IMPLEMENTING FILTER ALGORITHM TO THE OPERATING SYSTEM USING DNS SERVER

Abhineet Sinha, Vishal Kumar

Abstract— **This paper reviews about the content filtering techniques of the web pages that are available on the internet. These content filtering techniques helps in removing particular types of encrypted data from that webpage that are harmful for the society both technically as well as socially. As soon as the internet and social networking came into existence the transfer of various types of viruses and unauthorized data which is illegal in law have became a biggest threat to the industry. This paper contains various types of filters such as software filter or hardware filter depending upon the requirements and the resources available to the user. This paper also shares various techniques that will help the user to decide which type of filter is best suited for him. Moreover it will broadcast various methods of filtering like IP blocking, DNS filtering and URL filtering etc. and the best suited method to create a filter that will block a site by using the host file.**

Index Terms— **webpage, filter, encrypted data, IP, DNS, URL.**

I. INTRODUCTION

Today, social networking sites had gained much popularity. They have become the greatest source of communication, share a considerable amount of human views, exchange of several types of data like text, videos, etc and even provide employments. Suppose, if somebody wants to search any desired information, the data mining process is known to have the most efficient part in it. The search engine select the input, compare it with all the record saved in the database of the engine. The record in the database is again selected and respective URL is displayed. Now generally the information, advertisement or message given on that webpage is shown as it is, without any change known as general walls. These walls may have that advertisement which is of no use to that user or may have unauthorized or encrypted data. So keeping all this is mind, social networking sites must be equipped with the facility that if something unauthorized is available there on the webpage we have searched for, it will filter the page and remove all its unauthorized contents. This paper reviews about the various techniques and methods of doing it.

Manuscript received Sep 28, 2014

Abhineet Sinha, Student B.tech, Electronics and Computers Engineering, Dronacharya College of Engineering, Khentawas, Gurgaon, India

Vishal Kumar, Student B.tech, Electronics and Computers Engineering, Dronacharya College of Engineering, Khentawas, Gurgaon, India

II. INTERNET FILTER

An Internet filter is a hardware or software that restricts the information that is delivered over the Internet. Filters can greatly reduce the flow of harmful content into your computer. They can block access to websites, e-mail, chat, or other Internet-based communications based on category, site, or content.

For many years the Brethren have warned us of the dangers that accompany the Internet, and have counseled us to employ some technological barriers to the unending flow of filth that permeates the otherwise wonderful and extremely useful virtual world of the Internet.

Recall President Hinckley's warning in 2002, when he said: "*Guard your homes. How foolish it seems to install bars and bolts and electronic devices against thieves and molesters while more insidious intruders stealthily enter and despoil*" [1],

or more recently when Elder Oaks told us in April conference, 2005: "*We must also act to protect those we love. Parents install alarms to warn if their household is threatened by smoke or carbon monoxide. We should also install protections against spiritual threats, protections like filters on Internet connections*."[2]

.If you are attempting to prevent accidental access to inappropriate content then most filters can be considered useful. Many filters also have other features, such as time controls, chat logging, reporting and other useful capabilities. All of these features keep us safe, and helps providing us with more information regarding how our computers are being used. From this perspective, it would be justified to say that filters work.

One of the most significant side-effects of installing a filter is the false sense of security that it provides. Most teenagers can get passed through any filter if they want to by satisfying some conditions. Moreover parents need to know how this is done so they can watch for the warning signs. Also be sure to use the tools that the filter provides, such as usage reports, blocked site reports, etc. A filter is not a silver bullet, and it is not a set-it-and-forget-it solution.

Increasing individual accountability is one of the most effective ways of filtering content. It is a good practice to place the computer in a public place, and to limit the use of the Internet to certain times when others are around. Windows Vista/7 and Mac OS X offer time limits on internet access, as do most filters. Many home routers now also offer availability schedules for protecting non-computer devices.

The only full proof filter is, as President Faust once explained, the personal moral filter: "As the traffic on the communications highway becomes a parking lot, we must depend more and more on our own personal moral filters to separate the good from the bad."[3]

2.1 Filter types-

An analogy might be helpful as we discuss the different filter technologies. Let's consider the content on the Internet to be analogous to mail that is delivered to your home. A filter could be thought of as a guard that is hired to sort through your mail before it is delivered to you. This guard could be asked to remove any junk mail, or even mail from any individual or company, and set it aside so you don't have to deal with it. The guard would then review each piece of mail before handing it to you.

Filters work in similar fashion, sorting through the content that your computer requests, and preventing certain content from entering your computer. To understand the different filter technologies, let's relate them to this guard, and where he might intercept our mail before giving it to us. There are three basic forms of filters used today, namely:

2.1.1 Software

This is the most common filter, and it comes in the form of an application that is downloaded from the Internet or purchased in a store, then installed on your computer. The filter interjects itself into the communication chain between the applications on that computer and the Internet so that it can have an eye on the communication, and perform its guard duty. Software filters are usually the most robust, and offer the greatest level of protection – not only from pornography, but from other dangers as well (such as online predators, online gaming, etc).

