacks

SONG Chun-Yu, LIAN Long-Ying, WANG Yan-Tao, GAO Dian-Wu

(College of Computer and Information Engineering, Heilongjiang Institute of Science and Technology, Harbin 150027, China)

Abstract: DDoS attacks are a major threat to internet and almost all of DDoS attacker use TCP Flooding attacks. Based on lots of studying, a network monitoring machine is presented. The machine can detect TCP Flooding attacks for local area network and solve problems of other security production.

Key words: TCP Flooding; DDoS; flow monitoring

在当前互联网的各类安全威胁中, 分布式拒绝服务攻击(Distributed Denial-of-Service, DDoS)的危害尤为显著. 它本质上是一种以阻止合法用户正常访问目标服务为目的的网络攻击, 具体实现上有两种攻击方式. 一种是利用目标系统的软件脆弱性, 向目标主机发送畸形报文致使系统崩溃或死锁. 另一种是向目标持续发送大量无用报文, 占用目标的网络带宽和主机资源, 使之降低或丧失向合法用户提供服务的能力.

目前市场上存在的网络安全产品在面对第一种方式的 DDos 攻击时均能有效的检测出来, 但是对于第二种形式的攻击, 抵御起来要困难得多. 因为这类报文内容是合法的, 并不携带任何恶意代码, 很难使用特征码匹配的方式进行检测, 并且 TCP Flooding 攻击流量与突发性的大规模正常流量十分相似, 难以区分, 因此对检测系统的灵敏性要求很高.

针对以上现状, 本文提出了一种网络流量监测机制, 可以布置在局域网的关键点处, 当发生针对内网的 TCP Flooding 攻击时, 能有效的检测出来, 基本不会存在漏报的情况, 误报率也很低.

1 TCP Flooding攻击原理分析

TCP 是一种面向连接的、可靠的、基于字节流的传输层通信协议, 它是许多重要应用层服务(如 Web 服务、FTP 服务等)的基础. TCP 报文头包含 6 个标识位, 分别是 URG、ACK、PSH、RST、SYN、FIN. 通信双方通过将报文的不同标识置位来实现语义的相互传递. TCP Flooding 攻击就是利用协议的脆弱性, 通过向目标服务器发送大量带特定 TCP 标识的连接请求, 消耗服务器的系统资源, 从而降低其服务提供能力.

TCP 建立连接需要三次数据的传输, 首先客户端向服务器发送一个 SYN 标识置位的数据包, 服务器在堆栈中为该请求分配一个传输控制块保存相关信息, 同时向客户端返回一个 SYN 和 ACK 都置位的数据包, 客户端再返回 ACK 置位的数据包, 这样双方才建立起连接, 接着可以收发数据了. 数据传输完毕后, 服务器收到对方发来的 FIN 或者 RST 置位的数据包时才会释放分配出去的系统资源. 由此可知, 当服务器端收到对方发来的第一个 SYN 包时, 就要为对方分配系统资源了, 如果一直未收到对方的 ACK 包, 那么只能等

① 基金项目:黑龙江省教育厅科学技术研究项目(12523053)
收稿时间:2012-11-13;收到修改稿时间:2012-12-12

到时钟超时才能释放资源. 如果攻击者向服务器发送大量的SYN请求, 同时将请求报文的源IP地址设置成虚假的, 使得服务器收不到 ACK 回应报文, 这样服务器的堆栈空间会很快被耗尽, 而合法的连接请求无法被响应. 如图 1 所示.

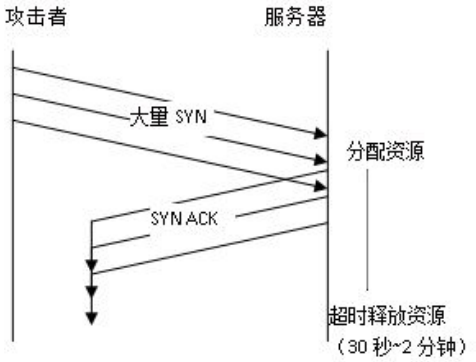

图 1 TCP Flooding 攻击示例图

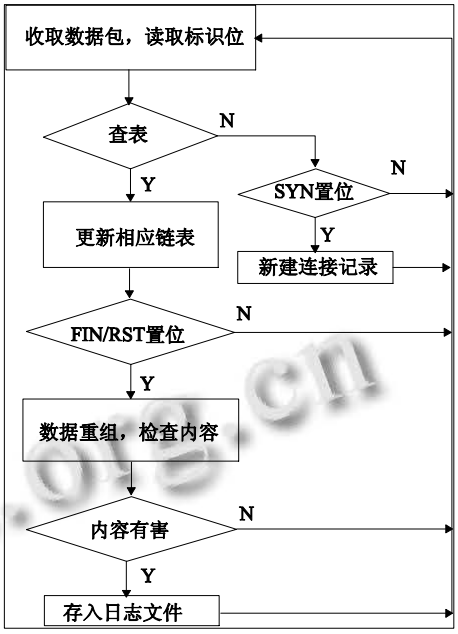

图 2 基于 TCP 的流量监测系统流程图

2 基于TCP的流量监测机制

因特网中 90%的数据流都是基于 TCP 的数据流, 90%以上的 DDoS 攻击也都是针对 TCP 设计实施的, 因此基于TCP的流量监测机制是各种网络安全设备必不可少的组成部分. 这方面的技术[1-3]已经出现了很多, 但是没有一种是适合于所有场合的, 都各自有自己的侧重点. 下面提出的一种基于 TCP 的流量监测机制是适合于局域网的能够进行流量内容监测并且能抗 TCP Flooding 攻击的技术.

