用ISAPI过滤器实现Web的访问监控

孙焕东 赵东升 张华 (北京医学信息研究所网络信息中心 100850)

摘要：作为Internet服务商或网络管理员，如何对用户的Web访问实现认证，以监测用户的合法访问，是网络计费管理中不容忽视的重要问题。本文介绍了一种通过ISAPI的过滤器实现Web帐号监控的方法，该方法将用户IP地址与其帐号捆绑在一起来认证用户的帐号，从而基本上杜绝了盗用他人帐号的问题，实现了基于web的访问认证，使网络计费更加公正合理。

关键词：Web访问 ISAPI过滤器 网络计费 访问认证

1 引言

不管是Internet服务商，还是Internet系统管理员，都需要考虑对用户上网进行计费。要完成计费，可能有不同的计算方式，可以按IP地址，也可以按用户帐号。一般地，在局域网上的用户，大都按用户访问的通信量计费，而电话拨号上网的用户，则都按上网时间计费[1-4]。为了达到公正合理的计费，必须设计有效的用户监控机制，以防止用户盗用他人的身份上网和逃避计费。对于以IP计费及监控的方法，我们曾开发过有效的技术[1,2]，以保证网络计费的公正合理性。这里主要介绍通过HTTP代理服务访问Internet中，对上网帐号的认证监控问题，以保证用户的合法使用。

为防止盗用他人的帐号，除了用户要管理好自己的口令外，还要建立安全的帐号使用规则，如用户的口令不得少于若干位，用户登录的次数是有限的，用户应当定期更改口令等。这些规则可以部分地保证用户安全地使用自己的帐号，但不能杜绝他人的盗窃，原因是有些用户不注意设置可靠的口令。在一个通过用户帐号访问Internet的网络上，人们盗窃帐号的主要目的是通过浏览器查阅信息，所以只要防止用户以Web方式非法使用即可。我们采用的方法是采用ISAPI的过滤器，对用户帐号进行监控，一旦发现非法访问，就立即关闭该用户访问Internet的能力。

2 通过ISAPI实现HTTP的访问控制

ISAPI是基于MS Windows系统下Internet信息服务的应用程序接口，用户可以通过它实现动态Web的功能，它比CGI具有更好的运行效率。利用ISAPI，用户还可以访问数据库，建立基于Web的数据库系统。此外，还可以通过ISAPI实现基于Web的访问认证，建立HTTP的访问过滤器。ISAPI的过滤器有许多功能，如可以对访问用户的帐号进行认证，实现访问的重定向，对访问进行压缩，对访问口令实行加密，实现登录控制，进行流量分析等。ISAPI过滤器其实是运行在服务器端的一个Windows的动态连接库DLL，当用户通过HTTP向Web服务器发出请求时，该DLL就可以对所要处理的事件进行过滤，以完成赋予它的功能。在一个Web服务器上，可以建立多个过滤器，当客户通过浏览器发出HTTP请求时，Web服务器根据各个过滤器的优先级，逐个地处理每一过滤器中的事件。如果过滤器的功能是登录控制，则该服务器就可阻止不允许的访问。一旦一个高优先级阻止了HTTP的请求，则低优先级的过滤器就不会被执行（见图1）。过滤器作为一个DLL，它必须有自己的外部接口，它提供了三个接口函数：GetFilterVersion、HttpFilterProc和TerminateFilter。第三个函数TerminateFilter仅仅是结束过滤器要做的工作，一般可以不用，因为在DLL的入口点同样可以完成一些进入后和结束前的工作。

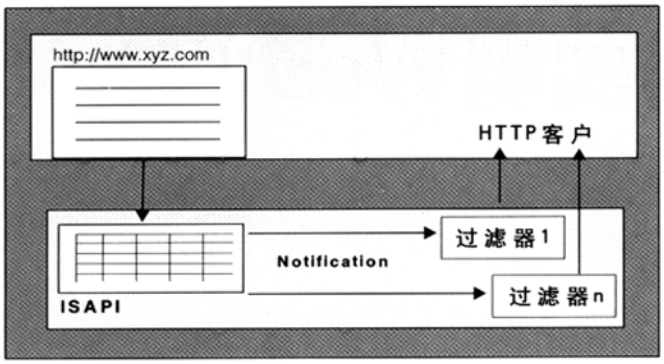

图 1 过滤器的工作过程

GetFilterVersion 函数是在 DLL 装入时调用的，它主要是让过滤器获取服务器的版本信息，设定过滤器要处理的事件。注意，用 GetFilterVersion 设定事件时，要尽可能少地设定所处理的事件数，因为设定过多的事件会极大地影响 Web 服务器的性能。过滤器可以设置下述事件：

