关于在交换局域网进行主动捕包的研究①

贺龙涛② 方滨兴 云晓春 汪立东 袁 林
(哈尔滨工业大学计算机科学与工程系 哈尔滨 150001)

摘 要 对在交换型以太网络下的捕包方法进行研究,提出了利用底层协议伪装攻击结合 IP 转发技术来进行主动捕包的模型,分析了主动捕包可以利用的几种底层协议伪装攻击及其特点。

关键词 交换网络,协议伪装,IP 转发,主动捕包

0 引言

网络捕包,即将网络上传输的数据捕获并进行分析的行为。在网络安全领域,网络捕包占有极其重要的作用。对于黑客攻击而言,网络捕包是一种有效的信息(用户名、口令等)收集手段,并且可以辅助进行 IP 欺骗[1];对于安全管理而言,捕包也是监控本地网络状况的直接手段,捕包还是基于网络的入侵检测系统(NIDS)的必要基础[2]。然而,通常意义上的网络捕包,是在广播式网络环境下进行的,而对于交换式以太网络环境,即使是将网卡设置成混杂模式,依旧只能捕获本该到达该 IP 的数据包。

本文提出主动捕包的概念,即主动采取措施,将交换以太网下指定的或全部的机器间网络通信引到攻击者机器的行为,并认述了将其付诸实践的方法。

1 主动捕包方法

在研究主动捕包前,有必要先分析一下局域网交换机的工作方式:交换机内部动态地维护一个地址映射表,通过查表,决定将收到的帧转发到对应的端口或者广播域。地址映射表的构造则采用了自学习的技术,即当交换机收到一个数据帧时,首先将帧中的源地址及对应的输入端口号记入地址映射表,以使交换机'了解'哪些结点附接于哪个端口(或者广播域)。同时根据帧中的目的地址,查找地址映射表,如果表中有对应的地址项,帧被转发到指定的端口;否则向所有其他的端口广播。主动捕包有两大类方式:旁路方式和插入方式。

1.1 旁路方式

如图 1 所示,这个思想还是源于广播网下的网络捕包,只是在交换网络下不能简单地将网卡设成混杂模式,而需要对所要捕包的网络进行适当的攻击。

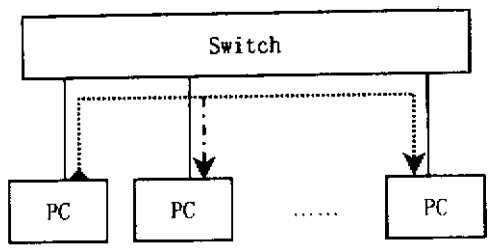

图 1 基于旁路的主动捕包

在交换以太网下,要想将到达某个主机 MAC 地址的网络数据帧旁路,主要的攻击对象就是交换机。对交换机的攻击可以采用 MAC 洪泛。

由以上对交换机的分析中,可以注意到以下两点:

(1) 交换机内部动态地维护一个地址映射表。显然交换机只有有限的存储器来存储地址映射表数据,那么攻击者就能够发送源 MAC 地址是各种 MAC 地址的以太帧,将地址映射表存储器耗尽。

(2) 当交换机不能在地址映射表中查找到接收到的数据帧中的目的 MAC 地址的时候,它将该数据帧向所有其他的端口广播。对于主动监听而言,可以很好地利用这个特性来进行旁路。对交换机进行 MAC 洪泛攻击,使得交换机的地址映射表存储器总是处于耗尽的状态,地址映射表里存放的总是一些假 MAC 地址,这样,在一个真正的数据帧到达交换机端口的时候,交换机就总是找不到该数据帧的目的 MAC 地址,于是它就总是将数据广播到各

① 国防科技预研跨行业综合技术(15.7.2)资助项目。
② 男,1974 年生,博士生;研究方向:计算机网络安全,网络应用,病毒防治;联系人。
(收稿日期:2001-01-05)

个端口去,实际上变成了一台 HUB,也就使得交换式局域网退化为广播式局域网。这样也就能够捕获同一局域网下的别的机器的网络数据了。

这种方式攻击的是交换机地址映射表存储器大小,因此存在以下局限:

