Anonymous Web Browsing and Hosting

MANOJ KUMAR
Department of computing, ITB Blanchardstown,
Dublin, Ireland
wss.manojkumar@gmail.com
ANUJ RANI
Department of Computer Science, ITM University
Gurgaon, India
anuanuj1989@gmail.com

Abstract:
In today’s high tech environment every organization, individual computer users use internet for accessing web data. To maintain high confidentiality and security of the data secure web solutions are required. In this paper we described dedicated anonymous web browsing solutions which makes our browsing faster and secure. Web application which play important role for transferring our secret information including like email need more and more security concerns. This paper also describes that how we can choose safe web hosting solutions and what the main functions are which provides more security over server data. With the browser security network security is also important which can be implemented using cryptography solutions, VPN and by implementing firewalls on the network. Hackers always try to steal our identity and data, they track our activities using the network application software’s and do harmful activities. So in this paper we described that how we can monitor them from security purposes.

Keywords- Anonymous Browsing, Email security, Web hosting, Https, SSL/TSL

1. Introduction
We know that internet play a vital role in our day to day life for communication. We share our sensitive data within the organization or outside by using internet but important thing is to secure the communication between two parties which are sharing their private information. So to achieve high privacy of communication we need to design and develop secure web browsing solutions by using highly secure communicative architecture. Web browsing highly rely on the features that a web browser supports to provide security. Web browsers like IE, Firefox, Netscape, Opera and Mozilla etc. can be installed on our machine. Even we use different-2 operating systems to install these applications. Security related to machines are also equally important for security concerns. As internet share huge amount of data and it is also flooded with many spyware, spam, viruses and Trojan horses which affects the security. Once these malwares comes into the system then they start to effect the OS services and starts to create security bugs. So to prevent the impact of these spy programs and to maintain high level of security we need to adopt secure web browsing solutions like SSL/TLS, VPN, HTTPS, secure PROXIES etc. In the following sections we will discuss about these security solutions and how they can be more effective to secure web browsing and machine security.

• When we browse the internet important aspect of security is the data security which we share over it. To maintain high privacy we focus on the cryptography and network security implementations. Physical security of data is also another aspect of security. We communicate with in the applications that runs on our system and we need specific security requirements like privacy or confidentiality, authentication, integrity and non-repudiation (Kessler, 17 july 2012). From cryptography side we focus on these purposes of cryptography that describe the authentication processes to access the data. Confidentiality means that the communication should be private between the user and the sender. Other aspect for cryptographic security is that data should not be altered during the communication phases. If these purposes are successfully implemented over the network no doubt that we can highly secure our communication. Another phase of security is network security which means to protect the network from outside world which tries to breach our network security. For network security we consider risk management, OSI model security, TCP/IP security and by using firewalls on the networks. Network security highly rely on the implementations of network layers including from physical layer to application layer of OSI model.

• Wireless security of a network is also important. Wireless networks are becoming more popular because communication is through satellite links which are fast. We can access the network anywhere anytime. When we communicate over the wireless networks hackers always try to breach the security. They are very susceptible to attack our networks so security of wireless network is a major concern from security aspects. In the following sections we discuss about where we have to put more security implementations.
Secure web browsing means to access the data over WWW (world wide web) that data can be description, articles or it can be any kind of information that we access through www programs. Accessing of web sites comes under web browsing. During the browsing we access many sites and a huge amount of data that is available over different servers. Some of the data is useful and secure but other data can hide malicious programs with it. When we access unsecure data over the web that results malicious programs in our computer that can be a virus, Trojan horse which later steals our sensitive information from the system. These spy programs breach the security and gives birth to unsure web browsing that means that our personal information is on risk. They even can damage memory in operating systems. Web browsing applications reads the data in the form of html/XML pages or any other form from the server. Browser interpret that data for display as a web page. During web browsing we access our email accounts that require more privacy and security so that no other person can use our information. For a secure browsing we have to consider following basic points-

- We have to use current version of browser
- We have to check that our web address should begin with “https”.
- We have to clear our web history and cookies after finishing a web session.
- We have to install antivirus plugins on the browser like scanit, McAfee extensions etc.
- Install firewall on your system
- Use different browsers for different activities.

We have to follow web security implementations during the browsing.

Even safari and Firefox are good browsers for general browsing but for more security we can use site specific browsers and we can close the java security holes in browsers (Rich Mogull, 20 aug, 2009). We can also use virtual machines for browsing.

