Poster: The MVP web-based framework for user studies in authentication

Sonia Chiasson, Chris Deschamps, Max Hlywa,
Gerry Chan, Elizabeth Stobert, Robert Biddle
Carleton University, Ottawa, Canada
chiasson@scs.carleton.ca, robert_biddle@carleton.ca,
{cdescham, mhlywa, gchan, estobert}@connect.carleton.ca

1. INTRODUCTION

Despite the ubiquity of password systems, knowledge-based authentication remains an important and active research area. Many current systems have low security, and even then users often devise insecure coping strategies in order to compensate for memorability and usability problems. Alternative authentication systems, including various graphical password schemes, have received considerable attention in response. We have conducted a systematic review of the literature on graphical passwords [2], and found no consistency in the usability and security evaluation of different schemes. The situation is similar for text passwords, rendering fair comparison between schemes nearly impossible.

In our earlier authentication research, we have used both controlled lab studies and more extensive field studies. Lab studies can reduce the number of confounding variables and show whether more extensive studies are justifiable. However, the tasks of creating and logging in are typically in the foreground, whereas in real-life these are secondary tasks that receive little attention. Issues surrounding memorability and memory interference are also difficult to evaluate in a lab setting. Our lab studies used a typical approach involving a simple structure with repeated tasks. Field studies present more complex challenges.

In this paper, we present MVP (Multiple Versatile Passwords), a new framework for conducting user studies of authentication schemes thst can easily be deployed in both lab and field environments. It addresses ecological validity issues by using real websites with real content, making authentication a secondary task. MVP differs from systems such as OpenID [1] or single sign-on; its goal is specifically to serve as an instrumented platform for testing and comparing multiple authentication schemes.

2. MVP SYSTEM FEATURES

Figure 1 presents MVP's design. MVP supports:

Web-based usage: To integrate with participants' regular computer activities, the system must be easy to install and access. It should also function on several platforms to accommodate a wide variety of users. MVP is web-based and functions with most popular browser and operating system configurations, therefore allowing participants to complete assigned tasks from any web-enabled computer. The only modifications necessary are to server-side software, and these are minor. No modifications whatsoever are needed on users' computers.

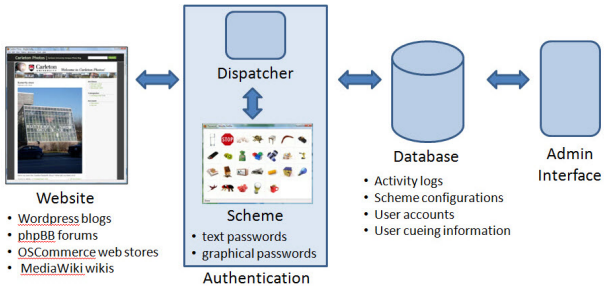

Figure 1: Diagram of the MVP framework.

Easy addition of new schemes: Instead of directly asking the user for a password, each website invokes the MVP dispatcher that opens a new window with the appropriate authentication scheme. The system is designed so that new schemes can readily be added to the system. It also allows for easy parameterization of schemes so that they can be tested at different levels of security. User accounts are initially defined by the system administrator, who selects the authentication scheme and the desired parameters.

By default, a simple plain-text password system is used. However, modules for other schemes can easily be written and added to the framework. So far, we have implemented a number of the main graphical password schemes identified in our survey [2], including Draw-A-Secret, Passfaces, PassPoints, and several variants of these schemes.

Each module works by taking the userid from the website and returning an encoded authentication string from the particular authentication scheme. The websites themselves remain responsible for authentication, using the encoded string as they would use an entered text password.

Ecological validity: MVP allows for lab studies, but is especially designed to be deployed and accessed by users in their regular environments over longer periods of time. The system allows authentication to become a secondary task, by supporting primary tasks on real websites that require users to log in as part of the process. Several popular open-source systems have been modified to use our MVP authentication system: Wordpress blogs, phpBB forums, OSCommerce on-

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
Symposium on Usable Privacy and Security(SOUPS) 2010, July 14–16, 2009, Redmond, WA, USA
.