要监测网络流量内容首先必须要建立连接数据表以便暂存流经的网络数据. 在计算机网络中唯一标识一条通信连接的是套接字, 即收发双方的 IP 地址和端口号. 那么当监测系统收到一个 SYN 置位的数据包时就在表中新建一条连接记录, 记录 ID 就使用套接字, 当这条连接的后续数据包到达时根据套接字查表, 将数据包缓存到相应的链表中, 当收到 FIN 或者 RST 置位的数据包时, 查表进行数据重组, 根据事先定义好的规则进行内容监测, 然后删除这条记录, 并根据检测结果决定是否将该条记录存入日志文件中.

为了使布置的监测系统能够及时处理局域网主干网上的大量数据流, 必须尽量减少查表时间, 因此引入了校验和算法来计算流入流出数据包的套接字, 把计算结果作为每条连接记录ID存入数据表中, 具体的处理流程如图 2 所示:

系统中所用的校验和算法就是 IP 协议和 TCP 协议中使用的检错算法, 很多的内容监测系统中都使用某种哈希函数[4]来提高网络流量处理效率, 本文提出的这种成熟的校验和算法也可归类为一种哈希函数. IP地址32位, 端口号16位, 那么标识一条通信连接的套接字共 96 位, 可分成 6 组输入哈希函数, 最后得到 16 位的值, 将这 16 位的值作为连接记录 ID 存入数据表中, 当收到数据包后, 取出套接字计算校验和然后查表.

为了更好的提高查表效率, 考虑到数据流局部性原理, 即在网络数据流中一个从主机 A 到主机 B 的数据包, 往往紧随另一个从主机 A 到主机 B 或主机 B 到主机 A 的数据包, 网络中的相邻数据包很可能高度相关. 也就是说, 连续收到的数据包是属于同一条通信连接的. 这样如果数据表中的某个连接记录被访问, 那么该记录可能很快再次被访问. 为了减少平均查找开销, 系统中使用的链表是自适应查找链. 自适应查找链是一种特殊的查找链. 当链中某个记录被访问后, 自适应查找链按照某种置换方法改变链中记录的顺序, 尽量使最近频繁访问的记录移动到靠近链头的位置, 以减少后续的查找时间.

3 TCP Flooding攻击检测算法

前面所述的流量监测机制能够有效检测网络流量

内容, 如何使这个监测系统也能检测出 TCP Flooding 攻击是下文中将要阐述的. 根据 TCP Flooding 攻击原理的分析, 可以归纳出 TCP Flooding 的行为特征来, 即不能建立起完整的 TCP 连接, 通常称为半连接或者脏连接. 当攻击者向局域网发起 TCP Flooding 攻击时, 那么监测系统会在单位时间内收到大量的这种半连接数据包. 如何检测出这些数据包并且把这些数据包收集下来进行进一步分析, 是下面要阐述的内容.

为了能够把半连接的数据包从正常用户的数据流中提取出来, 要把上节描述的监测系统进行一下改进. 除了原来的连接数据表外要增加一个初始数据表和一个预警数据表, 每当收到一个 SYN 数据包时, 先将其存入初始数据表中, 当收到这条通信连接的第三个连接 ACK 数据包时, 将这条记录移至连接数据表. 给初始数据表的每个表项设定一个时钟, 每隔一段时间扫描一次初始数据表, 将时钟到期的记录移至预警数据表, 当单位时间内预警数据表内表项数超过一定上限时报警. 算法的基本思想如图 3 所示.

接收：网络数据包
1. **读取标识位，计算套接字校验和，查找初始数据表**
2. **如果 SYN 置位**
    1. **如果未找到，新建一条连接记录存入初始数据表**
    2. **插入链表**
3. **如果 ACK 置位**
    1. **如果找到，插入链表并将这条记录移至连接数据表**
    2. **查找连接数据表**
4. **定期扫描初始数据表，将时钟到期的记录移至预警数据表**
5. **定期扫描预警数据表，当表项数超过上限时报警。**

图 3 TCP Flooding 攻击检测算法

这种算法实现简单, 在原流量监测系统的基础上, 只增加了 2 张数据表和一组时钟就可方便的检测出无论是来自外网还是内网的 TCP Flooding 攻击. 为了验证本监测机制的有效性, 在实验室内进行了模拟攻击检测测试, 结果表明本流量监测机制针对 TCP Flooding 攻击的漏报率为零, 误报率为 2.3%.

4 总结

在当前的各种互联网技术中, 网络安全已经成为主要研究热点之一, 各种网络安全设备如防火墙、IDS、网络安全态势感知系统、网络流量监测系统等层出不穷, 但是由于整个因特网各服务供应商使用技术上的异构性和管理上的开放性, 使得不可能存在一个适用于各种场合兼容所有其他安全设备的标准系统. 本文提出的是一种适用于局域网的可以检测出 TCP Flooding 攻击的流量监测机制, 原理简单, 实现容易, 满足保护内网的基本要求. 这种机制是在充分的分析了网络协议通信原理和 TCP Flooding 攻击原理的基础上提出的, 具有一定的理论和工程上的创新度.

参考文献

1 Sallay H, AIShalfan KA, Fred OB. A Scalable Distributed IDS Architecture for High Speed Networks.International Joumal of Computer Science and Network Security, 2009, 9(8): 9–16.

2 Gemona I, Miller DA. NEMESI:Using a TCP Finite State Machine against TCP SYN Flooding Attacks. University of St Andrews, 2006.

3 Li MH, Li M. An Adaptive Approach for Defending against DDoS Attacks. Mathematical problems in Engineering, 2010: l–12.

4 程光,龚俭,丁伟,等.面向 IP 流测量的哈希算法研究.软件学报,2005,16(5):652–658.