Poster: Community-Based Security and Privacy Protection During Web Browsing

[Poster Abstract]

Max-Emanuel Maurer
University of Munich
Department of Media Informatics
Amalienstraße 17, 80333 München, Germany
max.maurer@ifi.lmu.de

1. INTRODUCTION

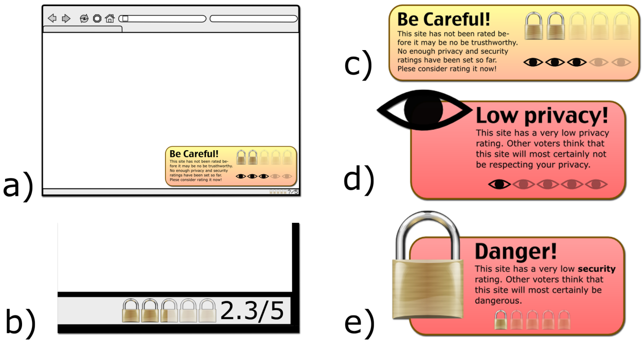
When surfing the web today people want to be secure and their data to remain private. Internet users however do not see the protection of their privacy or security as the primary goal of their activity. They do not care for their online security and privacy actively [3]. Frequently appearing unnecessary warning messages constantly lower the users' trust in those warnings. In this work, we present first ideas of a community based approach known from rating systems in online shopping to provide others with security and privacy relevant information on arbitrary websites. Such a system could then be used to warn users about critical websites and reestablish the users' trust in warning messages.

Using web browsers often leads to errors and warnings that do not denote any immediate danger to the user (e.g. blocking downloads). This leads to users constantly ignoring other warnings that would be really valuable to them [1]. On the other hand, there are cases (especially for phishing attacks) where the user is not alerted at all.

Since the browsers security warnings are not absolutely correct, users quickly get habituated to them. We recommend a new approach by using community opinions as in rating systems to make people more comfortable about the source of the warnings. We do this by creating a browser plugin that will be capable of collecting and displaying security and privacy ratings for different web sites.

Cranor et al. [2] presented in 2006 thoughts on "User Interfaces for Privacy Agents" and came up with a particular user interface that was able to visualize the P3P privacy preferences of a website. They called it "Privacy Bird". A little bird icon at the top of the browser tells the user how well his privacy preferences match the ones provided by the website owner using P3P. A problem with visualizing P3P is that the information which is matched to the users preferences is provided by the website itself. Like that websites can simply fake their privacy appearance.

Another idea to enhance user perception for security risks is security toolbars. Wu et al. [4] provided a good overview over existing toolbars in 2006. They categorized current approaches and compared them during a user study. They found people not noticing the warnings due to the fact that they have another primary goal besides their wish to be secure. Having users participate in classifying good and bad sites may raise the overall awareness for the problem space.



Be Careful!
This site has not been rated before it may be no be trusthworthy. No enough privacy and security ratings have been set so far. Plese consider rating it now!

Low privacy!
This site has a very low privacy rating. Other voters think that this site will most certainly not be respecting your privacy.

Danger!
This site has a very low **security** rating. Other voters think that this site will most certainly be dangerous.

Figure 1: Mockup images of the final plugin. Showing a) the browser screen b) the status-bar indication for a site c) the no-voters-yet-warning c) a critical privacy level and d) a critical security level.

2. PLUGIN CONCEPT

To carry out our idea of providing community ratings, we propose the idea of a browser plugin installed in the user's browser. The plugin is capable of displaying an average privacy and security rating for every site on the status bar of the browser (see figure 1 b). As long as privacy and security values are still within a certain threshold, the user is not interrupted browsing the web. In case she wants to know the current state of the community ratings she can inform herself looking at the status bar. In critical cases, additional dialogs are used to avoid the problem of a user not noticing a change. People with a registered account can add their opinion on the security or privacy of a site at any time. This is needed to prevent multiple votings for one site from different users.

2.1 Problem Cases

In two specific cases the user will be interrupted by a dialog box that needs her to take an action:

In case a site has received ratings below a certain threshold, the website access will be interrupted by an alert dialog (see figure 1 d-e). The user is told that the site is rated as insecure or as a possible privacy problem by other people in the community. Appearing dialogs are formatted in a way that their purpose is immediately clear. The style, position and look-and-feel of this dialog could also be adapted to the severity of the corresponding value.

