网上IP劫持攻击的研究*

赵欣 陈道蓄 谢立

(南京大学计算机软件新技术国家重点实验室 南京 210093)

E-mail: njzx@hotmail.com

摘要 当前,网上出现了一种基于TCP的主动攻击,称为IP劫持.这种攻击不同于以往的基于网络侦听的被动式网络攻击,它能绕过系统口令和S/KEY口令保护的防御,将网络连接完全接管,对网络安全造成了重大威胁.该文分析了这种攻击的实施原理,并提出了针对这种攻击的检测方法和防御技术.

关键词 IP,TCP,IP劫持,网络监视器,连接非同步.

中图法分类号 TP393

随着Internet在全球范围内的日益流行,网络攻击日益增多.许多攻击是由于系统管理员的安全意识不够强烈[1],暴露出明显的安全漏洞所造成的,如系统管理员口令设置不对,系统设置了许多权限控制不严的"信任主机"等,这些攻击一般可以通过加强管理员的安全意识和对系统的安全控制来予以防御.另外一些攻击是由于软件系统的错误或漏洞造成的,如著名的针对Win95和WinNT的OOB攻击和"泪滴"攻击.这一类攻击能通过对系统打补丁、弥补系统错误和漏洞来予以防御.还有一类攻击则是针对TCP/IP本身的运行机制进行攻击,其中最著名的就是Morris的DOS(denial of service)攻击和IP劫持[2~4].它们充分利用TCP/IP实现中的漏洞进行攻击,对系统安全威胁很大.本文对其中危害最大的IP劫持攻击的原理进行了分析和研究,并给出了针对这种攻击的一些检测和防御技术.

1 IP劫持

IP劫持不同于用网络侦听来窃取密码的被动式攻击方式(它可以用S/KEY加密技术予以防御),而是一种主动攻击方式.所谓IP劫持是指,当用户连接远程机器的时候,攻击者接管用户的连线,使得正常连线如同经过攻击者中转一样,攻击者能任意对连线交换的数据进行修改,冒充合法用户给服务器发送非法命令,或冒充服务器给用户返回虚假信息.这无疑将对用户和服务器造成巨大的危害.所以,分析和了解IP劫持的原理,并发掘出检测和防御这种攻击的方法是非常重要的.

我们将分几部分来介绍IP劫持攻击的原理和检测、防御手段.第2节简要介绍TCP的运行机制.第3节介绍IP攻击的原理及其引起的副作用.第4节介绍攻击的检测手段.第5节介绍一些IP劫持攻击的防御技术.第6节给出结论.

2 TCP运行机制

TCP提供了连在网上的两个终端节点之间的可靠的全双工流连接,每个TCP连接可以用一个四元组{源IP地址、目的IP地址、源PORT号、目的PORT号}来描述[5~7],每个发送字节都用一个32位的序列号标记,而接收方则用该序列号予以确认.本文把发起连接方称为客户方,而把接受连接方称为服务方.

* 本文研究得到国家863高科技项目基金(No.863-306-ZT02-03-01)资助.作者赵欣,1974年生,博士生,主要研究领域为分布式系统,并行计算.陈道蓄,1947年生,教授,主要研究领域为分布式系统,并行计算.谢立,1942年生,教授,博士生导师,主要研究领域为分布式系统,并行计算.

本文通讯联系人:赵欣,南京 210093,南京大学计算机软件新技术国家重点实验室

本文1999-02-07收到原稿,1999-04-22收到修改稿

下面引入一些变量来记录连接状态.

SVR_SEQ:服务方下一个字节发送时用来作标记的序列号.

SVR_ACK:服务方接收的下一个字节应具有的序列号.

SVR_WIND:服务方基于"滑动窗口"流量控制机制的接收窗口大小.

CLI_SEQ:客户方下一个字节发送时用来作标记的序列号.

CLI_ACK:客户方接收的下一个字节应具有的序列号.

CLI_WIND:客户方基于"滑动窗口"流量控制机制的接收窗口大小.

连接处于无数据交换的状态时,有 $CLI\_ACK=SVR\_SEQ$ 和 $SVR\_ACK=CLI\_SEQ$. 但当存在数据交换的时候,上面的关系式就应改为

$$SVR\_ACK \leqslant CLI\_SEQ \leqslant SVR\_ACK-SVR\_WIND,$$

$$CLI\_ACK \leqslant SVR\_SEQ \leqslant CLI\_ACK+SVR\_WIND.$$

TCP 包头中同攻击相关的参数有:

Source Port:源端口号.

Destination Port:目的端口号.

Sequence Number:报文中第 1 个字节的序列号.

Acknowledgement Number:期待收到的包的序列号.

