Fostering Content Relevant Information Security Awareness through Browser Extensions

Marius Potgieter, Craig Marais, Mariana Gerber

To cite this version:

Marius Potgieter, Craig Marais, Mariana Gerber. Fostering Content Relevant Information Security Awareness through Browser Extensions. 8th World Conference on Information Security Education (WISE), Jul 2013, Auckland, New Zealand. pp.58-67, 10.1007/978-3-642-39377-8_7 . hal-01463659

HAL Id: hal-01463659

https://hal.inria.fr/hal-01463659

Submitted on 9 Feb 2017

Fostering content relevant Information Security Awareness through Browser Extensions

Marius Potgieter, Craig Marais, and Mariana Gerber

School of Information and Communication Technology, Nelson Mandela Metropolitan
University, Port Elizabeth, South Africa 041 504 1111
s208108589@live.nmmu.ac.za (Marius Potgieter)
s204005264@live.nmmu.ac.za (Craig Marais)
Mariana.Gerber@nmmu.ac.za (Marianna Gerber)
http://www.nmmu.ac.za

Abstract. A call for adopting information security awareness amongst end-users has been suggested over the years. Adoption can occur through various methods. These methods each hold their own characteristics, whether being of a positive or negative nature. The challenge to find an appropriate method on which to establish and engage in a security dialog with a user has been written on extensively over the past few years. A number of common key points have been raised in research that addresses information security awareness and how it is conveyed to users. Additional to these common key points, this paper suggests using browser integration as a medium to promote security values and provide security suggestions based on a specific users behavioural pattern.

Keywords: information security, awareness, browser extensions, content delivery, brain-compatible learning, usability

1 Introduction

Personal security is something taken very seriously; people have some concept of what they find important to ensure their security [1]. This stems from peoples views and awareness of what could be seen as threats to their security. In the physical world these threats are aspects that people understand and can easily relate to. The consequences of not protecting against physical threats would mean a loss, which would result in a feeling or a sense of concern for people, since it could impact on their physical body or possessions. People use the web for many purposes; to interact socially, conduct business and purchase goods (amongst other activities), causing activities that would normally be conducted in the physical world to now also exists within the cyber world. Through their activities, engagement with and usage of the web, a digital persona is increasingly built [2]. This digital persona exists as information scattered over the web that relates back to the user it belongs to. This digital persona is just as vulnerable to an array of threats as the physical person [3]. Creating awareness of these threats is the core of information security awareness [4] [3].

The way people are informed about information security has been a topic of serious discussion for many years. Within the corporate environment the need for information security awareness has been recognised through international standards and policies [5] or information security culture [6]. These efforts have resulted in a noticeable level of awareness within companies [7][8]. Alarmingly the largest group vulnerable to the cyber security threats are home users [8]. Without targeting awareness programs directly at this vulnerable user group, a serious lack of information security awareness could exist [9].

Users commonly interact with the web through browsers. These web browsers provide a way for users to traverse the World Wide Web. Unfortunately the standard browsers do not make the user aware of the various dangers that the web contains. Web browsers, as they are, do not contain comprehensive means for making users aware of these threats, although most of them contain the functionality to extend their capabilities. These extendable capabilities are fittingly referred to as browser extensions (or plugins). These extensions can be designed to integrate into the browser to provide a specialised functionality. Extensions have access to what the browser is retrieving, presenting and traversing; and thus provide opportunities that will be explored.

This paper presents an approach to information security awareness that utilises the browser's own innate knowledge. This knowledge stems from what the browser is currently presenting to the user in a form of a web page or other activities performed on the web. This will be used to provide personalised and content-relevant awareness information to the user, warning against possible dangers that can be encountered. This paper, further, explores current security usability research to enhance user awareness, through browser extension, in a way that best suits the user. This approach will be validated using security usability for end-user applications that define criteria that increases overall usability [10].

This paper will employ logical reasoning and argumentation to develop an approach to deliver targeted information security awareness content by means of a model. This model will be implemented and then be critically analysed using above mentioned criteria.

This paper will provide background information on browsers and how they can be extended. It will then investigate Information Security Awareness and how it relates to browsers. A model will then be presented, applied and evaluated using leading studies in end-user usability.

2 Web Browsers

Web Browsers are used by users that want to interact with the World Wide Web. Commonly used browsers include are Chrome, Firefox, Internet Explorer, Opera, and Safari. The browser operates by retrieving information stored at various locations on the web and displaying the content to the user. The user requests what information is to be retrieved though the browsers address bar that forms part of the user interface. The interface also contains other features to assist the user in navigating the web. These include features like the back/forward button, bookmarking, refresh etc. All features, except the display that shows the requested web content, are considered part of the web browsers user interface.

