# [Short Paper] The MVP Web-based Authentication Framework

Sonia Chiasson, Chris Deschamps, Elizabeth Stobert,
Max Hlywa, Bruna Freitas Machado, Alain Forget,
Nicholas Wright, Gerry Chan, and Robert Biddle

Carleton University, Ottawa, Canada,
chiasson@scs.carleton.ca

**Abstract.** MVP is a framework allowing websites to use diverse knowledge-based authentication schemes. One application is its use in conducting ecologically valid user studies of authentication under the same experimental conditions. We introduce MVP and its key characteristics, discuss several authentication schemes, and offer lessons learned from running 9 hybrid (lab/online) and 3 MTurk user studies over the last year.

**Keywords:** Authentication, usable security, graphical passwords, MTurk

## 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. Alternatives such as biometrics or tokens raise other issues such as privacy and loss. Various graphical password schemes have received considerable attention in response. A systematic review of the literature on graphical passwords [8] shows no consistency in the usability and security evaluation of different schemes. The situation is similar for text passwords, making fair comparison between schemes nearly impossible.

We present MVP (Multiple Versatile Passwords), a framework for using diverse knowledge-based authentication schemes on websites. In particular, it allows user studies of authentication in the same context. These can be deployed in the field where ecological validity is improved by the use of real websites with real content, making authentication a secondary task. MVP is not a single-sign-on system; it serves as a platform for different types of authentication and therefore facilitates research in this area. Another testing framework for authentication was described briefly in a workshop paper by Beautement and Sasse [7]. It asked users to log in to claim credits as part of an online bartering game.

We have implemented several authentication schemes within MVP and so far have conducted 12 user studies with the system. We have also used it as a classroom platform for students to gain experience in running user studies. Amongst the schemes, we offer an implementation of Draw-A-Secret (DAS) [14],

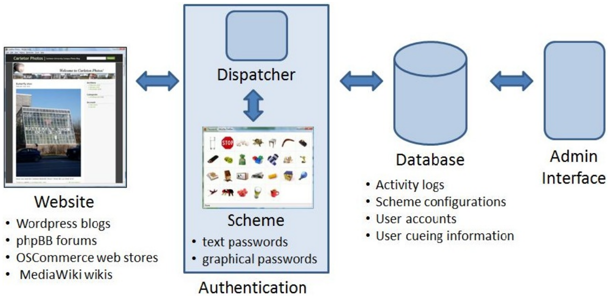


**Fig. 1.** Diagram of the MVP framework.

a recall-based graphical password scheme that to our knowledge has only been tested as a paper prototype. Our implementations of the cued-recall schemes PassPoints [16] and Persuasive Cued Click-Points [10] are the first in the literature to include fully functional systems using discretization, hashing, and image selection. The MVP implementations of recognition-based schemes such as Face (similar to the commercial Passfaces system) are the first to be implemented at password-level security strength rather than PIN-level security.

## 2 MVP system features

MVP has the following system characteristics:

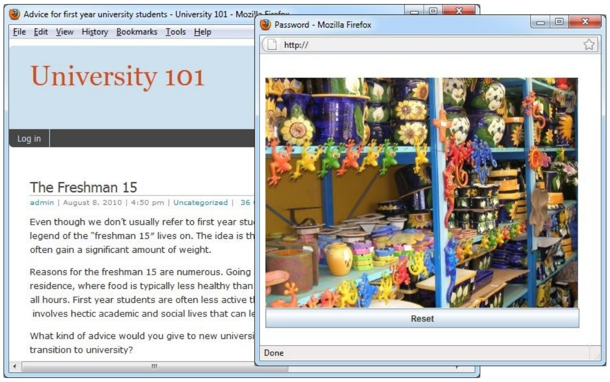
***Web-based usage:*** MVP is web-based (e.g., as a Wordpress plug-in) and functions with most popular browser and operating system configurations, therefore allowing participants to access the sites from any computer. The only modifications necessary are to server-side software, and these are minor. No modifications are needed on users' computers.

***Easy addition of new schemes:*** Figure 1 presents MVP's design. The website's password field is replaced by a button that invokes the MVP dispatcher and opens a new window with the appropriate authentication scheme. The dispatcher returns a password string based on the user input that is evaluated by the website as it would normally evaluate any entered text password. In this way, the websites remain responsible for authentication, while MVP controls which password scheme is displayed and its configuration.

