基于IP欺骗的SYN泛洪攻击

黄贻望,万 良,李 祥
(贵州大学 计算机软件与理论研究所,贵州 贵阳 550025)

摘 要:网络层的传输控制协议(TCP)向用户提供面向连接、高可靠性端到端服务,但TCP协议缺乏认证等相关功能,使得在网络层的通信存在很大的安全隐患,因此,需要对此攻击进行分析,找出这种攻击的关键点,模拟这种复合攻击,然后采取相应的预防措施。介绍TCP三次握手协议工作机制,并作了简单的形式化分析,同时分析了基于IP欺骗的泛洪攻击原理,在此基础上实现这种网络攻击技术并作相应的防范分析,从而为网络安全分析提供行之有效的方法。

关键词:TCP/IP;SYNflood;TCP序列号
中图分类号:TP393.08 **文献标识码**:A **文章编号**:1673-629X(2008)12-0159-03

SYNFlood Attack Based on IP Spoofing

HUANG Yi-wang, WAN Liang, LI Xiang
(Institute of Computer Software and Theory, Guizhou University, Guiyang 550025, China)

Abstract: The transmission control protocol (TCP) of network layer provided point-to-point service with communication-oriented and high reliable for user. But TCP absent authentification function, result in some secure risk in network communication. Introduced the work mechanism of three hand way of TCP protocol, and analyzed the principle of SYNflood attack based on IP spoofing, then implemented the technology of the network composites attack. Finally, provided some measures to avoid the network attack.

Key words: TCP/IP; SYNflood; sequence number of TCP

0 引 言

TCP/IP协议是因特网层的基础协议,IP协议是TCP/IP协议族中的核心协议,它独立于下层的网络技术实现,为上层协议提供服务;TCP连接正是建立在IP数据报服务之上,提供面向连接的、可靠的字节流服务,由于TCP三次握手协议缺乏认证机制,因此存在安全漏洞[1]。

1 攻击的原理

1.1 TCP协议的工作机制

TCP协议提供面向连接、高可靠性的通信服务。在利用TCP进行通信之前,通信双方需要建立一条TCP连接,TCP使用SYN(同步段)报文来描述用于创建一个连接的三次握手中的消息[2]。

三次握手协议步骤:

第一次握手:建立连接时,客户端发送请求包SYN(SEQ=k)到服务器,并进入SYN_SEND状态,等待服务器确认,请求标志syn=1;

第二次握手:服务器收到请求包,必须确认客户的请求包(ACK=k+1),同时自己也发送一个应答包(SEQ=q),即SYN+ACK包,此时服务器进入SYN-RECV状态,应答标志ack=1;第三次握手:客户端收到服务器的SYN+ACK包,向服务器发送确认包ACK(SEQ=q+1),此包发送完毕,客户端和服务器进入ESTABLISHED状态,完成三次握手。

创建一个TCP连接的三次握手过程中,要求连接双方都要产生一个随机的32 bit的初始序列号。如果在计算机重新启动之后,一个应用尝试建立一个新的TCP连接,TCP就选择一个新的随机数,可以保证新的连接不受原来连接的重复或延迟包的影响。

1.2 攻击原理

SYNFlood是一种利用TCP协议缺陷,发送大量伪造的TCP连接请求,从而使得被攻击方资源耗尽的攻击方式。在TCP连接的三次握手过程中,假设一个用户向服务器发送了SYN报文后突然死机或掉线,则服务器在发出SYN+ACK应答报文后是无法收到客户端的ACK报文的(第三次握手无法完成),这种情况

收稿日期:2008-04-07
基金项目:美国GeneChiu基金资助(GFC2006-001)
作者简介:黄贻望(1978-),男,湖南怀化人,硕士研究生,研究方向为模型检测与协议分析;李 祥,教授,博士生导师,研究方向为计算机理论与密码学。

下服务器端一般会重试并等待一段时间后丢弃这个未完成的连接,称为半连接握手状态,如果出现大量的这种半握手状态的连接,在服务器产生很多的请求队伍,最后的结果往往是堆栈溢出崩溃——即使服务器端的系统足够强大,服务器端也将忙于处理攻击者伪造的TCP连接请求而无暇理睬客户的正常请求,此时服务器失去了对客户端的响应,从而服务器端受到了 SYN Flood 攻击。

基于 IP 地址欺骗的 SYNflood 攻击是非法主机利用 TCP 协议中的缺乏认证机制的一种综合攻击手段。它是由多个技术综合组成的技术,首先要进行 IP 地址的伪造;其次是攻击主机的解除被信任主机和目标主机之机的信任关系;然后对目标主机的 SYNFlood 攻击或窃取机密信息。