After the users request is processed by the browser engine that fetches the content from the web and passes the content to the rendering engine to be processed, the rendering browser engine processes the content and displays the website for the user to see. Additional to having features, browsers also comprise components.

Components forming part of browsers are: the networking (used as platform independent method of making requests to the web), JavaScript Interpreter (that processes and executes JavaScript code that was part of the content received), UI Backend (this draws features on the screen like popup boxes or windows) and data storage (stores information on the local machine e.g. some websites use this to identify users that return to their website using cookies).

These components commonly appear in most standard web browsers that are available to users. Fig. 1 presents all the mentioned components of standard web browsers and their interrelationships, each browser will implement this structure to its own specifications.

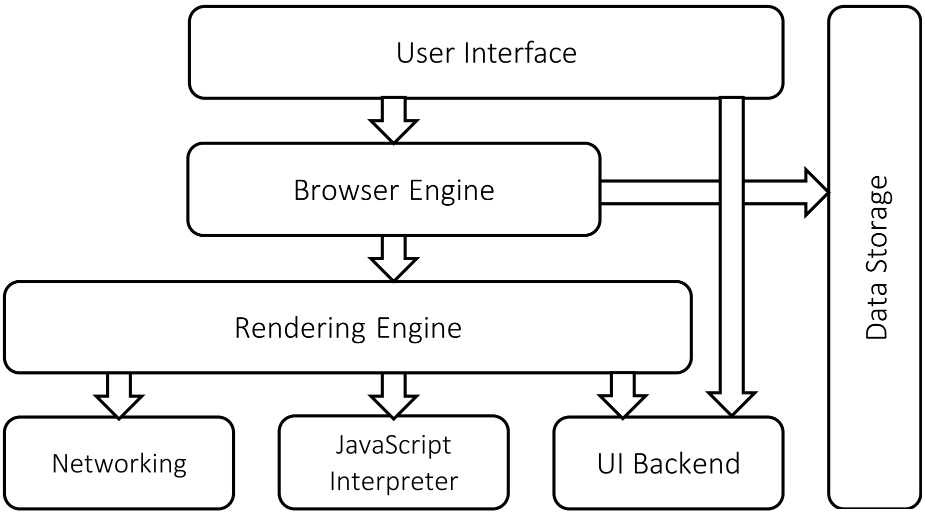

Fig. 1: Browser component relationship

3 Browser Extensions

Browser extensions are developed just like any other regular application, with the exception that it uses the browser as platform to run on. Each browser uses its own design and API (application programming interfaces) to create extensions.

These extensions are, thus, created for each unique browser type e.g. Chrome Browser, Firefox Browser. Once developed, these extensions are put through a simple evaluation system by the parent company that owns the targeted browser (Each company has its own specific evaluation criteria). This evaluation is to determine whether the extension follows the company standards of the particular browser and once approved, gets placed in the browsers extension library. These repositories of extensions (e.g. Google Chrome Store) are accessible to anyone who wants to add the extension to their browser. Some of these extensions, when installed, requests permission from the user to access personal data of the user to be used in the extension. Extensions that have been updated by their developers get updates (on the users machine) either automatically or by requesting the users approval. This ensures that the user is kept up to date with the current version of the extensions that they are using.

4 Information Security Awareness and Browsers

The aim of information security awareness is to make as many users as possible aware of the dangers that exist relating to the use of the World Wide Web. The vast majority of users interact with the World Wide Web through browsers. This makes it an ideal platform to launch a tool (in the form of a browser extension) that would provide appropriate information security awareness content to the user regarding their web activities.

Providing the user with information security awareness information or suggestions gathered from what is happening within the browser, provides relevance to the user. An Information Security Awareness Extension would utilise various methods of analysing possible information gathered from the browser that can be used to provide targeted awareness information to the user. This section will explore a few of those techniques.

4.1 Browser State Analysis

The browser state will provide information about what is happening with the browser as an application. These include examples like:

- *Security Level* e.g. what security protocol is being used by the browser; this would include the standard protocol - Hypertext Transfer Protocol (HTTP) and the more secure Hypertext Transfer Protocol Secure (HTTPS).
- *Loading State* of the webpage, either being uploading or downloading information.
- *Visited Webpage URL (uniform resource locator)* the website being visited has a specific location on the world wide web.
- *Installed or loaded Extensions / Plugins* e.g. extensions and plugins include applications that extend the capabilities of the browser as explained in previous section. These could include useful functionality like being able to play Adobe Flash material, but there could be the possibility that other extensions could be malicious.