MVP is designed for interchangeable use of different password schemes. The schemes are modular components that administrators can add and remove like server plug-ins. Password systems can be written in any web language. Currently, the password systems are written in either Java or JavaScript. The password schemes use PHP to communicate with the MVP dispatcher. A mySQL database stores administrative data to support the schemes.

MVP allows for easy parameterization of schemes so they may be used at different levels of security. User accounts are initially defined by an administrator, who selects the authentication scheme and the desired parameters for the website. A user may be assigned different schemes for different sites. Tools facilitate the process of defining multiple accounts. By default, a simple plain-text password system is used. However, modules for other schemes can easily be written and added to MVP. Currently, password schemes include PassPoints [16], Cued Click-Points [9], Persuasive Cued Click-Points [10], Draw-a-Secret [14], GrIDsure [3], PassTiles [15]; and recognition-based schemes using face, object, house, and word images. As well, MVP supports various text password systems.

***Ecological validity:*** MVP is especially designed to allow passwords 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. This allows the collection of more realistic usage data. MVP exists as a Wordpress plugin for blogs. We have also modified instances of other popular open-source systems, including phpBB forums, OSCommerce online stores, and the MediaWiki platform. Figure 2 provides a screenshot of the login interface for a Wordpress blog using PCCP as an authentication scheme, while Figure 3 shows the DAS, Face, and Word Recognition login interfaces.


Advice for first year university students - University 101 - Mozilla Firefox
File Edit View History Bookmarks Tools Help
University 101
Log in
Password - Mozilla Firefox
http://
Reset
Done

The Freshman 15

admin | August 8, 2010 | 4:50 pm | Uncategorized | 36

Even though we don't usually refer to first year stu
legend of the "freshman 15" lives on. The idea is th
often gain a significant amount of weight.

Reasons for the freshman 15 are numerous. Going
residence, where food is typically less healthy than
all hours. First year students are often less active t
involves hectic academic and social lives that can le

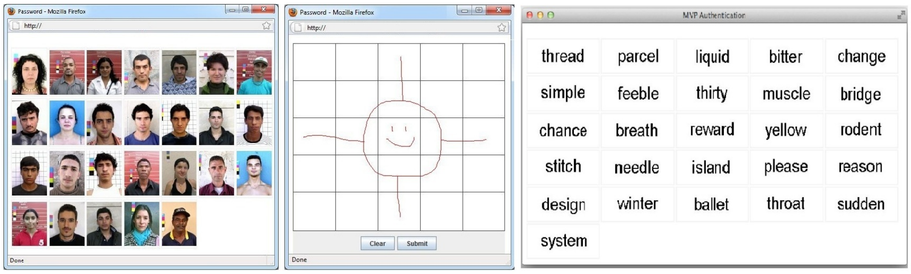
What kind of advice would you give to new universi
transition to university?

**Fig. 2.** A blog using PCCP for authentication.

***Instrumentation for analysis:*** Since user behaviour can significantly impact security, we collect and analyze data representing user choices and behaviour for susceptibility to security threats as well as for evaluating usability. MVP is instrumented to record all user interactions, including keyboard and mouse entries, timestamps, and details of the user's computing environment. Logging is done asynchronously with the server, allowing detailed data to be collected without creating delays affecting user experience. Data is stored in a mySQL database. Different authentication schemes can be tested under identical conditions while recording the same performance measures. We use LimeSurvey [4] running on our servers in conjunction with MVP to administer study questionnaires.

***Password reset without admin intervention:*** Forgotten passwords are to be expected, especially in long-term studies or studies requiring users to remember multiple passwords. MVP allows users to reset forgotten passwords without intervention from a system administrator. The real-time password reset mechanism minimizes disruption to users, encourage completion of assigned tasks, and supports the ecological validity of the system. MVP records details about password resets to allow later analysis of this user behaviour.

