企业网络信息安全

张　波
（云南烟草教育培训中心）

摘　要： 随着信息技术的迅猛发展，很多业务和数据都通过网络来传递和处理，因此对于网络安全提出了更高更严格的需求，尤其对于INTERNET这样的公众网络，只能从自身技术范畴考虑来加强对于网络安全的防范，从而保证业务和数据的保密和安全。对企业网络的外部安全威胁进行了分析,试图根据企业网络在局域网、广域网和外部网络的划分来分别针对其组网特点分析容易产生的安全问题，并提出一些解决方法。通过网络分段、以交换式集线器代替共享式集线器、划分VLAN的方法建设局域网；使用加密技术、VPN技术、身份认证技术建设广域网；依靠防火墙技术、入侵检测技术和网络防病毒技术解决与外部网络连接时产生的网络安全问题。

关键词： 网络安全；网络安全的外部威胁；安全控制

1　企业网络安全所受的外部威胁

网络信息技术的发展给企业单位带来了革命性的改革和开放，使得他们能够利用网络技术提高办事效率和市场反应能力，通过网络，他们可以从异地取回重要的数据，同时又要面对网络开放带来的数据安全的新挑战和新危险。对企业网络的最大的危险来自于外部威胁。

外部安全漏洞有多种形式。

a.使用IP欺骗的TCP序列号攻击。

在大多数UNIX实现中，存在着一个可以窃取TCP连接的安全漏洞。当TCP连接正常建立时，用户先发出一个TCP连接请求，服务器用一个含有初始序列号的回答报文确认用户的请求。对这个序列号没有特殊的要求，只要惟一即可。客户端收到回答后，再确认一次，就建立连接。TCP协议规范要求每秒更换序列号25万次，但大多数实现的更换频率远小于此，而且下一个更换数字往往是预知的。正是这种预知服务器初始序列号的漏洞，使得攻击者窃取TCP连接成为可能。从而发起攻击、偷窃或破坏数据。

b.利用源路径选项的安全漏洞进行攻击。

源主机可以使用IP源路径选项，强制报文通过一个特定的路径到达目的主机。这样的报文可以用来攻陷防火墙和欺骗主机。攻击者可以传送一个具有内部主机地址的源路径报文，服务器会相信这个报文并对攻击者发出回答报文。攻击者可以进行攻击。

c.利用路由信息协议（RIP）的安全漏洞进行攻击。

RIP协议用于在局域网中广播路由信息。通常，该信息是不受检查而被接受的。攻击者可以发送伪造路由信息给目的主机和路径上的所有网关，通过建立一条路由，使得所有源和目的的主机的数据包全部到达攻击者的主机上，这样攻击者就可以假冒该主机，检查或改变数据。

d.服务失效攻击（DoS,Denial of Service）。

服务失效攻击又称为拒绝服务攻击（DoS,Denial of Service），其攻击的基本特点是使系统资源耗尽。当对系统

资源的有效请求大大的超过资源的负载能力时，就会造成拒绝服务攻击。

以下是几种常见的服务失效攻击。

（1）邮件炸弹和邮件列表连接。

邮件炸弹是一种简单有效的侵扰工具，它反复传给目标接收者相同的信息，用这些垃圾拥塞目标的邮箱，使其无法正常工作。邮件列表将目标地址同时注册到几十个（甚至成百上千个），产生无数封邮件对目标进行攻击。两种攻击可以使目标系统的网络性能和服务器性能下降。

（2）广播风暴（Broadcast Flood）。

由于UDP没有流量控制，所以会被作为服务失效攻击的手段。攻击者向某个UDP服务器发送大量的UDP报文，将引起网络拥塞和主机性能下降，引起这个服务器的服务失败。

（3）Ping/ICMP淹没。

ICMP是一种消息和错误检测协议，用来在INTERNET上传送信息。Ping命令常常发送ICMP包，目的是检查指定的计算机是不是在网上。当很多包同时发送到一个IP地址的时候，服务器可能处理不过来，导致服务器速度放慢，最终由于Ping过时而中断连接。

