第25卷第3期 华东交通大学学报 Vol. 25 No. 3
2008年6月 Journal of East China Jiaotong University Jun. ,2008

文章编号:1005-0523(2008)03-0074-04

基于WFP系统的网络反黄系统过滤驱动研究

左黎明,汤鹏志

(华东交通大学 基础科学学院,江西 南昌 330013)

摘要: 随着互联网的普及,网络色情信息充斥了整个网络,严重败坏了社会风气,尤其对未成年人心理健康危害极大. 本文分析了Windows Vista平台下网络反黄系统开发原理和关键技术,并对Vista平台下一种新的网络过滤系统WFP进行了剖析,研究并设计了基于WFP系统和正则表达式的网络淫秽信息实时过滤驱动,提出了一种新的过滤技术,该技术采用正则表达式和独特的二级表结构,实践表明该系统设计具有良好的实用性.

关 键 词: WFP; 网络过滤; 内核; 驱动

中图分类号: TP316 TP311.5 **文献标识码:** A

随着互联网技术的普及,各种类型的个人站点和组织站点如同雨后春笋般地涌现,在丰富了互联网的内容和方便了人们进行交流与学习知识的同时,也带来了一种灾难-黄色淫秽信息的泛滥,给青少年身心健康带来非常不利的影响,相关职能部门的监督能力有限,因此开发各种能够有效过滤不良信息的网络反黄系统十分必要,而网络反黄系统的核心部分是不良信息识别分析模块和内核网络过滤驱动模块. Windows Vista(以下简称Vista)是微软公司推出的最新的桌面操作系统,是未来的主流操作系统平台. 相对于以前的NT架构的操作系统(包括win2000/winxp等),其网络结构变化非常大,原有的基于TDI、IPFIREWALL和传统NDIS网络过滤驱动的开发方法将逐渐得不到支持. 但是在Vista系统中,微软引入了一种新的网络过滤系统模型-WFP(Windows Filtering Platform). 目前国内外用于不良信息过滤的主要方法包括分级法、URL地址列表法、文本内容过滤技术和多媒体信息过滤技术等[1]. 本文提出了一种新的过滤技术,该技术采用正则表达式和独特的二级表结构,将匹配淫秽信息频率高的正则表置于一级表中,将出现次数一般和频度不太高的置于二级表中,此技术大大提高了反黄系统过滤驱动的效率.

1 网络反黄系统过滤关键技术分析

1.1 已有的过滤技术及其不足

文献[2]提出了一种通过优化词典匹配判定文本性质的改进算法,文献[4]提出了一种自学习的贝叶斯邮件过滤模型,文献[5]提出了一种基于特征词和局部语义分析的文本分类与过滤方法,在基于特征词统计特性分析的基础上,将特征词的知识属性和局部语法匹配引入信息过滤模型. 文献[6]分析了向量空间模型、关键词匹配算法等关键技术,提出了一个改进的Web文本内容过滤方法,但这些方法在驱动中实现并进行实时过滤是非常困难的,其主要原因是容易造成网络的中断和大规模丢包.

1.2 基于语义的淫秽信息自动识别算法

HTML是一个结构化的文档,分析其结构可以获得许多关于网页内容和类别的描述信息. 通过对大量网页的分析发现,要从HTML文档中提取有用的关键字,需要进行以下几个步骤的处理,首先通过

收稿日期: 2008-03-04

基金项目: 江西省自然科学基金资助项目(2007GZS1054);华东交通大学校立科研基金资助项目(07JC03).

作者简介: 左黎明(1981-),男,江西鹰潭人,讲师,软件工程师,理学硕士,主要研究方向为信息安全,非线性系统分析.

HTML 标志符过滤器,去除文本中夹杂的 HTML 标签,如〈BR〉,〈TR〉等,此后得到的是句子和短语的集合,我们再运用词典技术将集合切割成独立的单词,但这些词还不足以构成描述,因为许多单词并无确切的含义,再通过小词过滤器(small word filter) 过滤掉助词、介词、连接词等无意义词,至此文本已抽象成为关键字的集合,再以每个关键字为分量构造一个高维向量,其中每个分量的长度是用"TF* IDF"算法得到该关键字的权值.

