Poster: Password Entering and Transmission Security

Gamze Canova
Technische Universität
Darmstadt
gamze.canova@cased.de

Melanie Volkamer
Technische Universität
Darmstadt
volkamer@cased.de

Simon Weiler
Technische Universität
Darmstadt
simon.weiler@stud.tu-darmstadt.de

ABSTRACT

The most popular form of user authentication on websites is the use of passwords. When entering a password, it is crucial that the website uses HTTPS (for the entire content). However, this is often not the case. We propose *PassSec* - a Firefox Add-On to support users to detect password fields on which their password might be endangered. In addition, *PassSec* displays a non-blocking warning next to the password field, once users click into the password field. The user is provided with possible consequences of entering a password, recommendations and further information if wanted.

Categories and Subject Descriptors

H.5.2 [**Information Interfaces and Presentation**]: User interfaces—*user-centered design*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms

Security, Human Factors

Keywords

Usable security, user support, password security, security interventions

1. INTRODUCTION

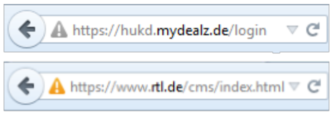
The most popular form of user authentication on websites is the use of passwords. This is mainly due to its convenience and simplicity. Protecting a user's password is crucial, especially because many users tend to reuse the same password for different services [5]. That is, once a password is, e.g. eavesdropped, this password could be reused by the eavesdropper for other services of the victim.

Ideally, a password should be entered only if the server is authentic and the website with the password field is using HTTPS, while all elements of this website are exchanged via HTTPS, and the transmission of the password to the server happens via HTTPS as well. Only in this case the owner of the password can effectively protect the password from falling into the wrong hands. However, there are many exceptions also from well known websites: (1) On some websites neither the main page is encrypted nor the password is transmitted to the server encrypted, i.e. via HTTPS, (e.g. `http://edition.cnn.com/`). In these cases, the password can be easily eavesdropped on the network. (2) Some websites do not use HTTPS for the main page with the password field, but only transmit the entered password via HTTPS to the receiving server (e.g. `http://www.gmx.net/`). One reason for this approach is that it is inefficient to use HTTPS for sending advertisement. Even if the password is transmitted to the server encrypted, the website with the password field is still vulnerable to manipulations and thus the entered password is at risk. On several websites the user can enforce to use HTTPS for the main page as well as for the transmission (e.g. `http://www.gmx.net/`). (3) Yet, there are some websites which do not encrypt all resources (e.g. `https://hukd.mydealz.de/login` or `https://www.rtl.de/cms/mein-rtl.html`). These resources are referred to as "mixed content"[1]. There are two types of mixed content: mixed passive and mixed active content. Mixed passive content cannot modify the Document Object Model (DOM) of a website. Thus, mixed passive content allows an attacker to see or replace, e.g. an image, served over HTTP with another image. The user's password itself is not endangered. Therefore, mixed passive content is treated as secure in our context. The Firefox browser warns from mixed passive content by means of a grey warning triangle (cf. Figure 1). Mixed active content, on the other hand, can modify the DOM of an HTTPS website. Thus, an attacker could potentially steal a user's sensitive data, e.g. his/her password, even if the password is transmitted to the server encrypted. As Firefox version 23 and higher by default blocks mixed active content we do not consider this case for *PassSec* and assume that our users use Firefox 23 and higher. The Firefox browser warns from mixed active content by means of an orange warning triangle (cf. Figure 1).

Users have to take quite some effort to find out whether the ideal case is in place or not: i.e. check for a padlock or whether the URL starts with https://. In addition, case (1) and (2) cannot be distinguished unless the user checks the source code of the website. As security is not a user's

CCS'14, November 3–7, 2014, Scottsdale, Arizona, USA.
ACM 978-1-4503-2957-6/14/11.
http://dx.doi.org/10.1145/2660267.2662387.

[1] https://blog.mozilla.org/tanvi/, Accessed: 14th August, 2014



https://hukd.mydealz.de/login

https://www.rtl.de/cms/index.html

Figure 1: Mixed passive content (top) and mixed active content (bottom) in Firefox browser

primary task [6] and many people might not be aware of these cases, it is likely that they enter passwords on such websites without being aware of any risk.

Our goal is to support users by means of a Firefox Add-On – *PassSec* – which checks, in case a password field is present, whether the above described suboptimal conditions (1) and (2) apply (condition (3) is already covered by Firefox 23 and higher) and changes the background color of the password field to red and adds a yellow warning triangle to it (cf. Figure 2). In [2] it has already been evaluated that the combination of a red background and a yellow warning triangle is well perceived as security warning. In case the ideal condition applies, *PassSec* indicates this as well: the password field gets a green border and a check mark icon (cf. Figure 2).

