Bringing Effective Security Warnings to Mobile Browsing

Max-Emanuel Maurer
Ludwig-Maximilians Universität
Media Informatics Group
Amalienstr. 17, 80333 Munich, Germany
max.maurer@ifi.lmu.de

ABSTRACT

With the newest generation of smartphones, internet usage on mobile devices finally hits the masses. Till now, security and privacy awareness of mobile internet usage has drawn few attention in research and industry. However, with its raise the number of users that employ those devices for security sensitive tasks like internet banking raises as well. Therefore, security and privacy mechanisms for mobile devices should be considered in future work. Most of the systems that have already been invented are optimized for desktop computers and cannot (or only hardly) be adopted to mobile devices. Another problem is limited screen space.

In this work, a symbiotic approach to security and privacy awareness on mobile devices is motivated and discussed. Mobile devices have several output channels. Those can be used and combined to deliver security relevant messages to users. Colors, vibration, sound and combinations of them might help to raise awareness. Metaphors based on hardware output might even enable to overcome weaknesses of current software based mechanisms like habituation problems.

1. SECURITY AWARENESS ON MOBILE DEVICES

Internet security and its awareness is an often discussed topic these days [3] [5]. The diversity and the potential of current web browser applications has highly increased in the last years. With this, the way of how security of such web pages is rated and the way it is presented to the users has changed as well. New security icons, location bar colorization and the visualization of Extended Validation SSL certificates have been introduced. Although studies so far show that even this is not enough [3], no efforts of any kind have been put into *mobile* browsing experience. Instead of at least using the insights that have been gained so far, browser manufacturers for mobile phones start off with old-fashioned UI elements (e.g. the padlock symbol).

With much research done on effectiveness of such warnings on standard browsers, efforts should be spent to protect users of mobile phones as well. Since more and more users use their mobile devices to browse the internet and read their emails, they are getting vulnerable when using this alternative way of browsing. Adopting the security concepts of today's browsers is not the only way to raise security awareness on mobile devices. Due to the different hardware of those small devices, other concepts of raising security awareness become possible incorporating other actuators.

To communicate security issues to the user is per se not an easy task. One problem with this is that the key concepts behind security and encryption are already complicated. Whitten and Tygar [5] showed in 1999 that the concepts of PGP for example are extremely hard to understand for the average user even when using a simple interface. Another related problem is that security is nearly never the users' primary goal [6]. In general, the user wants to achieve a certain task, without having any security trouble but also without being bothered with security decisions. In 2006, Wu et al. [6] evaluated the concepts of five different security toolbars summarizing them in three different test toolbars. They found out that none of them really helped to protect the users. Although those toolbars warned the users about phishing websites, they refused to believe them due to the professional look of the phishing site. Egelman et al. [3] tested phishing warnings of current browsers and compared active warnings to passive indicators. Active warnings – interrupting the users' current task – were found to be much more effective than passive indicators. With the new types of SSL certificates, the "Extended Validation SSL certificates" introduced the end of 2006, certificates became more reliable but again even harder to understand. Biddle et al. [2] evaluated a new concept to present certificate contents without using technical wording. They evaluated their new dialog against the standard IE dialog for different SSL certificate types.

Many of those findings are incorporated in today's desktop web browsers but when looking at mobile devices none of them has been obeyed so far. With an increasing number of people using their mobile device for security related tasks – e.g. checking email, ordering online or doing bank transactions – mobile security awareness gets just as important as it is on desktop computer nowadays. Different hardware characteristics of mobile devices should make it possible to raise the user's attention for security even more. Those hardware characteristics could make notifications and alerts more prominent than they normally would be on the small screen of a standard mobile device. Extra status indicators besides the display could be used to indicate security problems. This could be vibration alert or the keypad light for example. These are only a few of the existing hardware differences between standard computers and mobile devices that could be used. Using existing approaches in combination with the additional hardware features of a mobile device could lead to a greatly improved security awareness of users. Another approach could make use of some additional lightning hardware integrated in the body of the users mo-

Second International Workshop on Security and Privacy in Spontaneous Interaction and Mobile Phone Use (IWSSI/SPMU)
May 17, 2010, Helsinki, Finland

