园区网建设中的分层安全控制方案

桂林空军学院 沈军 李彦希

摘要：本文从危害园区网信息安全的六个方面的主要因素进行分析，论述了建立完善的园区网安全方案、保护网络系统核心资源的必要性，继之详细论述了园区网分层安全控制方案的内容，即：采用分层安全控制方案，将整个网络分为外部网络传输控制层、内外网间访问控制层、园区网内部访问控制层、操作系统及应用软件层和数据存储层，进而对各层的安全采取不同的技术措施。

关键词：网络安全 分层控制 Internet

近年来，我国现代教育技术得到了飞速的发展，园区网建设和网络教学不断普及。但是，对于大多数网站和园区网来说，网络管理员对于网络安全重视不够，对于网络本身存在的缺陷知之甚少。其实，网络安全是保证网络教学及其它网络应用的前提和基础，是网络使用者不得不面对的问题。随着网络应用的飞速发展、Internet应用的日益广泛，计算机网络安全问题变得尤为突出。今年年初，从美国的Yahoo!网站开始，美国、欧洲及我国的一些著名网站不断遭到黑客的攻击，参与这次大规模攻击的主机分别来自于加州大学、斯坦福大学的主机和Internet上的主机，这使人们对信息安全问题更加关注，同时也证明了作为Internet基础的大学网络是不安全的，防止园区网上的计算机被入侵，建立完善的网络安全方案、保护核心资源已迫在眉睫。

一、网络安全的主要威胁

影响网络安全的因素很多，既有自然因素，也有人为因素，其中人为因素危害较大，归结起来，主要有六个方面构成对网络的威胁：

1、人为失误：一些无意的行为，如：丢失口令、非法操作、资源访问控制不合理、管理员安全配置不当以及疏忽大意允许不应进入网络的人上网等，都会对网络系统造成极大的破坏。

2、病毒感染：从“蠕虫”病毒开始到CIH、爱虫病毒，病毒一直是计算机系统安全最直接的威胁，网络更是为病毒提供了迅速传播的途径，病毒很容易地通过代理服务器以软件下载、邮件接收等方式进入网络，然后对网络进行攻击，造成很大的损失。

3、来自网络外部的攻击：这是指来自局域网外部的恶意攻击，例如：有选择地破坏网络信息的有效性和完整性；伪装为合法用户进入网络并占用大量资源；修改网络数据、窃取、破译机密信息、破坏软件执行；在中间站点拦截和读取绝密信息等。

4、来自网络内部的攻击：在局域网内部，一些非法用户冒用合法用户的口令以合法身份登陆网站后，查看机密信息，修改信息内容及破坏应用系统的运行。

5、系统的漏洞及“后门”：操作系统及网络软件不可能是百分之百的无缺陷、无漏洞的。另外，遍程人员为自便而在软件中留有“后门”，一旦“漏洞”及“后门”为外人所知，就会成为整个网络系统受攻击的首选目标和薄弱环节。大部分的黑客入侵网络事件就是由系统的“漏洞”和“后门”所造成的。

6、隐私及机密资料的存储和传输：机密资料存储在网络系统内，当系统受到攻击时，如不采取措施，很容易被搜集而造成泄密。同样，机密资料在传输过程中，由于要经过多个节点，且难以查证，在任何中介网站均可能被读取。因而，隐私和机密资料的存储及传输也是威胁网络安全的一个重要方面。

由于网络所带来的诸多不安全因素，使得网络使用者必须采用相应的网络安全技术和安全控制体系来堵塞安全漏洞。在园区网的建设中，尤其需要采用分层安全控制方案以保证信息的安全。

二、分层安全控制方案

在园区网安全方面，可以采用多种技术从不同角度来保证信息的安全。然而，单纯的防护技术可能会导致系统安全的盲目性，这种盲目是对整个园区网系统的某个或某些方面的安全采取了安全措施而对其它方面有所忽视。因

