

## **A SECURITY CLASS PROJECT IN GRAPHICAL PASSWORDS**

Jake Spitzer, Cal Singh, Dino Schweitzer  
United States Air Force Academy, Colorado 80840  
dino.schweitzer@usafa.edu

### **ABSTRACT**

This paper details the development and implementation of a research project in support of a Computer Security and Information Warfare class. The purpose of the project is to teach students in-depth knowledge about a security topic and provide a research experience. This particular security project is graphical passwords and the goal of the project is to investigate a unique implementation of a graphical passwords scheme known as Cued Click Points (CCP). The CCP method has a large key space that reduces the likelihood of a successful attack using traditional techniques such as brute force or dictionary attacks. The project developed an implementation of CCP that combined the graphical approach with user's familiarity with navigating through Google maps. The user is presented with an image of the United States and simply clicks to where the 'key' destination is located using a zooming map levels approach. Google Maps and the Processing environment permit a simple implementation allowing the focus of the project to be on data collection and analysis. This paper will provide background on the CCP approach, describe the implementation, and present the results based on user feedback using the system.

### **INTRODUCTION**

Information security is an important topic for computer science students to understand. Many schools have begun teaching security topics throughout the CS curriculum through a variety of methods: separate security courses and tracks, integrating topics into existing courses, hands-on laboratories, and student competitions. The United States Air Force Academy has created a three-course sequence in security that teaches students topics such as information warfare, cryptography, and network defense. Students completing the three courses as part of their CS major, receive a special security designation on their transcript. A distinguishing aspect of our introductory computer security class is the use of a realistic student research experience to reinforce core concepts in the course [8]. The learning objectives for the research project are:

- Understand the entire research process from problem definition to final documentation
- Be able to conduct background investigation, develop a research plan, complete an implementation, collect and analyze data, and create a conference-ready poster and paper
- Explore and understand an aspect of computer security in depth

Students choose their research topic and are assigned a faculty mentor early in the course and work on the project throughout the semester with periodic turn-ins to monitor progress. This paper describes one such research project investigating a unique implementation of a graphical password system.

### **BACKGROUND**

Users employ passwords as a form of authentication to correctly identify themselves on a computer or communications network. Passwords provide security from outside threats by only allowing a user knowing the password to gain access to specific content. Passwords are used in a variety of devices, from personal computers and mobile phones, to websites and ATMs. Passwords can be simple numeric sequences, or PINs; complex combinations of letters, numbers, and special characters; or graphical images that a user can click or draw on. The most common type of password is the alphanumeric password which is vulnerable to dictionary attacks in which the attacking user or program tries common words and word combinations from a dictionary. With the speed of modern computers, thousands of possible passwords can be checked per second. One of the reasons that dictionary attacks are successful is that users tend to choose passwords that are easy to remember, such as words found in a

dictionary. Many password schemes have been proposed to create passwords that are easy to remember, but secure from dictionary attacks.

Graphical passwords provide one such alternative to traditional passwords approaches. The basic premise is that pictures are easier to remember or recognize than text. Several different schemes have been proposed for users to utilize pictures or drawings rather than entering text characters [2-7]. An example of such a scheme is the user selects a sequence of images as their password, and when authenticating themselves, they are asked to select their images from a set of random pictures. Another approach that attempts to defeat shoulder surfing is the user is presented with a random collection of icons and needs to click somewhere in the convex hull of their pre-selected icons. A different approach to graphical passwords is when the user draws a simple picture on a 2D grid. If the drawing touches the same sequence of grid points as the pre-selected sequence, the user is authenticated. A similar approach is based on the user entering their signature using the mouse.

A graphical password scheme of particular interest for this project is the Cued Click Point approach [1]. The user is presented with an image overlaid with a 2D grid. The user selects one of the grid locations which brings up a different image also with a grid. The sequence of selected grid coordinates represents the password. If a user mistakenly selects a grid location not in their authentication sequence, the resulting image would immediately be recognized as not being part of their normal image sequence. A sequence of five clicks is used as the password sequence. User studies from the CCP method showed users found the approach easy to use and remember.

