内部网未知计算机的防御策略研究

Defence Strategy for Intranet illegal Computer

王乐平　（上海市经济管理学校 200060）

摘要：本文基于以太网络通信的基本原理及智能网络设备的管理特性，探讨内部局域网中未知计算机或未知设备的发现方法，并给出快速有效阻止其网络通信的防御策略。

关键词：内网安全　网络防御策略　ARP　SNMP

1　问题的提出

计算机网络在各行各业中的应用已经相当普遍，内部网络所面临的安全问题日益突出。据 IDG 2004 年数据统计显示，80% 以上的网络安全事件来自于内部网络。随着网络规模的扩大及网络环境复杂性的提高，这一比例将有增无减。网络安全管理人员不经意的疏忽，便有可能造成重大的安全隐患和损失。例如，企业内部网络，由于网络系统升级或应用软件的外包开发，集成商的网络工程师根据用户的需要，安装调试内网的网络设备，或应用软件开发商在用户的内部网络开发、安装、调试应用软件等。这些外部人员因工作需要，经常携带以有线或无线方式接入内网的笔记本计算机，这些计算机若未经网络管理人员的许可接入内网，可能会有意（外部人员蓄意窃取、篡改内网敏感信息）或无意（笔记本计算机已感染了木马病毒等）对内部网络中的数据库、应用系统及网络设施等带来很大的安全威胁。如何及时地发现内部网络的这些安全威胁，并有效地进行自动防护，已经引起越来越多的网络安全管理人员的重视。

2　内网未知计算机的发现

2.1　未知计算机的判定

内部局域网中的计算机的每块网卡都拥有一个物理硬件地址，即 MAC 地址（48 bit），局域网中的数据链路层通信基于 MAC 地址，网络层通信基于 IP 地址。IP 地址分为静态 IP 和动态 IP 两种。在内部网络中，根据以下两种情况进行分析：

（1）在静态 IP 的局域网中。每台计算机都分配有一个固定的 IP 地址，可以对静态 IP 机器以绑定 IP、MAC 地址的方式来注册登记，将已注册登记过的计算机称为已知计算机。若网络中存在未注册登记过的 IP 和 MAC，如：新增机器、外部人员带入机器，或已注册登记但擅自修改了 IP 或 MAC 的机器等，可判定为未知计算机。

（2）在动态 IP 的局域网中。用 MAC 地址来注册登记内部网络的每一台已知计算机，若网络中存在未注册登记过的 MAC 地址，则具备此 MAC 地址的计算机可判定为未知计算机。

2.2　未知计算机的 ARP 通信

ARP（Address Resolution Protocol，地址解析协议）用于实现 IP 地址到 MAC 地址的映射。每台使用 ARP 的主机中，都保留有一个专用的内存区，通常称为 ARP 表（或 ARP 缓存），用来存放最近获取的 IP 地址与其相应 MAC 地址之间的映射关系。

当未知计算机需要与内网中的已知计算机通信时，若未知计算机的 ARP 表中没有已知计算机的 IP 与 MAC 的映射项，则未知计算机发送 ARP 请求广播包，此广播域中的所有已知计算机都可以收到该 ARP 请求包，并解析出此包中的目标 IP 地址，只有与目标 IP 地址相同的主机，才会回应给未知计算机一个 ARP 应答包，以使未知计算机获得已知计算机的 IP 和 MAC 的映射关系，并填入其 ARP 表中，随之进行后续的直接网络通信。

根据 RFC826 标准，ARP 以太包格式见表 1。

表 1　ARP 以太包

MAC header	ARP packet

MAC header(Ethernet transmission layer)见表 2。

表 2　MAC header

Ethernet destination address(48bit)	Ethernet sender address(48bit)
Protocol type (16bit)	

ARP packet(Ethernet packet data)见表 3。

表 3　ARP packet

Hardware type(16bit)	Protocol type(16bit)
Hardware address length(8bit)	Protocol address length(8bit)
Opcode(16bit)	
Source hardware address …	
Source protocol address …	
Destination hardware address …	
Destination protocol address …	

下面给出的一个实例是当一台具有静态 IP 的计算机连接到内部以太网时，发出的 ARP 请求包：其中 MAC header 实例见表 4。

表 4　MAC header 实例

FF:FF:FF:FF:FF:FF	00:07:E9:0A:1E:4F
0x0806(ARP)	

ARP packet 实例见表 5。

表 5　ARP packet 实例

0x0001(Ethernet)	0x0800(IP)
0x06	0x04
0x0001(ARP Request)	
00:07:E9:0A:1E:4F	
192.168.10.38	
00:00:00:00:00:00	
192.168.10.38	

2.3　未知计算机的发现方法

根据上述 ARP 工作原理可知，当一台具有静态 IP 地址的计算机在开机状态接入网络，或已接入网络再开机时，都会主动发送 ARP 请求类型的以太广播包，以通知在同一广播域中的其他在线计算机，这些机器在收到其 ARP 请求包后，将其 IP 和 MAC 地址存入自己的 ARP 表中，以便直接进行网络通信。

在此广播域中的每台已知计算机里预装安全节点模块，该模块用以接收刚接入内部局域网的计算机发出的 ARP 包，对其解析，得到 IP 和 MAC 地址。再以此 IP 和 MAC 地址作为关键字，查询已注册登记的内网计算机资源库，若资源库中没有此计算机的 IP 和 MAC 地址信息，则其为未知计算机。具有 IP 地址的设备都可以用这种方法来发现。

