Poster: Security Design Patterns With Good Usability

[Poster Abstract]

Hans-Joachim Hof
Muse - Munich IT Security Research Group
Munich University of Applied Sciences
Lothstrasse 64
80335 Munich, Germany
hof@hm.edu

Gudrun Socher
Department for Computer Science and
Mathematics
Munich University of Applied Sciences
Lothstrasse 64
80335 Munich, Germany
gudrun.socher@hm.edu

ABSTRACT

This poster presents work-in-progress in the field of usable security. The usability of security mechanisms is crucial to avoid unintended misuse of security mechanisms which lowers the security level of a system. It is the goal of the work presented in this poster to identify security design patterns with good usability. Requirements for security design patterns with good usability stem from existing usable security design guidelines. A collection of security usability failures is presented as well as examples of how misuse anti-patterns can be derived from these failures. Misuse cases will be used in future work to identify security design patterns with good usability.

Keywords

Usability, Security Design Patterns, Design Patterns, Usable Security;

1. INTRODUCTION

Previous works in the field of usable security have focused on the compilation of a design guide for usable security mechanisms [2, 3]. While these guidelines are of great help during the high-level design process of a product, there is still the need for more technical help for software developers during the fine-grain design and implementation processes.

Design patterns are a well-known approach for reusable solutions of common problems within a given context. They come in the form of a description or a template on how to solve a class of problems. They are an established way to formalize best practices in software design.

Security design patterns are reusable solutions to the problem of controlling a set of specific threats through some security mechanism, defined in a given context. Refer to [1, 4] for an overview of security design patterns. Usability design patterns as collected in [5] are great for effective interaction design. The goal of the work presented in this poster is to extend security design patterns in the usability dimension to patterns for usable security.

To identify security design patterns with good usability, a collection of security usability failures is used as well as the usable security design guidelines described above. Examples of misuse anti-patterns are identified for some of the usability failures. Based on these misuse anti-patterns, future work will identify security design patterns with good usability.

2. REQUIREMENTS FOR DESIGN PATTERNS FROM SECURITY DESIGN GUIDELINES

Previous work includes security design guidelines [2, 3]. These guidelines are general advises on how to design systems. The guidelines are:

- Understandability for all users,
- Empowered users,
- No jumping through hoops,
- Efficient use of user attention and memorization capabilities,
- Only informed decisions,
- Security as default,
- Fearless System,
- Security guidance, educating reaction on user errors, and
- Consistency.

These guidelines are used as requirements for the design patterns to be identified.

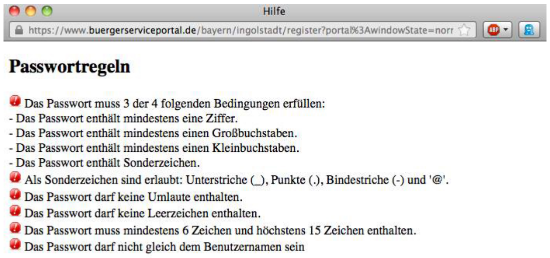
3. EXAMPLE SECURITY USABILITY FAILURES

The poster shows a collection of security failures that are used to identify misuse cases and that will be the input to the design of the security design patterns with good usability in future work.

Categories of the security failures presented in the poster include:

WiSec'16 July 18-22, 2016, Darmstadt, Germany

ACM ISBN 978-1-4503-4270-4/16/07.
DOI: http://dx.doi.org/10.1145/2939918.2942423



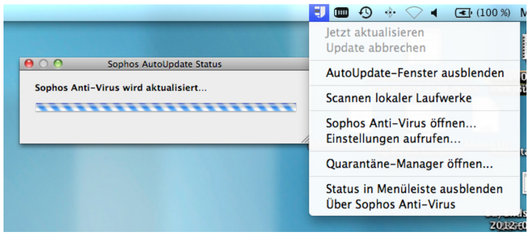
Hilfe

https://www.buergerserviceportal.de/bayern/ingolstadt/register?portal%3AwindowState=norr

Passwortregeln

- Das Passwort muss 3 der 4 folgenden Bedingungen erfüllen:
- Das Passwort enthält mindestens eine Ziffer.
- Das Passwort enthält mindestens einen Großbuchstaben.
- Das Passwort enthält mindestens einen Kleinbuchstaben.
- Das Passwort enthält Sonderzeichen.
- Als Sonderzeichen sind erlaubt: Unterstriche (_), Punkte (.), Bindestriche (-) und '@'.
- Das Passwort darf keine Umlaute enthalten.
- Das Passwort darf keine Leerzeichen enthalten.
- Das Passwort muss mindestens 6 Zeichen und höchstens 15 Zeichen enthalten.
- Das Passwort darf nicht gleich dem Benutzernamen sein

Figure 1: Password policy of the citizen portal of the city of Ingolstadt, Germany: unnecessarily complicated password rules, which are hard to understand, frustrate users rather than motivating them to choose strong passwords.