Figure 2: The login interface for a phpBB forum using PassPoints as an authentication scheme.

line stores, and the MediaWiki platform. Figure 2 provides a screenshot of the login interface for a phpBB forum using PassPoints as an authentication scheme. In lab and field studies, websites based on these systems are fully populated with real content to engage users realistically.

Instrumentation for analysis: To provide a thorough evaluation of an authentication scheme, both its usability and security must be considered. Since user behaviour can significantly impact security, it is necessary to collect and analyze data representing user choices and behaviour for susceptibility to security threats. MVP is fully instrumented to record all user interactions with the system, including keyboard and mouse entries, timestamps, and details of the user's computing environment. Data is stored in a mySQL database. MVP therefore allows for testing different authentication schemes under identical conditions while recording the same performance measures.

Password reset without admin intervention: Forgotten passwords are to be expected in authentication studies, especially in studies that span a long period of time or that require users to remember passwords for multiple accounts. To minimize disruption to users and encourage completion of assigned tasks in a timely manner, MVP users can quickly reset forgotten passwords themselves, without intervention from a system administrator. Details about password resets are recorded by the system to allow later analysis of this user behaviour. In MVP, password resets are triggered by clicking on the "forgot password" link on the given website. A temporary single-use text password is emailed to the user's registered email address. The user can then use this password to access the reset area of the website and create a new password using the assigned authentication scheme.

Training for new authentication schemes: Regardless of whether participants are introduced to a new authentication scheme in the lab or whether the entire study is completed remotely, researchers may choose to train participants to learn how to use the authentication scheme before it is used to protect their user accounts. MVP provides an interface for users to practice using new schemes and receive immediate feedback about whether they are entering passwords correctly.

3. INITIAL USER STUDIES

We have conducted two studies using MVP. Both studies used the same websites and followed a similar procedure.

Participants initially took part in a one-hour laboratory session where they received training on how to use the websites and authentication schemes, and created accounts on three different websites. The accounts were for a Wordpress photo blog about a local university campus, a Wordpress blog offering advice to first year university students, and a phpBB forum intended to identify the best locations on campus for various activities (e.g., the best place to buy coffee). In each case, participants' main task was to comment on a specific blog post or forum thread, tasks which required them to log in. In the week following the lab session, participants received email asking them to complete further tasks. Two tasks were assigned on each of Day 1, Day 3, and Day 6. These tasks were similar to those completed in the lab and could be completed from any web-enabled computer.

Study 1: The goal of this first study was to determine the usability of PCCP, a click-based graphical password system where passwords consist of one user-selected click-point per image on a sequence of images. The 24 participants were university students from different disciplines (though none were studying computer security). They used MVP on a variety of computers and platforms without problem. The participation rate was high during the at-home tasks. Several participants mentioned enjoying the websites and inquired whether they would be available beyond the study.

Study 2: A second study compared the usability and security of recognition-based graphical password schemes, similar to Passfaces but using different types of images. The 60 participants were randomly assigned to one of three groups, each group using a different image type (houses, faces, or random objects). Participant completed a one-hour lab study, a one-week at-home component, and a 15-minute follow-up lab session where they completed post-test questionnaires.

These studies showed that participants could use the system from a variety of locations and platforms without difficulty and engaged with the web content as their primary tasks. When users forgot their passwords, they were able to reset them without difficulty. Finally, our instrumentation allowed us to recover detailed information about usage, enabling later analysis. For the two specific studies above, we are currently concluding our analysis and will publish those results elsewhere.

4. CONCLUSION

MVP is a web-based authentication framework for conducting more ecologically valid user studies of authentication schemes. It uses instances of real web-based applications that have been modified to require login using configurable, interchangeable authentication schemes. Initial studies using the system have been successful in allowing us to conduct ecologically valid field studies that permit analysis and comparison. Future work includes adding more authentication modules, adding a wider range of web-based applications, and conducting larger, longer-term comparison studies of various authentication schemes.

5. REFERENCES

[1] OpenID website, accessed May 2010.

[2] R. Biddle, S. Chiasson, and P. van Oorschot. Graphical passwords: Learning from the first generation. Technical Report TR-09-09, School of Computer Science, Carleton University, Ottawa, Canada, 2009.