一种针对 SYN-Flooding 攻击的防范方法*)

黄 勤 廖 伟 刘益良 李 楠 杨 洁
(重庆大学自动化学院 重庆 400044)

摘 要 针对 SYN-Flooding 攻击的特点,分析了几种防御 SYN-Flooding 攻击的方法,本文提出了一种 TCP/IP"一次握手"协议防御方法,即服务器对客户端的传输连接响应通过代理服务器判断,按照前向神经网络的时间统计概率 PE 值后排序提交,解决了分布式拒绝服务攻击,特别是系列攻击和重复攻击对资源过量占用引起系统瘫痪的问题。攻击防御实验表明,本文方法防御 SYN-Flooding 攻击有明显效果。

关键词 SYN-Flooding,防范对策,握手协议

Study on Defense against a SYN-Flooding Attack

HUANG Qin LIAO Wei LIU Yi-Liang LI Nan YANG Jie
(School of Automation, Chongqing University, Chongqing 400044)

Abstract The existing mehods of defense against SYN-Flooding attack have been analyzed. And then, a new method called TCP/IP-"Shake hands once" to prevent the SYN-Flooding attack, in which the system crashes because of the source exhausted, is pointed out in this article. The response of the server on the clients for transfer is made by the attorney, and the service of the server to the clients will be arranged according to the PE. The result of the experiments shows that the method is more effective than others.

Keywords SYN-Flooding, Defense against, Agreement of shake hands

1 引言

计算机和网络安全事件日益频繁地发生着,网络攻击的破坏性越来越大,攻击方式也越来越多。分布式拒绝服务(DDoS)攻击是在传统的 DoS 攻击基础之上产生的一类攻击方式。DDoS 可在很短时间内造成被攻击主机的瘫痪,其攻击的单机信息模式与正常通信无差异,故在攻击发动的初期不易被确认。当计算机遭受攻击时,具有下列攻击现象:被攻击主机上有大量等待的 TCP 连接;网络中充斥着大量的无用数据包,源地址为假;大量的高流量无用数据,造成网络拥塞,使受害主机无法与外界正常通讯;利用受害主机提供的服务或传输协议上的缺陷,反复高速发出特定的服务请求,使受害主机无法及时处理所有正常请求;严重时可能造成系统死机。

2 DDoS 攻击实例—SYN-Flooding 攻击原理

SYN-Flooding 利用了 TCP/IP 协议的固有漏洞,面向连接的 TCP 三次握手是 SYN-Flooding 存在的基础。第一次:客户端发送一个带有 SYN 标记的 TCP 报文到服务端,指明端口号以及 TCP 连接初始序号等信息;第二次:服务端在接收到来自客户端的请求之后,返回一个带有 SYN+ACK 标记的报文,表示接受连接,并将 TCP 序号加 1;第三次:客户端接受到来自服务端的确认信息后,也返回一个带有 ACK 标记的报文,表示已经接受到来自服务器的确认信息。服务器在得到该数据报文后,一个 TCP 连接才算真正建立起来,开始全双工模式的数据传输过程。但当客户端发送一个 TCP 连接请求给服务器,服务器也发出了相应的响应数据报文之后,由于某些原因(如客户端突然死机或断网等原因),客户端不能接受到来自服务器的确认数据报文,这就制造了只有第一次和第二次握手的 TCP 半连接。由于服务器发出了带 SYN+ACK 标记的报文却并没有得到客户端返回相应的 ACK 报文,于是服务器便进入等待并进行 SYN+ACK 报文重发。当恶意的客户端构造出大量的这种 TCP 半连接发送到服务端时,服务端处于等待的过程中,且会耗用大量的 CPU 资源和内存资源来进行 SYN+ACK 报文的重发,这就是 SYN-Flooding 攻击。

3 目前主要防御对策与措施

由于目前使用的网络协议 IPv4 无法判断正常的 TCP 连接请求和黑客发出的假连接请求,因此有效防范措施应当在系统遭受攻击时仍能够允许正常的 TCP 连接。

增大系统 Backlog 的大小是一种最为简单的防御方法。但当攻击量比较大的时候,BACKLOG 队列还是会很快被填满,造成系统瘫痪。而且一味加大 BACKLOG 队列长度将消耗大量系统资源,使系统性能下降。

缩短 SYN-Timeout 时间和设置 SYN-Cookie:设置 SYN-Cookie 即给每一个请求连接的 IP 地址分配一个 Cookie,如果短时间内连续受到某个 IP 的重复 SYN 报文,以后来自于该 IP 地址的包会被丢弃。但如果攻击者以数万/秒的速度发送 SYN 报文,同时利用 SOCK_RAW 随机改写 IP 报文中的源地址,则该方法将毫无用武之地。

