企业内部用户网络访问监控系统的研究与实现①

Research and Implementation of Monitor System of Enterprise Users Access Network

石　恒　王　勇　(桂林电子科技大学 网络中心 广西 桂林 541004)

摘　要： 在企业建立的内部网络中，为了防止员工滥用网络资源、通过网络向外传播机密数据，需要对用户的网络访问进行监视和控制。在研究了 Winsock2 SPI 技术之后，提出一种基于 LSP 监控用户访问网络的方法，并利用该方法实现了网络访问监控系统。该系统能监视每个用户访问网络的具体情况，可以针对不同用户使用的应用程序制定不同的网络访问控制规则，并且能按制定的规则控制应用程序的网络访问。

关键词： 内部网络 SPI LSP 网络访问 控制规则

1　引言

随着 Internet 技术不断发展，众多企业纷纷开始建立起企业内部的局域网络。但是网络通讯方便的背后，隐藏着管理上的漏洞，一个企业对外网络通讯不设防的情况下，企业便无法控制员工的上网行为，紧接着员工怠惰公事上网聊天、泄露公司机密数据[1,2]。如何监控内部网络，越来越受到人们的关注，相关研究相继展开[1,3,4]，各种内部网络监控系统也如雨后春笋般被开发出来。目前的监控系统从系统架构上可以分为两类：旁听架构式和主从 Client/Server 架构式。旁听架构的监控系统有黑匣子——旁听版[2]、NET-CROWN 等，此类产品只能在用户作出非法操作之后才能发现，例如用户登陆非法网站，因此，这类产品只能做事后取证、秋后算帐之用，对员工起恫吓作用而已。若要对员工进行实时的监控，当属主从 Client/Server 架构的产品，这类产品有黑匣子——企业版[2]、脉杰网络监控等，此类产品在用户主机上安装监控代理，监控功能强大，可以实时监控用户的诸多行为，例如 USB 使用监控、网络访问监控等等。这类产品在实现网络访问监控功能时，通过对特定端口上的网络地址监视，进而实现对网络访问的控制，因此，目前它们只实现了对 IE 浏览器之类使用固定端口的程序进行监控，对于其他应用程序访问网络就无法监控了。

鉴于 Windows 作为一种桌面操作系统已经广为采用[5]，而现在开发的网络应用程序都使用 Winsock2 来进行开发[6]，通过对 Winsock2 SPI 技术的研究，本文提出了一种基于 LSP 监控用户网络访问的方法。该方法由于实现了监控所有应用程序对不同网络地址的访问行为，与传统网络访问监控方法相比，该方法具有对网络访问监控的颗粒度更细、监控所有应用程序两大特点，因此，更具有实用的价值。

2　Winsocket SPI概述

Winsock2 SPI(Service Provider Interface)服务提供者接口建立在 WOSA(Windows Open System Architecture，Windows 开放系统架构)之上，是 Winsock 系统组件提供的面向系统底层的编程接口。Winsock 系统组件向上面用户应用程序提供一个标准的 API 接口；向下在 Winsock 组件和 Winsock 服务提供者(比如 TCP/IP 协议栈)之间提供一个标准的 SPI 接口。多数情况下，一个应用程序在调用 Winsock2 API 函数时，系统会调用相应的 Winsock2 SPI 函数，利用特定的服务提供者执行所请求的服务。SPI 分为两

① 基金项目:国家自然科学基金(60872022)
收稿时间:2008-12-18

个部分：传输服务提供者和命名空间提供者。传输服务提供者提供建立连接、传输数据、行使流控制、出错控制的服务；命名空间提供者和传输服务提供者类似，只是它截获的是名称解析的 API 调用，如 gethostbyname 等[7]。Winsock2 SPI 体系结构如图 1 所示：

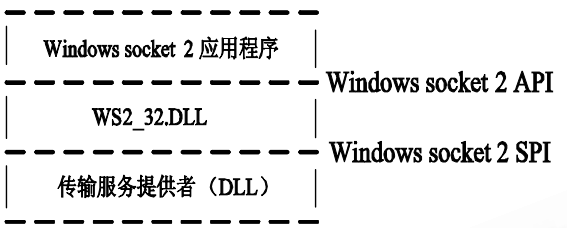

图 1　Winsock2 SPI 体系结构

传输服务提供者又分为两种：分层服务提供者和基础服务提供者。分层服务提供者将自己安装到 Winsock 编录里，位于基础服务提供者之上，也可能位于其它分层提供者之间，并截获应用程序对 Win- sock API 调用[6]。基础服务提供者公开一个 Winsock 接口，直接执行一种协议，如 TCP/IP 协议。当一个根据分层提供者创建套接字的应用程序作出一个 Winsock 调用时，系统将调用传递到分层服务提供者(Layered Service Provider，缩写为 LSP)，LSP 又将该请求传递给一个基础服务提供者，由基础服务提供者来执行适当的动作[7]。其体系结构如图 2 所示：

