文章编号：1005-8451（2009）09-0044-04

基于TCP/IP模型的企业网络安全威胁和对策研究

贾迎芳[1]，解亚龙[2]
（1.中国水电建设集团 房地产有限公司，北京 100048；
2.中国铁道科学研究院 电子计算技术研究所，北京 100081）

摘 要：企业信息化程度越来越高，信息安全成为关乎企业生命的重要因素，按照TCP/IP网络模型分析企业信息系统面临的各个层面的安全威胁，研究安全策略、技术手段和管理制度防范这些威胁。

关键词：TCP/IP模型；网络安全；信息系统；安全策略
中图分类号：TP393 **文献标识码**：A

Study on enterprise network security threats and solution based TCP/IP Model

JIA Ying-fang[1], XIE Ya-long[2]
(1.Sinohydro Realestate Co. Ltd, Beijing 100048, China;
2. Institute of Computing Technology, China Academy of Railways Sciences, Beijing 100081, China)

Abstract: With the development of information technology, network security played more and more important role in an enterprise network. It was given a comprehensive analysis about security threats of the enterprise network by the TCP/IP reference model. Based on the above analysis, the security strategy against threats was presented to guarantee the network security.

Key words: TCP/IP model; network security; Information System; security solution

由于企业内部信息网络运行着大量需要保密的数据和信息，如果系统的安全性被破坏，造成重要信息的丢失，势必会产生很大的损失。因此，构建安全的网络安全保障体系是企业信息化建设中不可忽视的内容之一。本文着重以TCP/IP模型为参考，分析各层网络面临的威胁，提出防范这些威胁的对策。

1 企业信息网络的安全现状

目前，国内企业相继实施了企业内部的信息化系统，如OA办公系统、邮件系统和信息发布系统等，这些信息化系统在企业的生产和经营活动中发挥着越来越重要的作用，整个企业的经营活动都离不开信息化系统的支撑；但是企业网络面临的威胁和风险也越来越严重，今天的企业信息网络面临的威胁分布于TCP/IP模型的每一个层面上，如图1。

1.1 数据链路层威胁

根据安全威胁的特征来分析，来自第2层的（数据链路层）攻击主要包括：MAC地址泛滥攻击、DHCP服务器攻击、ARP欺骗、IP/MAC地址欺骗。

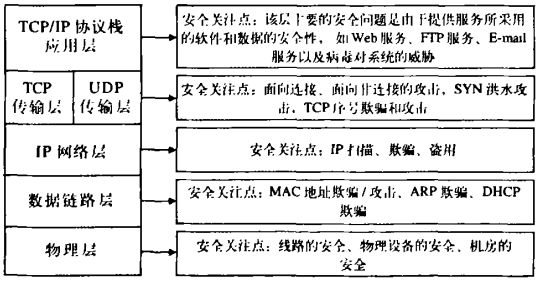

图1 基于TCP/IP模型的企业信息系统面临的安全威胁

1.1.1 MAC地址泛滥攻击

交换机会主动学习客户端的MAC地址，建立、维护端口和MAC地址的对应表，以此建立交换路径，这个表就是CAM表。MAC/CAM攻击是指黑客利用攻击工具发送大量带有虚假源MAC地址的数据包，这些新MAC地址被交换机CAM学习，很快塞满MAC地址表，这时发往新目的MAC地址的数据包就会被广播到交换机的所有端口，交换机就会像HUB一样工作，黑客则可以利用Sniffer工具监听所有端口的数据流量。此类攻击不仅造成安全性的破坏，同时大量的广播包降低