## OUR APPROACH

### Concept

Critics of the graphical passwords point out that such systems may require an inordinate amount of storage space for images, can be difficult to learn to use, can take longer than traditional passwords to enter, and may be hard to implement across multiple systems. Our approach eliminates the need for high disk space by using an online picture database, and calling an external server each time the user clicks. To create a system that was easy to learn, we based it on the familiar user interface of zooming into Google maps. Users are familiar with zooming into a specific area of interest, such as a street location. By overlaying a 2D grid on the map, and zooming into the grid being clicked, navigating to a specific location is equivalent to selecting a sequence of images in the CCP technique.

### Implementation

An advantage of basing our system on Google maps is that we can take advantage of the well-defined Google Maps API. Specifically, for our implementation, we made use of the Static Maps API, which returns a map image when passed the appropriate parameters in a URL to specify location, size, and zoom level. The API call can be invoked directly from a Java program to return a raster image to display. For this project, the Processing programming language and environment was used to create a prototype for testing purposes. Processing ([www.processing.org](http://www.processing.org)) is a Java-based language that is simple to learn and use, is specifically designed to support graphical applications, allows for rapid prototyping, and runs under multiple operating systems. The following lines of code are all that are necessary to retrieve and display a map image from Google maps.

```
float lon = 38.796908;           // lat/lon for center of map
float lat = -104.787598;
int zoom = 3;                   // zoom factor for map
size(480,480);                  // size of image on screen
String url = "http://maps.google.com/maps/api/staticmap?center="+
             lon+","+lat+"&zoom="+zoom+"&size=480x480&sensor=false";
PImage online = loadImage(url, "png"); // get image from Google
image(online,0,0);              // display to screen
```

The variables lat, lon, and zoom can be programmatically controlled to specify what location and zoom level to use for the map.

An implementation of this CCP method was written in Processing to collect data from users on the usability and memorability of the technique. First, a user is presented with a Google map of the entire United States with a grid overlaid on it as shown in Figure 1.

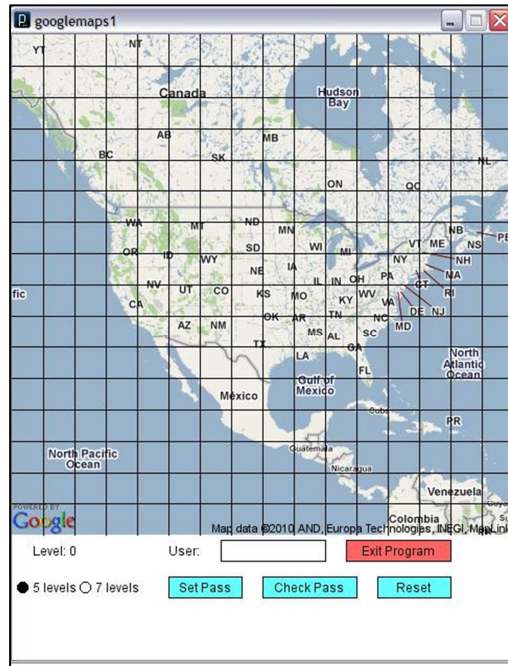


Figure 1. Opening screen of our CCP system.

The user enters their user name and selects the number of click levels they want to investigate, five or seven. They then select a grid location in the map which replaces the map image with a zoomed version around the selected grid point as shown in Figure 2. The image size and grid size (16x16) remain constant for each zoom level. The grid lines are intended to assist the user in selecting a specific grid location, versus an arbitrary point on the map that may be close to a border between two grid locations and thus give different results if the user clicks are slightly off during subsequent tries. Figure 2 also shows the level of map detail after five clicks.