计算机对特定内容的识别率需要达到一定的准确度,需要具备分类的基础知识库,将知识库的语义数学模型与网站内容的语义数学模型相比较,研判二者的相似度,给出分类及分级指数. 基础知识库的知识覆盖面和语义数学模型决定了机器内容识别的准确度. 我们可以通过以下方法进行搜集: (1) 通过门户搜索引擎,利用专用软件检索、识别、分类,将被门户分类的成人、色情等淫秽网址复制到数据库中; (2) 自己构造一个淫秽信息发掘网络,采用网络蜘蛛在网络中爬行访问,采用 QBE(Query By Example) 和 LSA(Latent Semantic Algorithm) 查询含有特定内容的网址,分析语义,判断网址的分数,运行的结果增量经过人工核查后发布到升级数据库中; (3) 还有一部分数据来源于人工检索,用户的反馈信息等; 在运行期同时结合关键字过滤,可以达到比较高的不良网址覆盖率.

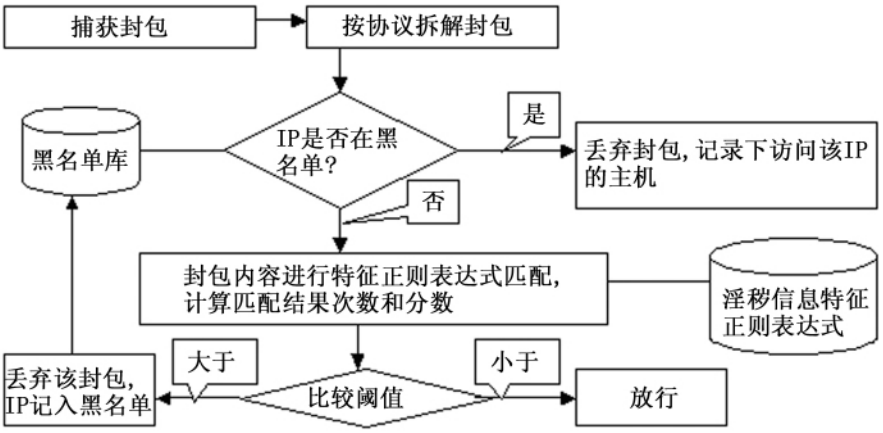

图 1　基于淫秽信息特征正则表达式的实时过滤流程

1.3　基于正则表达式的淫秽信息实时过滤

主动过滤是通过事先分析站点内容,判断是否存在淫秽信息,根据内容级别决定站点网址是否进入黑名单,在过滤驱动中直接丢弃该网址的封包. 但有不少情况下,我们无法根据黑名单使用过滤(比如: 浏览者或者淫秽站点使用了代理服务器) ,因此在这种情况下我们需要使用特定的正则表达式在驱动层对网络封包进行分析过滤. 如图 1 所示,首先捕获请求页面的所有网络封包,进入封包缓存队列,按协议拆解封包,如果该封包的来源地址已经在黑名单中,则抛弃所有该 IP 对应的封包,如果不在其中,则对封包内容进行预先格式化处理后,利用淫秽信息特征正则表达式进行匹配,计算匹配度,根据匹配度值决定是否放行或者丢弃,并将发现的新的淫秽站点 IP 添入黑名单.

2　过滤驱动设计与要点分析

2.1　WFP 过滤工作原理与要点

WFP 网络过滤体系从用户态(ring0) 到核心态有很多层,每一层又可以分成若干子层,根据实际需要可以在某一层设置回调函数拦截数据. WFP 网络过滤体系很像一个已经有了数据过滤引擎的防火墙[8-11],但是没有规则. 我们只要在用户层的程序中给 WFP 引擎设置规则,编写核心态的 callout 驱动处理 WFP 抓到的网络数据包,就可以按照我们预先的要求对数据包进行加工或者反馈相关信息. 实际上,callout 就是加载用户特殊用途的回调函数机制.

callout 是 WFP 系统提供的扩展其功能的一种机制,callout 由一组 callout 函数组成,每组有三种函数,ClassifyFunction 处理收到的网络数据,例如端口号、IP 地址等. NotifyFunction 处理加载、删除 callout 事件. FlowDeleteFunction 删除层与层之间关联的上下文. callout 由 callout 驱动具体实现,每个驱动可以注册多个 callout.

