# 基于 DCOM 的主机安全实时监控系统的设计与实现*

周春娟
(苏州大学 计算机科学与技术学院, 江苏 苏州　215006)

摘　要: 随着网络技术的迅猛发展, 网络管理人员迫切需要一种能够实时监控网络状态的有效措施和解决方法。通过分析企业网络的拓扑结构, 开发了基于 DCOM 技术的主机安全实时监控系统。介绍了系统的功能模块, 阐述了该系统的设计原则、总体框架和实现技术等。该系统的运用解决了企业内部网络管理的混乱, 提高了网络的有效性和可靠性。

关键词: DCOM; 监控站; 代理
中图分类号: TP393　　文献标识码: A　　文章编号: 1671－5322(2005)01－0031－04

随着计算机技术、网络技术的飞速发展, 网络已经深入到生活的各个领域, 面对日益庞大的网络, 网络安全管理显得越来越重要。网络管理人员在整个网络运行期间, 能否实时监控联网计算机的运行状态对网络安全具有极其重要的作用。为此我们开发了基于 DCOM 的主机安全实时监控系统, 其目的是为了能够对联网的每一台计算机进行实时监控, 为网络管理人员提供实时数据, 保证网络的正常运行。

## 1　系统设计

### 1.1　系统概况

主机安全实时监控系统的建立是根据企业网络安全的需求开发的实时监控软件, 由两个子系统组成: 监控站(Monitor)和代理(Agent)。监控站安装在网络管理人员的计算机上, 用于实施对联网计算机的各种操作; 代理安装在每台联网的计算机上, 主机一启动, 代理在后台自动隐藏运行; 监控站根据代理发送的数据进行采样分析, 实现对网络安全的实时监控。主机安全实时监控系统的运行环境具有很强的通用性, 无论是监控程序还是代理程序, 可以运行于 Win98、WinNT、Win2000 或 WinXP。下面就系统做详细介绍[1]。

### 1.2　系统功能

①网络状态信息采集。分区域实时扫描记录网络各类设备运行状况和网络接入端口信息, 比对发现各类异常和违规使用的计算机和违规设备。

②网络实时监测。对需要不间断运行的计算机和网络设备的状态进行实时监控, 确保设备正常运行。包括对网络、操作系统、数据库和应用软件等多个层次的运行状态的监控。及时将报警信息以短消息等多种形式, 发送给设备管理人员。也可以根据需要, 将报警信息发布至特定对象。

③“一机两用”检测。“一机两用”是指计算机或网络设备既连接企业信息网又连接国际互联网的违规行为。“一机两用”检测功能对所有联网主机监测, 发现“一机两用”行为, 立即中断与企业信息网络的连接并锁定该主机。

④“敏感信息”检测。“敏感信息”检测功能能发现企业网络上设定范围内的 HTTP、FTP 等网站、共享目录, 并能在授权的情况下按照用户的设定收集网站和机器中的特定信息。

