Enhancements to the Anti-Phishing Browser Toolbar

Bruno Lorentin[1,2]
[1]Polytech' Nantes
44306 Nantes Cedex 3 France
bruno.lorentin@gmail.com

Kristiina Karvonen[2]
[2]Helsinki Institute for Information Technology
P.O.BOX 9800 TKK 02015 Finland
kristiina.karvonen@hiit.fi

ABSTRACT
In this paper, we describe an Anti-Phishing Toolbar for a Web browser that combines what we think of as the best elements in already existing anti-phishing toolbars, together with some usability enhancements. We also report on the initial feedback from our usability tests.

1. INTRODUCTION
Phishing attacks have become a pretty permanent and growing obstacle to safe and swift Internet usage. Despite the growing awareness of how such attacks take place, they stay successful, as both the means how a phishing attack may happen and the number of phishing websites are growing. In December 2007, the APWG [3] identified 25 328 unique phishing websites.

One reason why phishers are winning over anti-phishers may be that the attackers are, in fact, more aware of the basic principles of human behaviour, utilising the very weaknesses of humans that open the possibility for phishing attacks: the limited attention span and the disruptive nature of usage of internet, especially mobile users; motivational aspects ("just get the job done"); weakness for flattery or willingness to help others (social engineering), and so on. Dealing with information overflow can also mean that, as [2] have showed, a major part of users do not look at the security clues given by web browsers, or do not know where to find security information. A phishing attack may also succeed because users seem to make an unconscious decision if a website looks safe or not in just 50 ms [4], probably making users vulnerable for picture-in-picture phishing attacks: trust is already there, before it is ever questioned on a conscious level.

In this paper, we present our initial work on enhancements built on top of existing tools to fight against phishing attacks in order to develop a new anti-phishing toolbar for FireFox 3.

2. EXISTING TOOLS
Passpet [7] asks users to choose a label to the websites asking for passwords and/or personal data. Then, users can later check if the label is written as a proof that it is not a spoofed page. Passpet asks users to remember a single master password and then generates unique passwords based on this master password and the label chosen by the user for each website, so users won't have to remember multiple passwords, which is difficult [1].Thanks to a cookie placed on their machine, a website using SiteKey [5] can display a picture on the login form to ensure users that they are on the good website. Dynamic Security Skin (DSS) [6] proceeds approximately in the same way but unlike SiteKey the feature is based on the client side.

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.

Symposium On Usable Privacy and Security (SOUPS) 2008, July 23-25, 2008, Pittsburgh, PA, USA.

3. THE ANTI-PHISHING TOOLBAR
We try to build a new toolbar which regroups the best ideas of existing tools and seek to improve on their usability by making the information they provide more noticeable and easy to understand. Our Anti-Phishing Toolbar is realised as a toolbar extension for Firefox 3 and included in the web browser. It has seven parts, each one used to describe a security statement related to the web page (fig. 1).

Figure 1: An overview of the Anti-Phishing Toolbar

3.1 The Features of Anti-Phishing Toolbar
We have decided to keep the labels idea used by Passpet. Users can, then, add a label to websites but to improve this concept users can also add a picture and choose the font of the label to make it more difficult to spoof. The label is displayed on section 2 in fig. 1. We are also building a unique password for each website based on the hashing of the label, the master password and the domain name, just as Passpet does. But in order to avoid users to change the label of websites regularly asking for new passwords, we also added the *date* when the label was created to the parameter of the hashing function. This way, if user wants to change his password, he just has to ask the toolbar to generate a new one.

The toolbar also inspects the structure of the web page to find frames that do not belong to the domain name displayed on the address bar, or frames that contain other frames. The results are shown in section 7 of the toolbar. Section 3 indicates if the web page uses SSL-Encryption or not. To give an additional clue to users, we also show them the name of the domain of the website (to detect tricky URL like www.paypal.gotyou.com) and the number of times they already went on that domain (section 6).

Based on these elements, the three first sections of the toolbar are colored to describe the *safety* of the web page From the safest to the least safe, the colors are: green, blue, yellow and orange. Section 1 presents a scale to make the interpretation of the color easier. Fig. 2 explains how the color is chosen, based on what elements are found on the website: **Frame** (suspicious frame element?); **Label** (corresponding label exists?); **HTTPS** (website uses SSL encryption?); **Password** (website asks for a password and/or personal information?); **In history** (user has already been more than 5 times on this web page). So the idea is to make the toolbar do the work for the user in checking for and combining various security information and then showing it to the user in a usable and understandable manner.

