On the Design of a "moody" Keyboard

Alexander De Luca, Bernhard Frauendienst, Max Maurer, Doris Hausen
Media Informatics Group, University of Munich,
Amalienstr. 17, 80333 Munich, Germany
{alexander.de.luca, max.maurer, doris.hausen}@ifi.lmu.de, frauendi@cip.ifi.lmu.de

ABSTRACT
To counter the increasing number of online threats for users' privacy and security, this paper explores the design of an ambient security indicator, in form of a standard keyboard illuminated in different colors, and equipped with additional buttons and vibration functionality. We present the results of a focus group study, which notably influenced the design, and discuss a prototypical implementation called MoodyBoard.

ACM Classification Keywords
H5.2 [Information Interfaces and Presentation (e.g. HCI)] User Interfaces – Input devices and strategies, evaluation.

Keywords
Privacy, security, awareness, ambient information, MoodyBoard.

INTRODUCTION
Using the web, users are exposed to manifold privacy and security threats. Phishing, viruses and man-in-the-middle attacks are only some of them. Even though modern browsers like Internet Explorer, Firefox or Chrome implement several security mechanisms they often do not succeed in supporting the users. Thus, insecure user behavior can raise significant privacy and security problems [1, 3].

One of the most common reasons for such behavior is users having wrong mental models of security applications. It is not surprising that when asked about their strategies for using security dialogs, users often answer that they would just press "OK" whenever an application shows security warnings [5]. Another reason for the ineffectiveness of current browser warnings is habituation effects [2]. That is, users are so often confronted with (unimportant) warnings that they get used to ignoring them.

Warnings are either interrupting the user's current workflow or displayed unobtrusive (e.g. SSL certificate visualizations). However, inside the browser's chrome only blocking warnings seem to have a measurable effect on security [7]. This is mostly due to the fact that users simply do not become aware of them since they usually only occupy a limited area of the screen's real estate (mainly due to usability reasons).

In this work, we explore how other areas of the users' surroundings can be used to provide them with privacy and security relevant information. The most important alarms – e.g. fire alarm or loudspeaker announcements – are still detached from the user's screen. With the means of ambient visualization, our main idea is to utilize a piece of hardware that is available already at each computer and is part of the users interaction routine anyway – a keyboard. As a matter of fact, these devices are always in the periphery of the user's field of view and at the same time offer plenty of free, unused space for providing ambient information. We are using the keyboard as an unobtrusive, ambient display to provide privacy and security related information. The primary means of transporting information to the user is based on the keyboard being able to glow in any color. Based on the metaphor that the keyboard can become angry (e.g. red) if users behave insecurely, we coined the prototype "MoodyBoard".

The main contribution of this note is to provide insights on whether and how hardware based security and privacy awareness mechanisms can support users in handling threats of every day Internet use. The results of a focus group were used to explore different design choices for a prototype, which will be discussed in this work.

FOCUS GROUP
We conducted a focus group to gain insights about people's knowledge and ideas concerning privacy threats related to Internet use. With this, we wanted to get to know how users handle them and how they use privacy and security features offered by their browsers. In a second step we emphasized our proposed system – the MoodyBoard – and questioned the participants on how they would use it, how they would design it, what they would do differently and where else they would use it.

Design and Conduction
Usually, focus groups should consist of six to twelve participants and should not be too heterogeneous. We recruited eight participants (plus two backup participants) for this study. All of them were in their twenties and had good background knowledge of the Internet. Also, all of the participants were frequent Internet users, having

DIS 2010, August 16–20, 2010, Aarhus, Denmark.

Figure 1: a) Security warning (e.g. a Phishing website). b) "Submission insecure" warning (e.g. having input a credit card number). c) Help button, which can be used to get further information on the current warnings.

advanced knowledge of Internet services. To ensure this, we recruited students from respective lectures on multimedia and the Internet. Even though it was taken care of that all users had good knowledge of the Internet, they were not chosen based on their experiences with threats, privacy and security.

The following questions were provided to the participants in a consecutive order to stimulate discussions:

1. When using the Internet, which threats for your privacy and personal data do you encounter?
2. What security measures does your browser provide to protect you from these threats? (And how do they influence your behavior)

Between questions two and three, the users got an introduction on the basic concept of MoodyBoard: using a keyboard as an ambient output device for security and privacy relevant information. In this version, a color-only version of MoodyBoard was presented to the participants. Additionally, they were shown some mockup images of how such a keyboard could look like.

3. Having been given an instruction about MoodyBoard, which information could be presented by MoodyBoard? Which use cases can you imagine?
4. Do you believe that MoodyBoard can influence your behavior when encountering previously discussed threats?
5. Can you imagine any other ways to present information with MoodyBoard?
6. Can you think of any other application areas for this technology, especially use cases beyond Internet security in the browser? Would you suggest transferring this concept to other platforms e.g. mobile phones?

Besides the eight participants, four other persons were present at the study: one moderator, two minute writers and one camera operator. Food and drinks were provided to the participants to make them feel more comfortable during the discussion.

