**Journal of Computer Science, 9 (2): 159-168, 2013**
ISSN 1549-3636

doi:10.3844/jcssp.2013.159.168 Published Online 9 (2) 2013 (http://www.thescipub.com/jcs.toc)

# Home Users Security and the Web Browser Inbuilt Settings, Framework to Setup it Automatically

**Mohammed Serrhini and Abdelazziz Ait Moussa**

Department of Mathematics and Computer Science,
Faculty of Sciences, Oujda, Morocco Av Med VI, BP 717 60000 Oujda, Morocco

Received 2012-09-21, Revised 2013-01-31; Accepted 2013-04-01

## ABSTRACT

We are living in the electronic age where electronic transactions such as e-mail, e-banking, e-commerce and e-learning becoming more and more prominent. To access online for this services, the web browser is today's almost unique software used. These days' hackers know that browsers are installed into all computers and can be used to compromise a machine by distributing malware via malicious or hacked websites. Also these sites use JavaScript to manipulate browsers and can drive user system to failures. Each browser have inbuilt features setting that define his behavior, unfortunately most of end users are unwilling to enable or disable this features securely, because many of them still do not understand even basic security concepts nor variety of security technologies present in a browser. This study will deeply discuss specific modern browser inbuilt features settings and associated security risks and we present a framework developed to enhance user surfing safety by configuring automatically all installed browsers features settings securely, we call it Automatic Safe Browser Launcher, to solidify the claim, we check each browser before and after with free tool (browser_tests-1.03) which is a collection of test cases to test browser vulnerability. The more configured security features your browser has, the better protected you are from online threats.

**Keywords:** Web Browsers Security, Web Surfing Security, Home User Security, Browser Setting

## 1. INTRODUCTION

Most of home users use their home computers, laptops, now smart phone's and others devices to surf to internet, they are increasingly exposed to security threats while using their home computers Furnell *et al*. (2007). Internet users are becoming more vulnerable to security threats due to the use of information communication technologies; things have become even more complicated especially in the later browser versions (Furnell, 2009). Home users does not have luxury of a "watchful eye" as users accessing the internet from their corporate workstations (Kritzinger and Solms, 2010), the majority of home users are vulnerable targets specially a novice users are likely to face a range of internet threats as theirs unfamiliarity with the technology can limit their ability to recognize the threats and understand the requisite protection to protect themselves (Kritzinger and Solms, 2010; Kumar *et al*., 2008) they stay vulnerable unless safeguards are automatically provided for them (Furnell *et al*., 2008). Browser has become one of the most preferred endpoint adaptable computing platforms ever conceived. Browser ubiquitous availability, flexibility and extensibility. Made them also an increasingly popular target of attack.

Variety of computer problems can be caused by non secured browser, An attacker can create a malicious web page or send it by email, that compromise systems as the site is visited, install Trojan software or spyware that will steal his information, take control of his computer,

**Corresponding Author:** Mohammed Serrhini, Department of Mathematics and Computer Science, Faculty of Sciences, Oujda, Morocco Av Med VI, BP 717 60000 Oujda, Morocco

destroy files providing system to failure and use user computer to attack other computers.

Exploiting vulnerabilities and misconfigured features setting in browsers has become a popular way for attackers to compromise computer systems attack like Operation Aurora 2010, software vulnerabilities are exploited and directed at browsers through use of compromised or malicious web sites. Most of internet users think that theirs browser is only the software that they can visit a web site by tapping URL and click to green "Go". Users therefore in many cases use theirs browsers without any idea that this software needs to be correctly configured for safe browsing, because not all of them still understand the variety of security technologies present in a browser, modern browser can have more than 1,500 new features (Baum, 2010).

Some information security risks that can arise without securely configured web browser:

- Web browser and extensions installed on the User computer can be out of date
- User can download and use rogue web browsers (Boyd, 2006)
- Arbitrary website close the browser window will cause a user losing work or state being performed in another tab within the same window
- Automatic installation of viruses, add-ons, Trojans, key loggers and malwares that drive students system to failures, or browser unusable
- Hacker stealing sensitive information (like credit card numbers, passwords, personal documents)
- Log on information student ID and passwords can be intercepted and misused; password can be stored by web browser, risk if computer shared with others persons, it is activated by default in all browsers

Please note that the examples above are not the only actions and risk.