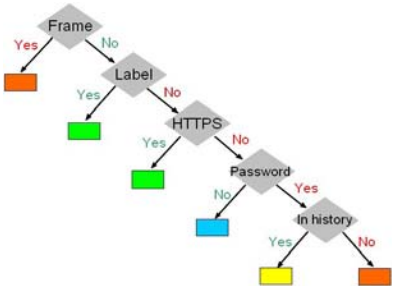

Figure 2: How the toolbar chooses the level of safety

The most common phishing attacks should be stopped by our toolbar. The use of a label to identify the website is a good shield against spoofed website, picture-in-picture attacks and man-in-the-middle attacks. These attacks can also be detected via the display of the number of visits and of the domain name and the icon to prove if a website uses SSL encryption or not. As the password management part works only with labeled websites, it gives another protection since even if users do not look at the toolbar, when they will try to fill the password field it won't be available. In addition, if a phisher succeeds in inserting additional frames on a legal website, our toolbar will detect them and explain to users where these frames come from. In case of DNS attacks or if phishers have inserted javascript code in a web page, we will not be able to detect it.

4. USER STUDY

In order to test if the usability really is there, we are running usability tests with end users. Our test consists of 5 parts. Part 1 is used to obtain demographic data. In part 2 users evaluate seven messages, some more and some less technical, describing the status of a web page. These messages correspond to the information we want the frame inspector to display. In part 3 users evaluate the toolbar based on screenshots.

Figure 3: Toolbar security icons

Each picture represents a different type of website users can be faced with. In this part we try to see how they interpret the different sections of the toolbar and if they can identify each section. In part 4 we ask users to give us their opinion about lock icons (fig. 3), shown one by one. Finally, the last part asks people to give us feedback about the toolbar and the survey.

4.1 Results

Initial test results with users with no expertise in security show that the toolbar might help users pay attention to elements in the website that tend to go unnoticed. For example, after investigating the domain name in the toolbar, user reported that she was not familiar with it (nordea.dk) as it seemed to be Danish, while she was used to the Finnish version of the bank site.

Fig. 4 shows rearrangement of the toolbar sections before and after pilot test, where user had felt the green elements in section, 1-3 to be confusing because of the section 7 showing "suspicious elements". After rearrangement, a user reported that "there too much green, less would be convincing enough" – clearly showing that the green colour and especially the green ok mark are very powerful indicators for end users.

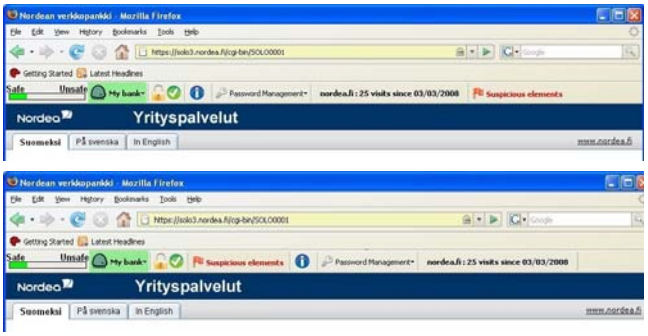

Figure 4: Above the initial toolbar, below rearranged

The same was true of the security icons – the green "ok" mark (Fig. 3, 5th from left) was unanimously voted as "most safe". With most dangerous icon, there was more variation, votes scattered between the 3 right-most icons in Fig. 3.

5. FUTURE WORK

At this point, the toolbar is only a prototype and all the features are not working yet. We are conducting more usability tests to choose the right path to follow concerning the *look and feel* and which security messages to adopt. Once the toolbar is completely functional, we will run new usability tests to ensure that the use of the toolbar is intuitive enough and noticeable enough over longer periods of time and usage. We also want to display clear information about security certificates. By clicking on the information button (section 4, fig.1), users are shown non-technical information they need to know with a clear message to be sure that all points are understandable.

6. REFERENCES

[1] Adams, A. and Sasse, M.A. Users are not the enemy. Communications of the ACM, 42(12):40-46, 1999.

[2] Dhamija, R, Tygar, J. D. and Hearst, M. Why phishing works. In CHI '06: Proceedings of the SIGCHI conference on Human Factors in computing systems, pages 581-590, New York, NY, USA, 2006. ACM Press.

[3] A. P. W. Group. Phishing activity trends. report for the month of December, 2007, December 2007.

[4] Lindgaard, G, Fernandes, G., Dudek, C. and Brown, J. Attention web designers: You have 50 milliseconds to make a good first impression! Behaviour & Information Technology, 25(2):115{126, March 2006.

[5] Bank of America. How bank of america sitekey works for online banking security.

[6] Dhamija, R. and Tygar, J. D. The battle against phishing: Dynamic Security Skins. In Proceedings of the 2005 Symposium on Usable Privacy and Security (Pittsburgh, Pennsylvania, July 06 - 08, 2005). SOUPS '05, vol. 93. ACM, New York, NY, 77-88.

[7] Yee, K. and Sitaker, K. Passpet: convenient password management and phishing protection. In Proceedings of the Second Symposium on Usable Privacy and Security (Pittsburgh, Pennsylvania, July 12 - 14, 2006). SOUPS '06, vol. 149. ACM, New York, NY, 32-43