(1)IP 地址伪造。

IP 地址的伪造很容易实现,IP 地址伪造技术的实现形式并不复杂。首先创建一个具有 IP 报文格式的结构,然后在该结构中源地址一项上填写虚假的 IP 地址,最后将该报文写入输出设备发向 Internet。

(2)SYN 洪水攻击及 TCP 序列号猜测。

假设,A:代表目标主机;B:代表信任主机;X:代表不可达主机;I:代表攻击主机;(P)Q 主机 P 伪装主机 Q,为了使用 TCP 交换数据,主机必须建立三次握手的三步过程,需要进行如下步骤:

(1)A $---$ SYN(ISN_A) $--->$ B;

(2)A $<---$ SYN(ISN_B)/(ACK ISN_A+1) $---$ B;

(3)A $---$ ACK(ISN_B) $--->$ B

这是信任主机 A 与目标主机 B 之间正常的 TCP 连接,它们是通过序列号 ISN 进行认证联系的,攻击主机 I 要进行对 B 的攻击,就要解除 A 与 B 之前的信任关系,即猜测出它们之间 TCP 通信的序列号。攻击 I 首先向信任主机 A 发送大量的 SYN 请求,同进信任主机 A 向 I 发回确认包(SYN/ACK),攻击模式如下:

(1)Z(x) $---$ SYN(ISN_x) $--->$ B;

Z(x) $---$ SYN(ISN_x) $--->$ B;……

(2)X $<---$ SYN(ISN_B)/ACK(ISN_x+1) $---$ B;

X $<---$ SYN (ISN_B) /ACK(ISN_x+1) $---$ B;……

(3)X $<---$ RST $---$ B(发送复位信息)

在(1)中,攻击主机发送大量的 SYN 请求给目标(记住这段的目标是被信任主机)以未决的连接塞满它的 backlog 队列;(2)中目标响应以 SYN/ACK,发送到了以为是 SYN 来源的地方,在此期间任何连到此 TCP 端口的请求都被忽略;(3)中目标主机 B 发送 RST 复位信息。

攻击者猜测目标主机的 TCP 的 32 位的序列号,攻击者连接到目标的一个 TCP 端口预先试探攻击,完成三次握手,但是攻击者会保存目标主机发送过来的初始序列号 ISN,攻击者需要知道目标和它信任的主机间的往返时间(RTT ,round - trip time),RTT 是精确计算下一个初始序列号(ISN)所必需的,只要 X 猜测的初始序列号大于等于 A 实际的初始序列号,连接就会被接受。攻击者在攻击过程中由于无法获知被攻击者的响应,因此只能通过猜测被攻击者所处的状态来控制住攻击的节奏才能取得成功。猜测 TCP 序列号成功,则攻击主机 I 可以伪装成信任主机的 IP 与 TCP 序列号与目标主机进行通信或进行攻击。

2 攻击的实现

由前面的 IP 地址欺骗的 TCP 洪水攻击的实现机理,关键是实现基于虚构 IP 地址的 TCP 洪水的攻击,使用原始套接字可以实现虚构 IP 地址的 SYN 发送[3]。

一个 TCP 报文由三个部分构成:20 字节的 IP 首部、20 字节的 TCP 首部与不定长的数据段,由于只是发送一个 SYN 信号,并不传递任何数据,所以 TCP 数据段为空。要实现虚构 TCP 包,就要定义相应的数据结构来组成 TCP 数据包[2]。

首先,根据 TCP 报文格式,定义一个结构 TCP_HEADER 用来存放 TCP 首部:

```
typedef struct tcphdr
{
  USHORT th_sport;
  USHORT th_dport;;
  unsigned int th_seq;unsigned int th_ack;;
  unsigned char th_lenres;
  unsigned char th_flag;USHORT th_win;
  USHORT th_sum;USHORT th_urp;
}TCP_HEADER;
```

通过正确的数据填充这个结构并将 CP_HEADER.th_flag 赋值为 2 能制造一个 SYN 的 TCP 报文,通过大量发送这个报文可以实现 SYN Flood 的效果。但是为了进行 IP 欺骗从而隐藏自己,也为了躲避服务器的 SYN Cookie 检查,还需要直接对 IP 首部进行操作,定义一个 IP_HEADER 来存放 IP 首部:

```
typedef struct iphdr
{
  unsigned char h_verlen;
  unsigned char tos; unsigned short otal_ len; unsigned short i-
```

```
dent;
    unsigned short frag_and_flags;
    unsigned char ttl; unsigned char proto;
    unsigned short checksum;
    unsigned int sourceIP; unsigned int destIP;
}IP_HEADER;
```

