Web Browsers Security Web-Lab

http://dx.doi.org/10.3991/ijoe.v9i3.2681

M. Serrhini, A. Ait Moussa
Faculty of Sciences, Oujda, Morocco

***Abstract*—One of the biggest created software platform is Web Browser. Today's platform is unique software used to access online data for lot of electronic transactions services such as e-mail, e-banking, e-commerce, and e-learning etc. Hackers know that browsers are installed into all computers, smart phones and tablets. Soon other devices such as TV, cars and others, can be used to compromise all these devices. All browsers have enabled or disabled features that define their behavior for executing good material and stopping malicious attacks. Unfortunately most of the users are unwilling to setup these features correctly to enhance their safety, because many of them still do not understand even basic security concepts. This paper presents Web Browsers Security Web-Lab where student can practice and test online the real security threat and risk that he was. Also could be exposed to with his browser, and describe two part outline for achieving this work. First an application launched at student side that will automatically detect all installed browsers and check their features configuration setting, and based on the finding prepare to student tailored work programs for practicing browser security online. Second parts Web-Lab platform, where student simulates and consolidates his knowledge in the field of information security in modern's browsers.**

***Index Terms*—browsers security simulation, online awareness security, security practice web-lab.**

I. INTRODUCTION

To access to the web material (texts, image, audio, video, animation, etc.), the student use his/her browser to communicates with server hosting the needed services application is handled via a transport protocol HTTP. Then, a transport protocol defines data formats, but also the algorithms for packaging and unpackging application payloads shows the data format as HTML, CSS and other media (pdf, mp3, flash etc.). The browser can read with plug-in and the true plug-in, are any software deployed by the server to the client that extend the functionality of the browser JavaScript, which make sites more interactive. Most of students use their home computer, laptop to surf to the Internet, and they are increasingly the exposure to security threats while using their PC systems [1]. Internet users are becoming more vulnerable to security threats due to the use of information communication technologies according to [1] [2]. This vulnerability is due to the fact that they do not possess the knowledge to understand and protect themselves. Most of internet users think that their browser is only the software that they can visit a page by tapping URL and click the green "Go" button. Internet users therefore in many cases venture into internet without any idea of what the risks are and what they must do to protect themselves. Students are likely to face a range of internet threats as their unfamiliarity with the technology can limit their ability to recognize the threats and understand the requisite protection [3].

Students browse internet to access to lot of services site, and they use the browser, all of these browsers have repeatedly been affected by vulnerabilities or are not securely configured, that have allowed hackers to do practically anything on student computer, and all he does was to visit a website and it could take control of his computer.

The features of the browsers define theirs behaviors, it is essential for students to understand the functionality and features of the browser they use. This is for understand what different features do will help them to determine how they affect to functionality browsers and the security of theirs computers. This indicate specially, what features does browsers have to help protect the students from dangerous downloads, and to help secure the connection between them and browsed sites, to help defend against browser attacks, and does theirs browsers filter to help block phishing sites.

Lot of factors made browser security problem worse 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 without considering the risks of their actions.
- Many computer users believe that because they are skilled at generation word processing documents, and presentations and 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 page are not accessible unless users enable certain features or install more add-ons, putting the computer at additional risk as depicted in Fig. 1

The evolution of the browser has won a great experience, and there are several ways that modern browser can help prevent common internet security pitfalls [4]. Often, the browser that comes with an operating system or downloaded from vendor site, are not setup in a secure default setting. This is, because vendors will enable lot off features by default to improve the computing experience and to appear as the fastest as concurrent, Hence the need to reconfigure them securely to avoid myriads attacks from the web.