## 1.1. Main Web Browser Functionality

There are five contemporary major web browsers used today Internet Explorer, Fire-fox, Safari, Google Chrome and Opera (http://gs.statcounter.com/#browser-ww-monthly-201107-201207-bar).

To access to the web materials (texts, image, audio, video, animation,) user uses his web browser to communicates with web server hosting the service application via a transport protocol HTTP as shown in **Fig. 1**, a transport protocol defines data formats but also algorithms for packaging and unpackaging application payloads, the data format is HTML, CSS and other media (pdf, mp3, flash) that browser can read with plug-in, true plug-ins are any software deployed by the server to the client that extend the functionality of the browser, JavaScript make web sites more interactive. Browser features setting define de way that browser will display and interact with all web content.

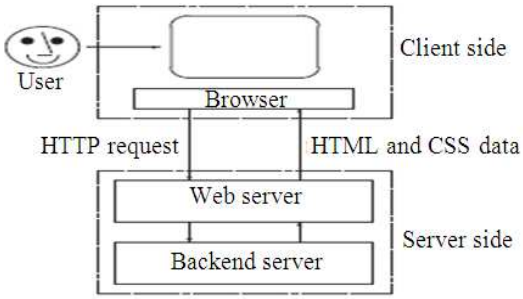



**Fig. 1.** Web 1.0 application


**Fig. 2.** Example of web browser internet explorer with enabled feature auto installs add-ons

## 1.2. Factors that Made User Web Browser Insecure

The evolution of the web browser has won a great experience, there are several ways that modern web browser can help prevent common internet security pitfalls (Zalewski, 2008). But Often, the web browser that comes with an operating system or downloaded from vendor web site are not setup in a secure default setting, because vendors will enable lot off features by default to improve the computing experience and to appear as the fastest than concurrent, the browser wars are back (Wisniewski, 2012), Hence the need to reconfigure them securely to avoid a myriads attacks from the web.

Lot of factors made browser security problem worse (Dormann and Rafail, 2008) as the following:

- Browsers vendor by default enable lot of features settings, this can decreased consequently security
- Increase number of links that users tend to click on web without considering the risks of their actions
- Many computer users believe that because they are skilled at generating spreadsheets, word processing documents and presentations, they know everything about computers

- Many users fail to set up their browsers security settings, by mere negligence or ignorance
- Antivirus, firewall and others endpoint security simply are not sufficient in the face of today's browser threats
- Some content of web page are not accessible unless users enable certain features or install more add-ons, putting the computer at additional risk **Fig. 2**

Multiple web browsers may be installed on the user computer. Other software applications on his computer, such as email clients or document viewers, may use a different browser than the one user normally uses to access the web. Also, certain file types may be configured to open with a different web browser. Using one web browser for manually interacting with web sites does not mean other applications will automatically use the same browser. For this reason, it is important to securely configure each web browser that may be installed in home user computer.

### 1.3. Related Works

Research activities in the area of security in modern browsers are a recent development. EMA (2010) introduces a tool named Dell KACE secure browser that virtualizing the browser against security threats, specifically for the browser that features enterprise manageability. The secure browser is a virtualized browser that offers control over browser execution; optional white and black list control over browser processes; constraints on changes to the browser and its extensions, add-ons and other browser enhancements; and resilience against browser attacks. But its only work with Firefox and lot of features are enabled by default like JavaScript, password Remember and designed for enterprise.

Louw *et al*. (2007) describe two implementations of this mechanism a drop-in solution that employs JavaScript and a faster, in-browser solution that makes uses of the browser's native cryptography implementation. Also discuss techniques for runtime monitoring of extension behaviour to provide a foundation for defending threats posed by installed extensions.

Accuvant (2011) in their quantitative approach intituled browser security comparison built criteria and comparatively analyzed the security of Google Chrome, Microsoft Internet Explorer and Mozilla Firefox. While similar comparisons have been performed in the past, previous studies compared browser security by considering metrics such as vulnerability report counts and URL blacklists.

