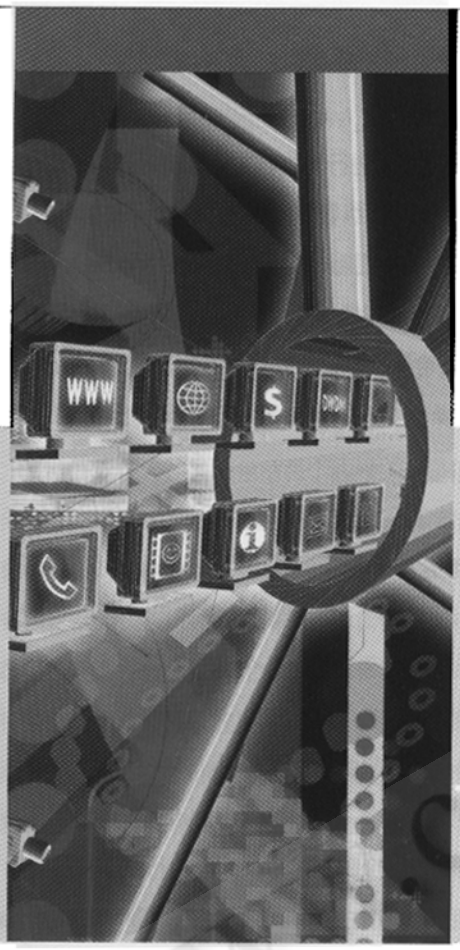

网络综合监控系统的设计

Integrated Network Supervising System Design

摘　要：本文围绕网络中的计算机和设备的远程监控和管理问题，提出了一套系统设计方案，其中涉及到信息的获取，多协议的并发通信，多机屏幕同时监视，鼠标和键盘的操纵等远程控制，基于连通性检测、路由追踪和SNMP协议的网络设备的监控，以及相关的网络安全性问题。

关键词：计算机监控 网络设备监控 多线程 屏幕监视 远程控制

刘荣辉 刘光昌 （广州 暨南大学 电子信息工程系　510632）

随着网络中的计算机和设备的与日俱增，对互联网上特别是企业内部的计算机群和网络设备的有效监控和管理，及其相关安全性问题，是网络时代亟待解决的一个课题。强大而又不完善的网络技术是信息时代的双刃剑，因此在对远程计算机和设备进行监控时还要对安全问题给予高度的重视。

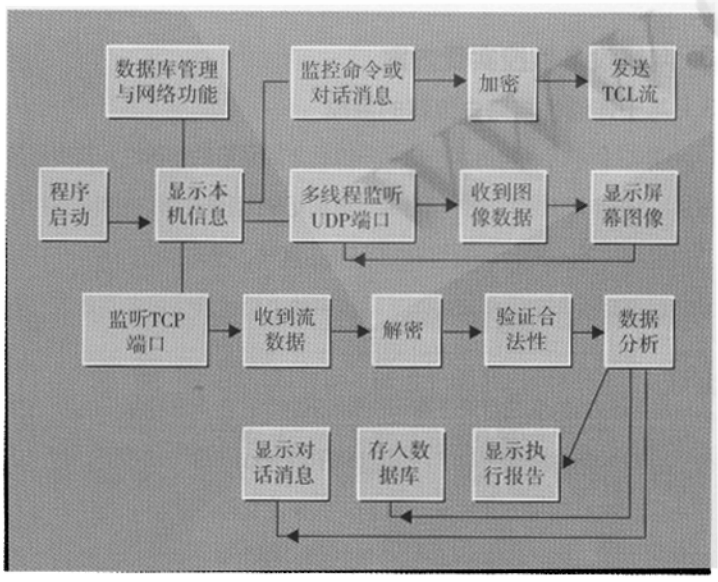

图 1　主控机的流程图

1　系统设计思想

本系统参考受控机/主控机模型，基于多种协议进行一点对多点的通信，采用多线程技术以实现一台主控机可同时对多台受控机和设备进行实时的远程监控和管理。系统主要以C++Builder为开发工具，计算机监控的系统流程如图1、2所示（网络设备监控流程略）。

受控计算机开机后自动启动客户端程序，用各种途径搜集本机信息，再将加密后的信息数据流发送给主控机，并进入监听状态。主控机产生多个线程监听来自各受控机的信息，接收到数据时，首先进行解密和合法性验证，然后按一定格式分离出各种信息存入数据库。主控机也可以根据受控机的IP随时向受控机发送经加密处理的信息查询命令、屏幕图像请求命令、鼠标键盘的控制命令以及其他控制命令。正在监听待命的受控机接收到监控命令数据后，也首先将数据解密，验证其合法性，再按照主控机的命令执行相应的操作，然后将操作结果数据加密后返回给主控机。