负反馈策略:正常情况下,OS 对 TCP 连接的一些重要参数有一个常规的设置,一旦服务器受到攻击,系统将根据攻击

*)本文研究得到重庆市自然科学基金项目(CSTC,2004BB2181)资助。黄 勤 副教授,研究方向为信息安全领域和计算机硬件技术;廖 伟 硕士研究生,研究方向为信息安全领域。

的判断情况做出反应：即减短 SYN-Timeout 时间、减少 SYN-ACK 的重试次数、自动对缓冲区中的报文进行延时等等措施。如果攻击继续，超过了系统允许的最大 Half-Connection 值，系统会将任何超出最大 Half-Connection 值范围的 SYN 报文随机丢弃，以保证系统的稳定性。这样便可以通过负反馈手段在一定程度上阻止 SYN 攻击。

退让策略：假设一台服务器在受到 SYN-Flooding 攻击后迅速更换自己的 IP 地址，那么攻击者仍在不断攻击的只是一个空 IP 地址，而防御方只要将 DNS 解析更改到新的 IP 地址就能在很短的时间内（取决于 DNS 的刷新时间）恢复用户通过域名进行的正常访问。

分布式 DNS 负载均衡：基于 DNS 解析的负载均衡能将用户的请求分配到不同 IP 的服务器主机上，攻击者攻击的永远只是其中一台服务器，这既增加了攻击者的成本，并且过多的 DNS 请求有助于追查到攻击者的真正踪迹。

防火墙 QoS：网关型防火墙布局中，客户机与服务器之间的所有数据交换都是通过防火墙代理的。由于所有 TCP 报文均需经过防火墙转发，故效率比较低，且增加了防火墙自身的负荷，因此该架构不适用于大型网站。

4 TCP/IP“一次握手”法

4.1 基本原理

在计算机系统中，系统在处理正常的任务时，有时需根据某些特定的情况决定是否完成其它“请求”事务。面对这种情况，计算机设计人员有两种方案来解决这个问题。一种是查询方式，即询问外设是否有需要服务的请求，如有，则转向处理该请求；否则，继续询问。另一种是中断方式，当外设有请求时，则中断系统当前的处理任务，转而完成该请求服务；否则继续处理原任务。这两种方法各有特点。“查询方式”响应慢，占用系统资源；“中断方式”响应快，系统资源利用率高，如图 1。

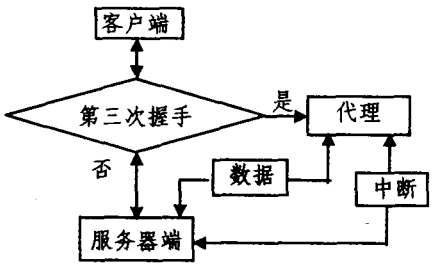

图 1 “一次握手”法原理示意图

在 TCP 协议的传输过程中，只有三次握手完成后，才开始传输数据。如果将 TCP 协议的三次握手改为“一次握手”就不会出现 SYN Flood 攻击。在客户端和服务器端设计一个中间代理，该代理不对系统的传输起任何作用，仅需记住客户端和服务器端完成了几次握手，在前两次握手过程完成后，代理进入第三次握手的等待中，而此时服务器端不理会这个客户端对服务器端的请求。虽然服务器端与客户端的三次握手没有什么变化，但由于服务器端不等待客户端的第三次握手响应，故不占用系统资源。对于正常连接，当第三次握手响应进入代理时，代理就对服务器端发出“中断请求”，服务端开始数据交换；对于非正常的连接，代理始终不向服务器端发出“中断请求”，服务器端的资源就不会被占用。

4.2 具体过程

“一次握手”法的工作流程如图 2。

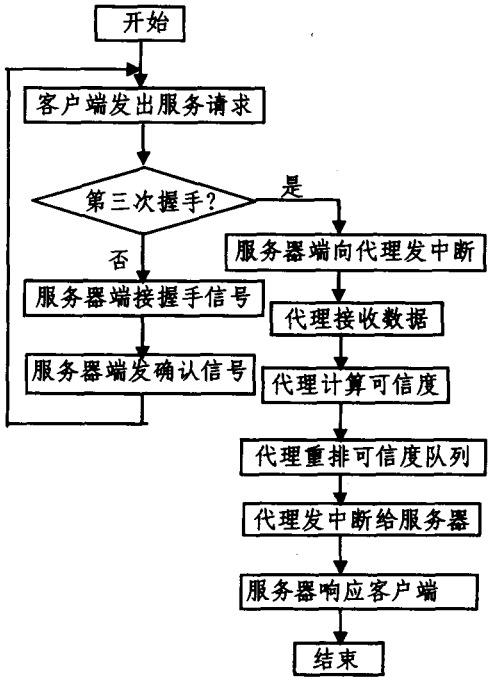

图 2 “一次握手”法工作流程示意图

（1）客户端对服务器端进行连接请求，代理判断是否是“第三次握手”协议。如果是第三次握手，转入代理程序；否则，直接进入服务器端。

（2）服务器端接收到某客户端的前两次握手协议之后，服务器端对代理发出数据传输中断请求，服务器端则将需要的信息（含主机和网络的代理可接受的数据）传输给代理。此后服务器端将进入下次受理连接的等待中。