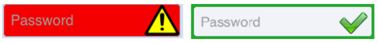


Figure 2: Dangerous (l) and secure (r) case

PassSec has further functionalities: It always checks whether the website is accessible via HTTPS. Furthermore, if a user focuses the password field, by e.g. clicking on it, *PassSec* displays a dialog next to the password field. This dialog includes the possible consequence of entering a password on this website, states a recommendation, such as using the provided option of always opening this website via HTTPS (if applicable), and the option for further information about the consequences or providing more details. Note, if the user does not focus the password field on this website, this dialog does not show up at all. This way, we ensure not to unnecessarily disturb the user.

The goal of this poster is to present the dialogs for different scenarios and discuss their contents.

2. CONTENT OF DIALOGS

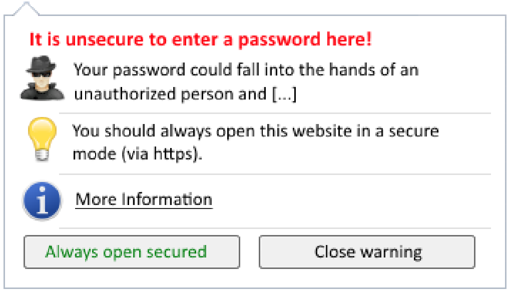
This section deals with the content of the scenario specific warning dialogs. We distinguish different scenarios, e.g. we distinguish entering a password to log into a website, setting a password when registering on a website, or changing a password. All these scenarios can happen in situations described in (1)-(3) or with the ideal situation (main page uses HTTPS and password transmission is via HTTPS as well). We do not distinguish situations (1) and (2) for the warnings, as both endanger the user's password. Additionally, in these scenarios the ideal situation could be available, i.e. a switch to HTTPS. In this case the user is provided with this option.

All dialogs first display a short version (cf. Figure 3) and every section of the dialog can be clicked on in order to unfold the specific parts (cf. Figure 4). Each dialog consist of four parts: headline with the problem statement, consequence(s), recommendation, and further information. The headline is always the same. All dialogs provide two options (while due to the passive characteristic of the dialog, none of them needs to be selected in order to continue and enter the password): "Close warning" and another one depending on the situation. In case HTTPS is available *PassSec* provides the option to switch to the HTTPS website and always open the respective website via HTTPS: "Always open secured". In case HTTPS is not available *PassSec* provides the option to trust the respective website, i.e. add an exception so that the warning will not appear anymore: "Trust this website". Recommendable options are highlighted in green and those that are not recommended in red.

We make use of wordings that are easy to understand, as abstract as possible, and not technical as recommended in [1], i.e. we do not use terms like encryption. The consequence part of the dialog is supported with the icon of a spy. The recommendation part is supported with a light bulb, which is standing for idea. Finally, the more information part is supported with the well-known "i".

In the following we summarize the contents of the different warning dialogs:

HTTPS available: Figure 3 and Figure 4 show the short resp. long dialog of this scenario (either the website does not use HTTPS and the password is transmitted via HTTPS or no HTTPS is made use of at all). Here, the user is first told that his/her password could fall into an unauthorized person's hands. The password could be used to access the user's personal data. As opening the website with HTTPS is possible in this scenario, the user is recommended to always open this website in a secure mode (via HTTPS). We provide this option with the aid of an "Always open secured" button. By highlighting this option in green we want to encourage the user to click on this button. By clicking on "More Information" the user can obtain more information on the topic of secure password entering and transmission. The button "Close warning" only closes the warning. The next time a user focuses the password field the warning will reappear.



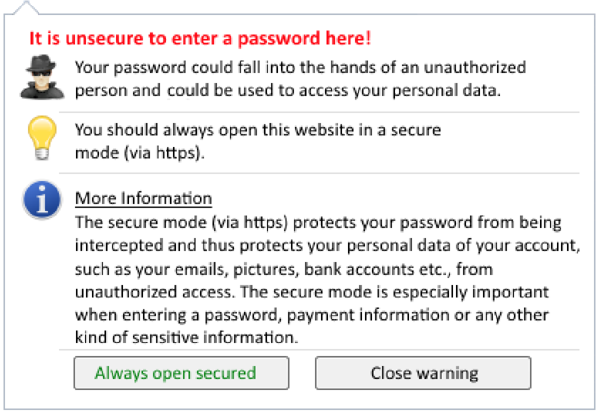
It is unsecure to enter a password here!

Your password could fall into the hands of an unauthorized person and [...]

You should always open this website in a secure mode (via https).

Figure 3: Short warning: HTTPS is available

HTTPS not available: Figure 5 shows the dialog of this scenario (either the website does not use HTTPS and the password is transmitted via HTTPS or no HTTPS is made use of at all). Here, the user is first told that his/her password could fall into an unauthorized person's hands. The password could be used to access the user's personal data. As opening the website with HTTPS is *not* available in this scenario, the user is encouraged to use at least different passwords for different websites in case he/she wants to enter a password. By clicking on "Trust this website" the user can always trust this website, which will result in not showing



It is unsecure to enter a password here!

Your password could fall into the hands of an unauthorized person and could be used to access your personal data.