- *Default Homepage* is commonly set by the user depending on their preferences. It remains possible for third party applications (or extensions) to modify this preference. It is common for spyware or adware to modify this preference to redirect the user to a website containing misleading information.
- *Stored Login Usernames and Passwords* are commonly kept stored within the browser in a secure database on request of the user. This is commonly stored once the user created a registration form on a website for the first time or used the login information for the first time to access the website.

4.2 Web Content Analysis

Once the webpage has loaded the content is available for analysis. The content would be in the form of HTML files, possibly with imbedded JavaScript. The content of a website could also include third-party code in the form of applications (or applets) e.g. Adobe Flash. These include examples like:

- *Webpage Content (HTML)* is generally what the user sees displayed on the browser window. The content includes simple text, images, links to other webpages etc. that is used to navigate the World Wide Web.
- *Input Fields* are used to gather information from users in the form of textbox fields, checkboxes, dropdown fields etc. These fields would require the user to input personal information such as first name, surname, date of birth, personal address etc.
- *Password Fields (Login information)* are used to authenticate a users identity. The password field gets displayed when creating a user account for the first time and for subsequent login sessions (when not stored as discussed previously).
- *Credit Card Input Fields / Other E-Commerce Payment options* will become available when purchasing or providing payment on a website. Many website use third-party services in this regard e.g. PayPal.
- *Rich Media Content (e.g. Adobe Flash, Microsoft Silverlight etc.)* are development platform applications outside the scope of the standard browser development engine (JavaScript). These are commonly embedded within the browser content as packaged applications that run on their own engine that needs to be installed inside the browser (like with Microsoft Silverlight) or on the computer (with Java JRE).

4.3 Data Storage Analysis

Data regarding the users behaviour on websites sometime get stored in the form of cookies or other storage locally on the users machine. Data storage includes:

- *Cookies and Internal Databases* contain information gathered about the user when visiting a website that stores certain information about the user and that visit to their website (also referred to as a web session). An example of this is the shopping cart created while purchasing from an online store.

As seen in these analysis techniques, the browser provides a wealth of information regarding exposure that the user has to the World Wide Web. This information can be used as event triggers to supply the user with information, targeting specific threats by providing specific awareness information, applicable to the users current browser content or behaviour.

An example would be to provide the user with targeted awareness information about creating a secure password, once the Web Content Analysis has seen that a password field exist within the web content. The Browser State Analysis would then provide information if the password for that specific website already exists, or not. If no password has been created for that website, the browser extension will assume (through simple induction rules within the extension) that the user is about to create a password for the first time and supply the user with a tutorial on how to create a secure password. If a password already exists for the site, information regarding general password security will be displayed [11]. A model for such browser extension will be discussed.

5 Awareness Model and Design

A model for browser extension to address the lack of content relevant information security awareness associated with dangers of using the World Wide Web is depicted in Figure. 2. This model will be referred to as the Targeted Awareness Browser Extension Model. The model consists of engines that will provide the targeted awareness content to the user through the extensions user interface. An implemented example of this model will be the Information Security Awareness Extension.

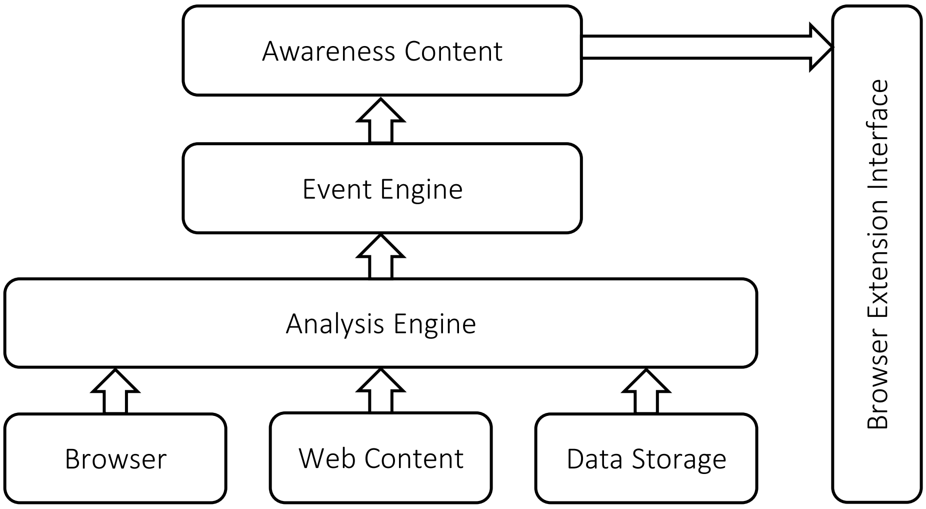

Fig. 2: Targeted Awareness Browser Extension Model

The components of this model will now be explored in further detail.