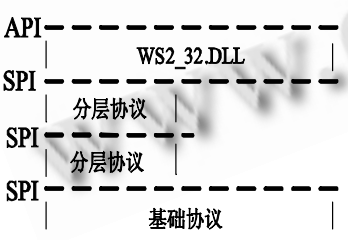

图 2　分层服务提供者的体系结构

3　监控系统总体设计及框架

本系统采用 C/S 架构，由运行于服务器上的监控中心和安装在受控主机上的监控代理两部分组成。通过运行在各受控主机上的监控代理服务，将受控主机的网络访问状态、网络访问请求报告给监控中心，并接受监控中心的控制指令，更新网络访问控制规则文件。

监控中心是网络管理员对网络进行实时监视、集中控制的地点。它可以随时向网络中任何一台受控计算机的监控代理发出命令，让它们实时汇报其宿主主机的网络状态；同时，把收集到的信息动态的显示出来。另一方面，监控中心还可以根据管理人员的要求，配置某台受控主机的网络访问控制规则文件，并向该主机传送该文件；同时，它还处理来自受控主机的网络访问询问，并相应的修改该主机的规则文件，而后把管理人员回答的结果返回给询问主机。

监控代理是监控中心派驻在各受控主机上进行具体监控的实施者。首先，它把 LSP 安装在受控主机的 Winsock 编录中，并且重新排序目录，使新安装的 LSP 入口首先出现[6]。接着，监控代理记录应用程序的每次网络访问，包括访问开始的时间、使用的端口和访问的远程 IP。此外，监控代理接收监控中心发送过来的网络访问控制规则文件修改命令，按命令修改规则文件；同时它也向监控中心报告其宿主主机发出的网络访问询问。

按照监控系统的设计，本系统实现后总体框架如图 3 所示：

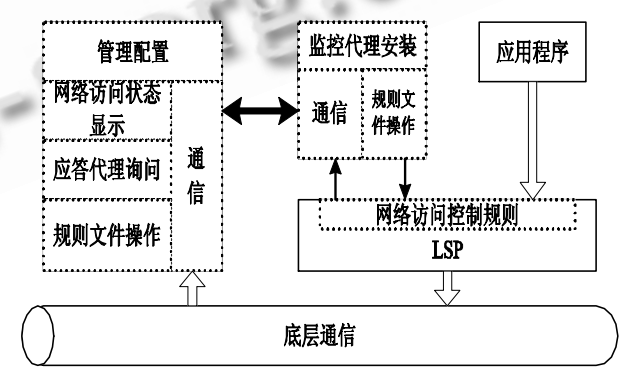

图 3　网络访问监控系统框架

本监控系统采用 C/S 架构方式，因此，系统的框架亦分为两大部分，包括运行于服务器上的监控中心和运行在受控主机上的监控代理。监控中心由下面的几个功能模块组成：

① 管理配置：方便管理人员管理系统，管理人员可方便配置内部网络中每一个用户的网络访问控制规则文件，也可以指定要显示网络访问状态的用户主机。

② 网络访问状态显示：实时的显示管理人员指定的一个或多个用户的网络访问状态。

③ 应答代理询问：弹出对话框，提示管理人员回答代理发出的询问；在管理人员一定时间内没有回答询问则以“拒绝访问”回答。

④ 规则文件操作：按管理人员的操作，添加、修改或删除各用户的网络访问规则文件，并保存之。

⑤ 通信：实现与监控代理的通信,对监控代理发出指令和接受受控主机的状态信息.

在受控主机上，监控代理方由以下几个模块组成：

① 监控代理安装：除了安装监控代理本身以外还负责把 LSP 安装在宿主主机的 Winsock 编录里，并排序 LSP，使自己的 LSP 处于编录的最顶端。

② 规则文件操作：根据管理中心发送的命令，操作规则文件。

③ LSP：此模块为监控代理方最主要的功能模块，也是整个系统的核心所在，实现本系统最为重要的功能——根据规则文件控制宿主主机的网络访问；同时，也向监控中心报告主机的网络活动。

④ 通信：实现与监控中心的通信，接受监控中心发出的指令和向监控中心报告受控主机的网络状态信息。

4 关键技术介绍

上面介绍了 SPI 技术、系统的总体设计以及系统的框架结构，下面介绍一下本系统实现的关键技术——构建可以监控网络访问的 LSP。该技术实现主要分为两部分的工作：首先，截获与网络访问的相关 Winsock 调用；其次，控制网络访问。

