一个网络行为实时监控系统的设计与实现*

Design and Implement of A Network Behavior Real-time Monitoring System

陆宇昱，李陶深

Lu Yumin，Li Taoshen

（广西大学计算机与电子信息学院，广西南宁 530004）

(School of Comp.，Elec. and Info.，Guangxi Univ.，Nanning，Guangxi，530004，China)

摘要：根据网络安全实时监控的技术要求，设计和实现一个分布式网络行为实时监控系统。该系统具有对指定网络行为进行实时跟踪、分析和处理获取信息、复原网页内容等功能。该系统采用了监听与识别数据包、分析数据包、减小丢包率等关键技术。

关键词：实时监控 系统结构 分布式 数据包 丢包率

中图法分类号：TP393.07 **文献标识码**：A **文章编号**：1002-7378(2005)04-0260-03

Abstract：A distributed network behavior real-time monitoring system is developed according to the demand of network real-time monitoring. This system has some functions，such as real-time track of an appointed network behavior，analyzing and processing of the acquired information，restoring of Web page content，etc. Some key techniques，such as monitoring and identifying a data package，analyzing a data package，reducing lost package rate have been used in this system.

Key words：real-time monitoring，system architecture，distribute，data package，lost package rate

随着计算机网络技术的迅速发展和广泛应用，信息全球化已成为人类发展的大趋势，网络系统信息的安全和保密逐渐成为计算机网络服务和应用进一步发展的关键问题。网络行为实时监控技术是网络安全研究的一个重要方向，受到人们极大关注。网络安全实时监控就是对网络入侵事件进行证据获取、保存、分析和还原，它能够真实、连续地获取网络或主机上发生的各种行为，能够完整地保存获取到的数据，并且能防篡改，对保存的原始数据进行网络行为还原[1]。

我们根据网络安全实时监控的技术要求，对指定的网络行为的实时跟踪、分析和复原等相关问题进行研究，设计和实现了一个分布式网络行为实时监控系统。

收稿日期：2005-06-24

作者简介：陆宇昱(1982-)，男，广西柳州人，本科生。

*广西科技攻关项目(桂科攻033008-9)和广西留学回国人员科学基金项目(桂科回0342001)联合资助。

1 系统设计

1.1 设计思想

分布式网络行为实时监控系统的设计思想是：(1)利用Sniffer技术的原理[2]，让网络实时监控系统的监听模块在网络底层工作运行，监听同一物理子层的数据报文信息；(2)采用监控子系统与中央监控系统相结合的分布式方式监控数据信息。监控子系统监听所有出入子网的网络数据，并进行相应的分析，将分析结果传送至中央监控系统。中央监控系统接收个子系统传来的分析结果，将动态信息与静态信息相结合，作进一步分析，可以将数据与数据库相比较或直接人为判断，从而做出决策。

1.2 体系结构

系统的结构框架设计如图1所示，系统按功能可分为远程实时监控系统和中央实时监控系统两部分，远程实时监控系统由所有的监控子系统组成。

在网络连接上，子网接入交换机或路由器，监控子系统采取100M以太网卡相连方式与该交换机或路由器连接。中央监控系统与中心交换机或路由器

的连接方式，也是采取100M 以太网卡与之相连。为了提高数据库的运行速度和可靠性，数据库服务器应与中央监控系统分离，相互间连接方式采用100M 以太网卡相连接。如果子网较少，且监控子系统与中央监控系统距离很近，鉴于这两个系统之间相互传输的数据量相对较少，监控子系统与中央监控系统可以采用 RS232 接口直接相连，形成不经过网络的专用通路。