SF_NOTIFY_SECURE_PORT——仅注意HTTP会话的安全端口。

SF_NOTIFY_NONSECURE_PORT——仅注意HTTP会话的非安全端口。

SF_NOTIFY_READ_RAW_DATA——允许查看原始数据。

SF_NOTIFY_PREPROC_HEADERS——预处理HTTP信息头。

SF_NOTIFY_AUTHENTICATION——对访问的客户进行认证。

SF_NOTIFY_URL_MAP——将逻辑地址 URL 映射到物理地址。

SF_NOTIFY_SEND_RAW_DATA——服务器将原始数据送回客户端。

SF_NOTIFY_LOG——记录访问的日志信息。

SF_NOTIFY_END_OF_NET_SESSION——结束客户的 HTTP 会话。

SF_NOTIFY_ACCESS_DENIED——注意服务器要返回的“401 访问拒绝”信息，过滤器可以分析导致错误的原因。

此外，还可以设置过滤器的优先级，有三个值：SF-NOTIFY-ORDER-DEFAULT、SF-NOTIFY-ORDER-LOW 和 SF-NOTIFY-ORDER-HIGH。缺省地可以设为 SF-NOTIFY-ORDER-DEFAULT，一般不要设成SF-NOTIFY-ORDER-HIGH，如果这样可能会导致服务器出现一些意想不到的故障。

HttpFilterProc 函数是对所设定的事件进行处理，它的调用格式为：

DWORD WINAPI HttpFilterProc(

PHTTP-FILTER-CONTEXT pfc, // 指向一个 HTTP-FILTER-CONTEXT 的信息，与 HTTP 的请求信息有关。

DWORD notificationType, // 处理的事件类型，应是 GetFilterVersion 所设定的类型。

LPVOID pvNotification) // 要处理的与 notification-Type 有关的结构，不同的事件类型对应不同的结构。

如果设置了 SF_NOTIFY_URL_MAP 事件进行过滤，则可以通过(pfc->GetServerVariable)(pfc,"REMOTE-ADDR",RemoteIPAdd,& IPAddSize)来获得客户端主机的IP地址等其他信息。过滤的事件应依需求来定，同一功能可以采用不同的方法。如果要对用户的访问进行监控，则可以通过处理SF-NOTIFY-AUTHENTICATION事件来实现，也可以通过SF-NOTIFY-URL-MAP事件间接地完成，这如同本文所采用的方法。

3 对访问的用户进行监控认证

利用ISAPI的过滤器，可以监控用户的访问帐号，这必须以 MS Windows NT 作为网络用户操作系统，以 MS Proxy2.0 作为代理服务器进行 Internet 访问。当用户通过浏览器请求 Internet 信息时，Web 服务器首先需验证用户的身份。如果没有过滤器时，服务器按 Windows NT4.0 系统的方式进行帐号及口令认证。当采用过滤器时，过滤器同样可以对用户的身份进行所需要的检验。我们的目的是设计一个过滤器，将用户帐号与主机 IP 捆绑在一起，即使某些用户非法地盗窃了他人的密码，由于IP不一致，也无法访问。把用户的 IP 及其帐号信息存放在一个文本文件 IPAccount 中，其内容如下：

202.38.152.100:zhoupk,junzx

202.38.152.101:yunzx

202.38.152.107:amms03,shiw,fangtao

202.38.152.113:wangjx,yanjunhua,chensj,duanjb

文件中每一行表示一台连网主机的信息，一个 IP 可以有多个用户使用。在某一IP上，除了列出的帐号外，其他帐号不能使用。

在建立此过滤器时，我们仅在GetFilterVision中设置 SF-NOTIFY-URL-MAP 事件，同时把过滤器的优先级设定为缺省的：SF-NOTIFY-ORDER-DEFAULT。一个帐号