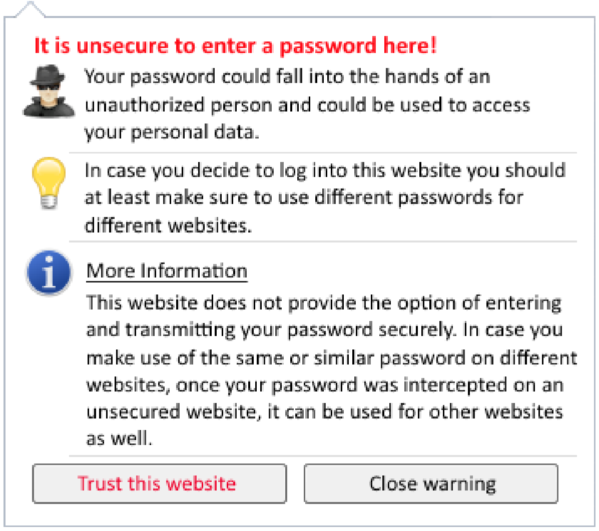
You should always open this website in a secure mode (via https).

More Information

The secure mode (via https) protects your password from being intercepted and thus protects your personal data of your account, such as your emails, pictures, bank accounts etc., from unauthorized access. The secure mode is especially important when entering a password, payment information or any other kind of sensitive information.

Figure 4: Long warning: HTTPS is available

this warning again, including the red background of the password field. As we do not encourage to do so, this option is highlighted in red. By clicking on "More Information" the user can obtain more information on the topic of reusing passwords on different websites.



It is unsecure to enter a password here!

Your password could fall into the hands of an unauthorized person and could be used to access your personal data.

In case you decide to log into this website you should at least make sure to use different passwords for different websites.

More Information

This website does not provide the option of entering and transmitting your password securely. In case you make use of the same or similar password on different websites, once your password was intercepted on an unsecured website, it can be used for other websites as well.

Figure 5: Long warning: HTTPS is not available

3. RELATED WORK

We report about the most related one: the approach proposed by Maurer et al. [3, 4].

The goal of Maurer et al. is to increase the users' security awareness when entering critical information, such as passwords or online banking credentials. Thus, every time a user is about to enter critical information, e.g. focusing a password field, a corresponding non-blocking dialog appears next to the corresponding field. The user is informed about what kind of information he/she is about to submit. Furthermore, the domain of the visited website is displayed and whether the sensitive information is transmitted encrypted or not. Users can decide whether to add this website to a whitelist or not. On white-listed websites the dialog will not be shown again. A side effect is the detection of phishing attempts: as soon as the user gets this warning, even if the website was white-listed before, the user should get suspicious and not enter any data.

Our focus is on password security while not only considering password entering but also password setting and changing scenarios. In addition, we distinguish different cases of HTTPS being in place as well as being possible, i.e. in particular we provide the option to always use HTTPS if possible; and we explain the risk and provide recommendations how to securely proceed.

4. CONCLUSION AND FUTURE WORK

We proposed an Add-On – *PassSec* – which is supposed to support users to assess how well their password is protected on a specific website. For different scenarios *PassSec* provides possible consequences, corresponding recommendations (e.g. using different passwords) and further information if wanted and needed. Using the Add-On has also potential to increase users' security awareness on entering sensitive data securely. As future work we plan to conduct a field study in order to analyze the user interactions w.r.t. whether the users follow our recommendations, e.g. opening a website with HTTPS or changing passwords on insecure ones.

Acknowledgements

This work is supported by funds of the Federal Ministry of Food, Agriculture and Consumer Protection (BMELV) based on a decision of the Parliament of the Federal Republic of Germany via the Federal Office for Agriculture and Food (BLE) under the innovation support programme

We thank Steffen Bartsch, Hubert Strauß, and Gildas Nya Tchabe for their support on developing *PassSec*.

5. REFERENCES

[1] C. Bravo-Lillo, L. Cranor, J. Downs, and S. Komanduri. Bridging the gap in computer security warnings: A mental model approach. *Security Privacy, IEEE*, 9(2):18–26, March 2011.

[2] N. Kolb, S. Bartsch, M. Volkamer, and J. Vogt. Capturing attention for warnings about insecure password fields–systematic development of a passive security intervention. In *Human Aspects of Information Security, Privacy, and Trust*, pages 172–182. Springer, 2014.

[3] M.-E. Maurer, A. De Luca, and H. Hussmann. Data type based security alert dialogs. In *CHI'11 Extended Abstracts on Human Factors in Computing Systems*, pages 2359–2364. ACM, 2011.

[4] M.-E. Maurer, A. De Luca, and S. Kempe. Using data type based security alert dialogs to raise online security awareness. In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, page 2. ACM, 2011.

[5] H.-M. Sun, Y.-H. Chen, and Y.-H. Lin. opass: A user authentication protocol resistant to password stealing and password reuse attacks. *Information Forensics and Security, IEEE Transactions on*, 7(2):651–663, 2012.

[6] R. West. The psychology of security. *Communications of the ACM*, 51(4):34–40, 2008.