首先我们编写一个 callout 驱动,用来处理 WFP 抓到的网络数据封包. 由于 WFP 抓到的数据只送到

callout 驱动不会送到用户层程序，所以这里必须用 驱动根据数据判定放行还是阻止.

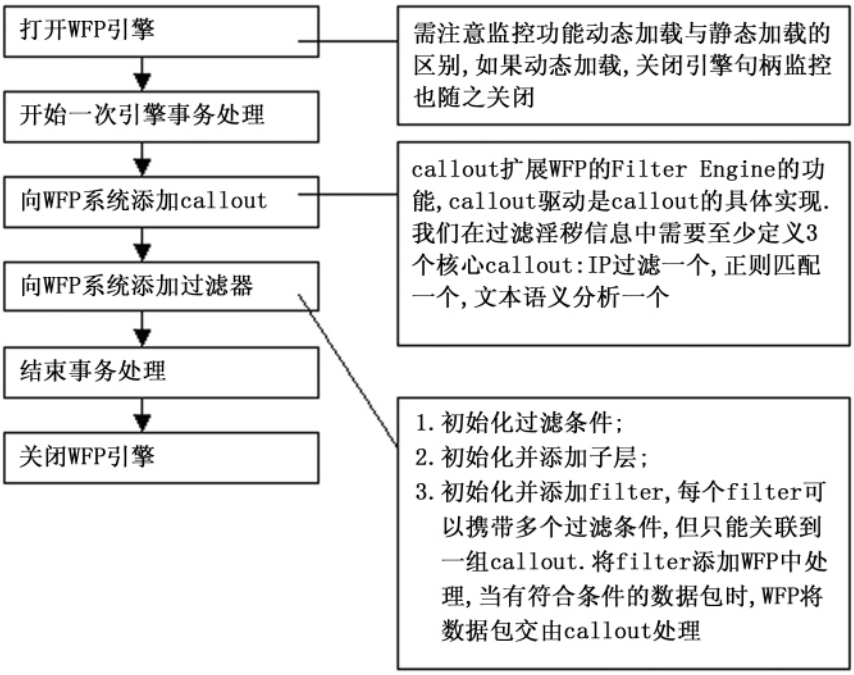

图 2 WFP 过滤驱动开发运行原理

我们还需要再定义 3 个核心的 callout：一个 IP 过滤 callout，一个正则匹配 callout，一个文本语义分析 callout，完成 callout，接着就是向 WFP 系统添加过滤器. 如图 2 所示，完成整个过滤流程.

2.2 实时淫秽特征正则表达式分析要点

在用淫秽特征正则表达式匹配之前，我们需要进行一些预处理. 来自不良网站的网络淫秽信息 HTML 页面封包中，含有大量与文本无关的信息，如分隔符、排版代码、表、图片、音乐、动画等对象，以及网页的脚本描述和链接其他标记. 通常自定义匹配 html 标记的正则表达式“<(.*) >.* <\/\1 >|<(.*) \/ >”，可以滤去所有的标记符.

另外，为了加快匹配的准确性和速度，正则表达式字符串使用二级表结构存储，一级表中存放最常用的和出现频率较高的，如过滤“做爱”、“激情脱衣”等常见词汇，比如正则表达式“做爱|激情(脱衣|视频)”. 而一般较少见的词汇放入二级表. 通常我们进行实时过滤时采用一级表，主动采集黑名单库的时候同时使用一级表和二级表. 一级表和二级表可以在在驱动对应的用户层应用程序中进行设定.

有些时候，单个词汇并不能认定为淫秽特征，我们需要根据实际情况和淫秽文本特征设定只要一个网页中同时出现多个词汇的一个序列，如“…上…摸…脱…日…爽…”，即认为是淫秽信息特征，由此构造特征序列表和对应的正则表达式“上* 摸* 脱* 日* 爽* ”. 当然这里为了降低误判度，需要设置一个匹配度阈值，只有当多个正则表达式匹配成功后才能认定为不良站点. 这里计算匹配度阈值的方法为：

匹配度 = 匹配条数/正则表达式总条目数.