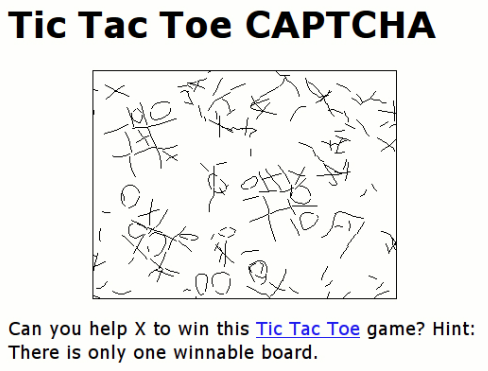


Sophos AutoUpdate Status

Sophos Anti-Virus wird aktualisiert...

(100 %)
Jetzt aktualisieren
Update abbrechen
AutoUpdate-Fenster ausblenden
Scannen lokaler Laufwerke
Sophos Anti-Virus öffnen...
Einstellungen aufrufen...
Quarantäne-Manager öffnen...
Status in Menüleiste ausblenden
Über Sophos Anti-Virus

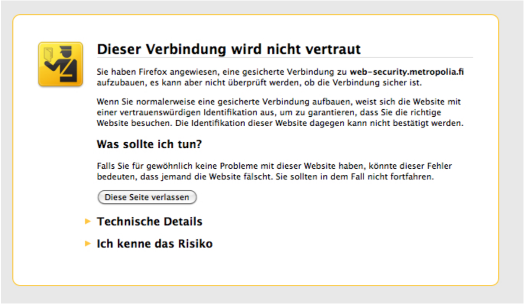
Figure 2: Forced update of virus scanner: no possibility to stop or postpone the update (see greyed out option in the drop-down menu).



Tic Tac Toe CAPTCHA

Can you help X to win this Tic Tac Toe game? Hint: There is only one winnable board.

Figure 3: Complicated Captcha: Complicated Security measures annoy users.



Dieser Verbindung wird nicht vertraut

Sie haben Firefox angewiesen, eine gesicherte Verbindung zu **web-security.metropolia.fi** aufzubauen, es kann aber nicht überprüft werden, ob die Verbindung sicher ist.

Wenn Sie normalerweise eine gesicherte Verbindung aufbauen, weist sich die Website mit einer vertrauenswürdigen Identifikation aus, um zu garantieren, dass Sie die richtige Website besuchen. Die Identifikation dieser Website dagegen kann nicht bestätigt werden.

Was sollte ich tun?

Falls Sie für gewöhnlich keine Probleme mit dieser Website haben, könnte dieser Fehler bedeuten, dass jemand die Website fälscht. Sie sollten in dem Fall nicht fortfahren.

Figure 4: Example of an unacceptable security choice: The explaination is too long. Given choices are difficult to understand. The given choice voids the security of the certificate system.

- Authentication usability failures: Password-based authentication often comes with bad usability. Figure 1 shows an example. In the example, a complicated password policy is enforced on the user without helping the user to use a strong password.
- Strict security enforcement usability failure: Figure 2 shows an example of a forced update that cannot be stopped or postponed by a user (greyed out option).
- Anti-Bot usability failure: Several services use so-called captchas (Completely Automated Public Turing test to tell Computers and Humans Apart) to hinder automated scripts (bots) to use this service. However, automated captcha solving algorithms get better and better, so captchas get more and more complicated, resulting in captchas like the one in Figure 3 that are extremely annoying for human users.
- Security decisions with unacceptable choices usability failure: Figure 4 shows an error message of the Firefox browser when it encounters a certificate of an unknown certificate authority (e.g. a self-signed certificate). As a user cannot verify such a certificate, a safe option would be to block the site. However in this case, many sites would be inaccessible. Firefox allows to add an exception to the security check, hence voids the security of the certificate system.

More categories are shown on the poster. The poster shows examples of misuse anti-patterns for these categories of security usability failures. For example, one of the misuse anti-patterns is called ”Enforcing a complicated password policy for password-based authentication”.

4. CONCLUSION

The poster shows several requirements for usable security mechanisms. A collection of examples for security usability failures are shown. The poster shows examples of how misuse anti-patterns can be derived from the security usability failures. These misuse cases will be used to identify security design patterns with good usability in future work.

5. REFERENCES

[1] E. Fernandez-Buglioni. *Security Patterns in Practice: Designing Secure Architectures Using Software Patterns*. John Wiley and Sons, 2013.

[2] H.-J. Hof. User-centric it security – how to design usable security mechanisms. In *The Fifth International Conference on Advances in Human-oriented and Personalized Mechanisms, Technologies, and Services (CENTRIC 2012)*, pages 7–12. IARIA, November 2012.

[3] H.-J. Hof. Towards enhanced usability of it security mechanisms – how to design usable it security mechanisms using the example of email encryption. *International Journal On Advances in Security*, 6(1&2):78–87, 2013.

[4] C. Steel, R. Nagappan, and R. Lai. *Core Security Patterns*. Prentice Hall, 2012.

[5] J. Tidwell. *Designing Interaces*. O’Reilly Media, Inc., 2nd edition, 2010.