Overall, the focus group session took 73 minutes, not including the introduction by the session chair.

Results

The results of the focus group are based on the video material recorded during the session and notes taken by two independent minute writers. The results support several of our initial assumptions and helped greatly to gain more insights and refine and adapt the designs for MoodyBoard.

Security and privacy awareness and understanding

Being frequent Internet users with strong technical background, it was not surprising that the participants had a somewhat good understanding of possible threats on the Internet. However, they lacked background knowledge of those threats and sometimes mixed up different terms. If these people already have problems correctly naming and explaining those threats, it seems rather unlikely that non-tech-savvy people have a chance of understanding them.

Most reported threats were Phishing, viruses and man-in-the-middle attacks. Surprisingly, the participants further named social networks and search engines like Google as a serious threat to the user's privacy since they *"collect and store any private information that they can get"*. Some participants even felt more frightened about this than about single attacks.

In this context, the participants were aware of several browser mechanisms to protect the user. These included blocking of Phising and malware websites, certificate confirmation dialogues and the possibility to delete cookies and the like when shutting down the browser.

Interestingly, one participant mentioned that he would only use websites that look trustworthy and are designed well. This is a common mental model when asking users about their perception of safety and trust on the web and can be a common pitfall for falling for frauds [4]. Many participants mentioned that they would just always click the dialogues away as they will pop up too often and do simply get annoying. This supports the existence of the "OK" effect as reported earlier [5].

During the discussion, it further turned out that the participants agreed that for understanding most (or all) of these security mechanisms, advanced technical knowledge is required.

Using MoodyBoard

Questions three and four were meant to stimulate the participants to discuss about possible use, advantages and disadvantages of the concept.

Unsurprisingly, the participants agreed that standard browser warnings should be somehow reused with MoodyBoard, including Phishing and certificate warnings. However, based on their experience, they worried that habituation effects might occur as well [2]. Furthermore, participants stated that browser warnings should not be replaced by the tool but enhanced with it. MoodyBoard was considered a *"very useful peripheral display, which does not interrupt the user during her current task"*.

In addition to these threats that we already considered in our initial concept, participants proposed to visualize common mistakes that might lead to insecure behavior like mistyping of common URLs (e.g. "googel.com" instead of "google.com").

Finally, the participants stated that in order to be able to trust the device, threat information should only be provided if a threat (or a secure situation) is detected with absolute certainty. In any other case, MoodyBoard should behave "neutral".

Enhancing MoodyBoard

Mainly question five and partially question four were used to make the participants discuss about possible ways to enhance MoodyBoard with further functionality.

Besides using colors to transport information, the participants were very creative in finding additional channels. While all of them agreed that they would not want to be distracted by sounds, they very much liked the idea of having vibration functionality. That is, the keyboard (which the users touch anyways during interaction) could easily provide haptic feedback as an additional information channel. They also proposed to combine vibration and colors for very urgent warnings. Another interesting idea that was discussed was the possibility to mechanically block or light single keys to transmit finer-grained messages. For instance, by making the Enter-key shine in red, the following information could be identified by the user: *"if you submit/confirm this, then there will be a security problem"*. Surprisingly, a lot of participants proposed special keys with additional functionality (e.g. to support standard security features of firewalls).

In addition to the proposed output and input capabilities, three other major enhancements were mentioned. The first one being an intelligent keyboard that learns from the user (e.g. recognizes sites that the user likes and does not warn about them anymore). Exploiting the physical detachment of the keyboard and the computer was mentioned several times. As an example, participants proposed to keep information at the keyboard and check it before sending it (and thus keeping it safe from potential threats on the computer like viruses etc.). Finally, it was proposed that the colors should be modifiable by the user since she might have different preferences and the meaning of colors often depends on the cultural background of a user (e.g. in China, the color red is considered a lucky color). Such color schemes could simply depend on the keyboard layout set in the OS.

Transferring the design

The final question was meant to provoke thoughts about further use of the concept and the possibility of transferring it to other platforms or devices.

Participants mainly mentioned that there are other possible devices that could be used. For instance, they mentioned that the screen border could show ambient light, which could eventually be more eye-catching. Other functionalities like vibration would not work in this solution. The user's mouse could again be used with vibration, color and the like.

Limitations

Focus groups are not meant to get a representative overview of a population. They are designed and conducted to get insights on a focused topic, product, design or prototype.

We used the focus group to get a chance to discuss possible use cases, scenarios and designs with potential early adopters of such a technology and therefore cannot and do not claim that the results have a representative value. However, they helped greatly to clarify many aspects of the concept and to refine the design of MoodyBoard.

FINAL DESIGNS

The initial design of MoodyBoard only provided for the whole keyboard to be lit in a single color. No additional buttons or signaling mechanisms where considered (see figure 1a).

Based on the results from the focus group, several additional concepts and enhancements have been considered. Some users argued that additional output channels like vibration or sound would increase the attentiveness of the device, which could be used to finer graduate threat levels. However, they highly argued against using sound. Thus, a vibration motor was incorporated in the design to test how users will react to this feedback channel in the context of security and privacy awareness mechanisms.