收稿日期：2009-07-22
作者简介：贾迎芳，工程师；解亚龙，助理研究员。

了交换机的性能。

1.1.2　ARP欺骗

以太网的主机需要根据MAC地址进行通讯，ARP协议就是负责将32 bit的IP地址解析成48 bit的MAC地址；在每台主机上都有一个ARP的高速缓存，这个缓存里存储了最近的IP地址到MAC地址的映射记录。由于ARP协议的设计弱点，ARP协议是建立在局域网中各个主机相互信任的基础上的，而且ARP协议是无状态的协议，任何主机即使在没有请求的情况下也可以做出应答，由于主机之间相互信任，因此ARP应答也无需认证，只要是来自局域网内的ARP应答，就会将其中的MAC/IP更新到本机的高速缓存中。ARP攻击的核心就是向目标主机发送伪造的MAC应答，并使目标主机接受应答中伪造的IP/MAC映射对，以此来更新目标主机的缓存。目前在企业网内部发生ARP欺骗的攻击很普遍，造成大面积断网，影响企业正常的生产运营。

1.2　网络层威胁

企业网络规划需要划分VLAN，多数网络管理者在划分VLAN之后，没有对VLAN之间的用户实施访问控制，这就为下面的网络层攻击提供了可能：

（1）一个网段用户的蠕虫病毒攻击可以直接波及所有网段，造成内网拥塞或广泛传播；

（2）基于源地址欺骗的攻击方式在网络中通行无阻。

DMZ是指“Demilitarized Zone”的缩写，中文称为“隔离区”、也称为“非军事化区”。它是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题而设立的一个非安全系统与安全系统之间的缓冲区。这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内通常放置一些必须公开的服务器设施，如Web服务器、公共DNS服务器等。在防火墙或路由器上设置DMZ区域有助于网络边界安全，但据调查很多企业网络边缘无DMZ区域，仅仅通过防火墙或路由器配置访问控制列表来限制互联网对企业内开放资源的访问，一旦内部主机出现安全问题被攻击获得管理员权限，内部主机就可以作为跳板直接对企业内用户、主机展开攻击。近几年来服务器遭到攻击的事件屡有发生，网络出口设计上的不尽合理带来的安全隐患是巨大的。

1.3　传输层威胁

TCP是传输层协议设计用于提供可靠的IP包传送，TCP使用了多个标记选项及序列号来重组网络包，攻击者可以利用基于TCP半连接的SYN Flooding攻击，让TCP无法完成3次握手过程，这就是当前流行的Dos攻击，并且危害程度相当大，并且没有办法彻底防范。

Dos攻击就是用超出被攻击目标处理能力的数据包消耗可用系统及带宽资源致使其瘫痪的一种攻击手段。传统的Dos攻击一般是由黑客控制单台机器直接向目标主机发起攻击；DDos是一种基于Dos的特殊形式的拒绝服务攻击，是一种分布的、协作的大规模攻击方式。攻击者一般不是直接发起攻击，而是通过控制很多傀儡机（被黑客入侵过或可间接利用的主机）向攻击目标发送大量合法或看似合法的网络包，搞“狼群”战术，从而造成网络阻塞或服务器资源耗尽而导致拒绝服务。

被DDos攻击时的现象有：（1）被攻击主机上有大量等待的TCP连接；（2）网络中充斥着大量无用的数据包，源地址为假；（3）制造高流量无用数据，造成网络拥塞，使受害主机无法正常与外界通讯；（4）利用受害主机提供的服务或传输协议上的缺陷，反复高速地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，严重时会造成系统死机。如图2。