Information Security is a new concept to most students. Developing an awareness course with live practice for all students ensures that a consistent message is delivered

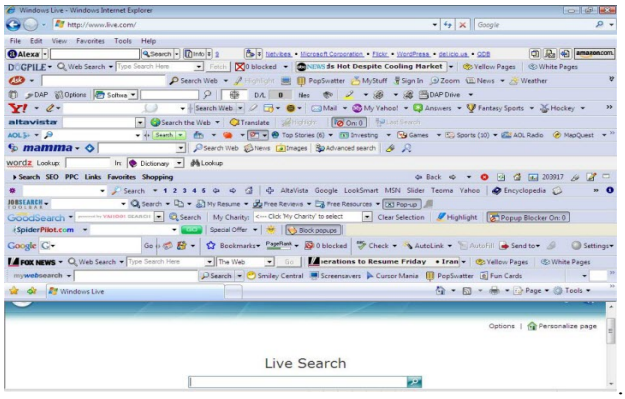


Figure 1. Example of Browser Internet explorer with enabled feature auto installs add-ons.

through visualization that benefit from Web-lab service philosophy as demonstrated in [5] [6] [7] [8].

Traditional techniques of teaching (i.e. lectures or literature) have turned out to be not suitable for security training, because the trainee cannot apply the principles from the academic approach to a realistic environment within the class. In security training, gaining practical experience through exercises is indispensable for consolidating the knowledge [9].

In this paper we present Browser Security Web-Lab project that provides a novel e-learning system for practical security training in the WWW and inherits all positive characteristics from offline security labs. The Browser Web-Lab server basically consists of a based testing by doing training environment. As expected result, student will develop his security knowledge and in consequence enhancing the security of his Web Browser.

II. RELATED WORKS

Our research activities in the area of training online security in modern web browsers are a new topic. We don't find similar work to compare our research with it but some works attract our attention.

One solution proposed by [10] [11] 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. These methods are not sure, that most of student can perform this task as expected, and doesn't cover all security topics in browsers.

Dell KACE 2012, introduces a tool named Dell KACE [12], being a secure browser that virtualizing this technique to investigate information, against security threats, specifically for the browser that features enterprise manageability. This secure technique is virtual offering control over the browser execution; which is optional white and black list control over browser processes. Also, constraints on changes to the browser and its extensions, add-ons 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 but not provide to the user any awareness training, it can be used only as Demonstration software programs for offline training.

Dedicated computer laboratories for IT (Information Technology) security have been created in many universities, e.g. described in [13]. Security experiments or exercises are usually arranged using small, isolated computer networks (three Computers). Compared to other approaches, dedicated Computer laboratories are ideal environments for practical security teaching because security exercises are performed by application of production software in real systems.

However, practical education by laboratory measures normally results in high costs. Dedicated networks require expensive hardware/software investments and intensive efforts to create, configure, and maintain laboratory environments as well as to prepare, supervise, and evaluate exercises. On the other hand, most security exercises require system level access to the operating system. This introduces the risk of misuse and inconvenience of administration. For security reason, dedicated networks are normally operated on isolated networks, which imply that such security laboratories pitifully fail to benefit a wider range of learners outside campus.

III. STUDENT SIDE APPLICATION ARCHITECTURE DESCRIPTION

All browsers have integrated GUI (graphical user interface) to configure browser features through options panels allowing enabling or disabling some features setting manually. But many users as their unfamiliarity with the technology they don't know what to enable and what to disable, also all browsers to display certain built-in functions. These systems, 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.

This section describes how to build such application that can empower the student side for training his browsers features settings. Also this tool can be used as standalone frame work as demonstrated in [14] to disable all features that can cause vulnerabilities and enable all features that enhance security as showed in our previous work.

The mains functionality of our application are:

- Detection of all 5 popular browsers installed in the student computer.
- Detection of enable or disable features and compares them with the requirement to secure the browser.
- Launching the online tailored security awareness practicing work program in Web-Lab platform where student can practice and test all security hole and risk of the features.

A. Browser detection

It's important to detect and secure all the five major browsers used today and installed in the home student 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. Each browser is well known by its famous image logo. The logo image of detected browsers is showed in application main window, in Microsoft Windows operation system. Each installed program has an entry in the key base registry. After execution, application detects installed browser and version from Microsoft Windows key base registry.