这里的信息来源于主机和网络中的数据，这些数据均经过数据标准化处理，并对客户端的可信度具有一定的影响。

（3）代理将接收到的数据按照一定的规则进行可信度排序，依据可信度的高低顺序选择待服务的客户端。

当 SYN-Flooding 攻击时，出现大量的没有第三次应答信号的申请，对于客户端的可信度，可利用神经网络的自学习能力，利用网络中的正常数据包和已知的攻击数据包训练神经网络，存储并提取信号识别攻击。

①*数据采集及处理* 利用常规方法检测网络数据包，每个数据包可以分为头部编码部分和数据部分。在此只考虑编码部分的检测。去掉数据部分后，编码部分只剩下：IP（长度、标志符、分片偏移量、寿命、协议类型、源地址、目标地址）；UDP（源端口、目标端口、序列号、确认序号、偏移量、控制码、窗口、紧急指针）；TCP（源端口、目标端口、长度）；时间变量。

②*神经网络的选择* 利用系统的多元化描述，考虑到系统识别变体或新入侵的需要，宜采用有较强泛化能力的 BP 类网络。为不失一般性和简便起见，可以采用单隐层全连接二值输出的前向反馈的神经网络，其结构如图 3。

设审计事项 E 由入侵的特征向量：$(A_1, A_2, \cdots, A_n; B_1, B_2, \cdots, B_n)$ 决定。其中 $A_i(I=0,1,\cdots,n)$ 为攻击特征；$B_i(I=0,1,\cdots,n)$ 为不确定特征项。令 PA_i 为 A_i 在攻击过程中出现的概率，PB_i 为 B_i 在攻击过程中出现的概率，PE 为 E 在攻击过程中出现的概率。对于原始的攻击矢量：

$PA_i=1(I=0,1,\cdots,n)$

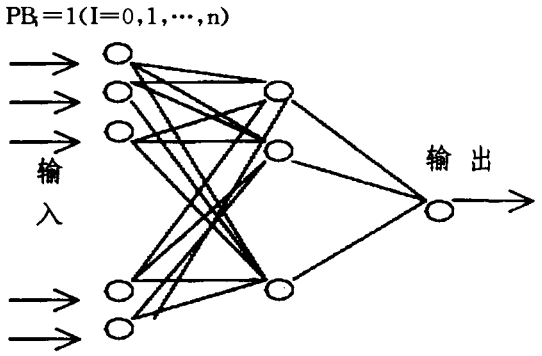

图 3 神经网络结构图

由审计事件计算得到 PA_i 与 PB_i 的值。将 PA_i 与 PB_i 进行权重计算得到 PE 的概率值。

本文中审计事项 E 是指客户端的可信度，将所有客户端的请求按照 PE 值的大小进行排序，改变服务器应答客户端的先后顺序。

(4)当代理收到客户端的"第三次握手"协议之后，结合其对客户端可信度的排序，受理客户端的请求，代理向服务器端发出连接中断请求，客户端和服务器端开始传输数据。

4.3 可行性论证

该方法有助于改善系统防范 SYN-Flooding 攻击的能力，它具有以下方面的品质。

(1)具有分布式均衡的能力。由于代理与服务器分别管理不同的服务，代理处理"第三次握手"协议，而服务器处理"第一、二次握手"协议，相当于增加了系统的处理器。

(2)适当缩小了 SYN-Timeout 值。由于代理将客户端的服务请求按照一定的原则进行了排序和优化，事实上缩短了 SYN-Timeout 时间，有助于加快网络的传输。

(3)利用了防火墙 QoS 的优点。其一，代理设计在防火墙内，没有暴露在客户端面前，增加了其安全性。其二，服务器端不存在大量消耗系统资源的中断申请，即客户端的连接响应由代理服务器按照时间统计概率 PE 值判断后排序提交。

4.4 前景

目前在 IPV4 的技术条件下，针对分布式入侵检测的方法很多，但是都没有一个完整的解决方案，特别是无法防御系列和重复攻击。随着 IPV6 技术的推广，使用该方法解决此问题将更加有效。

