Michaela Kauer, Florian Kiesel, Felix Ueberschaer, Melanie Volkamer, Ralph Bruder:

The Influence of trustworthiness of website layout on security perception of websites

Published in:
Jähnke, von zur Mühlen, Rechert, von Suchodoletz:
Current Issues in IT Security 2012, Duncker & Humblot, 2012,
p. 215-220.
ISBN 978-3-86113-115-1
ISSN 1862-7625

MICHAELA KAUER, FLORIAN KIESEL, FELIX UEBERSCHAER,
MELANIE VOLKAMER AND RALPH BRUDER*

The Influence of Trustworthiness of Website Layout on Security Perception of Websites

A number of studies have been done, which were concerned with the question: What makes a website trustworthy? In many cases, the design of a website played a major role for the trustworthiness perception of this site. On the other hand, a number of studies had been conducted to identify the impact of security indicators on trust of websites. In reality, you will find a combination of both trustworthiness and security indicators on a website. Until now, little research has been done to test the interference of trust and security indicators. Within this work the results of an online study on the interference between trust and security indicators will be presented. Overall, it can be said that each of the investigated security indicators can be influenced by the "look and feel" of a website, but that the extent of that influence depends on the kind of website. Additionally, it seems that trust indicators are more important for the overall judgment of a website, whereas security indicators seem to be more important for the decision whether to enter personal data on a website or not.

I. Introduction

The use of internet technology has spread widely through Western societies and the importance of the Internet is increasing worldwide, especially in China, India and Africa the rapid growth of new users continues (ITU World Communication, 2010). The technology is employed in various areas of the daily life of every man and woman. Internet use continues to grow, and the opportunities for criminals to defraud users match this development. The search for specific information can lead an user off the mainstream – big websites such as eBay or Google, which are easily found and identified – to smaller websites which may contain potential dangers. When encountering a website, the user has to make a decision. Does he trust the website or not? At this point, different factors come into play that influence his decision. He might rely on security indicators, which all current browsers have implemented, and therefore making an objective choice. Or he could judge a website by its content and layout, which would mark a subjective decision.

A number of studies have been done, which were concerned with the question: What makes a website trustworthy? In many cases, the design of a site played a major role for the trustworthiness perception (e.g. Walther et al. (2004)). All indicators which relate to design and the "look and feel" of a website (Fogg et al., 2001) will be referred to as trust indicators within this paper. On the other hand, a number of studies had been conducted to identify the

[*] Technical University of Darmstadt, Germany

impact of security indicators on the trust of websites (see Egelman (2009) for an overview). In reality, you will find a combination of both, trust and security indicators on a website. The examination of the interference of security and trust indicators and their impact on the perceived trustworthiness of websites will be in the focus of this paper.

The paper is organized as follows: The next section gives a short introduction into the state-of-the art for trust and security in web settings. Afterwards, the method of the pre-test and the main study will be presented. The paper proceeds with the result section and is concluded by the discussion.

II. Related Work

A. Trust

For a couple of years trust has been a major field of research in different types of science like psychology, social science or education. Every science has its own point of view, so there is no comprehensive definition. One important view is the importance of trust as a "complexity redactor" (Luhmann, 1968) which enables a decrease in complexity for all foreseeable futures. Since a few years the attention on "online trust" increases steadily. Online trust can be considered as „an attitude of confident expectation in an online situation of risk that one's vulnerabilities will not be exploited" (Corritore et al., 2002).

Confidence building of websites was considered in studies before. For example in 2001 Fogg et al. evaluated 51 different website elements. The analysis of the collected data showed which elements boost and which elements hurt perceptions of web credibility. Referring to Fogg et al. (2001) website elements can be classified into four different categories: domain name, design, text and interactivity. Because Fogg et al. (2001) gave a good overview over websites and their elements we stick to their classification and manipulate the websites in the pre-tests according to those four classes.

B. Security

One of the most prominent attacks in the internet is phishing. Phishing involves processes, where the criminal tries to gain access to login-data of his victims by using fake websites and emails. A further development of phishing is pharming which forwards the user to a fake website even if he enters the URL of a website manually into the address bar. Therefore, precise communication whether a website is secure or not is extremely vital. Current browser versions implement a variety of security indicators, both active (an action by the user is required to continue) and passive. There have been studies to determine the optimal design for these indicators, focusing on color, giving easily understandable recommendations, and placement. Separation of warning and content by interrupting the user's current task seem to work specifically well (Egelman, 2009). But what if security mechanisms fail and warning and website content are displayed alongside each other? What if there is no active warning but only contextual indicators? Content may influence the security perception of the website, because users may not recognize e.g. a warning indicator when trusting the site because of its „look and feel“ (Fogg et al., 2001). Overall, 5 passive security indicators were considered within this paper. This included the lock symbol combined with the "https"-prefix of an SSL-encrypted connection, because they are seen as the "best known and most successful security mechanism on the internet" (Gajek et al., 2005, p. 5). A more advanced concept is called "Extended Validation"-certificate. More rigorous background checks are conducted when someone applies for such a certificate. Unlike a normal certificate, EV-certificates include the legal information about the owner of a website (Egelman, 2009). Depending on what kind of certificate a website offers, differently colored security indicators are shown by the browser. The Internet Explorer 9 as well as the Mozilla Firefox color the address bar or the Site Identification Button green in case there is an EV-certificate. In contrast, if a visited website has been reported as a phishing-site, the address bar and the Site Identification Button are displayed in red in order to warn the user. The last two security indicators that are considered are a small blue stop-symbol to the address bar that is shown in the Internet Explorer 9 when ActiveX-content is blocked, and the notification bar, which is added when mixed content is integrated on a website and only the secure content is shown.