Grimes (2010) in his special report called web browser security deep dive, talk about today's web browsers have different security pros and cons and none offer a magic bullet against threats. Here's how to keep your Web surfing secure. Feature set and complexity. More features and increased complexity are the antithesis of computer security. Additional features mean more code available to exploit with more unexpected interactions. Conversely, a browser with a minimal feature set may not be able to render popular Web sites, which forces the user to use another browser or to install potentially insecure add-ons. Popular browser add-ons are often exploited by malware writers.

One solution proposed by (Dormann and Rafail, 2008) and by lot off university is to provide a web page with some photo of option panel setting, to assist users and to show them how to configure manually theirs web browsers features safely, this method are not sure that most of home users can perform this task as expected, Also no solution that will do this task automatically exist on the market.

## 2. MATERIALS AND METHODS

### 2.1. Deep Survey of Web Browser Features Setting and Associated Risks

One approach is to have a better control over the browser itself and the most effective way to do this is through the features of the browsers because they define theirs behaviors, it is essential to understand the functionality and features of the web browser **Fig. 3**, understanding what different features do will help to understand how they affect web browsers functionality and the security of users computers, specially what features does browsers have to help protect from dangerous downloads, to help secure the connection between them and web site, to help defend against browser attacks, DNS rebinding attacks (Jackson *et al*., 2007) and if theirs browsers have a filter to help block phishing sites.

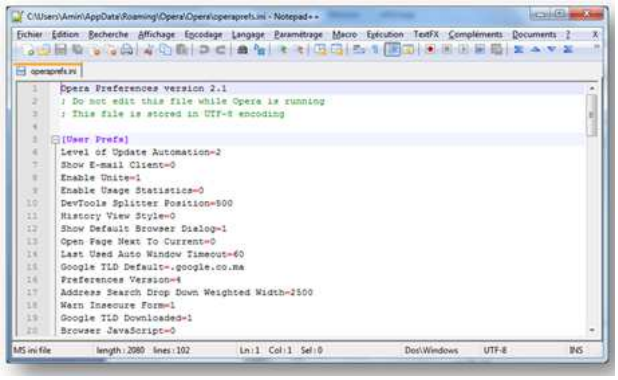
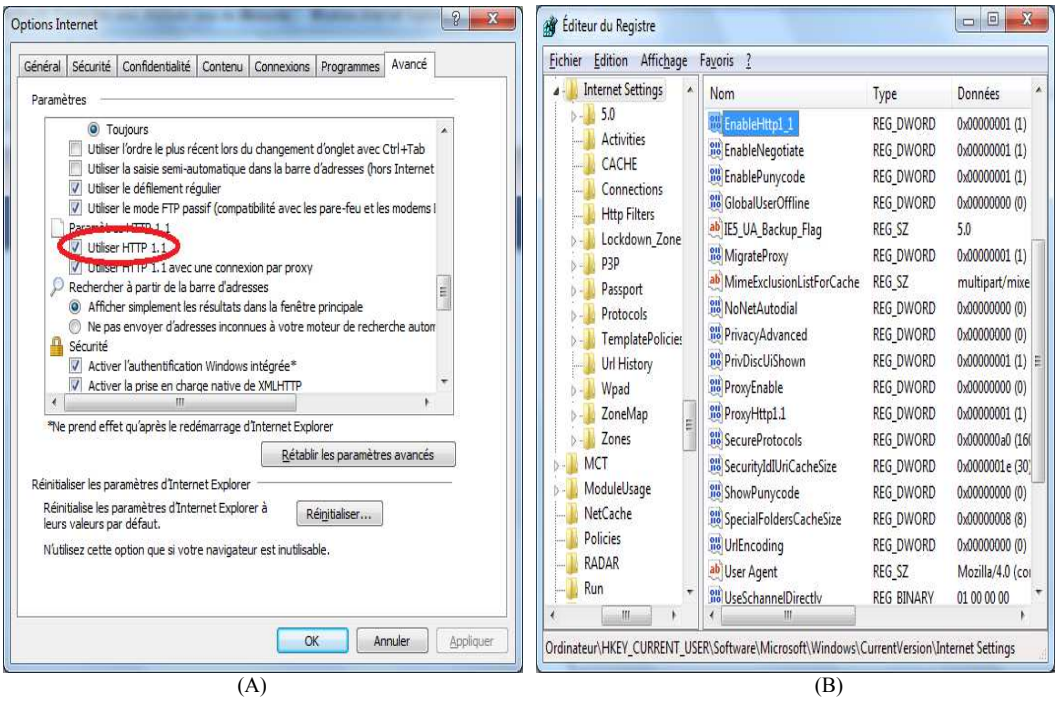