In our analogy, this option is like putting a guard at your front door. A software filter looks at a data as it arrives on your machine. It is important to note that because the filter is actually installed on your computer, the unauthorized content will exist on your computer, but the filter intercepts it before it displays on the screen.

2.1.2 Hardware

When you have a broadband Internet connection, or an always-on connection, there is a physical device that you must use to connect your computer to the Internet. This may be a cable modem or a DSL router; it all depends on what type of broadband connection you have purchased. Some of these routers, or modems, have built-in software that filters the Internet. This is an example of a hardware filter – the hardware device that brings the Internet into your home can be configured so that it will filter the content before it arrives on your computer. You do not need to install anything on your computer; the mere fact that your computer uses this device to access the Internet ensures that the content is filtered. Hardware filters are usually simplistic and would only prevent access to inappropriate content.

This option is similar to the guard standing at your mailbox, intercepting the mail directly from the mailman before it is placed in your mailbox. The unauthorized content is intercepted before it ever arrives on your computer.

2.1.3 DNS

Another option is to use a DNS service such as OpenDNS to provide filtering. This provides a free option with many of the benefits of having a hardware solution, without having to purchase additional hardware because it will probably work with your existing home networking hardware.

All that is required is to update the primary and secondary dns entries at the router to point to the opendns servers, and then open an account on open dns, which allows you to set your filtering options for your home network. Directions for doing so are on the open dns website.

This option has the advantage of filtering all of the devices in the home; including the computers, cell phones, TVs, game consoles, any device that would connect to your router, either hardwired or wireless. However cell phones connected to the Internet via a cell tower will not be filtered.

2.1.4 Internet proxy

Some Internet Service Providers (ISPs) will offer filtering as part of their service. If they don't, you could sign up with a service on the Internet, called a "proxy," that will filter your content on the Internet before sending it to your home. Since this works on the Internet, there is nothing to install on your computer. If this service is offered by your ISP, then there is usually nothing to configure – you simply turn this service on with your ISP, and it filters all content. If you are using a proxy service, then you must configure your individual computer to use the proxy filter. It doesn't necessarily install anything on your computer, but you do need to ensure that the computer is configured to use that proxy. Like hardware filters, Internet proxy filters are usually simplistic, and would not have the robust features of a software filter.

Continuing our analogy of a guard watching our mail, this would be comparable to our guard standing at the post office and inspecting each piece of mail before it is loaded onto the mail truck for delivery.

2.2 How to select a filter

Now that we understand the different types of filters, how can we determine which is the best type of filter that can provide the best services to us? There are some simple questions that you can ask yourself that will help you determine which filter will best fit your needs. They are:

A. What devices are you trying to protect?

Many devices today are Internet-enabled, and can be benefited from protection provided by these filters. It is important to keep in mind that we are not just talking about desktop computers, but also any laptops, gaming consoles, set-top TVs or any other Internet-enabled device in your home that uses your network to access the Internet. Remember that cell phones do not fall into this category, since they use the cell phone network for their Internet access. Just about everything else that accesses the Internet in your home uses your home network to do so.

If you have several devices that connect to the Internet, it is probable that you have a broadband connection. You might want to investigate the hardware solution first, since some of these devices do not support the installation of software. For example, many game consoles can access the Internet via a wireless connection in the home, but you cannot install any software on these devices. If you are able to use a hardware filter, then the device will automatically be filtered simply by the fact that it connects to the Internet through your hardware device.

B. What operating systems (OS) is running on your PCs?

An operating system is the application that interacts with the user to operate the computer. It is what "boots up" the computer and what you log in to for access to that computer (although not all operating systems require a login). The most

common operating systems are the several versions of Windows from Microsoft Corp. (Windows XP, Vista, and a few older versions), and a couple of versions for the Mac from Apple.

As a rule of thumb, if you have multiple operating systems in your home, you probably want to consider a hardware filter. A hardware filter doesn't require direct interaction with the OS and you don't have to worry about whether it will operate in the same way on all of your computers. However, there are a couple of software filters on the market today that support both Windows and Mac operating systems. If you only have two or three computers to filter and you have a heterogeneous operating system environment, you may want to do just a little bit of research before deciding that a software filter is not for you. Remember that software filters tend to be more robust, and protect from more dangers than hardware and Internet proxy filters.

In the latest shipping versions of operating systems for Windows and Mac, there are built-in filters that you can use for free as part of the system. They are not as robust as some of the commercial filters that you would purchase, but they are certainly better than no filter at all. Before you purchase a solution, check to see if you are running the latest version of the operating system, and whether the built-in filter will suit your needs.