Using a keyboard, others suggested additional buttons for special purposes would fit in adequately. Consequently, based on the need to provide information on the security and privacy issues to the users, a "Help" button has been designed, depicted in figure 1c, which when pressed displays additional information about the currently active notification. This way, a user can quickly get information on why a respective warning is shown.

Mainly in the context of usability improvements, the ability to separately light single buttons was proposed by some

participants. In this manner, messages and warnings can be attached more directly to, for instance, the submission of a form (see figure 1b). That is, MoodyBoard will be able to display messages with enhanced meaning. A simple example is the possibility to light the Enter-key. This way, the user does not only get information on *"there is something wrong"* but also hints on *"what could be the problem"*.

IMPLEMENTATION

Based on the initial concept and results from the focus group, different additional concepts were derived. The hardware foundation for the prototype (see figure 1) is a stock illuminated keyboard, namely a "Revoltec Lightboard XL2". It features translucent keys in a standard key layout lit by an electroluminescent (EL) foil. This piece of hardware seems to be most appropriate for creating a prototype similar to an end product for our prospective subjects. The EL foil has been replaced by a number of RGB LED stripes, allowing for higher light output and a vast amount of usable colors. Vibration functionality is implemented using a small motor with an unbalanced mass attached, well-known from alerts in mobile phones.

Finally, we are using the keyboard's light button as the "Help" button mentioned above.

The actuators and sensors are controlled by an Arduino (http://www.arduino.cc/) prototyping board, which also allows for easy communication with the computer via a USB connection.

For the prototype, the software side will is implemented in form of an extension for the Mozilla Firefox browser. A simple text based protocol is used to communicate with the Arduino over its virtual serial connection, sending values for color and vibration to the keyboard, and notifications that the help button was pressed from the keyboard to the computer. For future use an extra piece of software should control the keyboards mood and receive moods from arbitrary browsers or software similar to the often-used Growl (http://growl.info/) notifications on Apple computers.

DISCUSSION AND FUTURE WORK

Based on the insights of our focus group, different MoodyBoard functionalities were identified. Those will be evaluated firstly in small laboratory studies to figure out the advantages and problems of the different concepts. This is needed to make sure that all doubts are resolved and the suggestions of the attendants of the focus group can be fully integrated in our prototype. One thing that certainly needs to be tested thoroughly is the brightness of the keyboard. Some focus group attendants doubt they would notice the change in color or light of the keyboard when only looking at the screen. The result of this evaluation will identify which functionalities will be adapted in the final prototype.

Future studies will also have to explore the many different variables that have been mentioned during the focus group. How fine-grained shall the keyboard illumination be? Is the user able to notice color changes of only some keys and which information could be transported by such means?

Another important point is that illumination is not the only possibility to modify such a keyboard. Other senses could be stimulated additionally or instead.

Ideally, the resulting MoodyBoard will be set up in several typical households. Evaluation of ambient devices – like the proposed MoodyBoard – is not easy [6]. Performing such an evaluation in an artificial lab setting would lead to the user focusing on the device in a way not comparable to real life usage. With a long term study conducted in the user's own household or at her usual desk at work, the device is expected to become part of the user's daily life without playing a special role and gaining an unnatural amount of attention.

The positioning of the peripheral notification was also an important issue discussed in our focus group. Instead of the keyboard the user's screen border or her mouse could be equipped with lighting. The effect of using those devices should also be tested in future studies.

REFERENCES

1. Adams, A. and Sasse, M. A. 1999. Users are not the enemy. Commun. ACM 42, 12 (Dec. 1999).
2. Amer, T.S., Maris, J.B. Signal words and signal icons in application control and information technology exception messages – hazard matching and habituation effects. Technical Report Working Paper. Series 06-05, Northern Arizona University, Flagstaff, AZ, October 2006.
3. Egelman, S., Cranor, L. F., and Hong, J. 2008. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In Proceedings of CHI 2008, Florence, Italy, April 05 - 10.
4. Fogg, B. J., Marshall, J., Laraki, O., Osipovich, A., Varma, C., Fang, N., Paul, J., Rangnekar, A., Shon, J., Swani, P., and Treinen, M. 2001. What makes Web sites credible?: a report on a large quantitative study. In Proceedings of CHI 2001, Seattle, Washington, United States.
5. Lampson, B. 2009. Privacy and security. Usable security: how to get it. Commun. ACM 52, 11 (Nov. 2009), 25-27.
6. Mankoff, J., Dey, A. K., Hsieh, G., Kientz, J., Lederer, S., and Ames, M. Heuristic evaluation of ambient displays. In Proceedings of CHI 2003, Ft. Lauderdale, Florida, USA, April 05 - 10.
7. Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., Cranor, L.F. Crying Wolf: An empirical study of SSL warning effectiveness. In Proceedings of the 18th USENIX Security Symposium.