Data Offset:数据的偏移位置(因为存在变长包头).

Flag Bits:特定的控制信息.同攻击相关的有:

FIN:发送方没有更多的数据需要发送了.

SYN:连接双方同步序列号.

RST:连接重置.

ACK:确认信息.

Window:发送方的滑动窗口大小.

Checksum:TCP 包中包头和数据的校验和.

Options:TCP 选项,包括下面几种选项:

SEG_SEQ:描述该包的序列号.

SEG_ACK:描述该包携带的确认序列号.

SEG_FLAG:描述 Flag Bits 控制标记位的值.

客户方发送数据时会设置 $SEG\_SEQ=CLI\_SEQ$ 和 $SEG\_ACK=CLI\_ACK$. TCP,通过"三次握手"机制来建立连接.设客户方的初始序列号为 CLI_SEQ_0,服务方的初始序列号为 SVR_SEQ_0,连接建立完毕后,连接双方将处于 ESTABLISHED 状态.此时,有下面的等式成立:

$$CLI\_SEQ=CLI\_SEQ_0+1 CLI\_ACK=SVR\_SEQ_0+1,$$

$$SVR\_SEQ=SVR\_SEQ_0+1 SVR\_ACK=CLI\_SEQ_0+1.$$

当主机要关闭连接的时候,它将发送一个设置了 FIN 或 RST 控制位的包,对端主机收到后就进入 CLOSED 状态,并将同该连接相关的各种资源释放.通常情况下,含 RST 标志位的包是不被确认的.任何随后而来的报文都会被简单地抛弃.

当连接双方进入 ESTABLISHED 状态后,对服务方而言,只有收到的报文的序列号在范围[SVR_ACK, $SVR\_ACK+SVR\_WIND$]内,该报文才会被接受.对客户方而言,只有收到的报文的序列号在范围[CLI_ACK,$CLI\_ACK+CLI\_WIND$]内,该报文才会被接受.否则,报文将被抛弃,并且接收方会发送一个反馈报文,通知发送方合法的序列号范围.

3 IP劫持攻击的原理

3.1 连接非同步

通常,在连接建立完毕并且没有数据交换的状态下,有下面的关系式成立:

$$CLI\_ACK=SVR\_SEQ \quad 且 \quad SVR\_ACK=CLI\_SEQ.$$

此时的状态被称为"同步状态".若$CLI_ACK\neq SVR_SEQ$,$SVR\_ACK\neq CLI\_SEQ$,则称为"非同步状态".当连接处于非同步状态的时候,若有数据传送,将可能出现两种情况:

(1) 若$SVR_ACK<SEG_SEQ<SVR_ACK+SVR_WIND$,由于报文的系列号并不等于$SVR_ACK$,但处于合法范围内,则该报文将被缓存,供以后使用;

(2) 若$SEG_SEQ<SVR_ACK$或$SEG_SEQ>SVR_ACK+SVR_WIND$,则该报文被简单抛弃,并向数据发送方发送一个反馈包,以通告合法的系列号.

攻击者正是利用连接的非同步状态来进行IP劫持的.

3.2 攻击原理

在攻击中,攻击者诱使连接进入非同步状态,并使得数据在交换时,出现$SEG_SEQ<SVR_ACK$或$SEG_SEQ>SVR_ACK+SVR_WIND$(即上面介绍的第2种情况).此时,连接双方无法再进行正常的数据交换,而攻击者却能冒充合法客户方发送可以被服务方接受的报文.假定连接已经进入非同步状态,此时$CLI_ACK\neq SVR_SEQ$及$SVR_ACK\neq CLI_SEQ$,若客户方发送一个报文,并设置$SEG_SEQ=CLI_SEQ$和$SEG_ACK=CLI_ACK$,由于$SVR_ACK\neq CLI_SEQ$,所以该报文被认为是错误的报文并被抛弃.此时,攻击者通过网络侦听截获该客户方发送的报文,依此仿照相同的报文,并设置$SEG_SEQ=SVR_ACK$和$SEG_ACK=SVR_SEQ$,修改该包的校验和,然后向服务方发送该报文.显然,该报文将被服务方接受并处理.这里,我们令$CLT_TO_SVR_OFFSET$为客户方的发送序列号到服务方的认可序列号的差距,则$CLT_TO_SVR_OFFSET=SVR_ACK-CLT_SEQ$.而令$SVR_TO_CLT_OFFSET$为服务方的发送序列号到客户方的认可序列号的差距,则$SVR_TO_CLT_OFFSET=CLT_ACK-SVR_SEQ$.所以,有下面的等式:

$$SEG\_SEQ=CLT\_TO\_SVR\_OFFSET+CLT\_SEQ=SVR\_ACK$$
$$=CLT\_TO\_SVR\_OFFSET+SEG\_SEQ,$$
$$SEG\_ACK=CLT\_ACK-SVR\_TO\_CLT\_OFFSET=SVR\_SEQ$$
$$=SEG\_ACK-SVR\_TO\_CLT\_OFFSET.$$