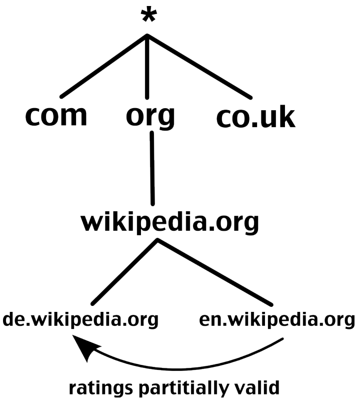


Figure 2: Ratings in one particular branch of a tree might also be partially valid for another branch.

Another special case would be if the user visits a site no one or only a few people have rated before. In this case the site can either be not well-known or perhaps denote a newly created attack. In case of phishing sites the correspondent famous site will usually have a much higher rating count than the phishing site itself which makes it easy to detect those fraudulent sites. In case a user is one of the first for visiting a site she is made aware of that fact and is instructed to first closely examine and then vote for it (see figure 1 c).

All alert boxes appear right next to the usual status indicator but overlay the users main browsing window to gain her attention (see figure 1 a). Assuming a vast spread of the tool, ratings for most of the sites will exist such that the appearing of unnecessary warnings will be reduced to a minimum.

2.2 Adapting Knowledge

The data collected from the plugin for specific web pages could also be used to calculate findings for related webpages without them being rated explicitly. All ratings are related based on their URL in a tree-like fashion. This tree allows to calculate security and privacy data for similar web sites (see figure 2). An example: With the subdomain “en.wikipedia.org” rated very well for security and privacy this could also hold to some extent for other subdomains like “de.wikipedia.org”.

Within the tree it would also be possible to calculate a security and privacy index for top-level domains. This has to be done with extreme care and has to be closely evaluated to not eventually warn about trustful web pages just because its server being in a certain country.

3. EVALUATION IDEAS

For evaluating our plugin we recommend two different evaluation approaches. A first evaluation should be conducted lab-wise whilst a second bigger evaluation should be a long-term field evaluation.

3.1 Lab Evaluation

Evaluating the plugin in a lab study will help to greatly understand how users handle the interface presented to them. It will also be possible to find out whether they are able to distinguish between a security and a privacy rating. Another advantage of a preliminary lab-evaluation will be the possibility to evaluate crucial situations that will not happen everyday during normal usage (e.g. a phishing scenario).

The lab evaluation will reveal general problems of the plugin design and can be used to test all borderline situations. Incorporating the results from the lab study into the plugin should lead to a prototype for a field evaluation.

3.2 Field Evaluation

With a field study the real life performance of the plugin will be measured. In a field study the number of unknown or unrated web sites that are hit by users should decrease quickly to an acceptable level. Another important outcome of this study should be to identify the best thresholds for warning messages to show up. The plugin could be made publicly available to test its performance with many more internet users.

How much and which data to collect in such a study is a major issue to think about whilst especially privacy issues should be taken into account. The long term study will show whether such a community-based approach will be able to reestablish the users’ trust in warning messages and browser ratings.

4. FUTURE WORK

As a first future step, the plugin technology and a supporting backend server technology are currently implemented. The lab-study will then be used to confirm or enhance the plugin architecture and the way it presents itself to the user. This will also give first insights on the possible impact of such a system. After that the plugin will be rolled out to a set of real test users using it during a long term study. The so collected quantitive and qualitative data will provide close insights on using community-aspects and whether crowd intelligence is able to correctly decide on website ratings.

5. CONCLUSIONS

The past years have shown that the concept of rating systems can be used in many cases to reduce fraud in specific domains. With our approach we want to try to apply this idea to the problems of internet security and online privacy.

The main goals we try to reach with such a system is reducing the amount of false positives that is still too high for todays web browsers and reinforce peoples trust in browser warnings by using a community aspect with their appearance.

6. REFERENCES

[1] T. Amer and J. Maris. Signal words and signal icons in application control and information technology. Technical report, Tech. Rep. Working Paper Series–06-05, Northern Arizona University, Flagstaff, AZ, 2006.

[2] L. F. Cranor, P. Guduru, and M. Arjula. User interfaces for privacy agents. *ACM Trans. Comput.-Hum. Interact.*, 13(2), 2006.

[3] R. Dhamija and J. D. Tygar. The battle against phishing: Dynamic security skins. In *Proc. of SOUPS*, New York, 2005. ACM.

[4] M. Wu, R. C. Miller, and S. L. Garfinkel. Do security toolbars actually prevent phishing attacks? In *Proc. of SIGCHI*, Montréal, Québec, Canada, 2006. ACM.