B. *Browser features configuration detection*

There are two way to read and change browser features setting, in our algorithm that we use both. First method is to read features from preference file in the browser installation directory, and second is to read it from the entry of features in the windows key base registry.

1) *Detection from browser preferences file.*

The major browsers according to the literature study (Opera, Safari, Firefox and Chromnium) [15] [16] [17] allow user to modify 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 and strictly forbid the modification of this files, but suggested to create another file named (user.js) and to place it in the same Firefox directory profile.

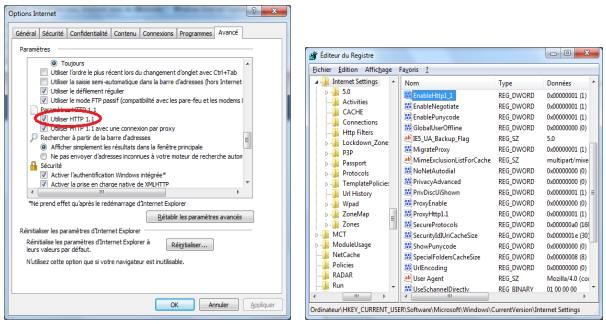
Our algorithm parses state of each feature in browser preference file, check if it have enabled or disabled setting state, compare it with security need, and if the value isn't safely configured the application will change it in the preference file. Firefox needs to be restarted to apply the change.

2) *Detection from the key registry of windows.*

The second solution is to change the security settings in the windows key Registry as shown in "Fig. 2," This is realized, manipulating the registry entry corresponding to the feature in question. Then, this configuration has been implemented in our application for Microsoft internet explorer, because this browser is part of the windows operation system, and for Google chrome (Chromium Projects) [18]. It is important to note that in some cases, the registry entry corresponding to some features, and is not in the registry, in this case the solution, is to create it.

C. *How Application is used for Browser Security Web-Lab.*

To start practical security training program, student must download the application from Web-Lab platform, which is easy to use, no training, installation or configuration is needed, only with the application execution will check the student computer, to detect all installed five major browser, as depicted in "Fig. 3," all installed browser logo images are showed in the main first window after detection. Then, student click on his favorite browser logo, second window is launched as shown in "Fig. 4,", where all enabled or disabled state of selected browser features setting supported by the application is shown with descriptive awareness messages explaining to student about the security risk he could be exposed with each features. After check browser setting, when a bad configured feature is detected the application will prompt student a red color message alerting him to reconfigure it automatically by a click to button activate/deactivate in this window. Blue color message if well configured feature. Finally to practice by doing and to visualize how the feature will affect his security, student must to click on the button Learn More. Then, he will be directed to the lab link of the corresponding feature in Browser Security Web-Lab platform, where he can practice and to visualize the security threat result directly in his browser.



(A) (B)

Figure 2. Internet explorer features setting to check (B) base registry entry for this feature.

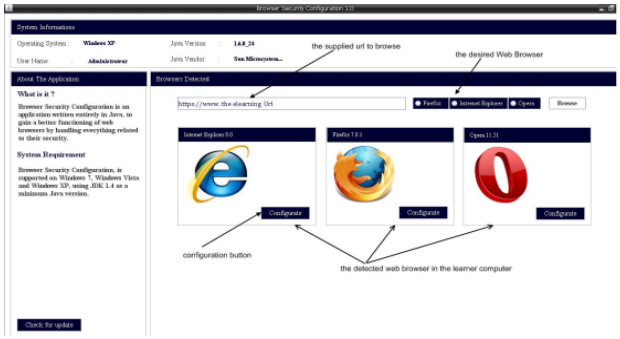


Figure 3. Browser Security Configuration Main Menu.