4.1 截获 Winsock 调用

LSP 是作为一个标准的 windows 动态连接库来执行的，必须将一个名为 WSPStartup 的单一函数条目导入到这个链接库里边。当系统调用 LSP 的 WSPStartup 时，它必须通过一个作为参数传递的函数派遣表公开 30 个附加 SPI 函数，LSP 就由这 30 个 SPI 函数组成[7]。该函数如下：

```
int WSPAPI WSPStartup(
...
WSPUPCALLTABLE UpcallTable //Ws2_32.dll 提供的向上调用转发的函数表结构
LPWSPPROC_TABLE lpProcTable  //指向 SPI 函数表结构，用来返回 30 个 SPI 服务函数
);
```

所有的 SPI 函数都经由 LSP 的分派表——lpProcTable 参数导出。先把 lpProcTable 保存起来记为 g_NextProcTable，然后截获 lpWSPAccept、lpWSPConnect、lpWSPSendTo、lpWSPRecvFrom 四个函数(这些函数涉及到网络访问)，使其分别指向自己编写的 WSPAccept、WSPConnect、WSPSendTo、WSPRecvFrom 四个函数，这四个函数先调用网络访问控制函数 GetAccessIP 检查远程 IP 以决定是否提供服务，然后调用被截获的函数(在 g_NextProcTable 中保存)实现网络传输功能。

4.2 网络访问控制

当应用程序调用服务提供者时，那些实现截获的函数首先调用 GetAccessIP 检查远程 IP，以判断是否提供服务。GetAccessIP 函数功能实现的关键是加载网络访问控制规则文件，根据应用程序在规则文件中对应的规则进行控制。规则文件以如下格式保存信息：首先是文件头，以一个 RULE_FILE_HEADER 结构来描述，其中定义了控制规则数目等重要信息；后面则是网络访问控制规则，其定义如下：

```
struct RULE_FILE
{
    FILE_HEADER header;        // 文件头
    REMOTEIP_CONTROL
    IPControls[MAX_IP_CONTROL];// 网络访问控制规则
};
```

网络访问控制规则亦为自定义的一种数据结构，他直接决定着是否允许应用程序对某一远程 IP 进行网络访问，其定义如下：

```
struct REMOTEIP_CONTROL
```

```
{
TCHAR szApplication[MAX_PATH]; //  应 用 程 序 名称
BOOL bIPControl;      //  是否进行网络访问控制
ULONG ulDenyIP[MAX_IP_CONTROL];//拒绝 IP 组
int nDenyIPCount;     //  记录拒绝 IP 的数量
ULONG ulPassIP[MAX_IP_CONTROL]; //放行 IP 组
int nPassIPCount;     //  记录放行 IP 的数量
UCHAR ucAction;       //  采取的动作，询问时使用
};
```

LSP 对网络访问控制的过程如下：GetAccessIP 首先根据调用被截获 SPI 函数的应用程序名称在规则文件中查找其对应的控制规则，接着根据 bIPControl 的值判断是否进行网络访问控制，若允许，则放行；否则分别在拒绝 IP 组和放行 IP 组中查找，并按查找到的相应结果进行控制。若 GetAccessIP 在规则文件没找到应用程序对应的控制规则，或者在拒绝 IP 组和放行 IP 组也没找到应用程序欲访问的远程 IP，LSP 则通过通信模块向监控中心发出询问，由管理人员决定是否放行。

5 总结

本文研究了 Winsocket2 SPI 技术，通过构建 LSP，实现内部用户网络访问监控系统，对网络访问监控技术的探索有一定的研究价值。本系统已经在校园网上进行试用，取得不错的效果。系统能实时的显示用户的网络访问；也能根据网络访问控制规则控制不同用户的网络访问；系统亦能根据管理人员对 LSP 询问的回答结果进行网络访问控制；而且本系统并不影响正常的网络活动。

参考文献

1 陈德军.基于企业内部网络的监控系统研究[硕士学位论文].南京:南京理工大学, 2005.

2 Using Guide_CN. http://www.dci.net.cn/.

3 耿保建,董金祥.基于代理的内部网络安全监控系统.计算机应用与软件, 2006(9):119－121.

4 熊帆.内部网络用户行为监控技术的研究与实现[硕士学位论文].成都:四川大学, 2006.

5 戎健,王以刚.基于 Winsock SPI 的主机访问控制应用.计算机工程与设计, 2005,(8):2261－2262.

6 王艳平,张越.Windows 网络与通信程序设计.北京:人民邮电出版社, 2006:13－164.

7 Jones A, Ohlund J. Network Programming For Microsoft(Second Edition).北京:清华大学出版社, 2006:220－240.