IPv6 具有实名认证机制。IP 地址与用户身份的一一对应性，使非法占用 IP 资源作为攻击其他计算机的平台的可能性大大降低，即没有大量的攻击资源的出现。进行 SYN-Flooding 攻击时，攻击者不能构造虚假的 IP 地址，换言之，IP 地址是真实而有效的。代理对于客户端的可信度排序的准确性，使从根本上解决 SYN-Flooding 攻击成为可能。

结束语 随着 Internet 的发展，最常见的拒绝服务攻击将是网络安全的一大劲敌，特别是 SYN-Flooding 攻击。根据实验验证，该方法是一种有效而经济的 SYN-Flooding 攻击防御方法。

参 考 文 献

1 叶芳，吴中福，刘永国．网络入侵的聚类算法研究与实现．重庆大学学报，2004，27(3)
2 Lee W, Stolfo S J, Mok K W. Mining audit data to build intrusion detection models. In: Proc. of the 4th Intl. Conf. 174 on Knowledge Discovery and Data Mining , New York, NY, AAAI Press, Aug. 1998
3 (美)Richard Stevens W.《TCP/IP 详解》卷一：协议[M]. 北京：机械工业出版社，2000
4 http://www. nsfocus. com/
4 http://www. xfocus. net/
5 Allen J, Christie A, et al. state of the pratice of Intrusion Detection Technologies, CMU/SEI, 2000. 6
6 方勇，龚海澎，胡勇，欧晓聪. 一种针对 SYN-Flooding 攻击的防范对策. 四川大学学报，2004(1)

(上接第 70 页)

表 1 HC 算法对初始 S 盒非线性度的改善情况

初始非线性度	改善后的非线性度					
	90	92	94	96	98	100
80	0	0	0	1	0	0
82	0	0	0	7	0	0
84	0	0	3	19	12	0
86	0	2	9	61	36	0
88	0	1	15	262	129	0
90	0	5	60	767	395	0
92	0	3	110	1966	1128	0
94	0	0	29	1922	1936	1
96	0	0	0	254	850	1
98	0	0	0	16	0	0

表 2 MHC 算法对初始 S 盒非线性度的改善情况

初始非线性度	改善后的非线性度					
	90	92	94	96	98	100
80	0	0	0	0	1	0
82	0	0	0	1	6	0
84	0	0	0	4	28	2
86	0	0	0	9	98	1
88	0	0	0	48	353	6
90	0	0	0	97	1123	7
92	0	0	0	222	2939	46
94	0	0	0	124	3682	82
96	0	0	0	6	1033	66
98	0	0	0	0	14	2

结束语 本文通过对双射 S 盒的 Walsh 谱的研究，给出了一个提高 S 盒非线性度的充分条件，并提出了 MHC 算法。与文[8]的 Hill Climbing 算法相比，它能更加有效地提高 S 盒的非线性度。同时，对 10000 个随机生成的双射 S 盒进行了实验，实验结果也证明了 MHC 算法对随机 S 盒非线性度的优化效果明显高于 Hill Climbing 算法。

本文的工作也可以和基因算法结合起来，演化地生成密码性能强的 S 盒。

参 考 文 献

1 Data Encryption Standard. FIPS PUB 46, National Tech. Infor. Service. VA, 1977
2 Daemen J, Rijmen V. The design of Rijndael: AES - The Advanced Encryption Standard. Springer, 2002
3 Rijmen V, Daemen J, Preneel B, et al. The cipher SHARK. Fast Software Encrytion, 1996. 99～111
4 Daemen J, Knudsen L R, Rijmen V. The Block Ciphe Squarer. Fast Software Encrytion, 1997. 149～165
5 冯登国，吴文玲. 分组密码的设计与分析. 北京：清华大学出版社，2000. 67～69
6 Anderson B J, Biham E, Knudsen L R. The Case for Serpent. In: AES Candidate Conf. 2000. 349～354
7 Millan W, Clark A, Dawson E. Smart Hill Climbing Finds Better Boolean Functions. In: Workshop on Selected Areas in Cryptology 1997, Works hop Record, 1997. 50～63
8 Millan W. How to Improve the Nonlinearity of Bijective S-boxes. ACISP '98, Berlin: Springer-Verlag, LNCS vol. 1438, 1998. 181～192
9 Millan W, Burnett L, Carter G, et al. Evolutionary Heuristics for Finding Cryptographically Strong S-Boxes. ICICS' 99, Berlin: Springer-Verlag, LNCS vol. 1726, 1999. 263～274
10 陈华，冯登国，吴文玲. 一种改善双射 S 盒密码特性的有效算法. 计算机研究与发展，已录用
11 Chen H, Feng Deng-guo. An Effective Evolutionary Stategy for Bijective S-boxes. IEEE Congress on Evolutionary Computation, Accepted, 2004