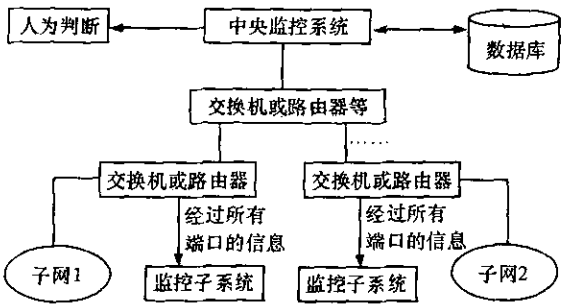

图1 网络行为实时监控系统的结构框架

1.3 子系统功能

在系统功能上，中央实时监控子系统由接收模块、分析模块、控制模块、显示模块、智能判断模块和警报模块构成。其中，接收模块接收从所有监控子系统传送来的数据；分析模块对网络数据包进行分析，提取出有用信息；控制模块将分析模块修改的标识位发送给各监控子系统，各监控子系统执行跟踪和锁定。智能判断模块的功能是判断用户是否登录违规网站和未经授权的网站，是否非法进入某一服务器，如果判断出用户的网络活动存在这些行为，则由警报模块根据智能判断模块的处理结果发出不同级别的警报。显示模块的功能是显示分析模块的分析结果和警报，当需要还原网页时则显示网页内容。

监控子系统由监听模块、识别模块、分析模块、显示模块和传输模块构成。监听模块负责将所有流经的数据都读入缓冲区；识别模块根据每个网络数据包的特征、识别数据包的类型，将数据包提取；分析模块负责对准确提取的数据包进行分析；显示模块负责将这一级监控系统的监控信息和分析结果在窗口界面显示；传输模块将分析结果传输到中央监控系统作进一步分析和判断，并且接收中央监控系统根据网络情况的变化发来的控制信息。

2 关键技术

2.1 监听与识别数据包

网络实时监控系统是通过对网卡编程实现网络通讯，对网卡的编程是使用套接字方式来进行。但是，通常的套接字程序只能响应与自己硬件地址相匹配的或是以广播形式发出的数据帧，对于其他形式的数据帧（如已到达网络接口但却不是发给此地址的数据帧），网络接口在验证投递地址并非自身地址之后将不引起响应，也就是说应用程序无法收取到达的数据包。网络实时监控系统的首要任务恰恰是从网卡接收所有经过它的数据包，这些数据包既可以是发给它的也可以发往别处。显然，要达到此目的，网卡不能按正常的模式工作，而必须将其设置为混杂模式。

编程实现时，这种对网卡混杂模式的设置是通过原始套接字实现，这也有别于通常使用的数据流套接字和数据报套接字。在创建原始套接字后，需要通过 setsockopt()函数来设置 IP 头操作选项，然后再通过 bind()函数将原始套接字绑定到本地网卡。为了让原始套接字能接受所有的数据，还需要通过 ioctlsocket()来进行设置，而且还可以指定是否亲自处理 IP 头。至此，在完成了网卡模式的初始化设置后，就可以开始对网络数据包进行实时监听。对数据包的获取仍像流式套接字或数据报套接字那样通过 recv()函数来完成，但是与这两种套接字不同的是，原始套接字此时捕获到的数据包并不仅仅是单纯的数据信息，而是包含有 IP 头、TCP 头等信息头的最原始的数据信息，这些信息保留了它在网络传输时的原貌。通过对这些在低层传输的原始信息的分析就可以得到有关网络的一些信息。由于这些数据经过网络层和传输层的打包，因此需要根据其附加的帧头对数据包进行分析。根据系统的设计思路，就可以写出网络实时监听和识别数据包功能的实现代码。在编程时，将原始套接字设置完毕后，就可以通过 recv()函数从网卡接收数据。接收到的原始数据包存放在缓存区中，然后就可以根据前面对 IP 数据包、TCP 数据包、UDP 数据包等数据包的段头结构描述而对捕获的数据包进行分析。

2.2 分析数据包

监听网络数据包是网络行为实时监控系统的基础，分析监听到的数据包则是系统的关键环节。发现任何网络异常行为，采取相应的处理措施，都要依据数据包的分析结果进行。

分析数据包的工作包括跟踪用户、锁定用户正在使用的IP、记录登录网页网址和网页内容还原。

跟踪用户是随时从数据包中查询用户是否上网的信息。如果从数据包搜索到有关用户名和用户密码的信息，则将用户添加到列表。在搜索数据包的数据段，查找用户名时，我们采用扫描效率较高的