(1) 由于使用的是洪泛攻击技术,这样会使得网络负载很重。这是所有洪泛攻击都固有的问题。

(2) 攻击的有效性依赖于交换机地址映射表存储器大小。当交换机存储器足够大的时候,这种攻击就显得不是那么有效了。要增加有效性,方法就是加大洪泛攻击的力度,但这又会加重上一个问题。所以需要在中间取一个权衡,既要能够尽量使得交换机存储器趋于耗尽状态,又要使网络负载达到最小,以免引起局域网内使用者的注意。

总之,在交换网络使用如同在广播网络一样进行旁路的思想进行捕包,捕包率低,网络负载重,效果不是很理想,基本上不能达到网络捕包的目的。

1.2 插入方式

既然在交换网络下使用旁路的思想来进行捕包效果并不理想。这就需要用一个全新的思想来考虑,也就是说使用与旁路思想相对应的插入思想来考虑这个问题。

插入思想,就是主动想办法将要窃听的两台机器间的网络通信引到捕包者机器上来,再由捕包者机器将这些网络包转发到目的地址去。这样,对被监听者而言,如图 2 中点划线所示,还是在"直接"与通信对端机器进行网络通信,然而对于主动捕包者机器而言,如图 2 中虚线所示,它已经直接插入到被捕包机之间的网络通信中来了。

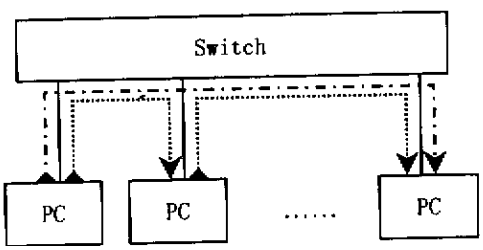

图 2 基于插入方式的主动捕包

基于插入思想的主动捕包,主要有两大环节:

(1) 进行底层协议伪装,对本交换局域网内的机器进行欺骗,将它们的网络访问都导向到捕包者机器上来。

(2) 进行包转发,在接收到一个以太包后,分析上层协议,根据上层协议指定的目的地址转发到相应的 MAC 地址去,以保证被欺骗机器的正常网络访问。

包转发,实质上是和路由器的工作基本相同的,区别只是在于路由器是在不同局域网之间进行包转发,而这里的 IP 包转发只是在局域网内进行转发。

已经有许多工具可以进行 IP 转发,本文对此只是作一个简单的实现:

(1) 保持一个局域网内各个 IP/MAC 的对应列表,根据捕获的 IP 包或者 ARP 包的源 IP 域进行更新。

(2) 收到一个 IP 分片包之后,分析 IP 包头,根据 IP 包头里目的 IP,找到相应的 MAC 地址。

(3) 将源 MAC 地址设成本机的 MAC 地址,目的 MAC 地址设成第二步查找到的 MAC 地址,将收到的 IP 分片包发送出去。

由此可以知道,在基于插入方式的主动捕包框架中,核心问题是如何进行底层协议伪装,对交换局域网内机器进行欺骗,将它们的网络访问都导向到捕包者机器上来。

2 利用协议伪装进行主动捕包

对于底层协议伪装而言,在局域网络层次上,主要有两种协议可以进行考察:数据链路层协议 ARP[3],IP 层协议中靠近底层的协议 ICMP[4]。

2.1 底层协议安全弱点分析

这些协议虽然在 TCP/IP 协议族中都是高效的底层协议,但是,它们是建立在各主机之间相互信任的基础上的,因此有不少安全问题:

无连接 这些底层协议没有连接的概念,攻击者可以随意发送协议包。任何时候都可以发送协议包,只要协议包是有效的,接收到协议包的主机就无条件的根据协议包的内容刷新本机协议相关的状态。

通信无需认证 出于传输效率以及实现简单性上的考虑,这些底层协议基本没做什么安全上的考虑。在收到协议包时,主机不检查协议包的合法性,而直接根据协议包的信息修改本机协议相关的状态。

