Principles for designing Out-Of-Band channels in Human-Interactive Security Protocols

Ronald Kainda

Oxford University Computing Laboratory
Wolfson Building, Parks Road, Oxford, OX1 3QD, UK

1 Introduction

Human-Interactive Security Protocols (HISPs) require users to carry out security critical tasks with high degrees of accuracy. Users, however, are usually faced with competing tasks and security is not their primary goal. As a result users are unmotivated to do security tasks with required attention and accuracy. To minimise the possibility of security failures without requiring undue effort from users, Out-Of-Band (OOB) channels must be designed based on a number of principles. Currently proposed methods have inherent weaknesses including forcing designers to choose between security and usability, being limited to specific application contexts, and failing to ensure that users carry out security critical tasks with required attention [1]. This work proposes principles for designing secure and usable OOB channels that, despite being faced with competing tasks, users are able to carry out security critical tasks with required attention and accuracy.

2 Principles for designing OOB channels

Principle of commitment This principle can simply be stated as 'a user is committed to a particular value/action without knowing what the outcome of such a value or action will be'. The outcome of a users' value/action is only revealed after s/he is committed to it. This principle ensures that users do not get their desired outcome when it is not supposed to be the case. The *principle of commitment* requires that a user is provided only with partial information that allows him/her to commit to a final outcome. For example, *manual copying and entering* [2] reveals partial information to a user that he/she uses to make a commitment by entering it into other devices. The user at this stage does not know whether this information will be accepted by other devices but it is up to these devices to determine whether received information is correct or not. By doing so, a user cannot force a device to accept a value that does not match its own digest.

Principle of unpredictability Users tend to learn and master how a system can be used with least effort. Over time users end up achieving their primary goals without consciously engaging with the subtasks involved. This phenomena is known as *habituation* or *user conditioning*. Habituation occurs in activities that have non changing task sequences and following a specific course of actions results in the same outcome every time. Habituation is bad for security because we want users to carry out security tasks consciously and accurately. The principle of *unpredictability* simply states that 'a user should not be able to predict the sequence of actions that lead to a particular outcome'. This principle differs from the principle of commitment in that it focusses on making a sequence of actions unpredictable while the latter makes it difficult for a user to determine an outcome based on a particular action. For example, in web browser Secure Socket Layer (SSL) certificate warnings, users know that they have to take one of the two actions (principle of unpredictability violated), either accepting or rejecting a certificate and they also know that accepting results in continuing to the intended website (principle of commitment violated).

Principle of single interaction path One secure design principle is to ensure that the path of least resistance is the most secure [3]. For example, Firefox 3.x web browser's implementation of allowing users to add exceptions of invalid, expired, or untrusted SSL certificates requires a user to single-click a rejection of the certificate and at least 4 clicks to accept the same certificate. The problem, however, is that in most instances users' desire to achieve their primary goals outweighs the effort required to accept a certificate. In HISPs, path of least resistance may mean an insecure route —for example, accepting a digest without comparing. Moreover, multiple paths to a single goal is likely to cause users difficulty in understanding an OOB method. The *principle of single interaction path* demands an implementation that provides a single path from start to end of a device association process.

Principle of design by context Systems must be designed to work within the context of operation. This is crucial because different environments pose different challenges on a system. Context may be classified as social, technological, and environmental. This principle refers to designing OOB channels within the context of an application in which they may operate. This requires thinking about specific user interactions, within a specific application context, that may hinder or help usability and security of OOB channels. Understanding the context in which an OOB method will operate is crucial to meeting human and contextual needs. There is a general consensus among researchers that device association process must be 'fast' to complete. However, fast usually means a user must spend as less time as she considers appropriate. This definition of fast neither provides useful information nor does it define the term itself. It may, however, be reasonable to think that a user is likely to measure the appropriateness of time spent on the association process in relation to the time spent on the primary task.

3 Summary and conclusion

The above principles were demonstrated by two proposed OOB channels. The channels were subjected to a usability experiment and results compared to studies of other methods. The comparison showed that the proposed methods are better in terms of effectiveness, efficiency, and user satisfaction. In addition proposed methods are applicable to a wide range of contexts without compromising security (See [1] for details on the methods and study). In summary, HISPs require users to carry out security critical tasks in order to establish secure device association. While device association is not usually a primary task for users, security critical tasks must be carried out correctly. Given users' lack of motivation and the demands of competing tasks, OOB channels must be designed such that users do not compromise the desired security.

References

1. R. Kainda, I. Flechais, and A. Roscoe. *Information Security Theory and Practice. Security and Privacy of Pervasive Systems and Smart Devices*, volume 6033 of *WISTP 2010, Lecture Notes in Computer Sciences*, chapter Secure and Usable Out-Of-Band Channels for Ad hoc Mobile Device Interactions, pages 308–315. Springer, April 2010.
2. R. Kainda, I. Flechais, and A. Roscoe. Two Heads are Better Than One: Security and Usability of Device Associations in Group Scenarios. In *SOUPS '10: Proceedings of the 6th symposium on Usable privacy and security*, 2010.
3. K.-P. Yee. User Interaction Design for Secure Systems. In *ICICS '02: Proceedings of the 4th International Conference on Information and Communications Security*, pages 278–290, London, UK, 2002. Springer-Verlag.