Password resets are triggered by clicking the "forgot password" link on the given website. When a user resets their password, they are emailed a URL that directs them to the website, where they are prompted to choose a new password with their assigned authentication scheme. In some cases, it can be desirable to discourage users from resetting their password each time they want to log in. MVP allows password resets to be delayed by any period of time (typically 5 minutes, and the user is warned about the delay). This time delay is intended to subtly discourages users from relying on password resets as a login mechanism.



| | | | | |
|---|---|---|---|---|
| thread | parcel | liquid | bitter | change |
| simple | feeble | thirty | muscle | bridge |
| chance | breath | reward | yellow | rodent |
| stitch | needle | island | please | reason |
| design | winter | ballet | throat | sudden |
| system | | | | |

**Fig. 3.** The Face, DAS, and Word Recognition login interfaces.

***Training:*** MVP provides an interface for users to practice using new schemes and receive immediate feedback about whether they are entering passwords correctly. MVP also supports audio/video tutorials, interactive demo systems, and static text/image help pages. Some schemes (e.g., PassTiles) include the option of practicing passwords directly within the password creation interface where users can show/hide their password and practice it until it is memorized.

***Administration tools:*** MVP includes several study administration tools. A notification system automates the process of emailing participants at specific intervals prompting them to complete at-home tasks. A log query system allows experimenters to retrieve information in real-time from the database about the activities of specific users. While experiments are in-progress, the query system is especially useful to monitor whether users are completing tasks and to troubleshoot any problems from users. A modified version of the MRBS [5] scheduling software allows in-person participants to sign-up for study sessions.

***Crowdsourcing functionality:*** Online crowdsourcing websites (such as Amazon's Mechanical Turk [1] — MTurk) are increasingly used as a source of participants for usable security studies, and MVP includes tools to help conduct studies using such systems. Crowdsourcing studies differ from traditional studies in the volume of system traffic, the pace of the study, and the methods of communication and payment. An MVP validation protocol verifies that the correct tasks have been completed, and users must validate their work to receive payment for that session. MVP tracks user identifiers from the crowdsourcing site (e.g., MTurk worker ID) and email addresses to reduce the possibility that a user participates multiple times in the same study or in closely related studies. The system also ensures that users cannot join partway through a multi-task study without having completed earlier steps.

# 3 MVP deployment for user studies

MVP has been deployed for 12 user studies over the last year (see Table 1). To situate the "Lessons Learned" from Section 4, we briefly describe their methodology and overall results. MVP was also used in a university course to give students a platform for learning about user studies. Seventy students in 8 groups ran user studies with approximately 200 participants overall.

## 3.1 Hybrid studies

We ran several hybrid studies of authentication systems. Participants initially took part in a lab session where they received training on how to use the websites and authentication schemes, and created accounts on two to four websites. The accounts were for various Wordpress blogs (e.g., a dream vacation photo blog, and a daily opinion poll site), and a phpBB forum to discuss the best locations for various activities. The websites were fully populated with real content to engage users realistically. In each case, participants' main tasks were to comment on a specific blog post or forum thread, tasks requiring them to log in. In the week following the initial session, participants received email asking them to complete further tasks from any web-enabled computer.

**Table 1.** Summary of MVP user studies. The number of sessions includes the total number of in-lab sessions and at-home tasks.

| Study Name | Number of | Number | Accounts | Pswd | Pswd | Study |
|---|---|---|---|---|---|---|
| | Sessions | of Users | Per User | Space | Selection | Type |
| 1. PCCP | 4 | 24 | 3 | $2^{43}$ | Chosen | Hybrid |
| 2. Recognition - image type | 5 | 60 | 3 | $2^{28}$ | Assigned | Hybrid |
| 3. Recognition - in-depth | 5 | 20 | 4 | $2^{28}$ | Assigned | Hybrid |
| 4. DAS | 4 | 26 | 3 | $2^{58}$ | Chosen | Hybrid |
| 5. PassTiles - user-choice | 4 | 33 | 2 | $2^{21}$ | Chosen | Hybrid |
| 6. PassTiles - memory type | 5 | 81 | 3 | $2^{21}$ | Assigned | Hybrid |
| 7. Text | 4 | 21 | 3 | $2^{36}$ | Chosen | Hybrid |
| 8. Text - memory type | 4 | 36 | 3 | $2^{36}$ | Assigned | Hybrid |
| 9. Text - interference | 4 | 20 | 3 | $2^{36}$ | Assigned | Hybrid |
| 10. PassTiles - MTurk | 4 | 77 | 3 | $2^{21}$ | Assigned | MTurk |
| 11. PassTiles - MTurk 2 | 4 | 92 | 3 | $2^{28}$ | Assigned | MTurk |
| 12. PCCP - MTurk Training | 4 | 30 | 3 | $2^{28}$ | Chosen | MTurk |

