即时通信监控系统的设计与实现

严 华[1,2],蔡瑞英[1]
(1.南京工业大学 信息科学与工程学院,江苏 南京 210009;
2.安徽邮电职业技术学院,安徽 合肥 230031)

摘 要:针对中小规模企业网(Intranet)对即时通信安全的实际需求,对企业广泛使用的MSN Messenger进行协议分析,然后基于网络嗅探(Sniffer)技术,设计并实现了一个MSN协议监控分析系统——MSNAnalyzer。该系统以监控内部网络和预防资料泄露为目的,主要针对即时通信的文字信息和文件传输。对影响系统性能的关键部分(如数据存储和数据分析)进行了分析,并给出了相应的解决方案。最后对设计的系统进行了性能测试,测试结果显示该系统具有良好的性能,系统可以在不改变现有网络配置,不影响网络运行效率的前提下,满足中小规模企业网对即时通信的安全需求。

关键词:网络安全;MSN协议;监控系统;中小规模企业网
中图分类号:TP302 **文献标识码**:A **文章编号**:1673-629X(2009)07-0242-03

Design and Implementation of Monitoring System of Instant Messaging

YAN Hua[1,2],CAI Rui-ying[1]
(1.College of Information Science & Engineering, Nanjing University of Technology,Nanjing 210009,China;
2.Anhui Vocational College of Posts and Telecom, Hefei 230031,China)

Abstract:Aims at the factual security requirements of medium and small scale enterprise network. By means of protocol analysis,detailly analyzed the application protocol of MSN Messenger. A MSN protocol monitoring system based on network sniffer was designed and implemented. Two main functions of the system are monitoring behavior of employees and preventing spilling of secret information. Also considered about issues that would affect performance of the system, such as packet storage and data analyzing. Finally, performance tests are made on the given system. The test result indicates that the system has good performance; it can satisfy network security requirements of small scale Intranet without affecting topology and efficiency of the network.

Key words:network security;MSN protocol; monitoring system;medium and small scale Intranet

0 引 言

随着科技的发展和计算机网络的普及,即时通信软件已逐渐融入人们的生活。即时通信软件为个人和企业提供了便捷、快速、高效的沟通方式。常用的即时通信软件有微软的MSN Messenger、腾讯QQ、Google Talk[1]等。即时通信技术在给个人及企业带来高效便捷沟通的同时也产生了一系列的安全问题。随着即时通信软件的普及和用户数量的快速增长,其已成为病毒和黑客攻击的主要对象。对于企业而言,即时通信技术使得员工的行为更加难以控制,容易导致泄露机密、窃取资料等事件的发生,这将给企业造成无法估量的损失。

针对中小规模企业网对即时通信安全的实际需求,对企业广泛使用的MSN Messenger进行了协议分析,并在此基础上设计实现了一个基于网络嗅探技术的MSN协议监控分析系统——MSNAnalyzer。该系统可以对企业内部网络进行实时监控,监督员工的上网行为,预防重要资料泄露等情况的发生,保护企业的信息安全,减少不必要的经济损失。

1 体系结构

该监控系统采集企业网络出口处的所有数据帧,通过对帧的IP地址进行分析提取出被监控客户机的数据帧并以一定的格式保存到文件中。然后,从文件中读取数据帧并将数据帧交给协议分析处理模块处理,处理后的结果以文件的形式保存在磁盘中。图1所示为该系统的总体结构示意图。图中,Sniffer是运行MSNAnalyzer程序的主机,Client1、Client2、Client3

收稿日期:2008-11-14;**修回日期**:2009-01-04
基金项目:安徽省高等学校自然科学研究项目(KJ2008B104ZC)
作者简介:严 华(1979-),女,江苏泰州人,硕士,讲师,研究方向为网络安全与应用;蔡瑞英,教授,研究生导师,研究方向为网格计算、网络安全技术。