动态性 也就是说,主机所保持的协议相关状态常常不是静态不变的,而是根据所接收到的协议信息包(有可能是主动发协议包请求应答,也可能是被动接收到协议指令包)进行动态更新的。

2.2 底层协议伪装分类

依据攻击的层次不同,可以将基于协议伪装的主动捕包分为两大类:

ARP 伪装攻击　这类攻击的攻击点是 IP 地址到底层 Ethernet 地址的映射关系。主要手段是对 ARP 协议进行伪装[5],发送假冒 ARP 应答报文。

路由攻击　这类攻击的攻击点是非局域网 IP 地址与本地网关的映射关系。主要手段是对 ICMP 协议进行伪装,发送假冒 ICMP 重定向差错报文或者假冒 ICMP 路由器通告报文。

2.3　ARP 伪装攻击

IP 地址到底层 Ethernet 地址的映射关系主要是靠 ARP 协议来实现的。对于网络主机而言,这个映射关系是存放在 ARP 高速缓存中的。要对指定机器上的 ARP 高速缓存进行修改,就必须研究 ARP 协议。

在以太网下,ARP 协议是这样工作的[6]:首先,网络通信源机器向网络广播 ARP 请求包,请求网络通信目的机器 IP 所对应的 MAC 地址;然后使用该 IP 的机器会向源机器发送一个含有其 MAC 地址的 ARP 回应包,这样源机器就知道向哪个 MAC 地址,也就是目的机器发送数据了。

除了 2.1 中所列出的安全问题外,ARP 还有一个问题:ARP 请求是以广播方式进行的。这个问题是不可避免的,因为正是由于主机不知道通信对端的 MAC 地址,才需要进行 ARP 广播请求的。这样,攻击者就可以伪装 ARP 应答,与广播者真正要通信的机器进行竞争。还可以确定子网内机器什么时候会刷新 MAC 地址缓存,以确保最大时间限度的进行假冒。

根据以上的讨论,可以使用以下步骤来进行 ARP 欺骗:

(1) 网络主机在不知道想通信 IP 对应的 MAC 地址时,会进行 ARP 广播请求,这样攻击者也就可以在接收到该 ARP 请求包之后以自己的 MAC 地址应答,进行假冒。

(2) 由于被假冒的机器所发送的 ARP 应答包有可能比攻击者的应答包晚到达,为了确保被攻击者机器上的缓存中绝大部分时间存放的是攻击者的 MAC 地址,可以在收到 ARP 请求广播后稍微延迟一段时间再发送一遍 ARP 应答。

(3) 由于各种操作系统对于 ARP 缓存处理实现的不同,一些操作系统(例如 Linux)会向缓存地址发非广播的 ARP 请求来要求更新缓存。在交换网络环境下,别的机器是不能捕获到这种缓存更新的,这就需要尽量阻止主机发送更新缓存消息,由 2.1 中的第 1 条分析知道,可以随意发送 ARP 应答包,这样攻击者就可以定时发送 ARP 应答包,不断的更新被攻击者的 MAC 缓存,阻止它主动发送非广播的 ARP 请求进行缓存更新。

2.4　路由攻击

在局域网环境下,ICMP 协议中有两种类型的报文可以修改局域网内主机上的非局域网 IP 地址与本地网关的映射关系。对于网络主机而言,这个映射关系是存放在路由表中的。要对指定机器上的路由表进行修改,就需要研究 ICMP 协议相关类型的报文。作者考虑的路由攻击有两种方式:

(1) ICMP 重定向差错伪装[7]

ICMP 协议包中类型 5 是重定向差错。重定向差错报文通常是由路由器发出的,通告网络主机有一个到达某一网络的更近的路由。重定向有两种类型:网络(指定 IP 网段)重定向与主机(指定 IP 地址)重定向,出于安全考虑,网络重定向已被取消,仅剩下了主机重定向。重定向消息的工作过程是这样的[6]:

网关(G1)从网络上接收到数据包后,检查路由表获得下一个网关(G2)的地址(X)。如果 G2 和指定的接收主机在同一网络上,则向源主机发送重定向消息,此消息建议发送主机直接将数据包发向网关 G2,因为网关 G2 更近,同时网关 G1 向前继续发送此数据包。

RFC 声明主机系统(路由器例外)必须遵循这个重定向,也就是说,在接收到由默认路由器发来的重定向 ICMP 包(其中重定向到的路由 IP 应该在同一局域网内)后,接收者会对系统的路由表进行更新。不像 ARP 缓存更新,路由表不存在过期问题。这样,攻击者就可以发送伪装重定向 ICMP 包,修改要攻击的主机的路由表。

因此,要进行重定向 ICMP 伪装是很简单的,只需按照报文格式,正确地填发一个主机重定向 ICMP 包即可,其中源 IP 为本地网关 IP,目的 IP 为被攻击者 IP。

(2) ICMP 路由器通告伪装

ICMP 协议中类型 9 与 10 是用来动态设置子网主机默认路由的,称为 ICMP 路由器发现报文,两个类型分别是 ICMP 路由器通告和请求报文。路由器通告报文由路由器发出,通告网络主机修改缺省路由。路由请求报文由主机发出,请求本网络的缺省路由。路由器发现报文的工作过程是这样的[6]:

路由器定期在所有广播或多播传送接口上发送通告报文,或者在监听到来自主机的请求报文后发

送路由器通告报文。主机在引导期间一般发送 3 份路由器请求报文,一旦接收到一个有效的通告报文,就停止发送请求报文。主机也监听来自相邻路由器的请求报文。这些通告报文可以改变主机的默认路由器。另外,如果没有接收到来自当前默认路由器的通告报文,那么默认路由器会超时。

由于网络主机只在引导时发送路由请求报文,这样就可以不必考虑路由请求报文的影响。可以使用以下方式来进行 ICMP 路由器通告伪装:

定期广播或多播伪造的 ICMP 路由器通告报文,伪造器通告报文中指定自己的 IP 为缺省路由 IP,并将优先级设到极大(一般设为 999 即可)。

在捕获到别的路由器发出的 ICMP 路由器通告报文后,立即发送伪造的通告报文,以保证局域网主机上的刚刚修改的缺省路由重新指向攻击者 IP。

2.5 各种协议伪装方式的特点分析

以上,作者对插入式主动捕包提出了 3 种协议伪装方法。由于每种伪装方法所使用的协议类型不同,那么协议差异必然会导致它们不同的特点:

(1)适用范围

由于 ARP 伪装进行的是本地 MAC 地址伪装,显然它可以伪装所有局域网内机器 IP,也就是说可以在局域网内任意两台机器的网络通信中插入 ;在对子网机器将网关 MAC 进行伪装后,可以在局域网内机器与局域网外机器间的网络通信中插入。

其余两种伪装均是路由攻击,因而只能在局域网内机器与局域网外的机器间的网络通信中插入。其中 ICMP 路由器通告伪装进行的是缺省网关伪装,可以在局域网内机器与局域网外的所有机器间的网络通信中插入 ;而对局域网机器进行 ICMP 重定向差错伪装,一次只能添加一个外网 IP 对应的路由,这就使得重定向伪装原则上只能在局域网内机器与局域网外的某些机器间的网络通信中插入。

值得注意的是有的网关对 IP 与 MAC 地址作了绑定,这时要进行插入攻击跨网段的主机间通信就十分困难了。

(2)各种伪装攻击的可靠性

只需对网络主机发送一个 ICMP 重定向包就可以成功地在网络主机上添加一条路由信息,而且除非人为修改,该路由信息不会丢失。所以,ICMP 重定向差错伪装可靠性较高。

路由器一般每间隔 450s 或 600s 就发送一次 ICMP 路由器通告报文,通告报文默认生命周期是 30min。通告报文使用广播或者组播方式,攻击者可以监听到网络上的路由器通告,然后发送伪装包,另外还可以定时发伪装包。所以,ICMP 路由器通告伪装实现稍微复杂一些,可靠性依赖于对路由器通告的捕包效率,一般而言,可靠性还是比较高的。