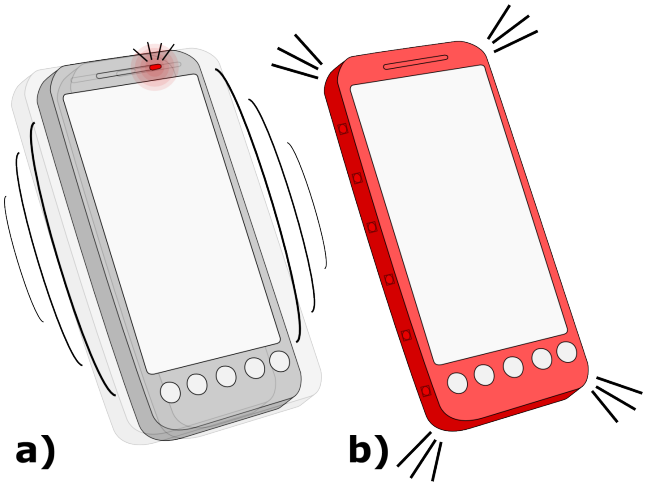

Figure 1: a) Using vibration or the status LED of the phone to indicate privacy threats. b) LEDs placed inside the phone's body can put the device into different 'moods'.

bile device to make it possible to express different 'security moods' of the device. Seifert et al. [4] already showed that using hardware features of mobile devices instead of desktop like functionality can be much more convenient for specific tasks.

2. HARDWARE INDICATORS

Indicating security or privacy threats using the hardware features of a mobile device is technically already possible with today's devices. Modern phone SDKs – like the iPhone SDK – provide methods to develop applications accessing hardware sensors and actuators. Using the Android-SDK, the notification LED is accessible to make it flash in an arbitrary color. Like this, it is possible to make the user aware of threats using multimodal feedback (e.g. visual and tactile as shown in figure 1a).

An important issue when thinking about the development of such indication mechanisms is to consider a model what one could call different 'threat levels'. Defining those threat levels makes is easier to define a set of actions that should occur when reaching it – e.g. flashing the LED, vibrating the device or displaying a dialog window. A high threat level should only be triggered in very rare cases. In case a user's phone vibrates and flashes each time she sends data unencrypted to a search engine, a real threat will be likely to go unnoticed [1]. In how far those levels should be transparent to the user has to tested.

Different threat levels could be indicated by colors. The color of a threat level could then be shown not only on a dialog on the device's screen but also using the status LED of the device or by using integrated color changing LEDs inside the body of the device. Like this the whole phone could be put into a specific 'mood'. This 'mood' could then be used to visually transport different threat levels. Figure 1b shows how a critical threat level could look like on an LED enhanced phone. An approach like this would make it important to evaluate what people think of glowing devices.

3. SYMBIOTIC APPROACH

As said in the introduction: recent work on the topic of privacy and security awareness makes it mandatory to change the way security issues are presented on mobile devices nowadays. The big question when implementing such mechanisms is whether to rely on the findings that have been done for desktop computers so far or to try out new ways that are eventually more suitable for mobile devices?

Possibly the best solution would be to use a combined approach. Since the displays of today's phones are a lot smaller than what we are used from the PC, mobile browsers try to completely abandon things like toolbars or indicators during the browsing process in order to save precious screen space. In case of a security issue that is worth being reported, the user should definitely be informed on the display using dialogs that orient themselves on what is current state-of-art in normal web browsers. Using the rest of the device's hardware for additional details could make those dialogs more effective.

4. OUTLOOK

A first step when building such a system will be to make some tests with a mobile device and to modify a running browser to be capable of alerting the user with new indicators, dialogs and additionally with hardware. This would enable new kinds of notifications – like the 'mood' mentioned above. Those new kinds of notifications would also have to be adjusted to current mobile phone notifications – e.g. incoming text message. The different 'threat levels' that can occur while browsing mobile websites need to be defined and mapped to notifications in case of a threat occurring.

All steps should be closely evaluated and compared to the current mobile device browsing experience and additionally to the ongoing research on desktop computers.

5. REFERENCES

[1] T. Amer and J. Maris. Signal words and signal icons in application control and information technology exception messages–hazard matching and habituation effects. *Journal of Information Systems*, 21(2).

[2] R. Biddle, P. C. van Oorschot, A. S. Patrick, J. Sobey, and T. Whalen. Browser interfaces and extended validation SSL certificates: An empirical study. In *Proc. Cloud Computing Workshop*, Shanghai, China, 2009.

[3] S. Egelman, L. F. Cranor, and J. Hong. You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In *Proc. CHI 2008*, Florence, Italy, 2008.

[4] J. Seifert, A. De Luca, B. Conradi, and H. Hussmann. Treasurephone: Context-sensitive user data protection on mobile phones. In *Proc. Pervasive 2010. Helsinki, Finland*, 2010.

[5] A. Whitten and J. D. Tygar. Why johnny can't encrypt: A usability evaluation of PGP 5.0. In *Proc. USENIX Security Symposium 1999*, 1999.

[6] M. Wu, R. C. Miller, and S. L. Garfinkel. Do security toolbars actually prevent phishing attacks? In *Proc. CHI 2006*, Montreal, Quebec, Canada, 2006.