⑤解锁操作。该功能可以使锁定的计算机恢复正常。

⑥远程强行关机。该功能可以使代理主机自动关机, 只有在发现代理主机正在进行具有较大破坏性时才使用该功能。

⑦代理定时自动升级。该功能定时扫描监控站, 如果发现监控站软件版本高于当前版本, 进行

* 收稿日期: 2004－12－03
作者简介: 周春娟(1979－), 女, 江苏南通人, 苏州大学硕士研究生, 主要研究方向为计算机网络安全。

代理软件升级。

1.3 系统拓扑结构

根据企业网络实际情况,每个部门都有局域网,且分属于不同子网,并通过路由器连接到企业主干网上,该系统具体拓扑结构简图1。

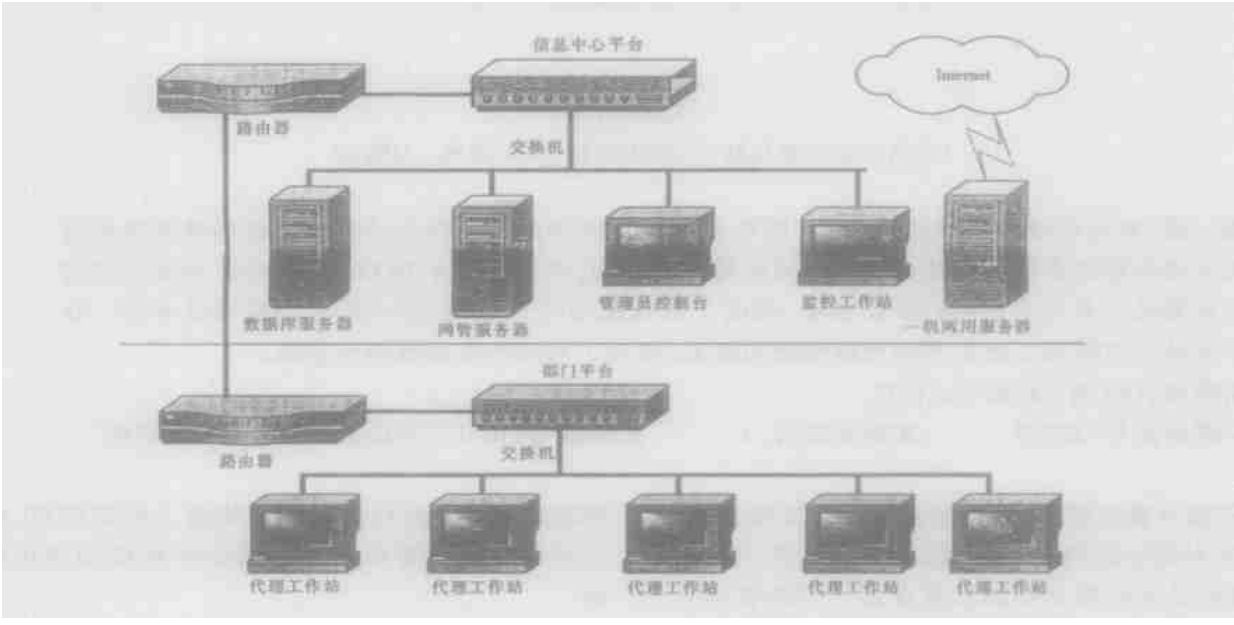


图 1 系统拓扑结构简图

**Fig. 1 Simple Picture Of System Structure**

1.4 软件体系结构

由于企业网络每个部门都有局域网,且分属于不同子网,采用 Client/Server 两层结构无法实现数据的统一管理,因此主机安全实时监控系统的开发采用了基于 DCOM(分布式组件对象模型)技术的Client/Server 三层体系结构见图 2。

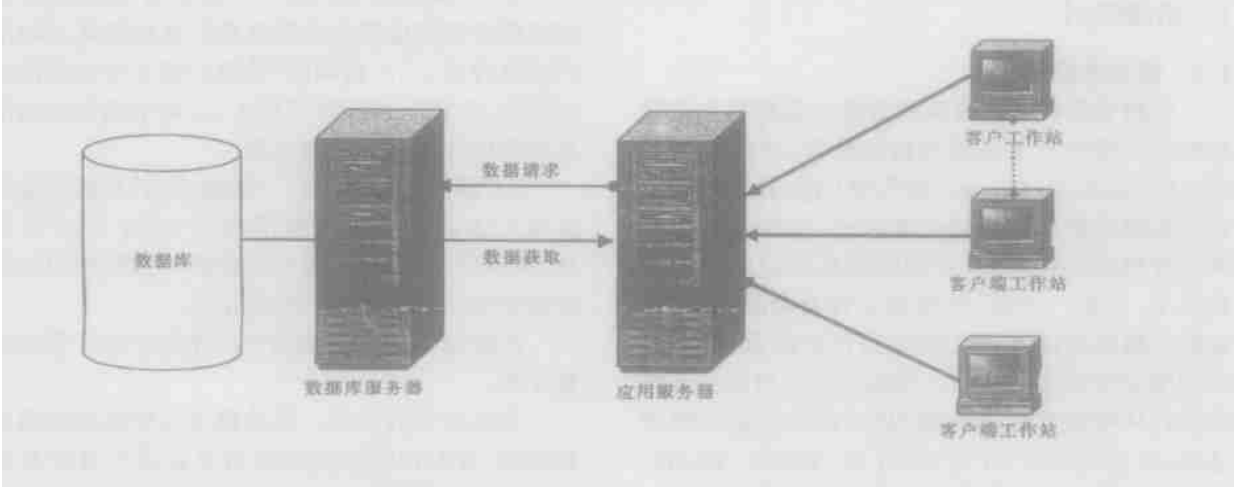


图 2 Client/Server 三层体系结构

**Fig. 2 Three Ties of Client/ ServerSystem Structure**

三层体系结构分布式系统将系统分为三个逻辑层次:

第一层:表示层。在表示层中包含系统的显示逻辑,位于客户端工作站。它的任务是向网络

上的服务器出服务请求,显示用户界面和服务器端的运行结果。

第二层:功能层。在功能层中包含系统的事务处理逻辑,位于应用服务器端,采用 DCOM 技术实现。它的任务是接受用户的请求,执行相应的扩展应用程序与数据库进行连接,向数据库服务器提出数据处理申请,而后将数据处理的结果提交给应用服务器。

第三层:数据层。在数据层中包含系统的数据处理逻辑,位于数据库服务器端。它的任务是接受应用服务器对数据库操纵的请求,实现对数据库的查询、修改、更新等功能,把运行结果提交给应用服务器[2]。

基于 DCOM 的客户/服务器三层体系结构从根本改变了传统的二层客户/服务器体系结构的缺陷,与两层体系结构相比,具有客户端负载小、系统灵活、使用方便、界面友好、开发和维护成本低等优势;与基于 Web 的三层体系结构相比又具有安全性好、客户端处理能力强、数据处理效率高等优点,体现了现代信息系统体系结构的发展方向。