**Fig. 3.** Opera preference files opera.ini




(A) (B)

**Fig. 4.** (A) Internet explorer features setting (B) base registry entry for this feature

The Secure Browser is a well configured browser that offers control over browser execution. Enabling or disabling some web browser features by vendor or user like (enable JavaScript, save password, auto install Add-ons) **Fig. 4** may lower security, these features may end up increasing the risk to the computer. Well know and cheapest way for attackers to compromise computer systems is exploiting vulnerabilities with misconfigured features in browsers, misconfiguration is major attack at the application layer this year's (OWASP, 2010). Good security requires having a secure configuration defined and deployed for the application; all these settings should be defined, implemented and maintained as many are not shipped with secure defaults.

## 2.2. Graphical User Interface GUI Options Panels and Uniform Resource Identifier URI

All web browser vendors propose to their users through the graphical user interface an options panels allowing them to enabling or disabling manually some features setting, but many users as their unfamiliarity with the technology don't know what to enable or disable, also all various web browsers to display certain built-in functions, have uniform resource identifier URI is an internal scheme about:conf in Firefox, opera:conf in Opera, chrome://chrome-urls in Google Chrome, URI shows an interface for viewing and setting a wide variety of configuration variables, many of which are not otherwise accessible through the GUI options panels.

Below we provide a detailed analysis of browsers features present in theirs GUI option panel and URI scheme and we describe associated security risks.

## 2.3. Updating Web Browser

### 2.3.1. Enable Auto Update

It is recommended to enable the auto update feature. Security updates are critical in ensuring that a home user is safe from known vulnerabilities. Microsoft latest security report reveals 340 million PCs use an out-of date browser are at risk.

## 2.4. Encryption Settings

### 2.4.1. Enable SSL 3.0 and TLS 1.0

Enabling these protocols will allow browser to enforce selection of higher SSL and TLS encryption key lengths and more robust protocols.

### 2.5. Enable Warning of Loading Mixed Content

Enabling this setting will alert a home user when some content on a secure communication channel is coming under a non secure channel. For example an SSL website can request part of content on a page under a non-SSL session. This can leave home user vulnerable to eavesdropping and Man in the Middle attacks.

### 2.6. Enable Warning of Using Weak Encryption

It is recommended to enable the warning for weak encryption. This will protect home user from the compromise of theirs data due to weak encryption.

### 2.7. Add-ons Settings

### 2.7.1. Disabling Auto Install of Add-ons

If malicious add-ons are installed automatically, a home user security could be completely compromised.

### 2.8. Enable Blocking of Reported Attack Sites

It is recommended to enable blocking of reported attack sites. This can help protect home user from accidentally visiting a known attack site. It can have privacy implications as a home user browsing activity is sent to a third party as part of the check.

Enable blocking of reported web forgeries. This can help protect home user from accidentally visiting a known phishing site. It can have privacy implications as a home user browsing activity is sent to a third party as part of the check.

### 2.9. Enable Online Certificate Status Protocol

Web browsers can validate a certificate if an OCSP server is specified by the certificate or an OCSP server can be configured manually. It is recommended to enable OCSP. To provide assurance on the validity of encryption certificates this option should be enabled.

### 2.10. Dynamic Content Settings

Dynamic content consists of scripts and native browser objects which can change the content of a browser window without the knowledge of a home user. This will show how to lock down dynamic content in browser.

### 2.11. Disable Closing of Windows Via Scripts

Preventing an arbitrary web site from closing the browser window will reduce the probability of a home user losing work or state being performed in another tab within the same window.

### 2.12. Disable Caching of SSL Pages

Browser can locally cache the content of SSL pages on disk. It is recommended that caching SSL content be disabled. This will protect home user confidential information from unauthorized disclosure.

### 2.13. Disable Downloading on Desktop

This will protect from downloading content on desktop and tricking home user into running malicious binaries.

### 2.14. Enable Virus Scanning for Downloads

This will ensure that a downloaded file is scanned for viruses before the home user has an opportunity to interact with the download.