（4）Smurf攻击。

Smurf攻击是一种影响整个服务器提供者或者整个网段的ICMP淹没。ICMP消息发送到一个广播地址，导致该子网上的计算机产生响应。当ISP被smurf掉后，所有的连接都慢下来，所有用户最终失去连接。

（5）Ping of Death。

Ping of Death 是一种稍稍复杂的攻击方式，它利用了网络最大传输单元（MTU）的限制。MTU取决于媒介和网络体系结构。如果包的大小超过MTU，它必须分割成几个较小的块，然后在目的地端重新组合起来。封装ICMP回执请求的IP包只能限于65535八位组。攻击者可以发送一个包，该包超过了回执请求数据段所允许的八位组个数。当目标计算机企图重组包的时候，它就崩溃了。

（6）SYN攻击。

攻击者可以使用TCP同步序列打乱通信。通信时由一个称为TCP三步握手的进程通过TCP建立会话。SYN攻击者发出大量的会话请求（同时使用一个欺骗性的IP地址），接受端的计算机将请求放在一个队列里，等待握手过程完成。通过不断排队使队列保持满的状态，攻击者阻止了其他会话请求的建立，导致合法用户无法连接服务器。

e.分布式拒绝服务（DDOS,Distributed Denial of Service）。

分布式拒绝服务攻击方法是攻击中继计算机，并偷偷在其上安装软件，作为攻击平台的一部分。虽然攻击者仍然是一个，但它可以使用代理来同时发起攻击。使DoS的威力数十倍的增加，危害性更大。

f.计算机病毒和蠕虫。

计算机病毒是一种程序，它可以在计算机之间复制和扩散，有些病毒是致命的，有些只是烦人而已。蠕虫是一种恶意的病毒，它在计算机上复制自己并破坏文件。蠕虫经常潜伏在电子邮件附件中，如可执行文件，文档包含的宏，或者页面脚本中。

g.特洛伊木马程序。

特洛伊木马程序将自己伪装成其他程序以取得信息。然后就可以利用用户名和密码取得对系统的访问。

2　企业网络安全的解决办法

鉴于目前的局域网是组网技术的主要方式，应用范围越来越广，同时，其安全性也日益突出，特对此论述几点看法如下。

2.1 安全问题

局域网基本上都采用以广播为技术基础的以太网，任何两个节点之间的通信数据包，不仅为这两个节点的网卡所接收，也同时为处在同一以太网上的任何一个节点的网卡所截取。因此，黑客只要接入以太网上的任一节点进行侦听，就可以捕获发生在这个以太网上的所有数据包，对其进行解包分析，从而窃取关键信息，这就是以太网所固有的安全隐患。

事实上，Internet上许多免费的黑客工具，如SATAN、ISS、NETCAT等等，都把以太网侦听作为其最基本的手段。

2.2 解决办法

当前，局域网安全的解决办法有以下几种：

a.网络分段。

网络分段通常被认为是控制网络广播风暴的一种基本手段，但其实也是保证网络安全的一项重要措施。其目的就是将非法用户与敏感的网络资源相互隔离，从而防止可能的非法侦听，网络分段可分为物理分段和逻辑分段两种方式。

目前，局域网大多采用以交换机为中心、路由器为边界的网络格局，应重点挖掘中心交换机的访问控制功能和三层交换功能，综合应用物理分段与逻辑分段两种方法，来实现对局域网的安全控制。例如：普遍使用的DEC MultiSwitch 900的入侵检测功能，其实就是一种基于MAC地址的访问控制，也就是上述的基于数据链路层的物理分段。

b.以交换式集线器代替共享式集线器。

对局域网的中心交换机进行网络分段后，以太网侦听的危险仍然存在。这是因为网络最终用户的接入往往是通过分支集线器而不是中心交换机，而使用最广泛的分支集线器通常是共享式集线器。这样，当用户与主机进行数据通信时，两台机器之间的数据包（称为单播包Unicast Packet）还是会被同一台集线器上的其他用户所侦听。一种很危险的情况是：用户TELNET到一台主机上，由于TELNET程序本身缺乏加密功能，用户所键入的每一个字符（包括用户名、密码等重要信息），都将被明文发送，这就给黑客提供了机会。