2.3 驱动中还要考虑的问题

除了在驱动层完成对淫秽信息过滤功能设计外，我们还要考虑整个反黄系统本身的安全性，因此需要在驱动中增加反黄系统自身进程的保护功能. 主要的方法是采用在驱动中通过 HOOK 内核函数 NtQuerySystemInformation() 和函数 ExpGetProcessInformation()，将自己的相关进程从返回结果中去除或者直接从 ActiveProcessLinks 摘除自身相关进程信息，即要把要隐藏进程的 EPROCESS 从 LIST_ENTRY 中摘除，这样反黄系统进程和服务将不在进程列表中出现. 同时建立一个守护进程，当用户在非授权或者输入关闭反黄系统密码错误的情况下通过一些特殊方法强制关闭进程时候，马上创建新进程，恢复保护. 另外，我们通过 BHO 挂钩技术和键盘输入截获，拦截试图通过 IE 浏览器(或者其它类型浏览器)打开搜索引擎时候输入的淫秽信息检索要求. 除此之外，对于匹配度阈值的选择，一级库一般要求其值在 2% -5% 之间.

3　实验结果与结论

通过实验,在 windows VISTA 平台下,硬件配置为 AM2 双核 1.7GMHZ,内存 1G 的普通 PC,开发工具选择 vc6.0,正则表达式分析器采用开源 C++库 boost 中自带的,一般利用一级表(264 个词汇)和特征序列表(197 个序列)过滤准确率可以达到 87%,网络速度几乎没有降低. 本文在文献[6]中算法基础上,结合实时淫秽特征正则表达式,取得了实时过滤较好的结果.

参考文献:

[1] 林建,张帆. 网络不良信息过滤研究[J]. 情报理论与实践,2007,30(4):534-539.

[2] 赖勇浩,谢赞福. 防干扰的不良网页过滤算法研究[J]. 计算机工程,2007,33(11):98-99.

[3] 汪琴,安贺意,秦颖. 网络信息过滤和个性化信息服务[J]. 情报科学,2007,25(6):858-863.

[4] 殷海波,宁绍军,王东. 基于内容的贝叶斯自学习邮件过滤模型[J]. 计算机应用与软件,2007,10(10):177-182.

[5] 曹　海. 基于文本内容分析的过滤技术研究[J]. 四川大学学报(自然科学版),2006,43(6):1248-1252.

[6] 于海燕,陈晓江,冯　健. Web 文本内容过滤方法的研究[J]. 微电子学与计算机,2006,23(9):51-54.

[7] 朱烨行等. 基于内容审查过滤的网络安全研究[J]. 计算机应用研究,2006,24(10):130-132.

[8] E. Al-Shaer,H. Hamed. Firewall policy advisor foranomaly detection and rule editing[J]. IEEE/IFIP Integrated Management IM'2003,2003,1(3):17-64.

[9] E. Al-Shaer,H. Hamed. Management and translation of filtering security policies[J]. IEEE International Conference on Communications,2003,12(5):147-151.

[10] E. Al-Shaer,H. Hamed. Discovery of policy anomalies in distributed firewalls[J]. IEEE INFOCOM'04,2004,3(3):112-114.

[11] A. W. Alain,Mayer,E. Ziskind,Fang. A firewall analysis engine[J]. Proc. of IEEE Symp. on Security and Privacy,2000,44(3):177-187.

Study of Filter Driver of Anti-pornography System Base on WFP

ZUO Li-ming,TANG Peng-zhi

(School of Natural Science,East China Jiaotong University,Nanchang 330013,China)

Abstract: With the popularity of the Internet,Internet pornography is flooding the entire network,which degrades social conduct,and especially has done great harm to the mental health of minors. The paper analyzes the principle and key technology of network anti-pornography system inside Windows Vista operating system. After discussing a new network filter system-WFP,the paper designs and implements a network anti-pornography real-time filter driver based on WFP and Regular Expression inside Windows Vista operating system. We put forward a kind of new filter technique which adopts a special second-class form structure. Practice shows that the system is a good practical design.

Key words: WFP; network filter; kernel; driver

(责任编辑: 周尚超)