### 2.15. Block Reported Web Forgeries

Enabling this feature will decrease the probability of a home user falling victim to a phishing attack or unknowingly disclosing sensitive information to an untrusted party.

### 2.16. Block Reported Attack Sites

Enabling this feature will decrease the probability of a home user browser or system being exploited by known malware.

### 2.17. Disable Displaying JavaScript in History URLs

This will ensure that JavaScript URLs are not displayed in the history bar. It is recommended to disable displaying of JavaScript in history URLs. Various browser elements, even a simple link, can embed JavaScript URLs and access the JavaScript protocol. The JavaScript statement used in a JavaScript URL can be used to encapsulate a specially crafted URL that performs a malicious function.

### 2.18. Network Settings

### 2.18.1. Enable SSPI Authentication

Browser can be configured to leverage the Microsoft windows Security Support Provider Interface (SSPI). It is recommended that this capability be enabled. This will protect home user from using weaker authentication.

### 2.19. Disable Referrer from an SSL Website

It is recommended to disable referrer from an SSL website. It is possible that the URL of the SSL protected,

referring site contains sensitive information. By preventing browser from sending this URL, via an HTTP referrer header, to sites referred to by the SSL protected site an avenue for information disclose is eliminated.

### 2.20. Disable Sending LM Hash

Browser can be configured to send an LM hash when authenticating to resources that request this authentication type. It is recommended that this capability be disabled. The LM hashing algorithm contains weaknesses that can be exploited to derive plain text authentication credentials.

### 2.21. Privacy Settings

Browser can provide information such as browsing history to internet resources which can result in the compromise of the privacy.

### 2.22. Accept only 1st Party Cookies

Cookies are used to track valid session on internet. Securing cookie handling will help secure a home user browser session. It is recommended to only accept 1st party cookies. These cookies are typically used to uniquely identify a home user session on a website. However, these cookies can be used by third party sites and malicious sites to track a home user activity on the web. Also, they can be used to store sensitive personally identifiable information. Cookie settings should be configured such that malicious websites cannot set the cookies.

### 2.23. Disallow Credential Storage

Credentials can be compromised if the computer is shared with other users. This setting will ensure that the passwords are not stored for websites.

### 2.24. Disable Prompting for Credential Storage

This setting will ensure that browser does not prompt for storing passwords which will be stored by browser. Stored credentials/sensitive data pose a risk as they can be compromised by malicious websites using information leakage bugs advisories in browser.

### 2.25. Delete History and form Data

Browser can store the sites visited, information typed in forms and downloads from internet resources. It is recommended to enable deletion of history and form data. If browser or other applications executing at equal or higher security contexts is compromised, potentially sensitive, persisted, form data is at increased risk.

### 2.26. Delete Download History

Browser can store downloads from internet resources. It is recommended to enable the deletion of download history.

### 2.27. Delete Search and form History

Browser can store search and form data from internet resources. It is recommended to enable deletion of search and form history.

### 2.28. Block Pop-Up Windows

A website might open with or without any home user interaction. These pop-ups can be used to open untrusted malicious content. By enabling the pop-up blocker all pop-ups will be blocked which will guard a home user against any attacks launched using a pop-up.

### 2.29. Clear SSL form Session Data

This will ensure that the form data stored in an SSL secure session is cleared when the session ends. It is recommended to enable clearing of SSL form session data.

### 2.30. Applications Settings

#### 2.30.1. Secure Application Plug-ins

Some active content such as audio and video can be automatically loaded by browser on websites. It is recommended to secure application plug-ins. Some malicious websites can have active content to exploit vulnerabilities in active content handling application plug-in. It is recommended as a defense-in-depth to always prompt when a website is about to load active content which is not trusted.

### 2.31. Advanced JavaScript Settings

Will provide guidance on how to use advanced JavaScript settings to guard against certain attacks.

### 2.32. Disallow JavaScript Ability to Hide the Status Bar

It is recommended to disallow JavaScript ability to hide status bar. Some malicious websites can use JavaScript to hide the status bar so that a home user cannot determine the location of the content for hyperlinks and downloads.

### 2.33. Disallow JavaScript Ability to Change the Status bar Text

Some malicious websites can use JavaScript to manipulate the text on the status bar so that a home

user cannot determine the actual location of the content for hyperlinks and downloads. It is recommended to disallow JavaScript from changing the text on the status bar.