因此，应该以交换式集线器代替共享式集线器，使单播包仅在两个节点之间传送，从而防止非法侦听。当然，交换式集线器只能控制单播包而无法控制广播包（Broadcast Packet）和多播包（Multicast Packet）。所幸的是，广播包和多播包内的关键信息，要远远少于单播包。

c.VLAN的划分。

为了克服以太网的广播问题，除了上述方法外，还可以运用VLAN（虚拟局域网）技术，将以太网通信变为点到点通信，防止大部分基于网络侦听的入侵。

目前的VLAN技术主要有三种：基于交换机端口的VLAN、基于节点MAC地址的VLAN和基于应用协议的VLAN。基于端口的VLAN虽然稍欠灵活，但却比较成熟，在实际应用中效果显著，广受欢迎。基于MAC地址的VLAN为移动计算提供了可能性，但同时也潜藏着遭受MAC欺诈攻击的隐患。而基于协议的VLAN，理论上非常理想，但实际应用却尚不成熟。

在集中式网络环境下，我们通常将中心的所有主机系统集中到一个VLAN里，在这个VLAN里不允许有任何用户节点，从而较好地保护敏感的主机资源。在分布式网络环境下，我们可以按机构或部门的设置来划分VLAN。各部门内部的所有服务器和用户节点都在各自的VLAN内，互不侵扰。

VLAN内部的连接采用交换实现，而VLAN与VLAN之间的连接则采用路由实现。目前，大多数的交换机（包括国内公司生产的低端产品，如华为、Dlink等）都支持RIP和OSPF这两种国际标准的路由协议。如果有特殊需要，必须使用其他路由协议（如CISCO公司的EIGRP），也可以用外接的多以太网口路由器（目前CISCO路由器在企业网络中占绝大多数）来代替交换机，实现VLAN之间的路由功能。当然，这种情况下，路由转发的效率会有所下降。

无论是交换式集线器还是VLAN交换机，都是以交换技术为核心，它们在控制广播、防止黑客上相当有效，但同时也

给一些基于广播原理的入侵监控技术和协议分析技术带来了麻烦。因此，如果局域网内存在这样的入侵监控设备或协议分析设备，就必须选用特殊的带有SPAN（Switch Port Analyzer）功能的交换机。这种交换机允许系统管理员将全部或某些交换端口的数据包映射到指定的端口上，提供给接在这一端口上的入侵监控设备或协议分析设备。

2.3 广域网安全

广域网的应用日益广泛，由于广域网大多采用公网来进行数据传输，信息在广域网上传输时被截取和利用的可能性就比局域网要大得多。如果没有专用的软件对数据进行控制，只要使用Internet上免费下载的“包检测”工具软件，就可以很容易地对通信数据进行截取和破译。

因此，必须采取手段，使得在广域网上发送和接收信息时能够保证：

(1)除了发送方和接收方外，其他人是无法知悉的（隐私性）；

(2)传输过程中不被篡改（真实性）；

(3)发送方能确知接收方不是假冒的（非伪装性）；

(4)发送方不能否认自己的发送行为（不可抵赖性）。

2.4 广域网安全解决办法

为了达到以上安全目的，广域网通常采用以下安全解决办法：

a.加密技术。

加密型网络安全技术的基本思想是不依赖于网络中数据通道的安全性来实现网络系统的安全，而是通过对网络数据的加密来保障网络的安全可靠性。数据加密技术可以分为三类，即对称型加密、不对称型加密和不可逆加密。