2. Web E-mail Security

During the email access high privacy is required so that no other person can steal information that can be mail content, user id’s and passwords or login information. So before using this service of web we have to sure about the security on our machine and browser. For web email we should put enough security so that confidentiality, integrity and authentication should not be breached. And this can be achieved by cryptography techniques and methods.

Points to remember when we use emails (al., 2012) -

- Password should be more than 8 letters with different characters and it also not contain personal information related to you.
- Ensure that internet connection should be secure.
- Clear the cache data
- Maintain different accounts for different activities
- You have to aware by the risks your hosting company or organization have
- Encrypt the messages which seems you uncomfortable sending

Hackers can use network packet sniffing for steal our passwords and personal information so we have to be sure that the network we are using should be secure. In these cases we can use encryption throughout the session which is done by making SSL/TLS connection with the email server. In case if email service does not providing these secure connection then it is better not to use the service.

So in my opinion for a company security services we should use secure browsers and also make sure that we have SSL/TLS connections for accessing the application layer services. For conformation SSL/TLS connection on your web browser it shows “https:” when you put web address or URL in the address box.

** For example http://www.gmail.com this indicates that SSL connection is not there.

** https://www.gmail.com this indicates that SSL connection is enabled on your web browser.

For encrypting the emails we can use public key cryptography software GPG (Gnu Privacy Guard). This software can help to manage the keys, encryption and decoding the emails.

Virtual private network is another option for email security. So a network administrator should use virtual private networks for an organization so that security can be enhanced. Be sure that VPN client is installed on your local machine for using email services. VPN connection is fully secured with SSL/TLS type of encryption.

We can use Thunderbird to make our email browsing more secure because it supports many interfaces as compare to web based email services. By using thunderbird we can achieve more privacy and security for email browsing. From (Mozilla, 2005-2012) we can download and install this application on the windows and can configure it according to our use using add-ons. It provides more secure mail features compare to other web email services. Thunderbird also provide us robust privacy and phishing protection. We can configure SSL/TLS, cookies settings and anti-virus add on for more security that can be done by managing the user email accounts.
PGP is another protocol that is used for email encryption. This will allow us to encrypt the mail and digitally sign over it. This protocol makes man-in-middle attack impossible. We can install PGP for Windows and later can attach with the Thunderbird for providing more privacy by choosing Enigma add-ons on it. We will describe the installation process and how to choose these add-ons for privacy later in the demonstration section of this paper.

3. **Working of HTTP and SSL for Security Purposes**

HTTP is used for secure transactions like online banking. It is secure version of http called hypertext transfer protocol secure (https). When we communicate using https on websites then website encrypts the session with digital certificate. We can install the SSL digital certificates on the website and after that it displays a padlock symbol on the browser that indicates that certificate is installed on the browser. By enabling this we can secure our website for communication. SSL follows the concept of public key cryptography that uses private and public keys for sender and receiver. SSL secure port is used for making secure connection between the user and the company.

So for more security, it is advisable to use SSL certificate on both sides i.e. client and server side (Kangas, 2009). Server provides the encryption methods to client for SSL cipher with symmetric key to use with the SSL cipher. Then client encrypts the message with server public key and sends it back to the server. On the other side, server does the work of decryption using these key concepts. During web hosting, we can purchase these certificates from certificate authorities (CA) for a time being that help to make your web hosting more secure.

Steps for creating SSL session between browser and server are -

1. The browser requests that server identify itself.
2. Server sends SSL certificate to browser.
3. Browser checks the trust of SSL certificate if found it sends a message.
4. Server sends digitally signed ACK to start SSL encrypted session.
5. Encrypted data is shared between them.

So above points shown in the diagram shows how SSL works or make mutual authentication between the client browser and server for secure communication.

The working is based on handshaking sequence between browser and server. After establishment of first session we can use it again.

4. **Web Browser Working and How User Activities can be monitored**

Web browser communicates with the server to display a web page. When we send a request to the server it goes through different networks and finally reaches the destination server which then responds us with that particular web page. Web browser uses hypertext transfer protocol to communicate with the server side. So browsing is a communication between the user requests to the server. All the browsers work in a similar fashion from fetching to display a web page on the window screen. In the (Ostrovsky, 2011) blog, he explained how a web browser actually works from request to respond. He described the steps for web browsing and working that are -

- In the first step of browsing on the internet we put URL in the address bar. For example, we type http://facebook.com.
- In the second step, browser lookup for the IP address of the domain name. Browser communicates with the DNS server.
Actual navigation start from this step to visit the IP address of the domain lookup. The DNS lookup works like it first checks all the caches including browser cache, OS cache, router cache, ISP DNS cache and can also recursively search for that IP. Browser caches DNS records for some time that is from 2 to 30 minutes.