2　计算机监控实现方案

2.1 计算机信息的获取与数据传输

使用强大的Windows API函数可获得大量的本机系统信息（计算机名，用户名，操作系统信息，CPU信息，目录信息，内存信息，硬盘信息等）；Windows的注册表中包含系统配置、PC机硬

件配置、Win32应用程序和其他用户设置信息。可通过WinAPI中的RegCgreateKey( )、RegOpenKey( )和RegQueryValue( )等函数操作注册表。

主控机与受控机之间以TCP/IP短连接方式进行控制命令的传输。本系统采用C++Builder提供的基于TCP/IP的NMStrm组件和NMStrmServ组件进行可靠的数据流传输。NMStrm组件负责数据流的发送，NMStrmServ组件负责接收数据流。用NMStrm组件的PostIt方法便可完成建立连接、数据发送过程。当NMStrmServ组件接收到数据流时，便会触发OnMsg事件，对接收到的受控机信息进行处理。

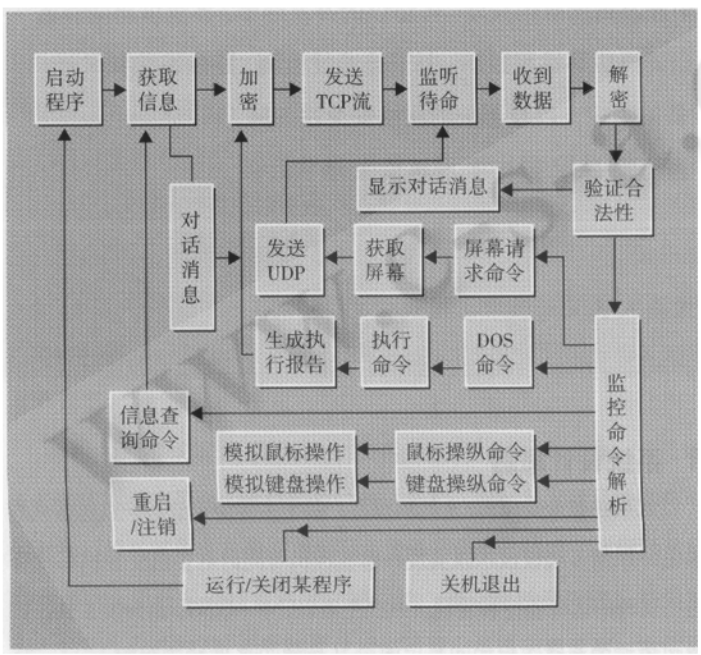

图 2　受控机的流程图

2.2 多受控机的屏幕监视

当受控机收到来自合法主控机的请求屏幕图象的命令流时，便截取屏幕图像存成Bmp格式内存流。再转化为Jpeg格式内存流，适当调节格式转化时的图像压缩率控制图像质量，然后用压缩算法将图像文件进行压缩后以UDP数据报的方式发送给主控机，主控机用多个线程接收不同受控机发来的图像数据，并在不同的Image控件中显示出来。采用TNMUDP控件（基于无连接的UDP）来实现图像数据的传输，受控机的TNMUDP控件的RemoteHost设置为主控机的IP地址，LocalPort与主控机的TNMUDP控件的RemotePort相同，RemotePort则与主控机的TNMUDP控件的LocalPort相同。

为实现同时对多部受控机的屏幕监视，为每个受控机在不同的端口上建立了独立的监听线程，利用多线程的并发性，各个线程接收到的数据可以互不相干地在不同的图像框中显示，各个线程定时地发送屏幕请求命令，便可动态地监视多部受控机屏幕的变化。

2.3 鼠标与键盘的远程操纵

受控机使用TServerSocket控件进行接收，主控机使用TClientSocket控件进行发送，基于TCP/IP进行操纵数据的传输。在显示受控机屏幕图像的Image控件上设置Click，DbClick，MouseMove，MouseDown等鼠标事件的处理函数，将相应的事件信息加密后发送到受控机，受控机收到鼠标控制信息并进行合法性验证和数据分析后，便用API函数中的mouse_event( )模拟鼠标操作，用SetCursorPos (X, Y)设置鼠标的当前指针位置。

受控机接收到来自合法主控机的键盘操纵命令时，便进行键值分析，按字符键、组合键或者控制键等各种情况，调用API函数中的keybd_event( )来模拟键盘动作。对于组合键，则要先用keybd_event模拟各个键按下，再以相反的顺序逐一模拟各个键松开。