为内网主机。

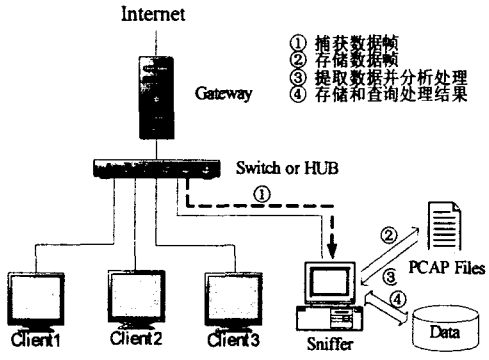

图 1　系统体系结构

MSNAnalyzer 工作的基本过程为:

(1)基于 Sniffer 技术从网络总出入口处采集网络数据(抓包)。

(2)存储数据帧。

(3)提取数据帧并进行分析。

根据分析,系统实现模型如图 2 所示。

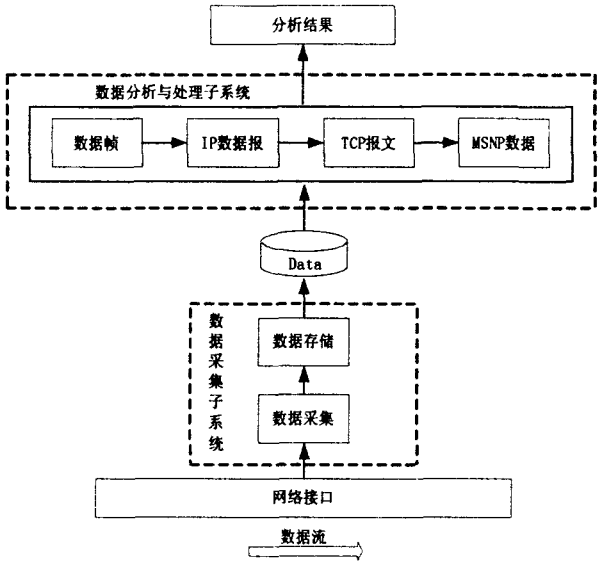

图 2　系统总体实现模型及模块划分

2　数据采集及存储

系统采用基于网络嗅探技术的数据采集方法,以 WinPcap 4.0.1 作为开发工具,Windows 平台下使用 WinPcap 从网络适配器嗅探数据十分方便,图 3 是使用 WinPcap 捕获网络数据包的基本流程[2]。

使用 WinPcap 开发应用程序除可以捕获数据包外,最大的优点在于 WinPcap 可以对数据包进行过滤。WinPcap 从网络适配器上嗅探到的是最原始的数据帧,这包括了所有流经的数据。如果不对数据包进行相应的过滤,将会捕获到许多无关的数据,这会增加系统的负担,使系统工作效率降低。

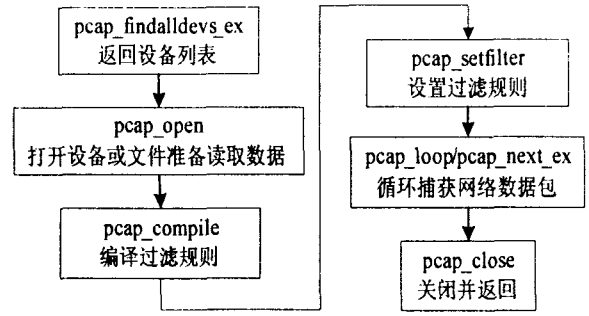

图 3　WinPcap 数据采集流程

在数据采集之后,采用什么样的存储策略来存储数据,以最大限度地保证采集到的网络数据包(Packet)不丢失,是系统设计中必须面对的一个重要问题。网络丢包的原因可能有很多,包括内存缓冲技术、磁盘 I/O 能力、包过滤及处理技术、数据流量大小、网络接口性能、CPU 处理能力等诸多方面[3,4]。

