Research on Host-Network Security

主机网络安全控制

许智敏（浙江省财政厅）

摘要：主机网络安全是计算机安全领域新兴的边缘技术，它综合考虑网络特性和操作系统特性，对网络环境下的主机进行更为完善的保护。本文提出了主机网络安全体系结构，并对其中的关键技术作了探讨。最后对主机网络安全的访问控制给出了实现方案。

关键词：主机网络安全 主机安全 网络安全 访问控制

1 前言

计算机网络的发展使计算机应用更加广泛和深入，但随之也使安全问题日益突出和复杂。通常情况下，人们从两个方面考虑计算机安全问题：主机安全和网络安全。但是，由于两者考虑问题的立脚点不同，它们各自采用的技术手段难以有机地结合起来，因此对于一些需要两者协同处理才能解决的问题，就不能得到有效的解决[1]。

2 网络通信链路加密安全

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：

除了发送方和接收方外，其他人是无法知悉的（隐私性）；

传输过程中不被篡改（真实性）；

发送方能确知接收方不是假冒的（非伪装性）；

发送方不能否认自己的发送行为（不可抵赖性）。

为了防止通信链路上的窃听、篡改、重放、流量分析等攻击可以选择以下几种方式：

2.1 链路层加密

对于连接各涉密网节点的广域网线路，根据线路种类不同可以采用相应的链路级加密设备，以保证各节点涉密网之间交换的数据都是加密传送，以防止非授权用户读懂、篡改传输的数据。

链路加密机由于是在链路级，加密机制是采用点对点的加密、解密。即在有相互访问需求并且要求加密传输的各网点的每条外线线路上都得配一台链路加密机，通过两端加密机的协商配合实现加密、解密过程。

2.2 网络层加密

鉴于网络分布较广，网点较多，而且可能采用DDN、FR等多种通信线路。如果采用多种链路加密设备的设计方案则增加了系统投资费用，同时为系统维护、升级、扩展也带来了相应困难。因此在这种情况下我们建议采用网络层加密设备（VPN），VPN是网络加密机，是实现端至端的加密，即一个网点只需配备一台VPN加密机。根据具体策略，来保护内部敏感信息和企业秘密的机密性、真实性及完整性。

IPsec是在TCP/IP体系中实现网络安全服务的重要措施。而VPN设备正是一种符合IPsec标准的IP协议加密设备，它通过利用跨越不安全的公共网络的线路建立IP安全隧道，能够保护子网间传输信息的机密性、完整性和真实性。经过对VPN的配置，可以让网络内的某些主机通过加密隧道，让另一些主机仍以明文方式传输，以达到安全、传输效率的最佳平衡。一般来说，VPN设备可以一对一和一对多地运行，并具有对数据完整性的保证功能，它安装在被保护网络和路由器之间的位置。设备配置见图1和图2。目前全球大部分厂商的网络安全产品都支持IPsec标准。

由于VPN设备不依赖于底层的具体传输链路，它一方面可以降低网络安全设备的投资；而另一方面，更重要的是它可以为上层的各种应用

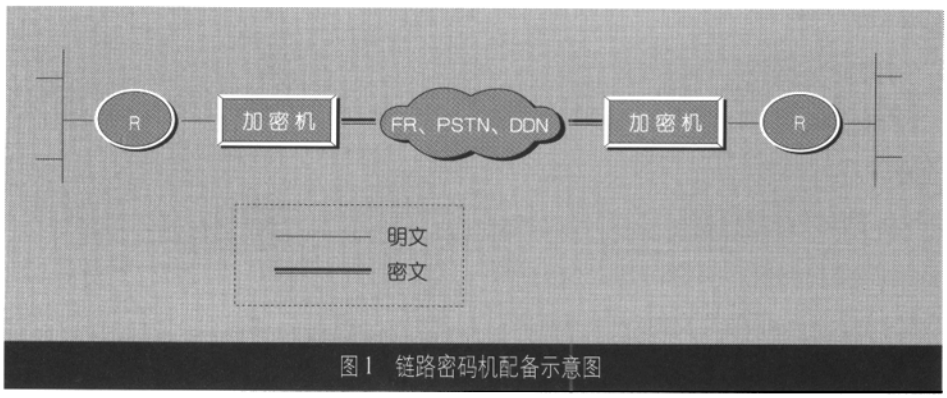

图1 链路密码机配备示意图

提供统一的网络层安全基础设施和可选的虚拟专用网服务平台，对政府行业网络系统这样一种大型的网络，VPN设备可以使网络在升级提速时具有很好的扩展性，鉴于VPN设备的突出优点，应根据企业具体需求，在各个网络结点与公共网络相连接的进出口处安装配备VPN设备。