### 2.34. Enable Warning when Entering Insecure Site

Browser can notify home user when he enters an insecure (non-SSL) site from an encrypted SSL site. It is recommended to enable warning when entering an insecure site. The recommended state will ensure the home user is aware that the confidentiality of the information they are sending in the given browser tab or window is no longer protected.

### 2.35. Enable Warning when Submitting Clear Text form Data

Browser can notify home user when he sends form data to an insecure (non-SSL) site. It is recommended to enable warning when submitting clear text form data. This will protect home user from sending clear text data to website which can be sensitive in nature.

### 2.36. Disable Scripting of Plug-in by JavaScript

It is recommended to disable scripting of plug-in using JavaScript. This will protect home user from malicious scripts exploiting vulnerabilities in different plug-in or abuse the features.

### 2.37. Enable auto Notification of Outdated Plug-in

Outdated plug-in can be vulnerable or unstable which can be exploited by malicious websites. It is recommended to enable this feature so that home user is notified and directed to update plug-in.

### 2.38. Enable Information Bar for Outdated Plugins

This feature automatically shows an information bar when installed plugins are out of date and notifies the home user to update the plugins. It is recommended to enable information bar for outdated plugins.

### 2.39. Description of how to Build an Automatic Framework

The majority of home users are likely to stay vulnerable targets with browser security risks unless safeguards are automatically provided for them, because it is not practical for most to perform this level manually to secure their web browsers correctly.

We describe here a frame work depicted in **Fig. 5** that can solve this problem and empower a home user side to take control of his web browsers features settings for safe browsing, this tool will disable all features that can cause vulnerabilities and enable all features that enhance security.

The mains functionality of our algorithm is:

- Detection of all popular web browsers installed in the home user computer
- Enable or disable functionality as required to secure the selected web browser
- Launching the selected browser

### 2.40. Browser Detection

It's important to detect and secure all the five major web browsers used today and installed in the home user machine, after first installation all browsers propose to users to be a default used one. if user have preference for one browser some application in his machine can launch another one, in order to distinguish between them, each browser is well know by it famous image logo, logo image of detected web browser as depicted in **Fig. 6** are shown in main windows of our tool when this browser is found, after execution algorithm will detect all installed web browser and version from the Microsoft Windows key base registry. Each installed program on windows system takes its place in the key base registry.

### 2.41. Browser Features Configuration

There are two way to change browser features setting, in our algorithm we use both, first method is to rewrite features in preference file of the browser from directory where browser is installed, second is to change it the entry of features in the windows key base registry.

### 2.42. Configuration with Browser Preferences File

The major browsers according to the literature study (Opera, 2012; Safari, 2012; Ruderman, 2012) allow users to modify web browser specific preferences file. Opera has preferences file named (operaprefs.ini). Safari has (com.apple.Safari.plist) but need to be transformed to XML file via Plist editor. Mozilla Firefox has (pref.js) Firefox strictly forbid the modification of this file, but suggested to create another file named (user.js) and to place it in the same Firefox directory profile.

Our algorithm search in the lines of the each preference file the desired feature to check its current value, to conclude whether the setting is enabled or disabled and compare it with the need value, if the value isn't well configured the application will change it in the preference file. Firefox needs to be restarted to apply the change.

