

AS/400 在 Internet 上的安全性

——如何在 Internet 上保护您的 AS/400 免遭非法“入侵”

在信息高速发展的今天,从 Internet 上可以获得许多有价值的信息。因此很多人都对 Internet 特别感兴趣。由此而产生的是许多人不顾一切的通过 Internet 访问您的系统,而并不考虑其是否被授权,以及对您的系统是否有足够的了解等,就擅自进行操作。当然有的在很大程度上是出于好奇,或者无知。但对您的系统会构成威胁,所以您需要在系统安全方面保持警惕。

以前 Internet 上的主机大多是 Unix, PC 或 Macintosh 等平台的产品,现在 AS/400 也可做为 Internet 的主机,通过网络连到全球的 Internet 网络上。用户可以通过网络或 PPP 协议或 SLIP 方式连接访问到全球的 Internet 网络上,所有这些联到 Internet 的系统都是支持遵从共同的 TCP/IP 协议的,即 TCP/IP 是 Internet 的基础。

从网络角度提供的安全保护功能——防火墙。它是通过防火墙控制本企业内部网络与外部 Internet 之间的相互访问的。实现防火墙功能的方法很多,可通过在现有的计算机上运行某些软件,也可用配好的“黑盒子”或运行专门防火墙软件的专用计算机等等。

* 其中 Packet Filtering 是实现防火墙功能的一个主要的技术,使得防火墙在网络中作为网络的安全员。在技术上 Packet Filtering 是通过控制 IP 地址的方式来实现防火墙的功能的。用 Packet Filtering 去识别被授权的 IP 地址方可访问您的主机。

* 另外一种方式在网络间通过路由器和网桥来保护您的 AS/400 主机。通过路由器和网桥作为内部防火墙控制网络间的相互传输。

* 还有一种方式通过 DNS (Domain Name System) 来控制网络上哪些主机可以作为 Internet Server 提供给用户进行访问,从而可以对您的 AS/400 主机进行相应的保护。

接下来谈谈从 AS/400 主机角度提供的保安措施。AS/400 作为 Internet 的主机,如果用户通过 Internet 访问 AS/400,用户需要有访问 AS/400 的用户 ID 和相应的口令,而且 AS/400 可以在其用户 ID 简要表中定义其初始菜单和运行的程序以及用户可操作的权限。这是 AS/400 本身的操作系统安全性的具体表现。

AS/400 本身操作系统是自成体系的,是非 UNIX

的系统故其本身很难遭到非法“入侵者”的破坏。在 UNIX 环境下,用户可以对其操作系统级进行操作,这是 UNIX 环境下安全性差的一个致命弱点,使之防不胜防。

通常情况下在 Internet 网络上,使用 Telnet 和 FTP 功能所涉及的口令在传输时是不做加密处理的。这就有可能被某些“入侵者”破译窃取。而在 AS/400 上您可以在设置用户 ID 简要表时,说明指出其权限只可读取小的文件集或只能在中间传输库中写数据,就好像在 SMTP 中发送 E-mail 一样。使其无法对您的主机系统有任何的影响。

AS/400 在其 OS/400 操作系统 V3R1 之后支持 TCP/IP 协议。故 OS/400 只允许您运行 TCP/IP 的应用。如 Telnet 和 FTP,而且还可根据您的需要控制限定哪些 TCP/IP 的应用可在 AS/400 主机上运行,哪些则不可以。

如何仅有一部分用户需要在 AS/400 上运行 TCP/IP,那么 AS/400 在 TCP/IP 的配置时提供一个端口限制功能。因为每个 TCP/IP 的应用至少分配一个端口号,如图 1 所示,对端口 20 加以限制,那么只有用户 PLUTH 允许使用 FTP 功能。故 AS/400 在 TCP/IP 环境中允许被授权者访问。有效地防止非法“入侵者”进入系统,从而破坏系统。

AS/400 提供给您能够控制 TCP/IP 传输的功能,在 OS/400 中用其增加 TCP/IP 路由命令 (ADDTCPRTE) 中的一个参数 (* DFTRUOE) 来控制将打包的信息传输到相应网络的目的地址中去。

而且 TCP/IP 遵从 AS/400 内部的保安功能。所以任何用户想去访问 AS/400 主机,必须具有用户 ID 和口令。另外,AS/400 的安全性符合美国国防部 C2 级标准,每个用户的 ID 和口令需要定期更改。

综上所述,随着 Internet 在世界广泛的使用和其规模的不断扩大,就要对您在 Internet 上的 AS/400 主机的保安予以足够的重视。根据您自身业务等因素的考虑,采用适合您的保安措施。既能充分利用 Internet 网络的资源又能保护您的系统免遭非法者的“入侵”。只有这样方可使您高枕无忧。

(IBM 公司 高热东)