2.4 远程命令控制

受控机接收到来自合法主控机的DOS命令时，在此命令后加上">Filename"后写入一个批处理文件中，然后用ShellExecute ( )函数执行这个批处理文件，就相当于执行这个DOS命令，而且执行结果会被重导向到Filename文件里，然后再从文件中读出执行结果以TCP流的方式发送给主控机。当受控机接收到运行其他程序的命令时，可执行：ShellExecute(Handle,"open",filepath,"","",SW_SHOWDEFAULT);

受控机接收到相应命令后，可以通过调用ExitWindowsEx( )函数来退出Windows操作系统。参数设为EWX_LOGOFF可注销当前用户，设为EWX_POWEROFF可终止其运行并关闭计算机电源（若系统支持软关机）。在NT中进行重启和关机必须有SE_SHUTDOWN_NAME权限，可用AdjustTokenPriviledge( )来获取此特权。

3 网络设备监控实现方案

3.1 基于连通性与路由追踪的监控

PING命令可以检测本机与另一主机之间网络的连通性，其实质是发送ICMP回显请求报文，然后等待返回ICMP回显应答。使用ICS控件工具包中的TPing控件，设置好其Address属性，便可实现Ping一个IP的功能，循环调用它，便可检测某网段中的主机或网络设备与本机的连通性。

Windows的系统目录下有一个tracert命令，可用ShellExecute执行批处理文件来调用此系统命令，与上述的执行Dos命令方法相同。然后定时从存储执行结果的文件中读数据，如果此文件不为空则说明命令已经执行完毕。如果要在tracert命令执行的过程中停止此命令的执行，便可用SendMessage中止批处理文件的运行：hWndcmd=FindWindow (NULL,Syspath.c_str());//获取程序窗口的句柄

```
if(hWndcmd!=0)
SendMessage(hWndcmd,WM_CLOSE,0,0);//向程序窗口发送关闭的消息
```

3.2 基于 SNMP 的并发监控

通过基于UDP/IP的SNMP简单网络管理协议，管理进程可以和网络设备中的代理进程通信，从而间接地读取和修改设备的管理信息库MIB中的信息。本系统可以对所有含支持SNMP的代理进程的网络设备进行监控，如路由器、交换机等。

网络设备监控模块包括两个线程：一是监视线程，以轮询的方式向各个网络设备的代理进程发送GetRequest等监视命令（包含超时重传机制），对接收到的Response进行解析，动态显示设备状态，存储设备信息；二是监听线程，用于监听网络设备在特定情况下发来的Trap数据包，进行数据解析后，发出声音报警信号，通知系统管理员进行相关处理，并写入系统异常日志表。另外，系统管理员对网络设备参数进行修改后，控制模块就会将所改变的参数形成SetRequest数据包，发送给相应的网络设备（含超时重传机制），并接收应答包。

4 系统安全措施

为防止黑客窃取受控机信息或伪装成合法受控机取得对受控机的控制权，系统采取了多种安全措施。

防止非法入侵本监控系统（基于IP寻址）的第一道防线是防火墙。可将所有受控机形成一个内部网络，通过包检查防火墙与外部Internet隔离。如果主控机也在内部网络中，则可在防火墙上过滤掉所有与内部主机的相应端口（本系统中使用的端口）进行通信的IP数据包，并且让受控机和主控机都使用保留的IP地址（如192.168.0.1），然后都通过代理服务器与Internet相连。如果主控机不在受控机构成的内部网络中，且受控机都使用保留IP地址，则必须在内部网络的代理服务器上运行一个代理程序，专门负责主控机与受控机之间的数据转发，并进行IP和Mac地址以及端口号的联合绑定验证。

信息加密技术是本系统的第二道安全防线，如果受控机与主控机都松散地分布在Internet上，则必须采用以下端到端的数据加密技术来确保系统的安全。主控机和受控机之间传输的数据按一定规则加入扰码，动态生成密钥进行加密，本系统采用MD5算法对信息进行加密处理。

参考文献

1 卿斯汉，密码学与计算机网络安全，清华大学出版社，2001年。
2 W.Richard Stevens著,范建华等译，TCP/IP详解卷1协议，机械工业出版社，2000年。
3 Gary R. Wright, W.Richard Stevens，TCP/IP详解卷2实现，机械工业出版社，2000年。
4 黄嘉辉，Internet与TCP/IP程序设计之C++Builder高手，清华大学出版社，2001年。
5 张万里、陈战林，C++Builder5.0高级开发技巧与范例，电子工业出版社，2001年。
6 朱时银、马承志，C++Builder5编程实例与技巧，机械工业出版社，2001年。