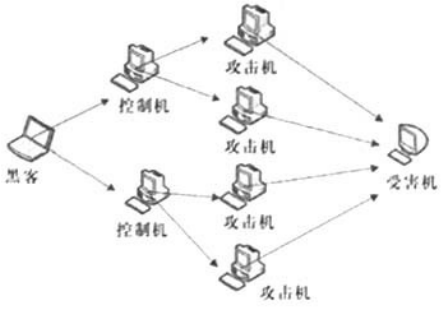

图2　DDos攻击示意图

1.4　应用层威胁

网络上常见的攻击有缓冲区溢出攻击、特洛伊木马攻击、各种蠕虫病毒、间谍软件和网络钓鱼等应用层威胁。

缓冲区溢出是一种系统攻击的手段，通过往程序的缓冲区写入超出其长度的内容，造成缓冲

区的溢出，从而破坏程序的堆栈，使程序转而执行非预期指令，以达到攻击的目的。目前利用缓冲区溢出的攻击行为已经相当普遍。

特洛伊木马攻击是指那些伪装成正常的程序，或者隐藏在正常程序中，诱导系统用户执行从而取得控制系统或者破坏系统的权限的一种常用攻击手法，在网络攻击中极为常见。

2 企业网络的安全策略

针对上面提到的各种网络威胁，分别讨论各层的安全策略。

2.1 物理层策略

从物理环境角度讲,地震、水灾、火灾和雷击等环境事故，电源故障，人为操作失误或错误，电磁干扰等都对信息系统的安全构成威胁，保证计算机信息系统各种设备的物理安全是保障整个网络系统安全的前提。物理层的安全设计应该从3个方面考虑：环境安全，设备安全，线路安全。采取的措施包括：机房屏蔽，电源接地，传输加密等。

2.2 数据链路层策略

利用VLAN技术将内部网络分成若干个安全级别不同的子网，从而实现内部一个网段与另一个网段的隔离，有效防止某一网段的安全问题在整个网络传播。因此，对于一个网络中某个网段比另一个网段更受信任，或某个网段的敏感度更高，将可信网段与不可信网段划分在不同的VLAN中，即可限制局部网络安全问题对全网造成影响。根据企业网络情况划分VLAN的数量尽量多一些，降低单点或小范围用户的网络行为对整网所造成的影响。

由于单纯依靠IP或MAC来建立信任关系是不安全的，理想的安全关系建立在IP加MAC的基础上，因此企业网络要求绑定IP地址和MAC地址。并且在企业网络实施802.1X用户接入认证技术，防止非授权用户接入网络和使用网络。

2.3 网络层策略

网络层的安全防护主要依赖于访问控制列表(Access Control List)的使用，ACL是路由器接口的指令列表，用来控制端口进出的数据包。ACL可以限制网络流量、提高网络性能，提供了网络安全访问的基本手段。ACL可以在路由器或3层交换机接口处决定哪种类型的通信流量被转发或被阻塞；例如，用户可以允许E-mail通信流量被路由，拒绝所有的Telnet通信流量。使用访问控制列表(ACL)来控制VLAN之间的访问，将内网用户间的访问做必要的隔离和限制；利用ACL防范假冒源IP地址攻击。

在内网和外网之间部署防火墙设备和入侵检测设备是目前常用的保证内网安全，隔离外部威胁的一个安全手段。

防火墙是实现网络信息安全的最基本设施，采用包过滤或代理技术使数据有选择地通过，有效监控内部网和外部网之间的任何活动，防止恶意或非法访问，保证内部网络的安全。因此，在各中心网络边界，以及内网与Internet边界都应安装防火墙，并实施相应的安全策略控制。另外，根据对外提供信息查询等服务的要求，为了控制对关键服务器的授权访问，应该把对外公开服务器集合起来划分为一个专门的服务器子网，设置防火墙策略来保护对它们的访问。

入侵检测技术(IDS)是通过从计算机网络系统中若干关键节点收集信息并加以分析，监控网络中是否有违反安全策略的行为或者是否存在入侵行为，它能提供监视、攻击识别和反攻击等多项功能，并采取相应的行动如断开网络连接、记录攻击过程、跟踪攻击源和紧急告警等，是安全防御体系的一个重要组成部分。

2.4 应用层策略

病毒是系统最常见、威胁最大的安全隐患，建立一个全方位的病毒防范系统是信息网络体系建设的重要任务。要实现网络环境下的病毒防治，仅靠单机版的杀毒软件是不可能的，必须安装网络版的杀毒软件，这样才能实现杀毒软件的远程安装、智能升级、远程报警、集中管理和分布查杀病毒的功能。另外还必须加强管理，提高使用人员的防毒意识和相应知识。

部署上网行为管理系统、电子邮件过滤等内容管理系统，根据内容的分类进行访问控制，杜绝色情、反政府、邪教等非法、不健康内容的接触和传播。阻断对含有病毒、木马等各种恶意代码，以及内容欺诈网站的访问，解决病毒和恶意代码通过电子邮件进入内网传播的问题。

