Graphical Password To Avoid Shoulder Surfing

Abstract and background

For a long period of time textual passwords were the most common type of access authentication. People often choose either short password or password that is easy to remember e.g. dates or information that is related to their personal information which also means easy to be broken by attackers. For instance, shoulder surfing attacker needs a less time to get these types of passwords. You may think that shoulder surfing is not that kind of serious attacks. But unfortunately it is common these days. Also it doesn't require a lot of technology to do. All you need is a camera or you can simply use your phone camera. And because of that we needed a new scheme to avoid shoulder surfing. It is called graphical password. In this research I will talk more about this scheme and show how it reduces the risk of shoulder surfing attack.

How it works

Second category is called recognition-based graphical password schemes there are many examples of these schemes. One of them is pass face. In pass face user asked to select a previously memorized face from a total of three screens with 9 images in each of them. Another scheme is deja vu by dhamija and perrig in 2000.the idea is to show an interface pane with total of 25 random is patterns. the user should choose his or her 5 predetermined images. after that weidenceck et al proposed a new scheme which is called convex hull click chc the key goal of it was to withstand the shoulder surfing attack. Users can find n icons in the scheme interface. In order to authenticate access users should click on icons that is inside the imaginary convex hull formed by pass objects which are pre-defined icons.

To show the relationship between types of images and the usability of recognition-based graphical password schemes Hlywa, Biddle and Patrick perform an experiment. They designed a scheme that is similar to pass face but with the ability to use different kinds of images. At the end they find that the type of images can really affect the usability of the scheme.

The third category is Cued-recall based graphical password schemes. Important example is PassMap by Yampolskiy in 2007. This scheme include map in which user can connect or disconnect paths on that map. Another example was proposed by Weideneck et al. it allows users to choose 5 points on a single image no matter what kind of images are being used. In 2007, Chaisson proposed Cued Click points (CCP)scheme which is similar to pass point with the ability to use multiple images per password. Also it has a higher level of security.

Security problems

Although, many Graphical password schemes was proposed to increase the security level but some of them is still vulnerable to Shoulder surfing attack.

Solutions and recommendations

Many researchers proposed graphical password schemes over time but a lot of them had the same problems which is shoulder surfing or the possibility of guessing them. To get rid of this serious problem, new techniques developed. One of them is the Conundrum-pass. The key goal of this technique is to reduce the risk of shoulder surfing and password guessing besides preserving the ease-of-use property. The idea of this technique based on dividing the image into multiple parts. In order to successfully authentication process, predetermined parts supposed to be selected by users. This technique can notably improve the security of the graphical password system. Also it has the ability of efficiently resist shoulder surfing.