浅谈计算机安全问题

□文／戴　虎(深圳雅昌制版厂厂长)

所谓计算机安全是指计算机软硬件、数据都应受到相应的保护，使计算机避免遭到非法及不良企图的用户的破坏。随着网络技术的发展及Internet的普及，人们可以利用计算机在网络上自由地进行信息交流。而对各种限制交流的信息大大增加了计算机爱好者的好奇心，在这种好奇心的驱使下，对网络进行破坏性进攻的能力也得以提高，计算机的安全保护变得不那么简单了。

1996年初，美国国防部宣布其计算机系统在一年前遭到25万次进攻，更令人不安的是大多数进攻未被觉察。这些进攻给国家安全带来的影响程度还未确定，但多数已发现的进攻是针对计算机系统所存放的敏感及机密信息。其中有2/3的进攻被认为是成功的，入侵者盗窃、修改或破坏了系统上的信息。正是由于这些犯罪的存在，美国联邦调查局的国家计算机犯罪小组建议采用防火墙作为防止计算机网络犯罪的措施。计算机安全问题逐步得到了重视。

在现代商业社会，利用各种手段通过计算机窃取商业机密，破坏计算机系统以达到各种不法目的事件时有发生。为保护计算机信息的安全，除了对安全问题加以重视外还需对计算机安全防护有一定了解。下面，主要向大家介绍有关安全策略，安全等级，及Internet防火墙的基本知识：

一、安全策略

在计算机界，开发网络站点安全策略时，可以采用两种主要的观点，这两个主要的立场形成了所有其它与安全有关的策略的基础，并控制着实现安全策略的过程。观点之一"没有明确允许的就是禁止的"这是研究安全问题的第一个态度，这意味着必须提供一个明确的并记录在案的服务集合，而所有其它的都在禁止之列。例如，决定允许提供匿名FTP的传输服务，但是拒绝telnet服务，就应当声明(以文字形式)支持FTP，拒绝telnet。观点之二"没有明确禁止的就是允许的"，这意味着除非明确指出一种服务不可用，则所有的服务均可用。例如若未明确说明禁止对一台指定主机进行telnet服务的话，那么就必须允许之。

二、安全级别

根据美国国防部开发的计算机安全标准——可信任计算机标准评估准则(俗称桔黄皮书)的规定，一些级别被用于保护硬件、软件和存储的信息免受攻击，这些级别均描述了不同类型的物理安全，用户身份验证，操作系统软件的可信任性等。这些标准也限制了什么类型的系统可以互相连接。桔黄皮书自1985年成为安全标准以来，一直没有改变过，它多年来一直是评估多用户主机和小型操作系统的主要准则。其它子系统如数据库与网络也一直是通过该准则的解释来进行评估的。该准则将安全等级定为A、B、C、D四个等级，其中B、C包括了B1、B2、B3、C1、C2几个子级别，安全级别中最高级别为A级，它包含了一个严格的设计，控制和验证过程。D级为可用的最纸级别。该标准说明整个系统都是不可信任的。对于硬件来说，没有任何保护可用；操作系统容易受到损害；对于用户和他们对存储在计算机上信息的访问权限没有身份验证，该安全级别较为典型的操作系统包括我们常用的MS-DOS，Windows，Mac-System等。

三、Internet防火墙

从前，在公寓的建筑物之间建有砖墙，以便火灾发生时，大火不至于蔓延。这些墙便自然地称为防火墙，当局域网连接至Internet时，就意味着允许了局域网用户与外部网络的接触联系。但是同时也允许了外部网络的用户与局域网的接触与交互，随着Internet的发展，网络安全成了我国计算机业界热门话题，网络管理是担心"黑客"(Backer也叫计算机迷)的攻击；一般用户害怕邮件被窃取；商业，企业界担心数据系统被人破坏；行政部门则关心如何将"黄货"拒之门外。从简单意义上说，防火墙是数据通信通过其进行流动的过滤器。如果入侵者试图非授权访问，防火墙可以进行阻击，不允许他们进入系统。通常被保护的网络，属于内部局域网，所防止的网络为不可信的外部网，同时也是入侵者的发源地。可以这样理解：防火墙是用于实施网络安全策略的一个工具，有许多情况下，需要身份验证，安全和保密增强技术来加强网络安全。