监控的过滤器，必须要有很好的响应速度，因为用户每次通过HTTP的访问，过滤器都要检测用户身份的合法性，所以每个过滤器处理的每一环节，我们都尽可能地减少系统的时间的占用。过滤器初始化时，先读入文件IPAcount的信息。这种信息可能依据不同的网络，其数目差别很大，其范围可能在几十台主机至几千台。为了减少系统的内存占用量，我们采用文件映射（File Mapping）方式存储这种信息。考虑到未来系统管理员可能修改此文件，过滤器此后每5分钟（或更长时间）检查一下该文件是否更新过，如果更新过，就重新读入，否则不读。当用户访问时，过滤器在HttpFilterProc函数中通过SF-NOTIFY-URL-MAP事件获取客户的IP地址和帐号名。然后根据IP与帐号对应表与访问客户的信息比较，如果发现了该客户的信息，则说明此客户是合法的，就返回SF-STATUS-REQ-NEXT-NOTIFICATION状态，允许客户访问，否则就阻止它的访问。

为了加速过滤器对客户的检查，我们采用了两项技术：一是Hash存储与搜索技术，不过所用的Hash算法是与网络中IP地址段相关联的，这一算法保证了搜索的唯一性，既加速了查找速度，又节省了存储空间。二是采用了状态记忆位，当一客户访问一次后，过滤器在短期内不再检查该客户是否合法，而是根据它上次访问的状态位（合法为1，非法为0）进行判断。客户的新访问与上次的合法性完全一致。为了防止漏测用户的访问，则过滤器设定了一个检测时间值，当小于此时间值时，依据上次状态位进行判断，当大于此时间值，就进行重新帐号测试。通过这些技术设计的过滤器，既有效地监控着用户的访问，又使访问响应未受到明显的影响。当然，在该过滤器中，根据需要还可以加入其他的帐号认证方式，以控制用户的访问。

4 过滤器的使用

当按需要设计了一个DLL的过滤器后，要使用它还必须安装，安装的方法如下：

（1）在MS Windows NT的注册表中，加入你要运行的过滤器。假如你的过滤器是FILTERS.DLL，则你应当在注册表的下述位置上：

HKEY_LOCAL_MACHINE＼System＼CurrentControlSet＼Services＼W3SVC＼Parameters＼FilterDLLs如果你的系统没有Filter DLLs，你应当以该名字加入一个子键。然后加入FILTERS.DLL的全路径作为它的值，如C:＼WINNT＼SYSTEM32＼FILTERS.DLL，当有多个DLL时，应当以逗号隔开，并将FILTERS.DLL复制到C:＼WINNT＼SYSTEM32下。

也可以不用上述方法，而专门设计一个安装程序来完成注册登记。

当上述安装在你的服务器上完成后，如果通过代理访问Internet，对于合法的用户帐号，则用户的访问会畅通无阻。当非法用户访问时，服务器要求客户三次登录提示，然后拒绝用户的访问。在该过滤器中，系统管理员还可以设定检测的时间，即过滤器多少时间检测一次，这定义在文本文件IPAccount中，它连同读该文件的时间放入同一行，如：

Seconds of filter and reading this file:180,300

上行表示每3分钟检测一次，每5分钟查看一下IPAccount文件是否更新过。

对于网络管理员的帐号，可以在此文件中作另外的说明，使其帐号不受主机限制。由于IP地址0.0.0.0不会被任何主机使用，所以用此地址后的帐号设置了一些管理员的帐号，如：

0.0.0.0:sysacc1,sysacct2

同时，管理员所使用的主机IP地址却不出现在该文件中，这样为网络管理与维护提供了更好的支持与方便性。

5 结束语

通过应用ISAPI过滤器，我们有效地解决了Web下盗用他人帐号的问题，使网络计费更加公正合理。我们将对Windows系统的认证及检测等问题做进一步的研究与开发，以更好支持网络的安全性。■

参考文献

1 *赵东升，孙焕东．基于Linux防火墙的网络用户计费和安全管理，《医学信息》，1999年第10期，P13-14。*

2 *孙焕东，赵东升．军事信息网络的安全保护与计费系统，《军事系统工程》，1999年第三期，P37-39。*

3 *孙焕东，赵东升，吴明虎，李雪莹．对Internet访问的监控与管理，《军事医学科学院院刊》，第25卷，1999年第四期，P286-288。*

4 *赵东升，孙焕东．基于Radius的拨号上网认证、计费和管理，《计算机系统应用》2000年第4期，P37-39。*