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。

3 网络访问安全控制

网络面临的安全问题主要在于：

(1) 如何控制网络不同部门之间的互相访问

(2) 如何对不断变更的用户进行有效的管理

(3) 如何防止网络广播风暴影响系统关键业务的正常运转，甚至导致系统的崩溃

(4) 如何加强远程拨号用户的安全认证管理。

针对以上几个方面，网络访问安全控制主要有以下几个方面：

3.1 虚网技术

针对上述的前三个问题，我们一般采用虚网(VLAN)技术。虚网是由一些端系统(主机、交换机或路由器)组成的一个虚拟的局域网。虚网超越了传统的局域网的物理位置局限，端系统可以分布于网络中不同的地理位置，但都属于同一逻辑广播域。虚网具有如下三个优点。

虚网的第一个优点是网络管理员能够轻易控制不同虚网间的互相访问能力。我们可以将同一部门或属于同一访问功能组的用户划分在同一虚网中，虚网内的用户之间可以通过交换机或路由器相互连通，网络管理员甚至还可以通过虚网的安全访问列表来控制不同虚网之间的访问。目前，实现虚网的划分有多种方法，我们可以按照物理端口来划分，也可以按照不同的网络协议如IP、IPX等进行划分，也可以按照MAC地址来划分，将来还可以根据应用类型来划分。具体采用何种划分办法要看用户的具体管理需求和所选用的网络产品。

第二个优点就是对广播信息的有效控制，这要求机构的域中包含的广播和多信宿组与用户位置无关，如果不考虑广播组整个大小的话，网络设计者、规划人员和管理员将可能不慎创建大型的平面网络拓扑，而在用户间却只有(甚至没有)广播防火墙，虚网是控制这些广播信息转发的有效技术，它们的布置结构最大限度地减少了对最终用户站、网络服务器和处理关键业务数据的骨干部分的性能影响，虚网的发展趋势是迈向更成熟的跨越网络园区的带宽和性能管理。

第三个优点是便于管理的更改，而整个网络范围内与用户增加、移动和物理位置变更相关的对管理工作的要求，也大为减少。由于网络管理部门精力有限，技术水平也参差不齐，所以这是很关键的要求，这从很大程度上方便了网络系统的安全访问控制管理。

3.2 路由器访问控制列表

路由器访问控制列表提供了对路由器端口的一种基本安全访问技术，也可认为是一种内部防火墙技术。访问控制列表一般是基于网络协议的，也就是说网络管理员必须对路由器接口上运行的各种协议分别进行配置，路由器访问控制列表分为静态和动态两种，通常采用静态的控制列表，能支持多种路由协议，而动态的控制列表只能支持IP协议，但提供相对多的安全功能，一般路由器访问控制列表的控制功能在于对每个接口控制包的传输，典型的参数包括数据包的源地址、目的地址以及包的协议。对于具体的协议，都有相应的一系列参数可以定义，对下属局对市局数据中心的访问都可以通过路由器访问控制列表来实现。

3.3 采用通信服务器

在安全方面有一个最基本的原则：系统的安全性与它被暴露的程度成反比。因此，建议引入通信服务器，各系统将要输出的数据放置在通信服务器中，由它向外输出，输入的数据经由通信服务器进入内部的业务系统，由于将数据库和业务系统封闭在系统内部，增加了系统的安全性。

3.4 加强内部拨号用户的安全认证管理

在网络规模较小，只少数的访问服务器提供远程拨号访问时，一般采用访问服务器的本地安全数据库来提供安全认证。随着网络规模的增长以及对访问安全要求的提高，一般需要一台安全服务器为所有的拨号用户提供集中的安全数据库，用户无需在每台访问路由器上增加或更改拨号用户安全信息，从而有助于实现统一的访问控制策略。

4 结束语

随着网络攻击手段不断多样化，简单的采用多种孤立的安全手段已不能满足我们的需求。主机网络安全作为一种边缘技术，结合了主机的网络特性和操作系统特性，对主机进行更为完善的保护。随着网络技术的发展，主机网络安全技术在计算机安全领域将占有越来越重要的地位。

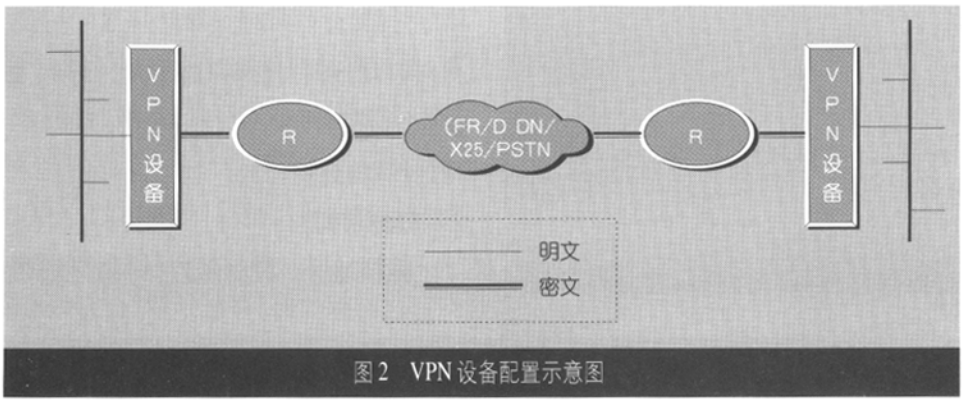

图2 VPN设备配置示意图