Boyer-Moore 串匹配算法[3]。该算法以自右至左的方式扫描模式和正文，一旦发现正文中出现模式中没有的字符，就将模式、正文大幅度的“滑过”一段距离，使字符串的查找极大提高了效率。

获得了用户信息意味着同时也获得了分配给用户的IP，于是就锁定了用户当前的IP 地址。根据IP 数据包的源地址或目的地址，将可以将数据包与用户接收和发送的数据对应上。如果只想对IP 进行跟踪，不想了解用户名，可以省略查找用户名的工作，只记录IP 的情况。IP 地址与用户对应上后，对用该IP 登录的任何网站的网址都能记录下来，这些网址就是用户登录网站的记录。系统查找网址时，也采用Boyer-Moore 串匹配算法，具体实现类似于查找用户名。

网页内容还原是将网页源代码从数据包当中完整地提取出来，经过组合，以HTML 文件的形式保存下来。ASP、JSP 等动态网页被打开时，服务器先解释文件，再将解释后的代码传输到用户浏览器。网页内容还原的步骤如下。

步骤1：判断。系统接收到数据包后，立即判断数据段是否非零、源端口号是否为80，满足这2 个条件的数据包才能被处理，否则监控系统不予处理，等待下一个数据包从缓冲区读出。若是在前面数据包的数据段还没有出现字符串“＜html＞”，满足条件的数据包进入程序的下一步骤；否则还需进行进一步判断，由数据段前几个字符判断是否为传输其他数据的数据包，从而跳过对一些无关数据包的处理。

步骤2：查找与识别。利用函数search _htm(int st，char d1[])查找HTML 语言的标识符，识别数据是否为源代码。函数search _htm()是依据BM 算法编写的，若查找不到HTML 语言标识符，search _htm()函数返回值为0，说明数据不是源代码。函数search _htm()执行查找时由形参st 控制，分为3 种情况：(1)当st＝0 时，该函数查找“＜html＞”。若查找到，则返回“＜html＞”的起始位置，认为数据为源代码；否则返回0。(2)当st＝1 时，该函数查找数据中是否存在HTML 标识符列表里的字符串。若查找到，返回1，说明数据是源代码；否则返回0。(3)当st＝2 时，该函数查找“＜/html＞”。若查找到，则返回“＜/html＞”的结束位置，认为数据为源代码；否则返回0。

步骤3：定位。上一步若是获得源代码的起始位置，置一字符指针指向该位置；若是获得源代码的结束位置，将“＜/html＞”的后一字符赋值为‘\0’，截掉此后的数据；若数据是中间部分的源代码，则将一字符指针指向数据的首字符。

步骤4：去除标识。数据包传输的源代码，有时会在源代码数据的开始或源代码当中出现一行如“××”、“×××”(×表示十六进制数)等形式的用于网络传输的标识符号。只有将这些标识符号去除，才能提取到连续的网页源代码。去除标识符号的方法是在出现标识符的位置将数据分段，然后进入下一步骤的提取。如果标识符出现在源代码之前，则跳过标识符，将一字符指针指向出现源代码的位置；如果标识符出现在源代码当中，则在前一段源代码结束的位置放一结束符‘\0’，将另一字符指针指向标识符后的源代码首字符。

步骤5：提取。收集前两步设置的字符指针，将分好段的数据组合，就能得到网页的其中一段连续的源代码。

步骤6：写入文件保存。将得到的一段连续的网页源代码写入文件保存下来，由函数save _htm()实现。该函数能自动计数，将不同页面的源代码写入不同的文件。

数据包的数据经过上述过程的分析、识别、处理和提取，就可以将网页进行还原。

2.3 减小丢包率

因为Internet 上流动的是海量数据，而且数据的流量是随机的，所以网络实时监控肯定存在丢包的情况，这是无法避免的。我们采取一些改善措施，使丢包率尽可能小。

(1)选用合适的缓冲区。先将监听到的数据缓存到缓冲区，减少丢失不能立即处理的数据。设置缓冲区的大小很重要，设置过小，还未处理的缓冲区数据可能很快被新数据覆盖；设置过大，处理完一次缓冲区数据的周期长，新数据覆盖缓冲区可能造成大量连续的数据丢失；设置适当，可使丢失的数据分散，能减小对数据连续性的影响。