攻击者只要通过网络监视器看到客户方发送的报文的SEG_SEQ和SEG_ACK,然后令

$$SEG\_SEQ=CLT\_TO\_SVR\_OFFSET+SEG\_SEQ,$$
$$SEG\_ACK=SEG\_ACK-SVR\_TO\_CLT\_OFFSET.$$

显然,服务方将接受这个伪造的报文,并完成该包中携带数据所代表的命令.这就构成了IP劫持攻击.

3.3 非同步状态的制造

为了进行IP劫持攻击,首先必须制造连接的非同步状态.攻击者可以用网络监视器(如SUN下的Sniffit,PC上的NetXray等)来侦听广播网段上的报文,从而监控并分析他准备攻击的机器上所发出的各种报文,并予以攻击.我们在此仅介绍两个常见的方法.

(1) 连接重置法

当连接C建立的初期,攻击者用网络侦听工具能窃取到客户方的连接端口号和序列号等重要信息.利用这些信息,攻击者就能冒充客户方,向服务方发送一个含有RST控制标记位的报文,要求重置该连接.当服务方收到这个报文后,就会重置连接C,并释放与该连接相关的所有资源.服务方不会对这个RST报文给出应答.然而,客户方已经收到服务方SYN/ACK应答包,认为连接成功并进入ESTABLISHED状态.随后,攻击者冒充客户方发出一个新的SYN连接请求,并在其中填写自己的系列号(不妨称之为ATK_SEQ_0).由于原来分给连接C的端口号等资源在短时间内尚未被服务方分配给其他连接,所以,服务方仍把这些资源分配给攻击者请求的

连接,然后初始化自身的初始序列号 SVR_SEQ_1,并发送 SYN/ACK 反馈报文.攻击者截获该反馈报文后,根据反馈报文中的服务方的序列号继续冒充客户方发送第三次握手的反馈包.服务方收到该反馈包后就进入ESTABLISHED状态.至此,攻击者已经制造了连接的非同步状态,然而合法连接的双方仍一无所知.这里,显然有 $CLT\_TO\_SVR\_OFFSET=ATK\_SEQ_0+CLT\_SEQ_0$ 和 $SVR\_TO\_CLT\_OFFSET=SVR\_SEQ_0-SVR\_SEQ_1$,其中 $CLT\_TO\_SVR\_OFFSET$ 的值是受攻击者控制的.只要攻击者合理调整 ATK_SEQ_0 的值,就能使客户方发送的报文的序列号不落在服务方所能接受的范围内,从而造成连接的非同步状态.

(2) 空报文法

攻击者可以采用发送大量空报文的方法来使连接进入非同步状态.例如,当客户方通过 telnet 远程连接某服务器来创建连接的时候,它所发送的数据将被攻击者侦听到.连接建立完毕后,攻击者可以冒充客户方向服务方发送大量的不含具体数据的报文,如在 telnet[8]连接中发送 IAC NOP 报文,服务方的 TCP 实现就会简单地递增 SVR_ACK 的值.由于 TCP 对无具体数据的报文是不给予回答的,所以,客户方对此毫无所知,从而造成了连接的非同步状态.我们不妨假设攻击者发送这种空报文的个数为 $ATK\_TO\_SVR\_OFFSET$ 个,则攻击者通过合理设计 $ATK\_TO\_SVR\_OFFSET$ 的值就能造成连接的非同步状态.采用这种方法,攻击者甚至不必在连接建立的时候就进行连接的非同步攻击.

3.4 TCP 应答风暴

在上面的分析中,我们没有考虑真正的客户方发送数据后报文被抛弃所带来的副作用.但是,这种副作用是客观存在的.

当客户方发送报文后,由于攻击者造成连接的非同步状态,所以服务方将这个报文抛弃,并发回 ACK 反馈报文,通告可接受序列号.同样地,由于连接的非同步状态,客户方又认为该 ACK 反馈报文不可接受,于是抛弃该报文,并向服务方发回 ACK 反馈报文.服务方又认为报文的序列号不能接受,于是继续抛弃该报文,并向客户方发回 ACK 反馈报文……如此往复,造成了一个无限循环,从而构成了 TCP 的 ACK 风暴.若客户方收不到服务方的确认报文,就会重新发送报文,这将进一步加剧 ACK 风暴.