## 2　系统实现

主机安全实时监控系统采用基于 DCOM 的三层 Client/Server 的结构,C++Builder6.0 作为主要开发工具,操作系统为 Microsoft Windows XP,数据库为 Oracle 8i。

### 2.1　应用服务器设计

应用服务器的设计是本设计的核心,也是分布式多层应用优点的体现。它一方面为客户端的请求提出服务;另一方面进行数据库物理位置定义,为数据库提供透明访问,进行性能调整等。

为达到上述功能,利用 DCOM 技术实现应用服务器的设计,该应用服务器具备如下功能:

(1)安全控制:主要针对可能操纵数据库的用户提供安全认证。

(2)实现业务逻辑:一方面根据用户提供的各种检索条件、组合检索条件,向数据库提出检索请求和得到检索结果;另一方面也提供更新数据库的服务。

(3)数据库定位:采用 ADO 技术提供业务逻辑的透明数据库访问。

(4)事务管理:提供多个用户同时对数据库更新和访问时的事务一致性管理。

### 2.2　主要模块设计

主机安全实时监控系统采用基于 DCOM 的 Client/Server 三层数据库应用模式,在系统设计中我们采用 C++Builder 6.0 的 DataSnap 中间件技术提供在客户端(客户端数据集 TClientDataSet)和应用服务器(DataSetProvider)之间传递封装包数据。

下面就代理自动升级和监控站登录管理模块作详细介绍。

#### 2.2.1　代理自动升级模块

主机安全实时监控系统是针对企业网络安全设计的,网络中随时会发生新的问题,需要定时地升级软件来阻断违规行为。升级软件的思路以及代码如下:

在代理软件(hostagent.exe)运行过程中,如果检测到服务器端的版本高于现在所使用的软件版本的话,启动升级程序(update.exe)到服务器下载新版本。解决的主要技术是使用剪贴板实现 IP 地址的动态交换,主要代码如下:

```
//在 HostAgent.exe 中把 ServerIP(服务器端 IP 地址)写入剪贴板
TClipboard * Clipbd=new TClipboard();
Clipbd->Clear();
Clipbd->SetTextBuf(ServerIP.c_str());//其中 ServerIP 为服务器端的 Ip 地址
delete Clipbd;
WinExec("update.exe",1);
Close();

//在 Update.exe 中将剪贴板内容写入字符串变量 Buffer
AnsiString Buffer;
if (Clipboard()->HasFormat(CF_TEXT))
  {
    try {
      Buffer=Clipboard()->AsText;
      strip=Buffer; //strip 用于获取 FTP 地址
      }
    catch (…)
    {
      WinExec("hostagent.exe",1);//如果升级出现异常的话,启动 hostagent.exe 程序。
      Close();
```

```
        return;
      }
    }[2-4]
```

2.2.2 监控站登录管理模块

主机安全实时监控系统的监控站实现对网络的实时监控管理,各类用户有自己的使用权限,通过主程序调用各模块进行网络情况的分析。下面为用户登录的主要代码:

```
SQL="select * form jig jigdm='"+TreeView->Selected->Text+"'";
Query->Data=Query->DataRequest(SQL);
if(Query->IsEmpty())
retrun;
else{
  AnsiString S1=Query->FieldByName("jsgdm")->AsString;
  Query->Close();
  SQL="select * form user where user='"+username+"' &&password='"+passw+"'";
  Query->Data=Query->DataRequest(SQL);
  if(Query->IsEmpty())
    ShowMessage("对不起,您没有权限使用本系统");
  else
    ShowMessage("欢迎您使用本系统");
```

## 3 结束语

目前,企业内部网络通过主机安全实时监控系统的运行,大大地提高了整个计算机网络的管理水平,实现了使整个网络真正处于管理人员的实时监控之下,使之能始终运行于高水平高效率的状态。

参考文献:


[1] 袁辉,刘亚文,邵文. C++Builder 网络编程核心技术[M]. 北京:机械工业出版社,2002.

[2] 陈周造,陈灿煌. C++Builder 4 彻底研究[M]. 北京:中国铁道出版社,2000.

[3] 程展鹏. Borland C++Builder 6 应用开发技术解析[M]. 北京:清华大学出版社,2003.

[4] 葛一楠,李智慧,方宏. 奇思异想编程序—C++Builder 篇[M]. 北京:国防工业出版社,2004.


# Design and Implementation of Host Security Real-time Monitor System Based On DCOM


ZHOU Chun-juan

Department of Computer Science and Technology, Suzhou University, Jiangsu Suzhou 215006, China)



**Abstract**: As network technology develops, network managers are eager to monitor the network situation effectively. This article analyses the structure of enterprise network develops the Host Security Real-time Monitor System based on DCOM and introduces the function modules and provides design principles, framework and implementation techniques of the system. The system resolves the disorders of the enterprise network management and improves the efficiency and reliability.



**Keywords**: DCOM; monitor; agent