***1. PCCP:*** Persuasive Cued Click-Points (PCCP) [11] is a cued-recall click-based graphical password system where passwords consist of one user-selected click-point per image on a sequence of images. The study's results support and confirm earlier lab-based studies of the usability and security of PCCP.

***2. Recognition - image type, 3. Recognition - in-depth:*** Face [6,12] is a recognition-based scheme where users must identify their assigned images of faces from among decoys. It was suggested that the human proficiency for recognizing faces would help with remembering such passwords [6]. We implemented Face and two variations where the type of image was modified to either everyday objects or houses [13]. A second study conducted an in-depth comparison of face and object images. In our configuration, 6 panels of 26 images were shown in sequence, each panel containing one of the user's 6 images. Results showed that objects were as easy or easier to remember than faces while houses was most difficult. No evidence was found to support higher performance for face images.

***4. DAS:*** Draw-A-Secret (DAS) [14] is a recall-based scheme where users sketch on a grid using a mouse. Our system used a 5 × 5 grid. Results showed that users often misunderstood the scheme (e.g., users drew their figure within one grid square, not realizing that this was equivalent to one dot in a square). Users also tended to draw simple figures that would be easily guessed, and often re-used passwords across different accounts.

***5. PassTiles - background type, 6. PassTiles - memory type:*** PassTiles passwords consist of a set of squares (tiles) on a grid [15]. The scheme was implemented with a blank background or an image behind the grid, or with individual objects in each tile. The systems used an 8 × 6 grid and a password consisted of 5 tiles. The first study allowed users to choose their own passwords while the second provided assigned passwords. Results showed that offering users the opportunity to combine memory retrieval methods (e.g., having an image or objects as a cue) may increase memorability of graphical passwords.

***7. Text:*** Text passwords with a minimum length of 6, including at least one digit and one letter, were also tested. Results showed that although users could quickly log in ($\approx 6$ seconds), the majority re-used passwords across accounts.

***8. Text - memory type, 9. Text - interference:*** These studies [17] tested different types of text passwords: 6 randomly assigned characters, 4 randomly assigned common words, and a recognition-based system where the "images" were words ("Word Recognition", Figure 3). Results showed only minor differences in memorability, but slower login times for the recognition scheme.

### 3.2 Mechanical Turk studies

MVP also enables fully online user studies with no in-person component. We have completed two MTurk studies and a third study is in progress.

***10. PassTiles - MTurk:*** Study 6 of PassTiles was replicated using participants from MTurk. Instructions were provided entirely through webpages and email. Results supported those found using the hybrid study.

***11. PassTiles - MTurk 2:*** A second MTurk study of PassTiles used an $8 \times 10$ grid and 6 tiles. Results were similar to the earlier studies, indicating that the larger theoretical password space did not negatively affect usability.

***12: PCCP - MTurk Training:*** We are currently investigating different delivery methods for training in online studies. Three instruction sets have been compiled for the PCCP authentication system: a static text/image webpage, an interactive demo webpage, and a video tutorial.

## 4 Discussion and Lessons Learned

Based on web server log information about their browsers, participants 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, providing evidence that participants engaged with the web content as their primary task. When users forgot their passwords, they reset them from home without intervention from an administrator.

In this section, we outline a number of lessons learned while running studies using MVP. This list is not comprehensive, but we hope that these findings may assist other experimenters in designing and conducting similar studies.

***Force logoffs:*** One problem with using real websites for experimental purposes is that they may not be configured appropriately for password studies. The Wordpress blogs were pre-configured to allow users to remain logged in. We enforced server-side logoffs, so that users would need to log in with each visit.

