IEMP\_Client说明文档

作者：钱成

目录

[IEMP\_Client说明文档 1](#_Toc83687157)

[1. 主通讯模块 3](#_Toc83687158)

[1.1 通讯规范 3](#_Toc83687159)

[1.2 动态密码 3](#_Toc83687160)

[1.3 系统操作模块（0x00） 3](#_Toc83687161)

[1.3.1 关机(0x01) 3](#_Toc83687162)

[1.3.2 重启(0x01) 3](#_Toc83687163)

[1.3.3 休眠（0x04） 4](#_Toc83687164)

[1.3.4 执行指定CMD命令行(0x06) 4](#_Toc83687165)

[1.4 文件操作类(0x02) 4](#_Toc83687166)

[1.4.1 服务端下载文件到本地(0x00) 4](#_Toc83687167)

[1.4.2 本地上传文件到服务器(0x01) 4](#_Toc83687168)

[1.4.3 列出文件列表(0x02) 4](#_Toc83687169)

# 客户端通讯模块

## 通讯规范

主通讯模块由Client发起监听，采用TCP通讯，默认监听48280端口，此监听程序不可通过配置文件修改或关闭。在服务端与主模块进行通讯时，最大的指令长度为65537字节，其中，前两字节（即0-1字节）为之后的数据总长度。举个例子，如果需要传送的指令总长度为25字节，则前两字节的值为0x17,0x00，代表后面的有效数据长度为23位，程序将准备好23个char的内存空间来接收这些数据。之后的8个字节（即2-9字节），为动态密码。动态密码相关技术，见本模块的“动态密码”章节。然后的2个字节（即10-11字节），为实际指令类型，第10字节为指令类型大类，第11字节为指令类型的小类。之后的字节根据实际指令的不同为空或为实际指令需要的数据，交由小类自行处理。

## 动态密码

动态密码首先依赖一个16字节长度的固定密码与本机时间。该16位固定密码通过配置文件存储，由部署程序随机生成，关于配置文件相关信息，见本模块“配置文件”章节。程序将通过本机时间计算出相应的UTC时间，并除以30后取整，以此得到一个每30秒加1的值。然后此值将被转换为4位char（由于内存大小一样，此处可以直接复制此值）。由16位密码与此4位char连接为一个20字节的数据，此数据将被计算md5值。MD5值为16位，但此处只需要8位，所以本程序会将第0位字节与第8位字节取和并存回第0字节，第1位字节与第9位字节取和并存回第1字节，以此类推，最后得到一个8字节的数据，为加密后的动态密码，由于有效期只有90秒（详见注解1），且无法被反向破解，所以可以明文通讯。

\*注解1：为避免通讯延迟与时间误差导致的问题，所以IEMP\_Client在接收到动态密码并验证时，会尝试与当前时间，+30秒时间，-30秒时间所产生的动态密码依次对比，任意密码匹配则会被认为匹配成功。

## 系统操作模块（0x00）

### 关机(0x01)

Windows操作系统下执行："shutdown -p" \*此命令在WinPE下不可用

Linux操作系统下执行："shutdown -h now"

### 重启(0x03)

Windows操作系统下执行："shutdown -r -t 0" \*此命令在WinPE下不可用

Linux操作系统下执行："restart"

### 休眠（0x04）

Windows操作系统下指令："shutdown -h" \*此命令在WinPE下不可用

### 执行指定CMD命令行(0x06)

执行此操作时，可以将需要执行的命令行连接在必要的11字节的通讯内容后，本程序将直接交由命令行执行。

### 创建新进程(0x08)

通讯规则同1.3.4，只是该指令将不会导致通讯模块被占用，适合需要驻留或运行时间较长的其他程序。

## 文件操作类(0x02)

### 服务端下载文件到本地(0x00)

此处设传入数据的第12位（前11位为传输必须字节），为本方法有效数据的第0位。首先，以C语言标准传入完整的文件路径。此字符串由0x00结尾，在其后，跟着8位char类型的值，此处代表长度为8字节的文件长度，在windows中为long long int类型，以此来支持超大容量的文件（本程序强烈不推荐使用该方案传输过大文件，内网群发100MB以上文件建议使用“BitTorrent模块”以增加效率）。然后将根据此文件长度接受文件并存储到相应的路径中，如该路径原本存在文件，则执行无提示覆盖。

### 本地上传文件到服务器(0x01)

同1.4.1，传输方向相反

### 列出文件列表(0x02)

此处设传入数据的第12位（前11位为传输必须字节），为本方法有效数据的第0位。首先，以C语言标准传入需要列出文件夹的路径以0x00结尾。在列出文件时，将根据每个文件的不同生成字符串并连接，对于每个文件或文件夹，第一位为文件类型，0x04为文件夹，0x08为文件，如果为文件夹，则在类型后有一个整数表示该文件名的长度，再跟着一个完整文件名。如为文件，则0x08后先跟随一个文件大小信息，最小为0，最大为一个long long int，表示文件名的方法如文件夹。

## 远程CMD（端口48281）

远程CMD由Client监听TCP 48281端口，收到的启动请求必须包括8个字节的动态密码+初始化命令行内容（一般为cmd.exe或powershell.exe），密码验证成功后会启动一个隐藏窗口的进程，并打开相应的输入输出管道，此时TCP连接keep alive，此后，程序将会把所有管道输出的内容直接通过该TCP连接发送给服务器，并将该TCP连接发送的所有请求全部输入到相应进程的管道中。注意1：任何时候以任何形式关闭TCP连接都会导致远程命令行进程被关闭，管道被释放。注意2：不要在一个远程CMD请求未关闭时对同一台被控机器打开一个新的远程CMD请求，这可能将导致未知错误。

## UDP心跳规则

心跳由Satellite监听UDP 48281端口，当客户端启动时，会首先发送一次上线信息（服务器地址来自部署器），包含EID(Equipment ID)，Version, Total Memory，CPU线程数，主板名称，操作系统名称，CPU名称。其中文本类型的信息采用类似Becode的方式，如“abc”字符串在bytes中记录为：“\x03abc”，即分割了字符串，又使处理程序对数据有更高效的读取，也可以拥有很小的体积，缺点是最大文本支持为256位，在本项目中涉及的基本信息没有大于256位字符串的，所以用这种方式传输刚好合适。在发送完成上线信息后，Client会每两分钟向该UDP服务器发送一个数据包，包含EID，内存占用量，与过去两分钟内CPU的平均使用量。由于UDP的特性，服务端应当在连续2次（即连续4分钟以上）未收到客户端的心跳数据包后，判定该设备离线。

# Satellite插件规范

2.1