然后通过 SockRaw = WSASocket(AF_INET, SOCK_RAW, IPPROTO_RAW, NULL, 0, WSA_FLAG_OVERLAPPED),建立一个原始套接口,由于 IP 源地址是伪造的,因此需要在 setsockopt 中设置 IP_HDRINCL 告诉系统填充 IP 首部并自己计算校验和:

```
setsockopt(SockRaw, IPPROTO_IP, IP_HDRINCL,(char *)&flag,sizeof(int));
```

计算校验和的函数为:

```
USHORT checksum(USHORT *buffer, int size)
{
  unsigned long cksum=0;
  while(size >1)
  {
    cksum+ = *buffer+ +;
    size- =sizeof(USHORT);
  }
  if(size )cksum + = *(UCHAR*)buffer;
  cksum = (cksum >> 16) + (cksum & 0xffff);
  cksum + = (cksum >>16);
  return (USHORT)(cksum);
  }
```

TCP 首部检验和与 IP 首部校验和的计算方法相同,在程序中使用同一个函数来计算。由于 TCP 首部中不包含源地址与目标地址等信息,为了保证 TCP 校验的有效性,在进行 TCP 校验和的计算时,需要增加一个 TCP 伪首部的校验和,TCP 伪首部定义如下:

```
Struct
{
  unsigned long saddr;
  signed long daddr; ar mbz;
  char ptcl;signed short tcpl;
}psd_header;
```

然后将这两个字段复制到同一个缓冲区 SendBuf 中并计算 TCP 校验和:

```
memcpy(SendBuf, &psd_header, sizeof(psd_header));
memcpy(SendBuf + sizeof(psd_header), &tcp_header,sizeof(tcp_header));
tcp_hader. th_sum = checksum((USHORT *)SendBuf,sizeof(psd_header) + sizeof(tcp_header));
```

计算 IP 校验和的时候不需要包括 TCP 伪首部:

```
memcpy(SendBuf, &ip_header, sizeof(ip_header));
memcpy(SendBuf + sizeof(ip_header), &tcp_header,sizeof(tcp_header));
ip_header.checksum = checksum((USHORT)SendBuf,sizeof(ip_header) + sizeof(tcp_header)),
```

再把计算过校验和的 IP 首部与 TCP 首部复制到同一个缓冲区中就可以直接发送:

```
memcpy(SendBuf, &ip_header, sizeof(ip_header));
sendto(SockRaw, SendBuf, datasize, 0, (structsockaddr *)&DestAddr,
```

由于整个 TCP 报文部分都是用程序设计,不需系统干涉,因此在 IP 首部中 IP 地址可以随机填写,如果伪造的源 IP 地址确实有人使用,他在接收到服务器的 SYN+ACK 报文后会发送一个 RST 报文(标志位为 00000100),通知服务器端不需要等待一个无效的连接,可是如果这个伪造 IP 并没有绑定在任何的主机上,不会有任何设备去通知主机该连接是无效的(这正是 TCP 协议的缺陷),主机将不断重试直到 SYN Timeout 时间后才能丢弃这个无效的半连接。所以当攻击者使用主机分布很稀疏的 IP 地址段进行伪装 IP 的 SYN Flood 攻击时,服务器主机承受的负荷会相当高,可以用 Netstat－n－p tcp→resault. txt 检测目标主机是否发生洪水攻击。

3　攻击的防范分析

3.1　限制半连接流量和缩短 SYN Timeout 时间

针对攻击者对目标计算机的 SYN Flood 泛洪攻击,在目标计算机设置检测功能,即发现不断到针对本机的 SYN 数据包,而又不做出应答,则认为是受到 SYN 泛洪攻击,拒绝与它连接,同时,由于服务器的应答有一个延迟时间(Request time),可以把这个时间延迟缩短[4]。

3.2　设置伪造报文过滤规则

伪造 II 地址的报文具有很明显的特征:

(1)经过网关或路由器且源地址是回环地址 127.0.0.1 的 IP 报文;

(2)经过网关或路由器且包含地址 o.0.0.0 的报文;

(3)在广域网上传输但却具有专用子网保留地址 10.*.*.* ,172.16—32.*.*,192.168.*.* 的报文(*号代表 0—255)。

还有些报文具有反向的源地址;在目标计算机中设置 TCP 报文的标志字段的过滤规则,把不合法的 TCP 报文在网络层过滤掉。

(下转第 165 页)

加了证书载荷,这个证书载荷中包含了分配给发起者的 HOST_ID。

I->R:HDR,SAi1,KEi,Ni,[CERTi]

I<-R:HDR,SAr1,KEr,Nr,[CERTREQ]