网络丢包的指标一般采用丢包率(Rate of Packet Loss, RPL)。计算公式为:L =((发送的数据包数 − 接收到的数据包数)/发送的数据包数)×100%。

众所周知,频繁的磁盘 I/O 显然会影响到系统的性能和效率,这在大的数据流量下尤为明显。为了避免频繁的磁盘 I/O,需要在数据存储时引入内存缓冲处理技术。在基于 WinPcap 的网络数据采集中,系统使用了多级内存缓冲,内核缓冲器和用户缓冲器的大小分别设置为 6MB 和 1MB,并设置内核缓冲器和用户缓冲器之间一次传送的最小数据块的大小为 512kB。

3　数据分析与处理

数据分析与处理分为四部分。首先是 Ethernet 数据帧处理,主要完成链路层数据验证、拆包,并将数据提交给 IP 层进行处理。IP 数据报的处理主要完成 IP 层数据验证、拆包,并将数据提交给传输层进行处理。TCP 分组的处理主要完成 TCP 层数据的验证、拆分及 TCP 重复和无序分组的处理,完成 TCP 会话重建,并将重组后的应用层数据提交至协议分析层处理[5]。协议分析主要完成应用层数据和最终用户数据的处理。对应用层数据主要进行命令解析和协议数据重组,对最终用户数据的处理包括聊天信息的提取、显示图片和自定义表情的提取、文件传输的提取等。MSNP 协议分析模型如图 4 所示。

3.1　命令解析

命令解析的本质就是分析字符串的含义,它类似计算机高级语言编译器中词法分析的功能[6]。MSNP 协议涉及多达几十个命令,服务器和客户端使用的命

令也不相同。系统对涉及信息传输的命令进行了重点解析,主要包括握手命令和数据传输命令。对于客户端命令,主要解析"ANS"和"MSG",服务器端主要解析"IRO"、"USR"、"JOI"和"MSG"。

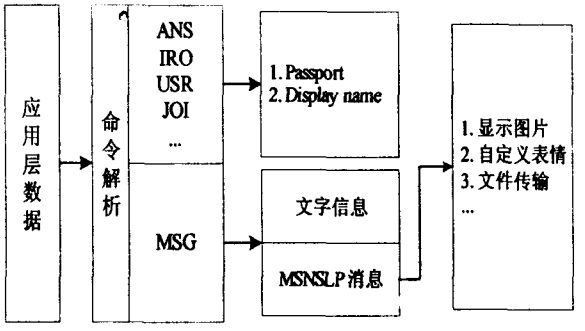

图 4 MSNP 协议分析模型

3.2 协议数据重组

协议数据重组主要针对 P2P 消息,当二进制头和二进制尾之间的消息内容大小超过 1202 字节时,消息会被分片传输。通常被拆分的 P2P 消息包括 MSNSLP 消息和实际传输的各种数据(如文件、表情)。二进制头中共有 9 个字段,其中"Data Offset"、"Total Data Size"和"Message Length"3 个字段和消息分片密切相关。这 3 个字段分别表示"总数据大小"、"数据偏移量"和"本条消息长度"。由于 TCP 处理模块已对重复和无序的数据流进行了处理,协议分析模块的输入是顺序的数据流,按顺序将数据取出即可。如图 5 所示。