C. Do you have laptop computers in your home?

If you have laptops in the home, it is highly likely that these laptops access the Internet when away from home as well. People can access wireless networks in school, in libraries, on buses, and in many other "hotspots" around town. If you want to be sure that these laptops are protected when away from home as well as when accessing the Internet in your home, then you would want a software filter or an Internet proxy filter. The reason is that the hardware filter would only protect the laptops when they connect to the Internet through the hardware device in your home.

D. Do you want to prevent inadvertent access, or are you trying to stop someone from their deliberate attempts to view inappropriate material?

If you are trying to prevent inadvertent access, then any filter will do. If, however, you are trying to prevent someone from deliberately deactivating the filter to seek out inappropriate content, then you want to look at the more sophisticated commercial software filters. Generally speaking, hardware filters are harder to get around than software filters, but most of the commercial software filters on the market today are built so that you have to have quite a bit of technical expertise in order to subvert them. The free filters tend to be easier to subvert as well.

E. How do you connect to the Internet?

If you use a dial-up connection to the Internet, then you typically would not have a gateway in your home, so a hardware solution would not be appropriate for your environment. Instead, you would look for a software filter or an Internet proxy filter.

F. Do you need to restrict the times that the Internet is used?

Some filters have time controls built into them, so that you can turn off access to the Internet during certain times. If you do not want anyone to access the Internet from midnight to 6 am, for example, most software filters would have the ability to enforce this, whereas most hardware filters would not. Those hardware filters that do allow this would normally be an all-or-nothing solution: in other words, with a software filter you could allow some people to access the Internet at certain times, and others would be more restricted. With a hardware filter, everyone has the same time restrictions.

G. How do you want to handle over-blocking?

Given the current state of filter technology, you can rest assured that you will be blocked when you shouldn't necessarily be. There will be times when you attempt to access a site that the filter thinks should be blocked, but you know the site to be OK. This is called over-blocking. With software filters, this is usually trivial to handle, as you can simply enter an administrator password and continue on to the site. With hardware and Internet proxy filters, many times you need to contact the administrator of the filter (like you're ISP, for example) and ask them to unblock the site. This usually takes time, and can be a source of frustration.

III. METHODS FOR FILTERING

Some common methods used for content filtering include: URL or DNS blacklists, URL regex filtering, MIME filtering, or content keyword filtering. Some products have been known to employ content analysis techniques to look for traits commonly used by certain types of content providers.

Requests made to the open internet must first pass through an outbound proxy filter. The web-filtering company provides a database of URL patterns (regular expressions) with associated content attributes. This database is updated weekly by site-wide subscription, much like a virus filter subscription. The administrator instructs the web filter to ban broad classes of content (such as sports, pornography, online shopping, gambling, or social networking). Requests that match a banned URL pattern are rejected immediately.

Assuming the requested URL is acceptable, the content is then fetched by the proxy. At this point a dynamic filter may be applied on the return path. For example, JPEG files could be blocked based on fleshtone matches, or language filters could dynamically detect unwanted language. If the content is rejected then an HTTP fetch error is returned and nothing is cached.

Most web filtering companies use an internet-wide crawling robot that assesses the likelihood that a content is a certain type. The resultant database is then corrected by manual labor based on complaints or known flaws in the content-matching algorithms.

A. IP blocking-

The access to a certain IP address is denied. If the target Web site is hosted in a shared hosting server, all Web sites on the same server will be blocked. This affects all IP protocols (mostly TCP) such as HTTP, FTP or POP. A typical circumvention method is to find proxies that have access to the target Web sites, but proxies may be jammed or blocked. Some large Web sites allocated additional IP addresses (for instance, an IPv6 address) to circumvent the block, but later the block may be extended to cover the new addresses.

B. DNS filtering and redirection-

The DNS doesn't resolve domain names, or returns incorrect IP addresses.[38] This affects all IP protocols such as HTTP, FTP or POP. A typical circumvention method is to find a domain name server that resolves domain names correctly, but domain name servers are subject to blockage as well, especially IP blocking. Another workaround is to bypass DNS if the IP address is obtainable from other sources and is not blocked. Examples are modifying the Hosts file or typing the IP address instead of the domain name in a Web browser.

C. URL filtering-

Scan the requested Uniform Resource Locator (URL) string for target keywords regardless of the domain name specified in the URL. This affects the Hypertext Transfer Protocol. Typical circumvention methods are to use escaped characters in the URL, or to use encrypted protocols such as VPN and SSL.

