Security Levels for Web Authentication

Abstract for SWITS 2011

Anna Vapen, anna.vapen@liu.se, PhD student at Linköping University

Supervisor: Nahid Shahmehri

Web users today have several accounts and identities on the Internet, which they use for a variety of purposes in everyday life, such as entertainment, banking and commerce. A new, increasingly growing application for the web is the variety of social networks and blogs which allows users to contribute with their own web contents. Users can also share and comment on existing contents. This interaction and personalization of the web requires the user to authenticate to prove their identity. Web sites, as the examples mentioned above, which require authentication often contain personal or confidential information that can be stolen by an attacker. The attacker can also use the account to act as the user online, possibly causing financial loss or damaging the user's reputation.

Authentication methods offer varying levels of security. Methods with one-time credentials generated by dedicated hardware tokens can reach a high level of security, whereas password-based authentication methods have a low level of security since passwords can be eavesdropped by an attacker while sent over a network, captured by keyloggers in the user's computer or guessed in an online guessing attack. It is also a likely that users which usually have many passwords to remember will write the passwords down or reuse them at several sites, which increase the risk of identity theft. Despite the security problems, password-based methods are dominant in web authentication since they are both easy to implement and easy to use. Dedicated hardware, on the other hand, is not always available to the user, usually requires additional equipment and may be more complex to use than password-based authentication.

Different services and applications on the web have different requirements for the security of authentication. Therefore, it is necessary for designers of authentication solutions to address this need for a range of security levels. Another concern is mobile users authenticating from untrusted computers and wireless networks. This in turn raises issues of availability, since users need secure authentication to be available, regardless of where they authenticate or which computer they use.

We propose a method for evaluation and design of web authentication solutions that takes into account a number of often overlooked design factors, i.e. availability, usability and economic aspects. Our proposed method uses the concept of security levels from the Electronic Authentication Guideline (EAG), provided by NIST. EAG defines four levels of security in authentication, 1 to 4 among which 4 is the level providing the highest security. In our proposed method we suggest adding two intermediate levels to make the security levels more fine-grained.

We focus on the use of handheld devices, especially mobile phones, as a flexible, multi-purpose (i.e. non-dedicated) hardware device for web authentication. Mobile phones offer unique advantages for secure authentication, as they are small, flexible and portable, and provide multiple transfer channels which can be used for sending authentication data. Phone designs, however, vary and the choice of channels and authentication methods will influence the security level of authentication. It is not trivial to maintain a consistent overview of the strengths and weaknesses of the available alternatives. Our evaluation and design method provides this overview and can help developers and users to compare and choose authentication solutions. Another goal of this work is to be able to provide flexible authentication solutions in which the user can choose the preferred security level depending on the current application and location.