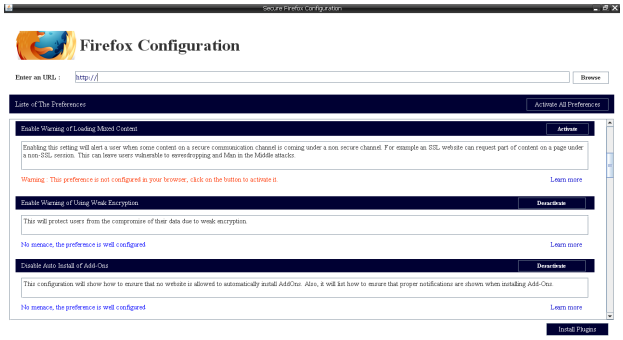


Figure 4. Checking result Firefox features configuration

IV. WEB BROWSER SECURITY WEB-LAB ARCHITECTURE DESCRIPTION

Web Lab as a service employing Web technologies over different networks (i.e. public Internet, campus wide network, or high speed private network) may become very interesting for Universities and research institutions. This system could follow this opportunity with the aim at extending their online offerings to external users and institutions. The proposed system was developed according to the ADDIE model (analysis, design, development, implementation, and evaluation) proposed in [19]. This instructional model is based on the systematic development of instruction and learning and is composed of seven phases: analysis, design, development, implementation, execution, evaluation, and feedback.

A. *Web lab infrastructure*

The system is based on the common three-tier-architecture of web-based applications that is organized into presentation tier, logic tier, and data tier.

In the client tier, the user (Student, trainee) interacts with the system through a web browser. The requests are handled by a web server. The contents of the web pages are generated dynamically by using PHP, JavaScript, HTML/CSS, Java for applet, and AJAX Techniques from the web server to the web browser on the client machine.

B. *The Web Browser security Web-Lab practical material content*

The content practical materials is set of web page most of them, and are inspired from one free open source frame work [20]. It is to test the modern web browsers, where this web page contains a risk to test directly in the student web browser. Also, let him to visualize the risk and allow student to learn security by doing. Web-Lab covers the most of the web browser security topics:

- Updating web browser
- Encryption settings
- Add-ons settings
- Dynamic content settings
- Network settings
- Privacy settings
- Advanced javascript setting

V. OPERATION OF THE WEB-LAB

The main operation of web browser security web lab is remote teaching of the students about existing link between web-browser security features configuration and online security threats. Student learns how to interact with his browser, reconfigure browsers features securely for future use and benefit from security technology present in most modern browsers that allow pre-checking each web page he visits and alert him if one is suspected of being malicious. This lets him make an informed judgment about whether he really wants to visit that page.

You're also safer on the web when you pay attention to visual cues in the browser, like checking the URLs you're sent to, and looking for an "https://" secure connection or extended validation.

The web lab is constituted of two parts as depicted in "Fig. 5," Application for checking student computer to find browser security hole and depend on the found prepare to student a tailored teaching program to access to Web-Lab for practicing online security risk simulation.

Bellow detailed description of how user uses application and simulates Web browser security in Web-Lab platform:

A. *How student start security-risk simulation in Web-Lab*

- Student launches application on his computer.
- Application detects all installed browsers in his computer and shows them in the main window as shown in "Fig. 3,".
- Student selects his favorite browser.
- The application will check the features configuration of the selected browser.
- Another window shows student the configuration state of all his browser features, if any features are detected not securely configured, an awareness message about the risk is provided with link to simulate the risk in Web-Lab platform as shown in "Fig. 4,"., also notification in red color alert him that this must to be reconfigured.
- To visualize the security risk, student click on link (learn more), he will be redirected to the web lab platform to simulate the risk and learn more about.

B. *How student will practice and visualize the security-risk simulation in Web-Lab*

After login in web lab platform, student will be redirected directly to the web page containing security risk simulation that student clicked to visualize and to learn more about.