First browser check the desired record in his own cache. In case browser does not have that record then browser make a call with the OS cache by \texttt{gethostbyname} call in windows to lookup that record. If result is a failure in these caches the process moves on to the router and ISP DNS caches which have their own cache to store information.

In case of recursive search ISP’s DNS server begins searching from root name server to towards Facebook name server. Root name server hit may not be necessary because normally DNS have the .com name server in his cache.

DNS lookup for the name server, .org server etc. and finally retrieves that domain name we are looking for.

- In the third step browser send http request to that domain server. GET or POST requests are used. GET request look like “GET http://facebook.com/ HTTP/1.1”. In this case host is facebook.com. GET request fetch the facebook.com by requesting with the server. GET request also sends other parameters like encoding, cookies, header information etc. by the URL only. POST method is mainly used for submitting the forms.

- In the fourth step Facebook server responds with permanent redirect like as shown below.

From the server it shows the respond with 301 moved permanently to tell the browser that go to www.facebook.com instead of //facebook.com. If user put wrong information regarding URL or if information is not found on the web then server responds by generating redirect sequences like 301 in this case.

- In the next step user put right URL in the address bar and sends back to the server with another GET request. Then server handle the request and send back HTML response to the user.

Finally browser starts rendering with the HTML document. After the communication setup between the browser and server, user starts working on the requested web pages and web services.

**It is important to understand that TCP connection is used before the http session so that a connection can be establish between client and server. After getting the response from http browser close the TCP session or can reuse for other services. We use SSL/TSL below http to make secure communication.**

5. Monitoring user activities

Monitoring is important so that we can track log activities over the internet and can protect our system. One way to monitor the system activity is browser history where we can see the log activities regarding web visits. From these web logs we can get an idea about the accessed websites on our PC. We can also block those web sites which are harmful for our system and from social aspects. Second way to monitor the web activity is by using monitoring software’s. We can use spyagent, webwatcher, PC Pandora, UAM (user activity monitoring) for monitoring the activities. These software have blocking and filtering capabilities. We can block porn sites, online game sites within an organization or at home. These software’s can generate reports based on erroneous data. If a user use some aggressive/ vulgar words during the surfing immediate report is generated by the monitoring software and that report send to the administrator.

UAM (Spectorsoft, n.d.) Records all the user activity like chatting, email sites and message boards during the internet session. We can also put these monitoring setting on the firewalls and proxies in an organization so that user activities can be tracked.

If we setup with UAM in a business oriented company we can monitor every activity from the employees and later we can manage content based filtering. So to prevent anonymous user activities we can use these software applications for monitoring and securing from harmful web sites.
In (Shinder, 2007) blog he explained 10 ways to monitor user activities in an organization. These includes

1. Use auditing to monitor access to files.
2. Checked cached web files.
3. Monitor the web access on firewall levels
4. Filter web access by URL’s
5. Filter web access by keywords
6. Monitor outgoing and incoming emails.
7. Monitor IM’s (instant messages)
8. Use keyloggers to capture typed data
9. Use screen capturing tools
10. Control what applications employees can install and run.

So as a security consultant we need to select these monitoring anonymous solutions in the company so that user activities can be tracked and security implementations can be achieved inside company.

Outside the company hackers monitor our activities using the web services. When we use Wi-Fi network our data is unsecure because anyone can see our email messages, web site information, telnet connection and messaging. But if we implement encryption and security then only we can secure the network. According to (Geier, 2009-2012) article to secure our network we can follow these tips so that no one can monitor our network and our information-

- Enable WPA and WPA2 encryption- by enable encryption on WPA we can secure our telnet connections, file transferring and login details etc.
- Use independent services like SSL instead of telnet so that we can secure our emails. By using this we can secure our online account too.
- Use VPN on public network- this concept encrypts all our internet communication. To access Wi-Fi and public networks we can achieve security using VPN connections.
- Password management utility- using this utility we can secure our private data. If we use different-2 passwords then it became difficult to hackers to get our information and other services like account details.

So for secure the monitoring we can use these tips. Security for monitoring activities inside and outside the company is important from security point of view.

6. **Securing Website Hosting**

Web hosting is a service which is provided by web host companies to individuals to store their information online that is accessible through web. In the present time scope of web hosting is increasing very extensively through cloud computing. Companies provide domains and space to the web user for uploading their files through FTP or web interfaces.

For complex sites like e-commerce, database and web interfaces required for managing web server. Data is updated on the server through internet so security is very important to focus on these kind of web services.