2.5 系统层策略

系统层安全主要是指服务器的安全。对于关键的服务器和工作站应该进行定期升级。控制用户对服务器的非法访问，防止服务器的数据被修改、删除或破坏。服务器访问控制主要包括制定相应的管理措施，防止非法用户直接操作服务器的控制台；操作完成后及时锁定账户；停止服务器上不必要的服务软件的运行；减少服务器上安装应用软件的数量；对服务器的各种操作进行日志记录，并定期审查日志，及时发现攻击迹象；限制服务器登录时间；对服务器数据进行定期的备份等措施。

2.6 网络安全管理

在网络安全中，除了采用上述技术措施之外，加强网络的安全管理，制定有关规章制度，对确保网络的安全和可靠地运行，起到十分有效的作用。网络的安全管理策略包括：确定安全管理等级和安全管理范围；制订有关网络操作使用规程和人员出入机房管理制度；制定网络系统的维护制度和应急措施等。

3 企业网络安全的实施实例

网络安全涉及到TCP/IP网络模型的每一个层面，网络安全的规划和设计要从系统的角度来考虑，图3是一个典型的企业网络的拓扑方案。从层次化的角度，企业网络可以分为接入层安全控制区、网络核心安全控制区、网络边缘控制区（DMZ）和服务器安全区，各区域的安全设置基本如下：

（1）接入层安全控制区：为防范2层的攻击，主要部署应用DHCP侦听、动态ARP防护、端口安全和802.IX接入认证等安全技术，这几种技术通常关联使用；为降低大量广播数据给网络带来的危害，在接口上开启广播报文限制；

（2）网络核心安全控制区：主要使用访问控制列表（ACL）来控制VLAN之间的访问，将内网用户间的访问做必要的隔离和限制；利用ACL防范假冒源IP地址攻击；

（3）服务器安全区：使用严格的访问控制限制内外网对服务器网段的访问，应用VLAN技术，进一步控制服务器之间不必要的访问；在应用层面部署漏洞扫描服务，定期对重要网段进行系统漏洞监测；部署网络防病毒软件，及时升级病毒库；

（4）网络边缘安全区：使用DMZ区域、内网和外网单向或双向的访问控制，禁止DMZ区域对内网的访问和外网对内网的直接访问；加强VPN服务的用户认证与资源访问的管理，避免门户大开现象的发生；

（5）部署上网行为管理系统、电子邮件过滤等内容管理系统，根据内容的分类进行访问控制；

（6）主机安全区：为及时安全地升级补丁，通过脚本为用户做病毒库升级服务指向，在全网推广杀毒网络版客户端的部署；

（7）在整个网络采用网络分析软件进行网络的流量监控和分析，对掌握整个网络情况进行安全隐患的分析和预警相当有效。

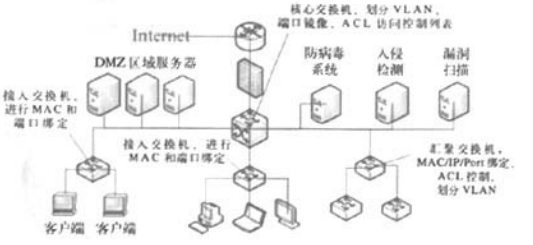

图3　典型的企业信息网络拓扑图

4 结束语

由于网络协议的开放性，使得计算机网络的接入非常容易，正是在这样的背景下，威胁网络安全的因素就非常多。本文按照TCP/IP网络模型，分析了各层网络面临的威胁，采用合适的网络安全技术和安全策略，从技术手段和行政管理上来防止这些威胁，为常见的企业网络安全威胁提供了一个参考蓝本和解决方案。

参考文献：

[1] 夏光封.校园网络安全体系研究与部署设计[M].合肥：合肥工业大学，2003.

[2] 陆余良，张永，刘克胜.ARP协议在局域网类型探测中的应用[J].计算机工程，2004，30（1）：195-197.

[3] 冯登国.网络安全原理与技术[M].北京：科学出版社，2003.

[4] 顾巧论.计算机网络安全[J].计算机学报，2003，5（14）：27-31.