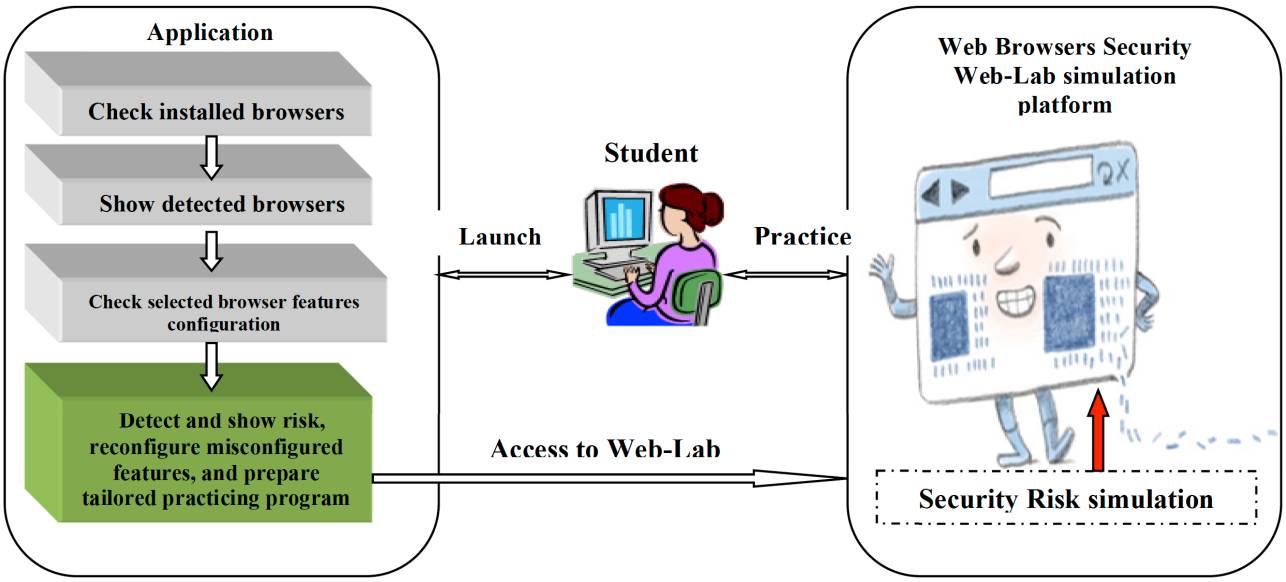


Figure 5. The operation of web browser security Web-Lab

Below two examples of how student will see the risks:

As shown in "Fig. 6," student will see the security risk of geolocation directly on his computer, the application will redirect him to Web-Lab platform were web page will show him his exact position in the world map and his latitude coordinates ("Fig. 6," shows the exact position of this article author the city Oujda Morocco). Student understands that this is due to activated geolocation feature in his browser allowing any web site to geolocate him, he could be exposed to big security risk for his privacy and even for his life, because the bad Hacker can uses this coordinates in online services such Google maps or Google street to view the house where he lives, the model of his car if Google Street has takes a photo of his car parked front of his house etc. detailed description all geolocation security risks are provided in this simulation web page.

Second example student will practice how malicious java applet expose his data and privacy to security threat, he will see that even if this feature is well configured and his browser alerting him with red color visual message if really he want to execute this application as shown in "Fig. 7," when student accept he will see how some java applets can read his data, take photo from his camera, record voice from his microphone, read his cookies and show the visited web sites history etc. In this example student will learn that he is safer on the web when he pay attention to visual cues in the browser, and must execute on his computer only a tierce application that he is sure from the provenance.

C. *Security in Web Browser security Web-Lab*

Security and privacy of student should be respected when you develop such Web-Lab solution for simulating web browser security risk directly in the learner computer, you must to take careful that contain material must be only for simulating the risk safely, and not to cause damage to simulate the risk, because this will dissuade student to use web lab, e.g if you need to show student how browser interact with his antivirus when he download a virus from web page, you can use an inoffensive virus test file such "eircar" from (http://www.eicar.org/85-0-Download.html) to simulate this risk, or when simulate the risk of malicious java applet ability to read a file from student system, you can ask student to write a text file containing his name that this applet will read and shows student name in his browser to explain him that some malicious applet can easy access to his disk files system.