其中不可逆加密算法不存在密钥保管和分发问题，适用于分布式网络系统，但是其加密计算量相当可观，所以通常用于数据量有限的情形下使用。计算机系统中的口令就是利用不可逆加密算法加密的。近年来，随着计算机系统性能的不断提高，不可逆加密算法的应用逐渐增加，常用的如RSA公司的MD5和美国国家标准局的SHS。在企业网络中广泛使用的Cisco路由器，有两种口令加密方式：Enable Secret和Enable Password。其中，Enable Secret就采用了MD5不可逆加密算法，因而目前尚未发现破解方法（除非使用字典攻击法）。而Enable Password则采用了非常脆弱的加密算法（即简单地将口令与一个常数进行XOR与或运算），目前至少已有两种破解软件。因此，最好不用Enable Password。

b.VPN技术。

VPN（虚拟专网）技术的核心是采用隧道技术，将企业专网的数据加密封装后，透过虚拟的公网隧道进行传输，从而防止敏感数据的被窃。VPN可以在Internet、服务提供商的IP、帧中继或ATM网上建立。企业通过公网建立VPN，就如同通过自己的专用网建立内部网一样，享有较高的安全性、优先性、可靠性和可管理性，而其建立周期、投入资金和维护费用却大大降低，同时还为移动计算提供了可能。因此，VPN技术一经推出，便红遍全球。

但应该指出的是，目前VPN技术的许多核心协议，如L2TP、IPSec等，都还未形成通用标准。这就使得不同的VPN服务提供商之间、VPN设备之间的互操作性成为问题。因此，企业在VPN建网选型时，一定要慎重选择VPN服务提供商和VPN设备。

c.身份认证技术。

对于从外部拨号访问总部内部网的用户，由于使用公共电话网进行数据传输所带来的风险，必须更加严格控制其安全性。一种常见的做法是采用身份认证技术，对拨号用户的身份进行验证并记录完备的登录日志。较常用的身份认证技术，有Cisco公司提出的TACACS＋以及业界标准的RADIUS。其中Cisco公司的CiscoSecure ACS V2.3软件可进行RADIUS身份认证。

2.5 外部网安全

这里所指外部网建设，通常指与Internet的互联及与外部企业用户的互联两种。无论哪一种外部网，都普遍采用基于TCP／IP的Internet协议族。Internet协议族自身的开放性极大地方便了各种计算机的组网和互联，并直接推动了网络技术的迅猛发展。但是，由于在早期网络协议设计上对安全问题的忽视，以及Internet在使用和管理上的无政府状态，逐渐使Internet自身的安全受到威胁，黑客事件频频发生。

对外部网安全的威胁主要表现在：非授权访问、冒充合法用户、破坏数据完整性、干扰系统正常运行、利用网络传播病毒、线路窃听等。

外部网安全解决办法主要依靠防火墙技术、入侵检测技术和网络防病毒技术。在实际的外部网安全设计中，往往采取上述三种技术（即防火墙、入侵检测、网络防病毒）相结合的方法。例如在外部网设计中，选用NAI公司最新版本的三宿主自适应动态防火墙Gauntlet Active Firewall。该防火墙产品集成了Gauntlet Firewall、CyberCop Scanner、CyberCop Monitor、WebShield for Firewall等套件，将防火墙技术、入侵检测技术与网络防病毒技术融为一体，紧密结合，相得益彰，性价比比较高。

以上从几个方面浅论了对局域网安全的认识，结合工作，网点数量日益扩大，业务范围不断扩充，并根据技术发展不断改进。

作者简介： 张　波，男，教育信息专业本科毕业，现任云南烟草教育培训中心讲师，曾发表论文《析网络多媒体教学》、《网络安全浅论》等，独立开发制作了《云南烟草通用工种数据库管理系统》软件。