ARP 高速缓存中一般对完整表项设置的超时值为 20min。ARP 伪装与 ICMP 路由器通告伪装基本相似,攻击者可以监听到网络上的 ARP 请求,然后发送伪装包,另外也可以定时发伪装包。然而,由于存在非广播的 ARP 请求,这就使得 ARP 伪装的可靠性依赖于定时发送伪装包的间隔,这使得它的可靠性比 ICMP 路由器通告伪装稍有下降。

(3)简单的发现与防范攻击的方法

使用 arp 命令可以查询主机 ARP 缓存的内容,仔细的使用者可以发现 IP 是否与其真正 MAC 地址对应。也可以使用 arp 命令来设置静态 IP/MAC 表项,从而防止 ARP 伪装攻击。

使用 route 命令可以查询主机路由表内容,使用者可以很容易发现路由表的异常。大部分操作系统都没有提供简单的防止通过 ICMP 路由器通告以及重定向差错伪装来进行路由攻击的方法。

3 结束语

网络监听对黑客技术与安全管理都是十分重要的。本文提出了主动捕包的思想,打破了交换网络不能进行监听的传统概念。实现了一个使用底层协议伪装与 IP 转发相结合的插入式主动监听框架系统。研究和讨论了可进行插入攻击的几种底层协议伪装。最后,对这些协议伪装的适用范围及可靠性进行了分析和对比,并简单介绍了相应的防范措施。

参考文献:

[1] Claerhout B. *Phrack Magazine*, 1996, 7(48):14

[2] Crosbie M, Spafford G. Defending a computer system using autonomous agents. Technology Report 95-002, USA: Purdue Univ, 1996

[3] Plummer D C. An Ethernet address resolution protocol. RFC826, 1982

[4] Posterl J. Internet control message protocol. RFC792, 1981

[5] 贺龙涛. 网络安全技术与应用. 2001, (1):38

[6] Wright G R, Richard Stevens W. TCP/IP illustrated volume 1: the protocol. Addison Wesley Publishing Company, 1994

[7] Bellovin S M. *Computer Communication Review*, 1989, 19(2):32

(下转第 110 页)

GaN-based Semiconductor Materials and Its Applications in Short Wavelength Optoelectronic Devices

Gu Biao[*,**], Wang Sansheng[*,**], Xu Yin[*,**], Qin Fuwen[*,**], Dou Baofeng[*],
Chang Jiuwei[*], Deng Xiang[*], Yang Dazhi[**,***]
([*] Electrical Engineering and Applied Electronic Technology Department, Dalian University of Technology, Dalian 116024)
([**] National Key Laboratory of Material Modification by 3-Beams,
Dalian University of Technology, Dalian 116024)
([***] Material Science and Engineering Department, Dalian University of Technology, Dalian 116024)

Abstract

GaN have the characteristics of wide bandgap, high thermal conductivity, large electron saturation shift velocity and low dielectric constant. They have wide applications in those fields such as high brightness light emitting diodes, short wavelength laser diodes, high performance UV detector, and high temperature, high frequency, large power semiconductor devices. This paper introduces the known characteristics, growth methods, heterostructure and its applications in optoelectronic and microelectronic fields of GaN-based semiconductor materials, followed by our opinions of the remaining difficulties and analysis for further studies.

Key words: GaN, Materials characteristics, Epitaxy growth, Semiconductor devices

(上接第 4 页)

A Study on Active Sniffing in Switched LAN

He Longtao, Fang Binxing, Yun Xiaochun, Wang Lidong, Yuan Lin
(Dept. of Computer Science and Engineering, Harbin Institute of Technology, Harbin 150001)

Abstract

The sniffing in switched ether network is studied, and an active sniffing model is put forward, which combines spoofing on low layers of protocol stack and IP forwarding. Based on this model, some kinds of spoofing attacks and their characteristics are analyzed.

Key words: Switched LAN, Protocol spoofing, IP forwarding, Active sniffing