***Ethics:*** In running user studies of any kind (whether lab, hybrid or online), not only it is important to obtain permission from the appropriate research ethics board, but also to give consideration to key issues such as privacy. In our online studies, email address and crowdsourcing identifier were the only identifying information collected about each participant, and this was never displayed publicly. Consent forms were completed online and included only the participant's email address as a "signature". All data collected in the study (including questionnaire data) was collected and stored on our servers, allowing us to have complete control of the data and ensuring that it is accessed only by authorized researchers. We are considering an email aliasing system to further anonymize data while still helpind to detect users trying to participate more than once.

***Practicing:*** In an early MVP study, we noticed a few participants with several logins immediately preceding a required study task. It appeared that before returning to the lab, participants were practicing entering their passwords! When running studies, and considering ecological validity, it is important to consider that participants may be putting in a different effort (whether greater or less) than they would in a real life scenario.

***Avoiding the task at hand:*** We have occasionally noticed that participants will develop coping strategies that avoid performing the correct task. In one study of text passwords, we noticed that instead of remembering their passwords, participants were resetting their passwords at every login because it was quicker and easier. In another study (of PassTiles), participants seemed to be coping with the study tasks by writing all of their passwords down. It is important to consider how participants may be circumventing your tasks, and either prevent them from doing so, or collect sufficient information to be aware of these coping strategies. Such behaviours may in fact reflect real-life behaviour and may offer important insight into the real usage of authentication systems.

***Global researchers, global audience:*** To our initial surprise, we could not post tasks on MTurk as non-US citizens. We instead use Crowdflower [2] as a intermediary that can post tasks to several crowdsourcing systems, including

MTurk. We also had minor issues with international participants who were running older computer systems and had slow or unreliable internet connections. Having a robust system that is compatible with a wide variety of environments is critical. The system should also be able to withstand significant web traffic when running MTurk studies and be robust enough to withstand users trying to cheat and circumvent the system in a variety of ways.

## 5 Conclusions

MVP is a web-based authentication framework which we used 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. Now that MVP has been tested with these shorter studies, we are preparing larger, longer-term (several months) comparison studies of various authentication schemes.

## References

1. Amazon Mechanical Turk, `https://www.mturk.com`
2. Crowdflower, `http://crowdflower.com/`
3. GrIDsure corporate website. `http://www.gridsure.com`
4. LimeSurvey: The open source survey application, `www.limesurvey.org`
5. MRBS, `http://mrbs.sourceforge.net/`
6. Passfaces Corporation. http://www.passfaces.com/
7. Beautement, A., Sasse, A.M.: Gathering realistic authentication performance data through field trials. In: SOUPS USER Workshop (2010)
8. Biddle, R., Chiasson, S., van Oorschot, P.C.: Graphical Passwords: Learning from the First Twelve Years. ACM Computing Surveys 44(4) (in press)
9. Chiasson, S., Biddle, R., van Oorschot, P.C.: A second look at the usability of click-based graphical passwords. In: ACM SOUPS (July 2007)
10. Chiasson, S., Forget, A., Biddle, R., van Oorschot, P.C.: Influencing users towards better passwords: Persuasive Cued Click-Points. In: BCS-HCI (2008)
11. Chiasson, S., Stobert, E., Forget, A., Biddle, R., van Oorschot, P.C.: Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. IEEE Transactions on Dependable and Secure Computing (TDSC) (2012 - in press)
12. Davis, D., Monrose, F., Reiter, M.: On user choice in graphical password schemes. In: USENIX Security Symposium (2004)
13. Hlywa, M., Biddle, R., Patrick, A.: Facing the facts about image type in recognition-based graphical passwords. In: ACSAC (2011)
14. Jermyn, I., Mayer, A., Monrose, F., Reiter, M., Rubin, A.: The design and analysis of graphical passwords. In: USENIX Security Symposium (1999)
15. Stobert, E.: Memorability of Assigned Random Graphical Passwords. Master's thesis, Department of Psychology, Carleton University (August 2011)
16. Wiedenbeck, S., Waters, J., Birget, J., Brodskiy, A., Memon, N.: Authentication using graphical passwords: Effects of tolerance and image choice. In: SOUPS (2005)
17. Wright, N.: Do you see your password? Applying recognition to textual passwords. Master's thesis, Department of Psychology, Carleton University (August 2011)