5.1 Analysis Engine

The analysis engine will provide the event engine with possible threats or targeted awareness information depending on the status or content of the browser. This information will be gathered from the users browser, web content and data storage, which comprise the lowest layer illustrated in the Awareness Model.

5.2 Event Engine

The event engine will determine whether something within the browser is generating a possible incident that can be raised as a topic of awareness to the user. The event engine will pass event information to the awareness content and allowing it to further target the user with appropriate content.

5.3 Awareness Content

The content provided by the extension will be directly related to a category or topic the event engine defined as relevant to what is currently occurring within the browser (as discovered by analysis engine). The way the content is structured will follow established brain-compatible techniques for providing information security education as defined by Reid [12] and using rich-media as discussed by Shaw [13]. This will provide a greater degree of understandability and learnability of the content and, thus, increases the diversity of the target audience that this browser extension could potentially target. Awareness content will be assigned a theme so that a user can easily identify the type of awareness information that is currently being displayed (e.g. with passwords the use of green as a topic colour would be considered an appropriate choice as an example of an assigned theme).

Further examples of targeted awareness information include:

- When the user visits a banking website (determined by the engine analysing the web address of the website being visited), appropriate content will be displayed about phishing attacks and how these can target the user.
- While posting comments on a Social Media Website (e.g. Facebook) the user will be provided information about possible privacy settings available, how to enable/disable them and the possible threats of ignoring them.
- An unknown website wants to load a third-party embedded application using Rich Media Content, the user will be provided with information about how malicious content can be distributed using such Rich Media Content.

5.4 Browser Extension Interface

The browser extension interface will consist of a vertical side panel within the browser application. This side panel will adjust the size of the browser window accordingly so that the content will create as little as possible intrusion into the users standard screen estate assigned to the browser. Using standard resolution used by a majority of the web user population [14] while having the browser extension open (active) there will be no significant reduction in the size of content within the browser window. This will promote a less intrusive design while still providing a visible interface that can be interacted with.

6 Awareness Extension Usability

When considering end-users, the usability of a security feature within an application becomes an issue. The way in which users interact with computers is an established field of study, referred to as HCI (Human Computer Interaction). The use of recognised HCI concepts in the design of security in computers have been suggested to improve user acceptance [15] of a system or application. Further study was done by Furnell [10] by identifying challenges users experienced in understanding security features within applications. However, evaluating security awareness usability as a feature within applications, has not been the subject of extensive study. This section aims to evaluate the usability of the Information Security Awareness Extension using criteria proposed by Furnell [10]. The following is a summary of these criteria:

- *Understandable* the information provided by a security feature needs to be presented in a meaningful way to the intended user population.
- *Locatable* users need to be able to have the security feature easily at hand.
- *Visible* - visibility of system status allows the user to observe the internal state of the system. Using status indicators and warnings will provide users with information about possible safeguards that need to be enabled.
- *Convenient* the security feature should not disturb the user from their regular routine. The feature could be considered as inconvenient or intrusive and thus negating or reducing the user experience of the feature.

The Information Security Awareness Extension will be evaluated according to the above mentioned criteria to emphasize and validate security usability. To achieve this, the criteria will now be discussed in relation to the Information Security Awareness Extension.

- *Understandable* Following recommendations for creating brain-compatible material for information security education [12] the content will accommodate a wide user audience, level of understanding and learnability. Since the awareness content that is generated and displayed to the user is content specific, the security message will be applicable to the user's current task. The awareness message will thus be meaningful to the user and can either be applied practically (in the case of the above mentioned example of creating a secure password while on a website asking for the user to provide a password) or that the message is of such relevance that user will take time to consider possible security threats.