D. *Effectiveness of the web browser security Web-lab*

The advantages of Web-Lab Security awareness Portal are the ability to have feedback from your Learning Management System (LMS). Data about yours students progress as showed in the "Fig. 8,", and also some extra quiz can give a view in assimilation of the security material. This information can be analyzed, in order to determinate the effectiveness of our security awareness program for the future improvement.

I. CONCLUSION

Many of us these days depend on the World Wide Web to bring the world's information through a web browser. What do we need to know to navigate the web safely and efficiently? It is therefore essential to ensure that student

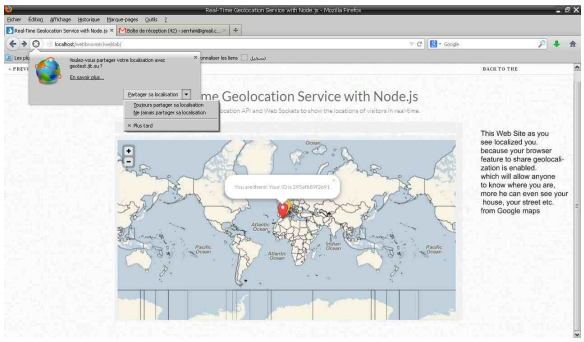


Figure 6. Example of Geolocation risk simulation

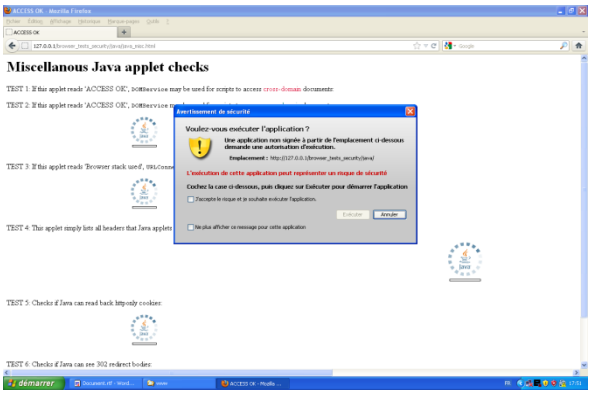


Figure 7. Example of browser alert behavior for malicious java applet simulation

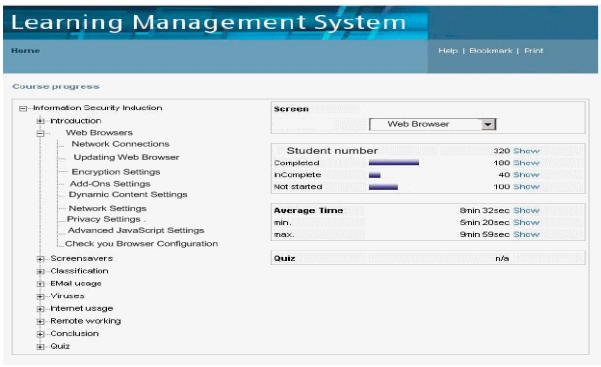


Figure 8. Feed back statistics

use a secured web browser, and learning to avoid possible security threats when they are online. Developing such awareness course with live practice for all students ensures that a consistent message is delivered through visualization and practice that benefit from Web-lab. This model must to be permanently updated, because the changes at the application level can be well illustrated by examining the evolution of the web browser. For this reason, has advanced fairly significantly over the years and is now used as the means of accessing a myriad of online services. Future research will concentrate on implementing such M-Weblab for Mobile systems platform like (android, IOS, Symbian), and others Linux system.