There are mainly three type of hosting available

- Share web hosting
- VPS (virtual private server)
- Dedicated hosting

Share web hosting is common to use because it is easily available and cheaper because one server is shared by many customers. But this type of web hosting is less flexible.

In case of VPS server hardware is shared by the clients but concept of virtualization makes them to use their own dedicated server. Virtualization provides partition of server to the clients.

Dedicated hosting provides a single server to the clients to share their resources on the web. This kind of hosting is expensive but clients have full control to access their root server (Hosting Services, 2012).

Many companies from small scale to high using web hosting services even individual also but question arise on security that how much a hosting provider provides security to your information. We have to choose the best hosting services which provides hard-wired firewalls, antivirus and anti-spy software applications, backup power supplies, lock-down server rooms, algorithmic encryption and redundant up gradation so that security can be maintained.
Security for web hosting can be achieved by -

6.1 **Virtual racks**- virtual racks are used to store the sensitive information and also known as dedicated networks. They are secured with hardwired firewalls, anti-everything barbed wire and monitored every time. So to add security for web hosting we need to take virtual racks.

6.2 **Firewalls**- to filter out the spam, viruses and Trojan horse firewalls play important role to secure the data. Firewall software should be installed on the server so that filtration of these spy applications can be removed. Hackers sits on the client or server side to monitor the activities and to harm our sensitive data. To achieve security firewalls are important to install on the network.

6.3 **SSL certification**- SSL provides encryption of data to maintain the privacy. When we use web hosting services SSL is important so that our data can be encrypted or decrypted when it is coming and going on the network. Hackers can monitor whether the web page is SSL enables or not based on the requests. If we don’t have SSL certificate then it can be a hole for communication.

6.4 **Analog security**- uptime service is also very important from host side. Uptime service means that your web site never goes offline. Analog security means that host is providing state of the art technology security to protect our server based on algorithmic based access. It is kind of physical security that helps to secure the server room so that no one can harm the servers. It uses smart door security to keep the server security that covers security paradigm for web hosting. Server should be up so that access to the site can be maintained all the time.

These factors are important for a company to secure the web hosting services that provide security to the users as well as to the company (Host, 2009).

From the host side, physical security to the server is also important to maintain security.

Other security concepts that are used for providing security are SFTP and backups. We use FTP protocol to transfer our files on the server. If we use SFTP for transferring our files that add more layers of security rather than FTP. So we need to make sure that host also provide us this protocol for secure web hosting. Before buy hosting services we also check about the backup policies provided by Host Company that is part of physical security. And we need to use updated software and vulnerable scanners because they are more vulnerable to remove the flaws. We described secure browsing methods in this paper are also applicable to secure the web hosting.

7. **More Ways to Achieve Web Anonymity**

Browser security can be achieved by disabling mobile codes that are JavaScript, java, flash and ActiveX. Disabling of these codes reduce attack risks. For example if ActiveX is not properly installed on the browser then it can increase the attack ability. The results from ActiveX are out of scope hare that can accessed by (Cert.org, 21 dec 2000). IE use Active-X implementations. So to make IE secure set its privacy, cookies and general security settings from the tools tab available in it. Other plug-in like flash are installed on the browsers they are also vulnerable to attacks because they have some programming flaws like buffer overflow. So we have to choose these plug-ins according to our browser supportability. Cookies store our information when we access the information on internet so we have to keep in mind that cookies are disabled or only enable for a single session. Our login information is stored in cookies so to prevent the attack we should care of cookies enabling and disabling options. We will discuss more on cookies later in this section.

If we use IE then we have to set security level. Either we can choose high or medium level of security to secure our web browser.

Time to time we need to update security software or applications which are installed on the browser or in the window. Updating these applications should be through original or reputed web sites. We can enable automatic updates on. To provide security on our browser we have to apply these settings so that attacks can be reduced. And also need to disable the unnecessary applications or plugin from the browser. Securing the browser can be done through-  

7.1 **TOR**

TOR is used for enabling online anonymity and security, it is an open source software. This is composed of client software and network of servers. It uses huge database composed by proxies which safe yours identities on the network. TOR provides IP security. No one can identify our IP address when we use TOR. Many people and organizations use TOR to access huge amount of information from internet. IT companies use this software to check their firewall settings. It can work with remote login applications, on our browser and with IM software’s. Disadvantage of TOR is that it cannot protect internet traffic when we run it. We can download and install TOR browser bundle to secure our identities include our IP and location etc. It was developed by US naval research laboratory as a “third generation onion routing project” to protect government communication (Kwang, 2011).  