D. Packet filtering-

Terminate TCP packet transmissions when a certain number of controversial keywords are detected. This can be effective with many TCP protocols such as HTTP, FTP or POP, but Search engine pages are more likely to be censored. Typical circumvention methods are to use encrypted protocols such as VPN and SSL, to escape the HTML content, or reducing the TCP/IP stack's MTU, thus reducing the amount of text contained in a given packet.

E. Man-in-the-middle attack-

GFW can use a root certificate from CNNIC, which is found in most operating systems and browsers, to make a MITM attack. On 26 Jan 2013, the Github SSL certificate was replaced with a self-signed certificate in China by, generally believed, the GFW.

F. Connection reset-

If a previous TCP connection is blocked by the filter, future connection attempts from both sides will also be blocked for up to 30 minutes. Depending on the location of the block, other users or Web sites may be also blocked if the communications are routed to the location of the block. A circumvention method is to ignore the reset packet sent by the firewall.

G. VPN Blocking-

Starting late 2012, GFW is able to "learn, discover and block" the encrypted communications methods used by a number of different VPN systems. China Unicom, one of the biggest telecoms providers in the country, is now killing connections where a VPN is detected, according to one company with a number of users in China.

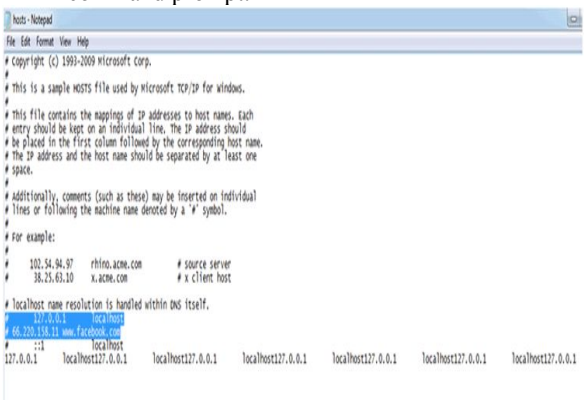
H. Network enumeration-

It has been reported that unknown entities within China, likely with deep packet inspection (DPI) capabilities, have initiated unsolicited TCP/IP connections to computers within the United States for the purported purpose of network enumeration of services, in particular TLS/SSL and Tor (anonymity network) services, with the aim of facilitating IP blocking.

IV. HOW TO BLOCK A SITE BY USE OF HOST FILE

Sometimes we do not want the users of a particular computer or network to open a particular website. For example we want our children or our friends to stop accessing a website then we needs to block that website on the computer or network. Although web browsers provide facilities to block a website but they do not work always and it is quite easy to undo the settings. So through this guide I will show you how to block websites by using computer's host file. By settings a password for your host file, other users will not be able to unblock the websites back. Here are the steps:

1) Open the 'Command Prompt' and type "notepad C:/Windows/System32/drivers/etc/hosts" and the host file will be open in Notepad.
2) Now in the host file find the line that says: "127.0.0.1 localhost,". Bellow this line type the IP address and name of the website that you want to block separating by a space. If you want to block more than one site write the similar details in individual line. For example if you want to block Facebook.com then write the following line:
   66.220.158.11 www.facebook.com
3) To find out the IP address of a website open the command prompt and type "ping www.facebook.com" and press Enter key. If a website has more than one IP address then write each one with the website name in separate line.
4) Save the host file after adding the details of all website that you want to block and close the host file and command prompt.



CONCLUSION

Content filtering is a fast-paced battle of new technologies and the relentless trumping of these systems by subversion and evasion. Altruistic development efforts by passionate programmers on a mission to support citizens in countries that block access to content will win, then lose, and then win again in a never-ending cycle. Other challenges include employees and kids who don't understand all the risks and don't think the abuse of a school- or company-provided computer and network is a big deal. Add new technologies, YouTube, and streaming sites, and the challenges and arguments for content filtering will not end anytime soon.

As we have explored, content filtering and its three objectives—accuracy, scalability, and maintainability—are at odds with each other. Accurate blocking makes it hard to scale and maintain, and easily scalable and maintainable

systems are not as accurate. Companies that make content-filtering technology are attempting to make these challenges easier to manage and maintain.

REFERENCES

[1] Overpowering the Goliaths in Our Lives, President Gordon B. Hinckley, Ensign, January 2002
[2] Pornography, Elder Dallin H. Oaks, Ensign, May 2005
[3] The Power of Self-Mastery, President James E. Faust, Ensign, May 2000

Author's Profile

Abhineet Sinha - Research interest is in the area of organization designs that maximize innovative patents. Under the Guidance of senior professor I wish to learn and analytically approach various research fields in depth . At DCE additionally, I also am a Resource Executive for the Society of Innovation Development.

Vishal Kumar – a diligent scholar and a hard working individual who continues his focused effort in order to achieve his goals. Working on this paper has been informative and revisiting and has created a curiosity about this field of research.