REFERENCES

[1] S. Furnell et al, "Assessing the security perceptions of personal Internet users," Computers and Security, vol. 26, pp. 410-417, 2007. http://dx.doi.org/10.1016/j.cose.2007.03.001

[2] E. Kritzinger, SH. Von Solms, "Cyber security for home users: A new way of protection through awareness enforcement," Comput-

ers and Security, vol. 29, pp. 840-847, 2010. http://dx.doi.org/10.1016/j.cose.2010.08.001

[3] N. Kumar et al., "Locking the door but leaving the computer vulnerable: factors inhibiting home users adoption of software firewalls," Decision Support System, vol. 46, pp. 254-264, 2008. http://dx.doi.org/10.1016/j.dss.2008.06.010

[4] Wisniewski. Chester. (2012, July). "Which browser is safest? The browser wars are back and this time you win," [Online]. Available: http://nakedsecurity.sophos.com/2012/07/16/which-browser-is-safest-the-browser-wars-are-back-and-this-time-you-win/ accessed 10 may 2013

[5] M. A. Bochicchio, A. Longo "Delivering Collaborative Web Labs as a Service for Engineering Education," International Journa of Onmline Engineering, Vol. 8, No. 2, 2012, pp. 4-10, http://dx.doi.org/10.3991/ijoe.v8i2.1897

[6] Grimaldi, D., Rapuano, S. (2009). "Hardware and software to design virtual laboratory for education in instrumentation and measurement. Measurement, 42, 485-493. http://dx.doi.org/10.1016/j.measurement.2008.09.003

[7] Atanasijević-Kunc M., Logar V., Karba R., Papić M., Kos A. (2011). Remote multivariable control design using a competition game. IEEE Transactions on Education, 54, 97-103. http://dx.doi.org/10.1109/TE.2010.2046489

[8] Gillet, D., Ngoc, A. V. N., Rekik, Y. (2005). Collaborative web-based experimentation in flexible engineering education. IEEE Transactions on Education, 48, 696-704. http://dx.doi.org/10.1109/TE.2005.852592

[9] M. Bishop, Education in information security. IEEE Concurrency, 8 (4):4–8, 2000. http://dx.doi.org/10.1109/4434.895087

[10] W. Dormann, J. Rafail, "Securing your Web Browser," 2008, [Online]. available: http://www.cert.org/tech_tips/securing_browser/ accessed 10 may 2013

[11] IS-Academia support [Online]. Available: http://wiki.epfl.ch/is-academia.support.en/browsers accessed 10 may 2013

[12] Dell kace, [Online]. available: https://www.kace.com/en/products/freetools/secure-browser accessed 10 may 2013

[13] G. Vigna. Teaching hands-on network security: Testbeds and live exercises. *Journal of Information Warfare*, 2:8–24, 2003.

[14] M..Serrhini et al., "Improve security of web Browser with stand-alone e-Learning awareness application," in International Conference on Multimedia Computing and Systems (ICMCS), IEEE Conference Publications, 2012, pp . 852-857. doi: 10.1109/ICMCS.2012.6320163 http://dx.doi.org/10.1109/ICMCS.2012.6320163

[15] J.Ruderman, [Online]. Available:http://www.mozilla.org/projects/security/components/ConfigPolicy.html accessed 10 may 2013

[16] Safari, [Online]. Available: www.apple.com/safari/features.html accessed 10 may 2013

[17] Guide to security and privacy in Opera, [Online]. available: http://www.opera.com/help/tutorials/security/control/ accessed 10 may 2013

[18] ChromiumProjects, [Online]. Available: http://www.chromium.org/administrators/configuring-other-preferencesaccessed 10 may 2013

[19] W. Dick, Carey, L., & Carey, J. O. (2001). The Systematic Design of Instruction (5th Ed.). New York Addison-Wesley, Longman.

[20] M.Zalewski.(2008-2009)."Browser security hand book test cases," [Online]. Available: http://code.google.com/p/browsersec/downloads/list accessed 10 may 2013

AUTHORS

M. Serrhini is engineer in computer sciences security and lecture with the department of mathematics and computer science at faculty of science university Mohamed Premier Oujda Morocco (e-mail: serrhini@gmail.com).

Prof. Dr. A. Ait Moussa, Jr., is with the department of mathematics and computer science at faculty of science university Mohamed Premier Oujda Morocco, His research interests are in the areas of e-learning, e-lab, virtual lab and M-learning (A_aitmoussa@yahoo.fr).

Received 20 January 2013. Published as resubmitted by the authors 12 June 2013.