而，在园区网安全上，我们采用分层控制方案，将整个网络分为外部网络传输控制层、内外网间访问控制层、园区网内部访问控制层、操作系统及应用软件层和数据存储层，进而对各层的安全采取不同的技术措施。

（一）外部网络传输控制层：

外部网络是指园区网路由器和防火墙之外的公用网。当前网络技术发展迅速，因特网四通八达，网上黑客手段多种多样，为了保证安全，可以从四个方面采取措施：

1、虚拟专网（VPN）技术：对于从专线连接的外部网络用户，采用虚拟专网（VPN）技术，它使架设于公众网络上的园区网使用信道协议及相关的安全程序进行保密，还可以采用点对点协议、加密后送出资料及加密收发两端网络位置等措施使虚拟专网更加可靠。

2、身份认证技术：对于拨号进入园区网的用户进行严格控制，在拨号线路上加装保密机，使无保密机的用户无法拨通；通过用户名和口令的认真检查用户身份；利用回拨技术再次确认和限制非法用户的入侵。

3、加密技术：在外部网络的数据传输过程中，采用密码技术对信息加密是最常用的安全保护手段。目前广泛使用的有对称算法和非对称算法两类加密算法，两种方法结合使用，加上数字签名、数字时间戳、数字水印及数字证书等技术，可以使通信安全得到保证。

4、物理隔离：公共网络及因特网上黑客日益猖獗，加上我国使用的计算机及网络设备的软硬件产品大多数是进口的，安全上没有很好的保证，因而将外部网络中的因特网与专用网络如军用网实现物理隔离，使之没有任何连接，可以使园区网与外部专用网络连接时，园区网与Internet无物理联系在安全上较为稳妥。

（二）内外网间访问控制层

在园区网和外部网络之间，可以采用以下技术来对外部和园区网网间的访问进行控制：

1、防火墙：是硬件和软件的组合，他在内部网和外部网间建立起一个安全网关，过滤经过的数据包，决定是否将它们转送到目的地。它能够控制网络进出的信息流向，提供园区网使用状况和流量的审计、隐藏内部IP地址及园区网网络结构的细节。

2、防毒网关：防火墙无法防止病毒的传播，因而需要安装基于Internet网关的防毒软件，具体可以安装到代理服务器上，以防止Internet病毒及Java程序对系统的破坏。

3、网络地址转换技术：当园区网内部主机与外部相连时，使用同一IP地址；相反，外部网络与园区网主机连接时，必须通过网关映射到园区网主机上。它使外部看不到园区网，从而隐藏内部网络，达到保密作用，同时，它还可以解决IP地址的不足。

4、代理服务及路由器：可以根据设置地址、服务、内容等要素来控制用户的访问，代理服务器及路由器起访问的中介作用，使园区网和外部网络间不能直接访问，从而保证内部关键信息的安全。

5、安全扫描：可以通过各种安全扫描软件对系统进行检测与分析，迅速找到安全漏洞并加以修复。 目前有多种软件可以对设备进行扫描，检查它们的弱点并生成报表。

6、入侵检测：可以采用一些安全产品对网络上流动的数据包进行检查，识别非法入侵和其它可疑行为，并给予及时的响应及防护。

（三）园区网内部访问控制层

在园区网内部，非法用户的登录和对数据的非法修改更加不易查出。当用户安全意识差、口令选择或保存不慎、帐号转借和共享都会对网络安全造成极大的威胁，从园区网内部访问控制层进行安全防护，可采取五种措施。

1、用户的身份认证：用户入网访问控制分为三步，即用户名的验证；用户口令的验证；用户帐号的验证。用户口令是入网的关键，必须经过加密，用户还可采用一次一密的方法，或者使用智能卡来验证用户身份。同时，可将用户与所用的计算机联系起来，使用户用固定的计算机上网，以减少用户的流动性，加强管理。