How TOR ‘onion routing’ works (FOWLER, 2012)-

- Firstly users run TOR software on his computer and request the server to download the data.
- In the second step user request pass through the other volunteer nodes in the network and finally request reached to the server which process requests. Picture shown below shows its working.

In the picture we can see that request gone through many nodes that is basically net of routers which are used to hide the destination information. A tunnel (made up by these nodes) is created between the user and the web server through which they communicate. Because of TOR, ISP is unaware about the user identity. TOR is only provide security when we use encryption otherwise it is insecure for communication. If we use TOR based web browser and https then combination of (TOR & HTTPS) provide us more security because TOR hide my IP identity and https help to make username and password secure. But in this case we have to disable the script services on the browser otherwise information can be stolen by the hackers. TOR can be used with VPN also for web anonymity.

7.2 Cookie Control and Proxies

Cookies are used to store the user information and data. When a user open a web page and put some details to submit the page then user information is stored in the cookies. Cookies can be on the browser and server side. Cookies store (keys + data) for example (firstname Manoj), (lastname Kumar) so name itself is a key value. Client or server use these cookies to fetch the data instantly because direct access to cookies reduce the access time on the web. With every page loaded in the browser create the cookies and they carry information from one session on the website to another. Web server send the information to the browser which then store the information as a cookie.

Cookies maintain the state of the web. Cookies main purpose is to acquire information for server browser communication without asking the information again and again. Some information like credit card number etc. are transferred in clear text that make cookies unsecure. So better way is to make cookies secure by using cryptographic techniques like message digest, digital signatures, MAC and encryption. Secure cookies can be issued by web server which secure the services. An example of cookie on the web is

<table>
<thead>
<tr>
<th>Domain</th>
<th>Flag</th>
<th>Path</th>
<th>Cookie_name</th>
<th>Cookie_value</th>
<th>source</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>acme.com</td>
<td>True</td>
<td>/</td>
<td>Name_cookie</td>
<td>Alive</td>
<td>False</td>
<td>12/2/2013</td>
</tr>
</tbody>
</table>

Different fields in the cookie identify the attribute values like name of the cookie, domain name and date etc. if secure flag is true then it is transmitted only over secure communication channel such as SSL.

There are three types of threats on cookies network threat, end user threat and cookie harvesting threat. Network threat is applicable when cookies are transferred on the network. Cookies stored on the user memory in a text file if anybody edit or temper with the cookies is a kind of end user threat. And if an attacker use some sites that accept cookies capture the cookies and use them for harvesting on other sites is kind of cookie-harvesting threat.
So to improve the security we can use password based, addressed base and digital based cookies to secure the authentication phase of cookies.

- IP_cookie contain the IP address of the user
- Psed_cookie contains the user password,
- Sign_cookie contains the signature that can be verified by public key cryptography.

Integrity of the cookies can be provided based on the attribute values information between the server and browser. HMAC are used for secret key based solution to protect the cookies. If web server share the secret key with cookie-issuing server then server creates MAC from the cookies that enhance the security for cookies. By implementing these cryptographic techniques we can enhance the security of the cookies (SANDHU, 2000).

Proxy or proxy server sits between the user and rest of the internet through which we access the web. Every request made by user goes through this proxy server. This is a good way to hide user information using proxy server. When we send a request for a web page it firstly handle by the proxy server that put his IP address in the request instead of using us that is we called anonymous proxy server. Mostly Web based proxies are used as anonymous proxy server. For secure web browsing we use web site of proxy service address box to put URL and send anonymous request to the server. Proxy server also help to delete the pages which contain some erroneous information. Use of recognized proxy server is secure then using the open proxies. So by using proxy server we can hide our information and secure our web browsing (Roos, n.d.).

By enabling browser extensions, security settings, using SSL, HTTPS and VPN we can more enhance the security on the WWW. If a website shows unsafe behavior avoid using it.

8. Conclusion

Security over internet is important concept to achieve high level of privacy during the browsing. Services like browsing, web hosting are only accessible by the internet. This work described secure mechanisms that shows that how we can make secure and better browsing experience. Web hosting is part of browsing so that is also equally important to secure hosting over the web. Physical and application security mechanisms like firewalls and virtual racks makes our web hosting more secure. Securing the email is a major concept where we need to implement more and more security implementations. Scripting languages like java script, VB and ActiveX are also introduce vulnerability to the systems. So it is up to us to decide that which browser supports these services for better security. For more security we can use different-2 browsers for different-2 applications and can also set basic secure settings on the browsers. We need to prefer dedicated web hosting which provides more security because client have its own server for share his resources.

In future we need to design more vulnerable solutions so that security of the data and web services can be enhanced.

References