- *Locatable* Since the browser extension will be integrated within the browser environment where most users are exposed to the threats of the World Wide Web, the awareness extension will always be active and displayed in a familiar location. The browser extension will supply information on an event-based system which will display content when it is appropriate to alert or inform the user of possible dangers.
- *Visible* The awareness content will provide users with visual indications of what is being displayed. Depending on the status of the event raised by the event engine, the content will either be an alert or guidelines and general information. Alerts will warn the user about possible threats and provide relevant content on the topic and its dangers (e.g. the browser analysis alert the event engine the user is not using a secure protocol while sending information over the web). Guidelines and general information will deliver non-critical content for the users consideration (e.g. while browsing a social media website like Facebook it will provide information on topics like cyber-bullying).
- *Convenient* as mentioned in the above section of the Browser Extension Interface we explored the reason why the extension will not intrude on the users regular routine. Other convenience factors include the fact that the browser extension will be publically (as well as freely) available on the browsers specific extension repository (e.g. with Google Chrome it Chrome Web Store). This provides a framework by which the extension can be updated. Since any changes made to the extension submitted to the repository will automatically update the users extension on his local machine. In this way the extension (and content) can be kept up-to-date without any further user intervention.

By evaluating the Information Security Awareness Extension against these criteria, it has been established that this approach follows recommendations by leading studies in information security usability with end-users.

7 Conclusion

The aim of information security awareness is to make users aware of the information security related dangers. This paper focused primarily on users information security awareness regarding the dangers associated with the usage of the World Wide Web and provided an information security awareness approach relating to these dangers. The platform on which awareness of these dangers are raised is ideally suited within browser extension. The innate knowledge provided by the browser can deliver targeted information security awareness content to the user on possible information security dangers. It also has been established that the design for such a browser extension should ideally conform to current security usability studies.

In response to this paper, further research will be done on how the implementation of such a browser extension can be achieved. Further investigation of this solution, towards promoting information security awareness by utilising browser extensions, will be reported on in subsequent papers.

References

1. L. Lazarus, *The right to security securing rights or securitising rights?* Cambridge University Press, 2012.
2. S. A. Williams, S. C. Fleming, K. O. Lundqvist, P. N. Parslow *et al.*, "Understanding your digital identity," *Learning Exchange*, vol. 1, no. 1, 2010.
3. Y. Wu, C. S. Guynes, J. Windsor *et al.*, "Security awareness programs," *Review of Business Information Systems (RBIS)*, vol. 16, no. 4, pp. 165–168, 2012.
4. N. Veerasamy and B. Taute, "Introduction to emerging threats and vulnerabilities to create user awareness," *Information Security South Africa*, 2009.
5. I. O. for Standardization and I. E. Commission, *ISO/IEC 27002*, ser. International Standard. ISO/IEC, 2007.
6. S. Furnell and K.-L. Thomson, "From culture to disobedience: Recognising the varying user acceptance of it security," *Computer Fraud & Security*, vol. 2009, no. 2, pp. 5–10, 2009.
7. S. Talib, N. L. Clarke, and S. M. Furnell, "An analysis of information security awareness within home and work environments," in *Availability, Reliability, and Security, 2010. ARES'10 International Conference on.* IEEE, 2010, pp. 196–203.
8. P. Wood, "Internet security threat report: 2011 trends," Symantec Corporation, 350 Ellis Stree, Mountain View, CA 94043 USA, Tech. Rep. 17, April 2012.
9. A. Stander, A. Dunnet, and J. Rizzo, "A survey of computer crime and security in south africa," in *of publication: Proceedings of the ISSA 2009 Conference.* ISSA, 2009, p. 217.
10. S. M. Furnell, A. Jusoh, and D. Katsabas, "The challenges of understanding and using security: A survey of end-users," *Computers & Security*, vol. 25, no. 1, pp. 27–35, 2006.
11. B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. C. Mitchell, "Stronger password authentication using browser extensions," in *Proceedings of the 14th Usenix Security Symposium*, vol. 1998, 2005.
12. R. Reid, J. Van Niekerk, and R. Von Solms, "Guidelines for the creation of brain-compatible cyber security educational material in moodle 2.0," in *Information Security South Africa (ISSA), 2011.* IEEE, 2011, pp. 1–8.
13. R. S. Shaw, C. C. Chen, A. L. Harris, and H.-J. Huang, "The impact of information richness on information security awareness training effectiveness," *Computers & Education*, vol. 52, no. 1, pp. 92–100, 2009.
14. w3schools. (2013, April) Browser display statistics. [Online]. Available: http://www.w3schools.com/browsers/browsers_display.asp
15. J. Johnston, J. Eloff, and L. Labuschagne, "Security and human computer interfaces," *Computers Security*, vol. 22, no. 8, pp. 675 – 684, 2003.