(2)采用分布式方式进行监控。监控子系统和中央监控系统相结合，子系统重在接收数据初步处理，中央系统重在处理和控制。分布式系统监控复杂网络可靠性远高于单节点的监控系统。

3 结束语

本文提出的分布式网络行为实时监控系统可以实现对指定网络行为进行实时跟踪，对获取信息进

(下转第268 页)

不会被轻易中止或退出。

当学生端计算机的键盘与鼠标被锁住后，学生端的计算机不能响应键盘与鼠标消息，但仍可正常接收教师端计算机发来的图像和语音信息。而这时一旦发生网络故障，学生端的计算机就会既收不到图像和语音信息，也无法操作计算机。为了应对这个问题，学生端接收程序在锁键盘与鼠标的同时，还要不断监测网络是否通畅（通过定时中断，检测是否收到网络数据来判断网络通断）。如果在规定时间（如300s）内收不到网络数据，就执行解锁操作，并弹出显示“网络不通”的消息框通知用户。从而避免计算机因收不到数据或解锁命令而处于“死锁”状态。

4 程序调试时应注意的问题

本系统在Windows 2000操作系统下工作正常，但尚不能兼容Windows XP环境。在调试和使用前，必须将所有计算机的显示属性作相同的配置（本文介绍的程序是针对学生端和教师端计算机的显示器属性均已设为1024×768像素，16位色彩的条件下设计的），否则，接收端显示的图像颜色和形状会与发送方不同。其次，为了使教师和学生端的屏幕上的鼠标位置相对应，要在学生端调用函数ClientToScreen()把教师端屏幕坐标转换为学生端的客户区坐标。

调试时，图像与鼠标坐标数据的传输发送并不是越快越好，因为广播数据报通讯采用的是UDP协议，它没有流量控制功能。当接收端的处理速度跟不上发送速度时，就会产生丢包现象。因此，在发送端用适当的软件延时作为简单的流量控制，可以改善系统的工作效果。在发送每段图像数据时，加上“Sleep(ms)”作短暂延时，可减少学生端的屏幕闪烁。教师端的鼠标坐标数据如果连续发送过快时，学生端计算机反应速度跟不上，会出现明显的鼠标停滞现象。因此，也需要在两段数据发送之间添加一短暂延时。

参考文献：

[1] 吴礼发. 网络程序设计教程[M]. 北京：希望电子出版社，2002.

[2] 陈 坚. 实例解释VISUAL C++.NET编程[M]. 北京：希望电子出版社，2002.

[3] 梁晨宝. 用VC++制作实时教学工程[EB/OL]. http://www.ccw.com.cn/htm/app/aprog/01_11_12_3.asp，2001-11-12.

[4] 张友生. 远程控制编程技术[M]. 北京：电子工业出版社，2002.

（责任编辑：邓大玉 韦廷宗）

（上接第262页）

行分析和处理，以及复原网页记录等功能。该系统的实现采用了监听与识别数据包、分析数据包、减小丢包率等关键技术。该系统还需要进一步完成的工作是：(1)应用并行处理技术，使接收过程、处理过程和分析数据包的各功能之间能够并行处理；(2)增强还原效果，使能还原的网页内容尽可能多，尤其要实现对图片的还原。

参考文献：

[1] Warren G Kruse. 计算机取证：应急响应精要[M]. 北京：人民邮电出版社，2003.

[2] 陈 千，马剑锋，焦 政，等. Sniffer技术在网络管理中的应用和研究[J]. 计算机工程与设计，2004，25(4)：536-539.

[3] 李 昀，李伟华. 面向入侵检测的模式匹配算法研究[J]. 计算机工程与应用，2003，39(6)：4-6.

（责任编辑：邓大玉）