远程控制系统

2012-09

课程内容

- 流套接字与数据报套接字回顾
- 远程控制系统流程

TCP 套接字编程（ cont.）

无连接的服务

远程控制系统

工作原理：

- 客户端接收用户输入的命令，客户端通过套接字将命令传送给服务器端，
- 服务器在收到用户的命令，对命令进行解析
- 在服务器端调用对应的命令
- 并将命令执行的结果发送给客户端，从而实现远距离控制的功能。

注：远程控制系统、木马、僵尸程序都属于远程控制类程序。

UDP 远程控制程序流程图

TCP 远程控制流程

命令的解析

- 采用管道实现

```
 int execute(char* command,char* buf)
{
    File * fp;
    int count;
    if (NULL== ( fp=popen(command,”r”)))
    {
          perror(“error\n”);
          exit(1);

    }
    int count=0;
    while((buf[count++]=fgetc(fp)!=eof)&&
count<2047);

    buf[count]=‘\0’;
    pclose(fp);
    return count;
```

试验题目

- 利用流套接字实现一个简单的远程控制系统：
  1. 客户端输入“ quit”, 客户端程序与服务器端程序打印退出信息，终止程序的执行；
  2. 客户输入命令，客户端将命令通过流套接字发送给客户端，服务器执行收到的命令，并将结果发送到客户端显示；
  3. 如果没有客户输入的命令，服务器发送命令非法信息，并在客户端显示该条信息。
  4. 编写实验报告：
     1. 列出程序运行状态、截图、配文字说明；
     2. 独立完成，打印报告，报告语言为中文，不少于 4 页 A4 ，封面上书写姓名、学号。