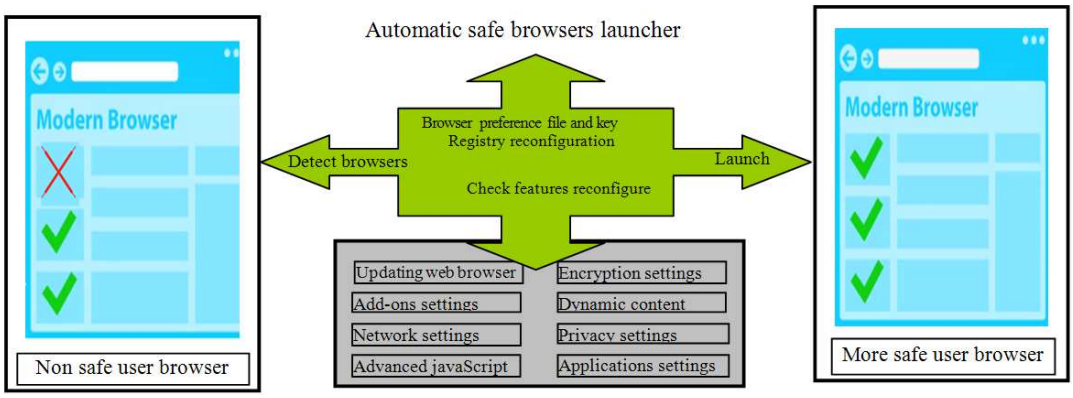



**Fig. 5.** Proposed algorithm functionality architecture


**Fig. 6.** Automatic safe browser launcher

### 2.43. Configuration from the Windows Key Registry

The second solution is to change the security settings in the windows key Registry, by manipulating the registry entry corresponding to the feature in question, this configuration has been implemented in our application for Microsoft internet explorer, because this browser is part of the windows system and for Google chrome Chromium Projects. It is important to note that in some cases, the registry entry corresponding to some features is not in the registry, the solution in this case is to create it.

## 3. RESULTS

### 3.1. Automatic Safe Browser Launcher

This application detect all installed major web browser in user machine as depicted in **Fig. 6**, when home user click on his favorite browser logo image, it will reconfigure and launch a selected web browser with feature setting at maximum needed for safe surfing, this kind of application is easy to use, so no training or configuration is needed.

For users who want to know a bit more about features configuration of theirs browsers, they can click in this application on button configurate under logo image of each detected browser, the algorithm will launch a windows as depicted in **Fig. 7 and 8** where all misconfigured features are shown with description of the security risk for user and advices to avoid this risk, this application can also be linked with e-learning awareness solution, behind a button (learn more) a web link to the e-learning security awareness platform.