根据 TCP 规定,凡是没有数据的 TCP 报文,若传送出现丢失,则并不重发.由于我们使用的网络往往是不可靠的,存在着丢失报文的情况,网络负载随着 ACK 风暴的发生大大增加,经过若干次 ACK 报文的传送,若其中某次 ACK 报文丢失,则该次 ACK 风暴就将结束了.

若攻击者不对客户方发送的数据给予 ACK 确认,则客户方会重新发送数据;若重新发送屡屡不能获得 ACK 确认,客户方将认为连接中断,从而退出连接.所以,攻击者往往会继续通过网络监视器监控网络,并向客户方发送确认信息.

4 攻击的检测和发现方法

通过分析攻击原理,本文提出了一些攻击检测和发现的方法.

(1) 非同步状态的检测

通过分析,我们发现,要进行这种 IP 劫持攻击,必须造成连接的非同步状态,那么,若能获得本地连接的发送序列号并通过某个加密连接发送到服务方,同服务方的接受序列号进行对比,就能简单地发现连接是否被接管了.

(2) ACK 风暴的检测

若能对网络进行监控和统计,就能发现,若出现 IP 劫持攻击,就会有连接的非同步状态.由于存在 ACK 风暴,此时 ACK 报文在所有报文中所占的比例大大增加,所以,若出现这种情况,就很有可能遭到了 IP 劫持攻击.

(3) 报文丢失率和重传率上升

由于 ACK 风暴造成网络负载过重,所以会出现大量报文丢失和报文重传的现象.所以,若有明显的报文丢失率和重传率上升的现象,就有可能是遭到了 IP 劫持攻击.

(4) 常出现意外的连接重置的现象

由于攻击者发送的报文也可能丢失,从而导致攻击并非每次都能成功,而没有成功的攻击往往造成连接的意外中断或重置.所以,若经常出现连接意外中断或重置也可能意味着受到了IP劫持攻击.

5 攻击的防御措施

对IP劫持攻击的防御可以从两方面着手:

(1) 在TCP的实现中加以防御.在TCP实现中,当连接一方收到RST报文时,应向连接对方发送一个RST报文,然后再重置连接,使得攻击者无法建立连接非同步状态,从而抵御用连接重置法进行的攻击.

(2) 在网络配置上加以防御.对子网外发起的攻击,可以设置路由器和防火墙来阻断非子网内的IP的连入,同时过滤掉有源路由的数据报文.对子网内部则要用加密的Kerberos方法在应用层进行加密,或采用加密TCP来加密数据,以防数据被修改.

6 结 论

本文分析了IP劫持攻击的原理,并介绍了一些检测和防御的方法.这些方法可有效地发现网络上的IP劫持攻击,并进行有效防御.在当前网络攻击越来越多的情况下,网络用户特别是网络管理员的安全意识也需要提高,以便切实保证系统和数据的安全.

参考文献

1 Braden R. Requirements for Internet hosts-communication layers. IETF RFC1122, 1989

2 IP Spoofing Attacks and Hijacked Terminal Connections. CERT ADVISORY CA-95-01, 1995

3 Shimomura T. Technical Details of The Attack Described by Markoff in NYT. Usenix newsgroups: comp. protocols. tcp-ip, comp. security. misc, 1995

4 Bellovin S. Security problems in the TCP/IP protocol suite. Computer Communications Review, 1989,19(2):32~48

5 Stevens W R, Wright G R. TCP/IP Illustrated Vol. 2——The Implementation. Reading, MA: Addison-Wesley Publishing Company, 1995

6 Comer D E. Internetworking with TCP/IP: Vol. 1——Principles, Protocols, and Architecture. 3rd Edition, Upper Saddle River, NJ, Prentice Hall, Inc., 1995

7 Stevens W R. TCP/IP Illustrated Vol. 1——The Protocols. Reading, MA: Addison-Wesley Publishing Company, 1994

8 Postel J, Reynolds J. Telnet protocol specification. IETF RFC0854. 1983

Study on IP Hijack

ZHAO Xin CHEN Dao-xu XIE Li

(*State Key Laboratory for Novel Software Technology Nanjing University Nanjing* 210093)

Abstract There is a kind of active attack based on TCP over the Internet, which is called IP Hijack. This kind of attack is different from the passive attack based on network sniffing. It can bypass the protection of system password and S/KEY, and get full control of the link between two end points. This can cause great harm to the network system. In this paper, the principle of this kind of attack is analyzed, the attack detecting technology and the protecting measures against IP Hijack are also given.

Key words IP, TCP, IP hijack, network monitor, link desynchronization.