响应者接收到发起者的 HOST_ID 后,向 IP 服务器发送请求要求根据发起者的 HOST_ID 查询发起者当前的 IP 地址,这样,IKEv2 发起者和响应者之间的协商就被转化成固定 IP 地址的情况,后续的协商过程和标准的 IKEv2 类似。

协商结束后,参加协商的 VPN 网关各自将协商好的 IPSec SA 通过 PF_KEY 通讯机制写入内核中的安全关联数据库中,以便以后再次使用。

2.4 地址通知机制

VPN 网关注册 IP 地址后由于某种原因,自身的 IP 地址可能再次发生变化。另外,网络、VPN 网关可能出现故障以至无法正常通讯,这可能导致使用过时的安全关联从而降低了系统的安全性。为此,扩展方案提供一个选项,允许管理员根据具体情况设置各个 VPN 网关每隔一个时间周期便向 IP 服务器提交自己当前使用的 IP 地址,消息交互和提交阶段一样。考虑到网络通讯效率,IP 服务器第一次接收到 VPN 网关提交的地址后必须发送反馈消息,但是对于后续的消息,只要提交的地址没有发生改变,服务器便可以不发送反馈消息。另外,如果某 VPN 网关提交的地址发生变化,IP 服务器便会根据 IDPD 得知和该网关进行 IKEv2 协商的所有 VPN 网关,也就可以通知这些 VPN 网关,以便它们做出相应的处理。

3 结束语

提出了针对 IKEv2 的扩展设计与实现,使 IPSec VPN 网关可以不必限制在固定 IP 环境下进行隧道建立,扩大了 VPN 的应用范围,与扩展前的 IKEv2 具有更广阔的应用前景。

参考文献:

[1] Microsoft C. Kaufman. RFC4306. Internet Key Exchange (IKEv2) Protocol[S]. 2005.

[2] Kivinen T, Tschofenig H. RFC4621. Design of the IKEv2 Mobility and Multihoming (MOBIKE) Protocol[S]. 2006.

[3] 陈　卓,张正文. Internet 密钥交换协议 IKEv2 研究[J]. 计算机应用与软件,2008,25(2):269-270.

[4] 韩旭东,汤　隽,郭玉东. 新一代 IPSec 密钥交换规范 IKEv2 的研究[J]. 计算机工程与设计,2007,28(11):2549-2552.

[5] 杜春燕,周晓东,陆建德. 一种基于 IKEv2 的 IPsec 远程访问实现方案[J]. 电脑与电信,2007(9):4-6.

[6] Lari I A, Jorma Y, Pekka L. A Proposal to Improve IKEv2 negotiation[C]//Emerging Security Information, Systems, and Technologies, 2007 International Conference. Valencia, Spain:[s.n.],2007:169-174.

(上接第 161 页)

具有伪造 II 地址的报文可能发生在 Internet 上的任何区域。因此要设置 IP 地址伪造就需要在 Internet 的各级网络采用包过滤技术,报文构造方式设置相应的过滤规则,以截获这些伪造 IP 地址的报文,解除 IP 的欺骗[5]。

3.3 解除信任关系

从 TCP 通信过程中,可以看出,两个主机之间的通信主要是通过它们 IP 地址建立起来的认证机制,那么解除这种认证关系,取而代之的是一种基于加密的可信第三方安全协议的认证机制,以增强身份签别功能。

3.4 防止序列号被猜测

TCP 序列号猜测成功的关键在于,系统为每个连接产生的初始序列号 ISN 不具有随机性。因此,采用新的 ISN 序列号生成技术,同时对生成的 ISN 进行 HASH 映射,增加序列号的随机和保密性。

3.5 增加认证机制

正常情况下的两个计算机的数据通信过程中,增加两方通信的认证机制,周期性地作一次身份认证,以防在数据传送过程的身份冒认出现。

4 结束语

文中做了 TCP 的三次握手协议的安全漏洞的分析及基本实现,针对性地分析了为解决这种综合网络攻击而采用的几种防范措施,为网络安全防预提供了可行的方法。

参考文献:

[1] 黄发文,徐济仁,陈家松. 计算机网络安全技术初探[J]. 计算机应用研究,2002,19(5):46-48.

[2] Wright G R, Stevens W R. TCP/IP 详解 卷 2:实现[M]. 陆雪莹等译. 北京:机械工业出版社,2000.

[3] 吉文华,于汇敏. 防 Dos 攻击的算法的分析和实现[J]. 计算机应用,2003,23(6):90-91.

[4] 寺田真後,萱岛信 . TCP/IP 网络安全篇[M]. 王　庆译. 北京:科学出版社,2003.

[5] 蔡　敏,叶　震,徐吉斌. 协议分析技术在入侵检测中的应用[J]. 计算机技术与发展,2007,17(2):239-241.