2、权限控制：这是针对网络非法操作提出的一种安全保护措施。用户和用户组被赋予一定的权限，网络控制

用户和用户组可以访问哪些目录、子目录、文件和其它资源及用户可执行的操作。

3、加密技术：为存放秘密信息的服务器加装密码机，对园区网上传输的秘密信息加密，以实现秘密数据的安全传输。

4、客户端安全防护：首先，应切断病毒传播的途径，降低感染病毒的风险；其次，使用的浏览器必须确保符合安全标准，使客户端的工作站得到安全保证。

5、安全检测：使用安全检测和扫描软件对网络设备和客户端工作站进行检测和分析，查找安全漏洞并加以修复，使用防病毒软件进行病毒查找和杀毒工作。

（四）操作系统及应用软件层

操作系统是整个园区网系统工作的基础，也是系统安全的基础，因而必须采取措施保证操作系统平台的安全。安全措施主要包括：采用安全性较高的系统，对系统文件加密，操作系统防病毒、系统漏洞及入侵检测等。

1、采用安全性较高的系统：美国国防部技术标准把操作系统安全等级分为D1、C1、C2、B1、B2、B3、A级，安全等级由低到高，目前主要的操作系统等级为C2级。在使用C2级系统时，应尽量使用C2级的安全措施及功能，对操作系统进行安全配置。在极端重要的园区网系统中，应采用B级操作系统。

2、加密技术：对操作系统中某些重要的文件进行加密，防止非法出版的读取及修改。

3、病毒的防范：在园区网主机上安装防病毒软件，对病毒进行定时或实时的病毒扫描及检测，对防病毒软件进行及时升级以发现和杀灭新型的病毒。

4、安全扫描：通过对园区网主机进行一系列设置和扫描，对系统的各个环节提供可靠的分析结果，为系统管理员提供可靠性和安全性分析报告，对系统进行及时升级以弥补漏洞及关闭“后门”。

5、入侵检测：安装基于主机的入侵检测系统，可检查操作系统日志和其它系统特征，判断入侵事件，在非法修改主页时自动作出反应，对已入侵的访问和试图入侵的访问进行跟踪记录，并及时通知系统管理员，使管理员可对网络的各种活动进行实时监视。

（五）数据存储层

数据存储在服务器或加密终端上，数据存储的安全性是系统安全性的重要组成部分。对数据的安全保护措施可以采用以下几种方式：

1、使用较安全的数据库系统：目前的大多数数据库系统是基于C2安全等级的。使用时，应尽量使用C2级安全措施及功能。在重要的园区网系统中，在B级操作系统的基础上采用B级数据库系统。

2、加密技术：对于要求保密的数据，采用加密的方法进行存储。加密存储可以通过连接在服务器或终端机上的加密机完成。

3、数据库安全扫描：采用安全扫描软件对数据库进行扫描和检测，为数据库管理系统找出存在的漏洞，以便及时升级系统、弥补漏洞。

4、存储介质的安全：可以通过磁盘镜像、磁盘双工、RAID技术等数据维护技术，再配合磁盘备份、光盘备份等技术来做到不会因某个硬盘的损坏而导致系统崩溃、数据丢失等灾难发生。

三、总结

园区网系统安全需要从多方面加以考虑，特别需要研究整个网络的安全策略，并在安全策略的指导下进行整体的安全建设。这里给出了一个分层安全控制方案，每一层采用多种技术手段进行实现。（见图1）

网络安全问题十分复杂，建立适当的安全策略、采用适当的安全技术、选择适用的软硬件工具，是信息安全的重要保证。

作者简介：

沈　军：1966年12月出生，副教授，硕士，桂林空军学院教育技术中心，训练模拟、网络工程，曾获多项军队科技进步成果奖，在各级学术会议发表论文多篇。

李彦希：1974年7月出生，助教，大学本科，桂林空军学院教育技术中心，计算机应用，省（部）级学术会议发表论文多篇。