工作流程如图 1 所示。

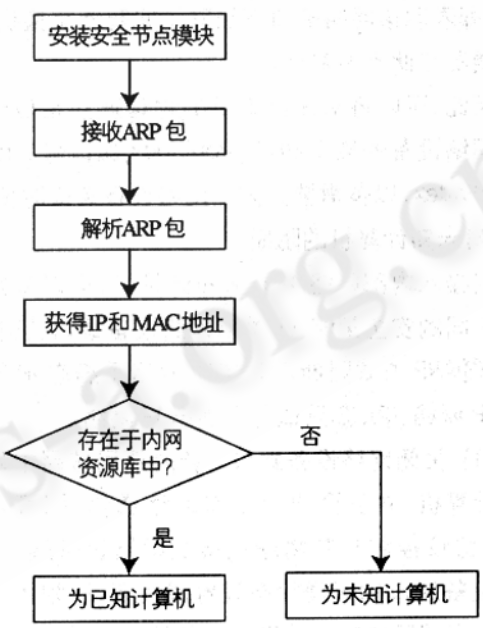

图 1　工作流程

3　对未知计算机的防御

目前，网络管理普遍使用 SNMP 协议(Simple Network Management Protocol，简单网络管理协议)，SNMP 协议工作在 ISO/OSI 模型的第七层(应用层)。该协议用于管理网络设备，提供了一种从网络上的设备中收集网络管理信息的方法，能够监控连接到网络

上的智能设备的运行状态和数据变化情况。利用SNMP协议,对网络设备状态的监控主要通过查询及设置这些设备中的数据库,即MIB(Management Information Base,管理信息库)中相应对象的内容来完成。

3.1 对未知计算机的定位

当发现并得到未知计算机的IP和MAC地址后,根据此MAC地址,通过SNMP协议,使用get命令可以读取智能网络设备(具有IP地址,如:智能网络交换机、路由器)MIB中的网络端口MAC列表,其对应的MIB对象为BRIDGE-MIB:dot1dTpFdbAddress,OID(Object Identifier,对象识别符)为1.3.6.1.2.1.17.4.3.1.1。

若此计算机的MAC地址唯一存在于某网络设备的某个端口MAC列表中,则说明此计算机连接在该网络端口上;若此计算机的MAC地址不唯一存在于某网络设备的某个端口MAC列表上,则该网络端口为级联端口,即表明该网络端口下级联了非智能交换机设备,这种情况在此不多赘述。

至此,可以将未知计算机的物理连接定位于某台智能网络设备的某个端口(PortIndex端口号)上,即IP + PortIndex,以备需要关闭此网络设备端口时使用。

3.2 对未知计算机的阻断

对接入内部网络中的未知计算机,可以分别采用三种不同的安全策略:①关闭网络设备端口;②拒绝IP访问;③ARP方式阻断。其中①适用于静态IP网络和动态IP网络,②、③只适用于静态IP网络。

(1) 关闭网络设备端口。若内部局域网中发现了未知计算机,并且需要阻止其网络通信,则可以通过SNMP协议控制与其物理连接的网络设备端口,将该网络设备端口的管理状态设置成关闭,以阻止未知计算机与局域网中其他计算机的通信。其对应的MIB对象为IF-MIB:ifAdminStatus,OID为1.3.6.1.2.1.2.2.1.7,OID属性为可读写(Read / Write)。用set命令将其对应的端口值设置为1,则端口打开;设置为2,则端口关闭。

当关闭了已定位的未知计算机所连接的网络设备端口后,间隔一段时间,由内部网络中的安全控制模块再打开该网络设备端口,以检测未知计算机是否仍然在线,若在线,则继续关闭该端口;若离线,则无需关闭该端口。

若未知计算机的网络连线更换到其他的网络设备端口上,使用上述方法,同样可以及时被发现和被阻断。

这种防御方式的优点是速度快,可靠性高。缺点是对内网中连接了非智能网络设备的端口部分不适用。

(2) 拒绝IP访问。当在内部网络中发现了未知计算机后,由安全控制模块将此未知计算机的IP地址分发给所有在线的已知计算机中的安全节点模块,并且将此IP列入安全节点模块的"拒绝IP列表",以拒绝与该未知计算机通信。

若发现未知计算机已离线,则安全控制模块通知所有在线的已知计算机,将此IP地址从各自的安全节点模块"拒绝IP列表"中删除。

这种防御方式的优点是速度快,可靠性高。缺点是对动态IP网络不适用。

(3) ARP方式阻断。当内部网络中发现了未知计算机后,安全控制模块立即通知与未知计算机在同一网段的已知计算机发送ARP阻断包,以阻断未知计算机在内部网络的通信。ARP阻断包由ARP应答以太包组成,其目标MAC和目标IP分别为内网已知计算机的MAC和IP,而源MAC为随机数,IP为未知计算机的IP。

这种防御方式的优点是适用于非智能网络设备组成的动态IP网络,缺点是可靠性不够高。

4 结束语

本文所述的网络防御策略,可以通过软件来实现,自动地完成未知计算机或未知IP设备的发现,并且及时加以通信阻断,以降低网络系统的安全风险。另外,也可结合IEEE 802.1x标准,使用网络接入数字认证技术,进一步加强网络接入的可信度。提高内部网络的安全水平,还需要技术与管理相结合,除综合采用多种安全技术(如入侵检测、防火墙、防病毒等)外,应该不断加强用户的安全意识、制定并执行严格健全的安全管理制度。

参考文献

1 Laura A. Chappell,Ed Tittel 著, TCP/IP 协议原理与应用,清华大学出版社。
2 Sean Convery 著, 网络安全体系结构,人民邮电出版社。
3 李卫 著, 计算机网络安全与管理,清华大学出版社。