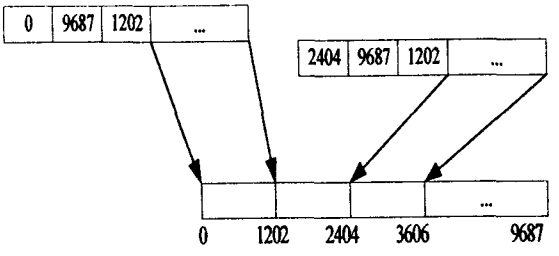

图 5 P2P 消息重组方法

3.3 数据存储

在协议数据重组之后,对重组的数据进行分析及数据提取[7,8]。分析主要针对 MSNSLP 消息,MSNSLP 消息负责会话的建立和结束。对 MSNSLP 的分析除取得传输的类型外,最重要的是提取文件名,以备存储时使用。显示图片和自定义表情的文件名封装在各自的 MSNObj 对象中,而传输文件的文件名以 Unicode 格式存储在 INVITE 方法的 Context 中类 CFileName 用于存储文件名,其结构如下:

```
// name of file transfered in a session
class CFileName {
public:
    CFileName();
    ~CFileNameTrans();
public:
    u_int m_nSessionID; // Session ID
    char * m_pszFileName; // Name of current file
};
```

其中数据成员 m_nSessionID 用于确定文件名和文件数据的对应关系。在数据提取完毕后根据 CFileName 和 CDataTrans 的 m_nSessionID 大小得到对应关系,进行数据存储。

3.4 性能方面的考虑

在数据流量比较大的时候,数据处理会导致大量的内存占用,从而降低系统的效率。对于协议数据重组模块,尤其是传输文件的提取,系统使用定时器机制和定量存储机制进行控制。

当接收到第 1 个分片的时候对相应的 CDataTrans 对象设置定时器。如果在定时器超时的时候仍没有接收到新的分片,就认为此次传输失败,将之前缓存的数据清除,释放所占用的空间。若有新的分片到达,还原定时器的超时时间。系统预设的定时器为 10 分钟,管理员可以重设超时时间。

对于大小超过 1MB 的文件,系统采用定量存储。当接收的数据大小达到一定量,便进行一次存储操作。当然,频繁的存储操作会增加磁盘读写的开销。系统预设大小为 1MB,管理员同样可以更改大小,以减少磁盘读写的开销。

4 系统测试

系统测试主要是对系统进行性能测试,目标是测试系统在给定工作环境下的性能,检查系统对指定数据的监听提取能力。监控服务器主机一台,客户机(目标主机)若干,客户机通过交换机连接在一个局域网中,并与 Internet 互联。对上述测试环境进行一个工作周(周一到周五)测试,每个工作日测试时间为 12 小时(早 8 点到晚 8 点),每个工作日客户机数量维持在 124~168 之间,测试结果如表 1 所示。

表 1 测试结果

数据类型	邀请数	捕获数	提取率
显示图片	2386	2359	98.9%
自定义表情	43827	42469	96.9%
文件传输	7359	4541	61.7%

从上表可以看出显示图片和自定义表情的提取率均在 96%以上,数据丢失的原因主要是由于丢包造成的,由于系统采用过滤策略进行数据包捕获,在网络流量比较大的时候,可能会导致一定的丢包率,而显示图

(下转第 248 页)

数据直接传送给监测中心 PC1；

(3)PC1 将实时接收 PC2 传来的数据，并通过数据包区分出数据的通道，完成每个通道的数据独自实时显示。

本系统运行的具体操作过程如下：

首先，在 PC1 下启动监测中心软件，运行数据监测模块，单击“开始采集”按钮，系统进入到监听端口的状态。

然后，在 PC2 和 PC3 下分别修改路由文件 route.ini，令 PC2 和 PC3 构建成网络。PC2 的路由文件内容如下：

59.64.180.1.0.0>59.64.180.183.0.0

59.64.180.3.0.0>59.64.180.1.0.2

59.64.180.100.0.0>59.64.180.183.0.0

保存好路由文件，运行 PC2 和 PC3 上的程序，此时可观测到 PC2 主进程的运行状态，主进程首先读取路由文件，初始化内存中的路由表，然后进入到数据处理阶段。此时系统已经正常运行起来，监测中心 PC1 也接收到监测点传来的数据。

3 结束语

本课题利用嵌入式和 Internet 网络的优势，设计并开发了一套教学监测系统软件。主要阐述了教学监测系统的软件设计，包括远程现场监测点的网络构建、主进程模块及数据处理算法模块等。实现了监测中心和监测点的网络化数据处理及传输，提高了教学监测系统的数据处理效率。本监测软件系统具有应用领域多样化和监测对象多样化的优势，为今后进一步开展这方面的硬件配套研究及相关软件的继续开发工作打下了良好的基础。

参考文献：

[1] 韩树人，周贤娟，鄢化彪，等. 基于嵌入式 Web 服务器的远程实时数据采集[J]. 计算机技术与发展，2008，18(1)：206－208.