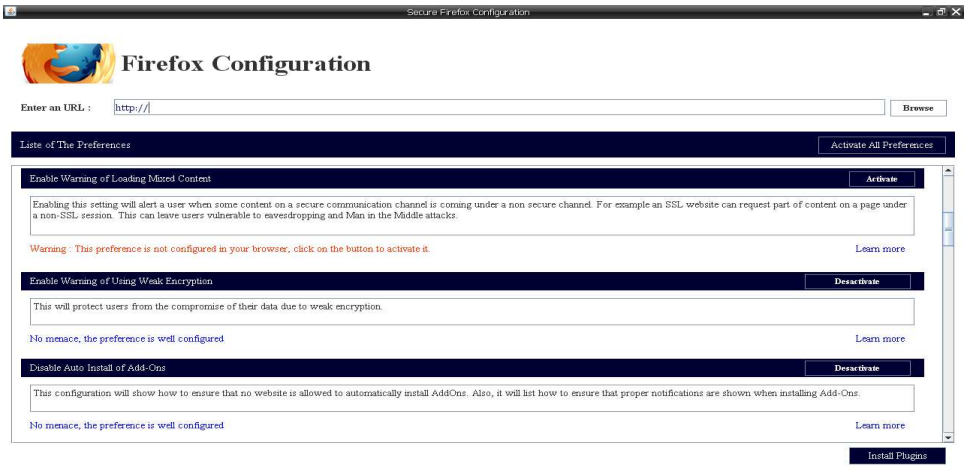



**Fig. 7.** Firefox automatic configuration features

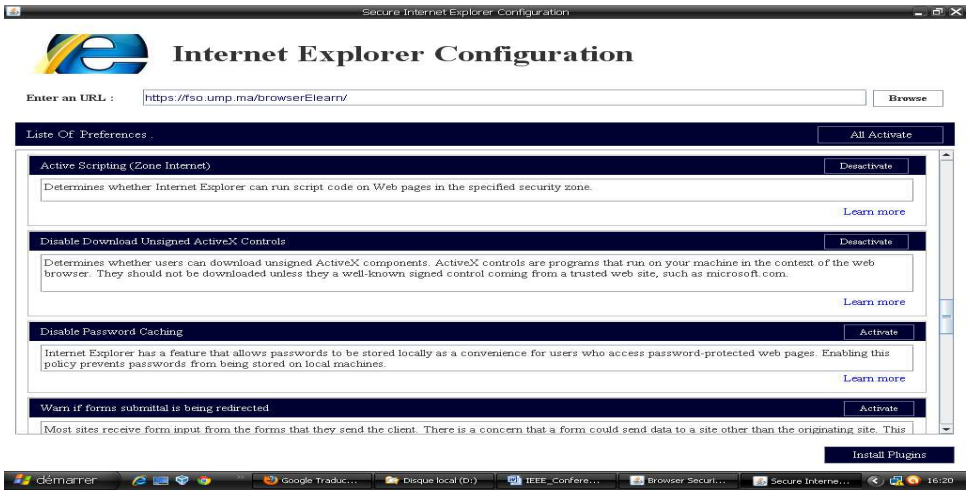



**Fig. 8.** IE automatic configuration features

## 4. DISCUSSION

Defense in depth with automatic solution remains a viable strategy and can play a central role. Its leverages from security features that modern browser has to introduce a new weapon in the battle against today's browser threats. the result obtained by our tool to confirm the need of such automatic solution to enhance security of browsing internet and in order to Check and support obtained security level of each detected web browser and reconfigured by our application, we use free downloaded framework (browser_tests-1.03 from http://code.google.com/p/browsersec/) it is a web server that contain a collection (more than 115 pages) of test cases web page. We found that more the browser has well configured features best the user is safe against common internet surfing vulnerabilities.

## 5. CONCLUSION

Accessing the web has many risks possibly with dire consequences for the home user who has limited information security knowledge specially with misconfigured web browser, By making automatic safe browser launcher that can empower home user side, by helping them to have secure tool to access to any web site and avoid them maximum of possible security

threats this freely available tool is one of the first such offerings, if not the first, of a secure features settings browser package automatically, This tool must to be permanently updated, because the changes at the application level can be well illustrated by examining the evolution of the web browser, which has advanced fairly significantly over the years and is now used as the means of accessing a myriad of online services.

## 6. REFERENCES


Accuvant, 2011. Browser security comparison.

Baum, N., 2010. Over 1,500 new features for Google Chrome.

Boyd, C., 2006. Rogue browsers-keeping Browsezilla and Co at bay. Netw. Sec., 10: 11-12. DOI: 10.1016/S1353-4858(06)70442-1

Dormann, W. and J. Rafail, 2008. Securing your web browser. Carnegie Mellon University.

EMA, 2010. Virtualizing the browser against security threats: The dell KACE secure browser. Enterprise Management Associates.

Furnell, S., 2009. The irreversible march of technology. Inform. Sec. Technical Report, 14: 176-180. DOI: 10.1016/j.istr.2010.04.002

Furnell, S., P. Bryant and D. Phippen, 2007. Assessing the security perceptions of personal internet users. Comput. Sec., 26: 410-417. DOI: 10.1016/j.cose.2007.03.001

Furnell, S., T. Valleria and D. Phippen, 2008. Security beliefs and barriers for novice internet users. Comput. Sec., 27: 235-240. DOI: 10.1016/j.cose.2008.01.001

Grimes, R.A., 2010. Web browser security deep dive how to stay secure on the internet.

Jackson, C., A. Barth, A. Bortz, W. Shao and D. Boneh, 2007. Protecting browsers from DNS rebinding attacks. Proceedings of the14th ACM Conference on Computer and Communications, Oct. 29-Nov. 2, Alexandria, Virginia, USA.

Kritzinger, E. and SH.V. Solms, 2010. Cyber security for home users: A new way of protection through awareness enforcement. Comput. Sec., 29: 840-847. DOI: 10.1016/j.cose.2010.08.001

Kumar, N., K. Mohan and R. Holowczak, 2008. Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls. Decision Support Syst., 46: 254-264. DOI: 10.1016/j.dss.2008.06.010

Louw, T.M.., J.S. Lim and V.N. Venkatakrishnan, 2007. Enhancing web browser security against malware extensions. J. Comput. Virol. DOI: 10.1007/s11416-007-0078-5

Opera, 2012. Opera's Settings File Explained.

OWASP, 2010. The open web application security project.

Ruderman, J., 2012. Configurable security policies.

Safari, 2012. Safari Features. Apple Inc.

Wisniewski, C., 2012. Which browser is safest? The browser wars are back and this time you win.

Zalewski, M., 2008. Browser Security Handbook.