C. Method

Pre-test and main study were both conducted in fall 2011. The pre-test identified the most influential design aspects on trust. Therefore, different websites were manipulated in the four classes (domain name, design, text, and interactivity). The study included 8 different websites: the most common websites for online-banking in Germany (Sparkasse and Volksbank), for online-shopping (eBay and amazon), online communities (Facebook and Google+) and additionally, two company sites (Coca Cola and Audi). Each website was manipulated four times. Each participant was asked to judge 8 screenshots of the websites: each of the included websites once, but only one manipulated version of each site. Participants were asked to judge the websites according to their trust on a seven point Likert-scale from 1 (not trustworthy at all) to 7 (very trustworthy).

The main online-survey was conducted to determine how different websites were perceived security-wise and how this perception interferes with the trust perception. Again, participants were asked to rate their trust on each page on a seven point Likert-scale from 1 (not trustworthy at all) to seven (very trustful). Each site had to be rated on a seven point Likert-scale from 1 (not secure at all) to 7 (very secure) and participants were asked whether they would enter their personal data on this website or not. The websites from the pre-test were used and additionally security indicators (lock symbol, colored address bar, Site Identity Button, stop symbol and notification bar) were integrated into the screenshots. Both online studies used screenshots from the Mozilla Firefox 7 and the Internet Explorer 9.

Overall, 117 participants attended the pre-test. The participants' average age was 23.6 years $(SD = 5.7)$. 74% of the participants were male. 99% see themselves at least at an average level of Internet experience. 23% see themselves as experts. The main study was attended by 132 participants with an average age of 26.5 years $(SD = 8.7)$. 70.5% of the participants were male. 98.5% see themselves at least at an average level of internet experience. 20% see themselves as experts.

D. Results

In the pre-test, for all websites using the official company name in the domain name increased trust and requesting unnecessary personal data decreased trust. But all other manipulations had inconsistent effects. Therefore, for this paper the results will be restricted to the two manipulations and the effects of security indicators.

The influence of the security indicators was investigated by integrating / removing them from the original website. It was shown, that the lock-symbol and the https-prefix did influence security ratings only on online-baking sites, whereas on other websites they go unnoticed. In contrast, the coloring of the address bar seems to be an appropriate way to inform users, because both colors (green and red) were always associated with an increase / decrease in security ratings independent of the type of website. Notification bar and stop-symbol did not have any effect and are therefore left out of the further analysis.

When pairing security indicators with different content manipulations, it becomes clear that each indicator shows inconsistency when it comes to conserving the security perception. In other words: all indicators can be biased by content. The ratio of cases with successful conservation to unsuccessful conservation of security rating is especially bad for the lock symbol and the "https"-prefix. Still, for the decision whether to enter personal data on a web page or not, security indicators were more important than trust indicators. This indicates that for an overall rating the "look and feel" (Fogg et al., 2001) of a website is important, but participants seem to be able to partially ignore this perception if they are guided into the direction of security.

E. Discussion

Overall, people are not able to separate their trust rating from their security rating of a website. Even those security indicators that are often noticed by users (lock-symbol and https-prefix) are not able to conserve a security rating when the context of a website is manipulated. For example, spelling errors or the integration of social plugins on the website of Sparkasse led to a decrease in security, even if no objective drop in security was induced. A perceived decrease in trust is especially critical for companies, because they might lose customers. In contrast, the objectively false perceived increase in security (as occurred for the Audi homepage when adding a animated banner) is mostly critical for customers, because they potentially trust websites that are not secure.

Because not all malicious websites can be automatically detected, further studies should concentrate on developing and testing passive security indicators that are as well noticed by the users as able to conserve a "right" security perception of websites.

References

CORRITORE, C. L. AND KRACHER, B. AND WIEDERNBECK, S. (2002), 'On-linetrust : Concepts, evolving themes, a model', *International Journal Human-Computer Studies* 58, pp. 737 – 758.

EGELMAN, S. (2009), 'Trust Me : Design Patterns for Constructing Trustworthy Trust Indicators', http://www.dtic.mil/cgibin/etTRDoc?AD=ADA502272&Location=U2&doc=GetTRDoc.pdf [10.10.2011].

FOGG, B. J. AND MARSHALL, J. AND LARAKI, O. AND OSIPOVICH, A. AND VARMA, C. AND FANG, N. AND PAUL, J. AND RANGNEKAR, A. AND SHON, J. AND SWANI, P. AND TREINEN, M. (2001), What makes Web sites credible?: a report on a large quantitative study, *in* 'Proceedings of the SIGCHI conference on Human factors in computing systems', CHI '01, ACM, New York, NY, USA, pp. 61 – 68.

GAJEK, S. AND SCHWENK, J. AND WEGENER, C. (2005), 'SSL-VA-Authentifizierung als Schutz vor Phishing und Pharming', http://www.ruhr-uni-bochum.de/nds/gajek/papers/GaScWe2005%20SSL-VA.pdf [28.10.2011].

ITU WORLD COMMUNICATION (2010), 'ICT Indicators database', Fixed wired broadbands subscriptions per 100 habitants, 2000-2010. http://www.itu.int/ITU-D/ict/statistics/ [21.10.2011].

LUHMANN, N. (1968), *Vertrauen: Ein Mechanismus der Reduktion sozialer Komplexität*, Stuttgart: Enke.

WALTHER, J. AND WANG, Z. AND LOH, T. (2004), ‘The Effect of Top-Level Domainsand Advertisements on Health Web Site Credibility’, *Journal of Medical InternetResearch* 6(3).