[2] 燕 延，陈保平，马增强，等. 网络化远程桥梁健康监测系统的设计[J]. 微计算机信息，2005(8)：39－41.

[3] Johnson P, Andrews D C. Remote continuous physiological monitoring in the home[J]. Journal of Telemedicine and Telecare, 1996, 2(2): 107－113.

[4] 施伟年，凌海宏. GPRS 网络上的两种数据传输协议[J]. 电力系统通信，2004(8)：20－22.

[5] Olaf F. Remote Monitoring and Control of Electrochemical Experiments via the Internet Using Intelligent Agent Software [J]. Electroanalysis, 1999, 11(14): 56－64.

[6] 宋克章，王月茹，冯胜章. 基于 ARM 的有线无线混合网网管实现[J]. 计算机技术与发展，2007，17(8)：190－193.

[7] James Won－Ki Hong, Ji－Young Kong. Web－based Intranet Services and Network Management[J]. IEEE Communications Magazine, 1997, 8: 100－110.

[8] 李艳霞，巩九洲，黎玉琴. 一种基于 Web Services 的信息集成方案[J]. 计算机技术与发展，2008，18(9)：105－107.

(上接第 244 页)

片和自定义表情文件比较都比较小，若干数据包的丢失对结果会有一定影响。文件传输的提取率只有 61.7%，原因主要有 3 个方面：一是丢包率；二是协议分析中对 NAT 穿越的判断结果；第三点，也是最重要的一点，当传输的双方位于同一局域网时，实际数据传输仅在局域网中进行，而不会通过服务器中转，这样系统仅能监听到传输邀请，而无法监听到实际传输的数据。测试结果没有对文字信息进行评估，因为文字信息的传输没有握手过程，难以评估。系统的设计实现能够保证在丢包率较小的情况下，使文字信息的提取率接近 100%。

5 结束语

针对中小规模企业网对即时通信安全的实际需求，研究、设计并实现了 MSN 协议的监控分析系统。首先分析了系统的功能和性能需求，并给出了系统的体系结构、总体实现模型。接着详细讨论了数据采集与存储策略，数据分析与处理的过程，重点研究了 MSNP 协议的分析。最后，对系统性能进行测试，并对测试结果进行了分析。

参考文献：

[1] 杨晓军，尚振宏，郭 琳. 全分布式 P2P 即时通信[J]. 计算机技术与发展，2008，18(3)：96－98.

[2] 胡晓元，史浩山. WinPcap 包截获系统的分析及其应用[J]. 计算机工程，2005，31(2)：96－98.

[3] 李雪莹，刘宝旭，许榕生. 基于 WinPcap 的网络监控系统性能优化[J]. 计算机工程，2004，30(1)：8－9.

[4] 廖俊云，范明钰，王光卫. 一种改进的基于 WinPcap 的快速抓包方法[J]. 计算机应用研究，2005，22(9)：235－236.

[5] Stevens W R. TCP/IP Illustrated, Volume 2: The Implementation[M]. [s.l.]: Addison－Wesley, 1995.

[6] 张永梅，靳雁霞. 编译原理学习与应用指导[M]. 北京：国防工业出版社，2006.

[7] Day M, Sugano H. A Model for Presence and Instant Messaging[S]. RFC2778, 2000.

[8] Day M, Aggarwal S, Mohr G. Instant Messaging / Presence Protocol Requirements[S]. RFC2779, 2000.