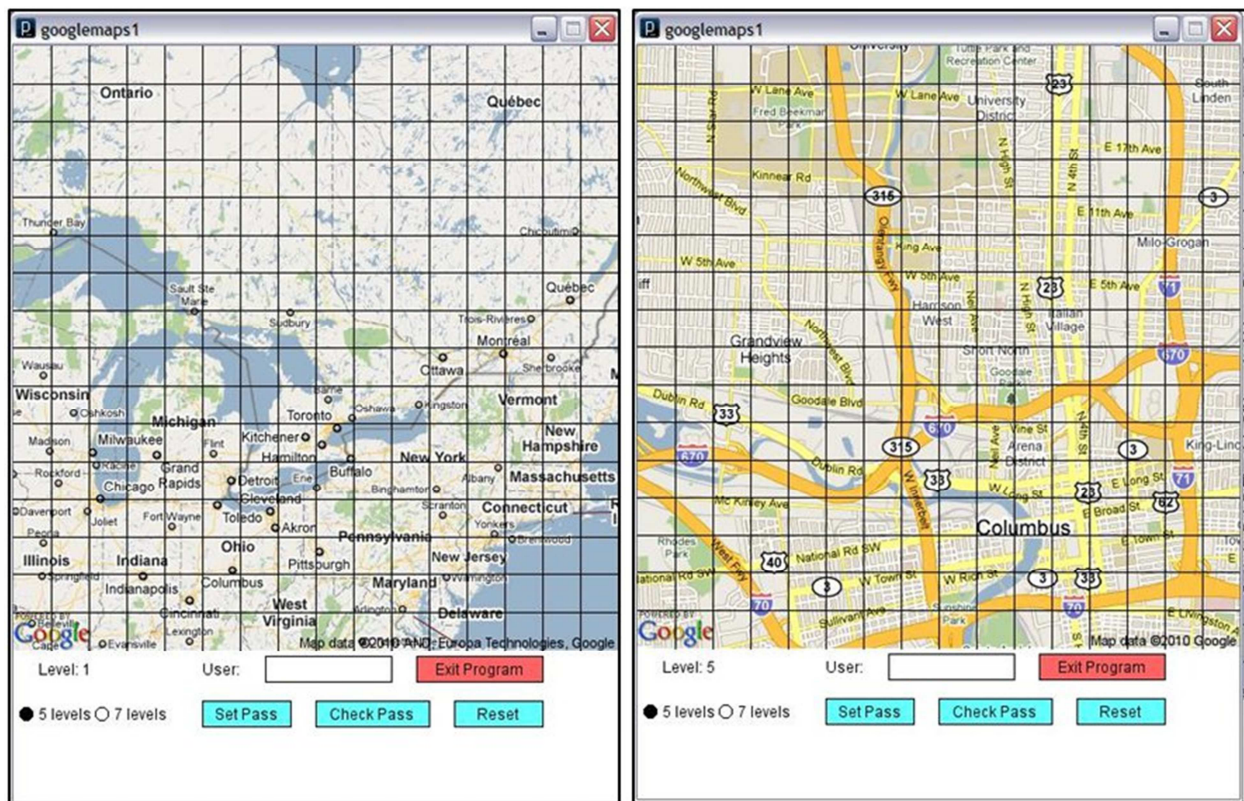


Figure 2. Zoomed map image after one and five clicks.

After five or seven clicks, the user can either set the password for the supplied user name, or check the entered password against a database of previously entered passwords. The sequence of selected grid locations (256 per zoom level) represents the password. At any point in the click sequence, the user can reset the system and start again from level 0.

## ANALYSIS

To analyze this graphical password scheme, we first look at the overall key space in comparison to a traditional alphanumeric approach. To determine usability, a survey of users was conducted based on how easy the system was to use and remember. Over 50 users used the system and reported their experience.

### Key Space Analysis

A simple key space analysis of clickable ranges on the graphical password system compared to that of an alphanumeric password is shown. Each click on the graphical image is equivalent to a typed character in a normal password. Assuming 94 available keys (shift and non-shift on a standard keyboard), a password of length  $n$  would have a key space of  $94^n$ . Since the grid size is 16 x 16, each click of the image has 256 possible values, so a sequence of  $n$  clicks has a key space of  $256^n$ . Figure 3 shows the increase in size of key space based on alphanumeric versus image clicks for increasingly large passwords. Eight clicks in the CCP system provide roughly the same key space size as ten characters.

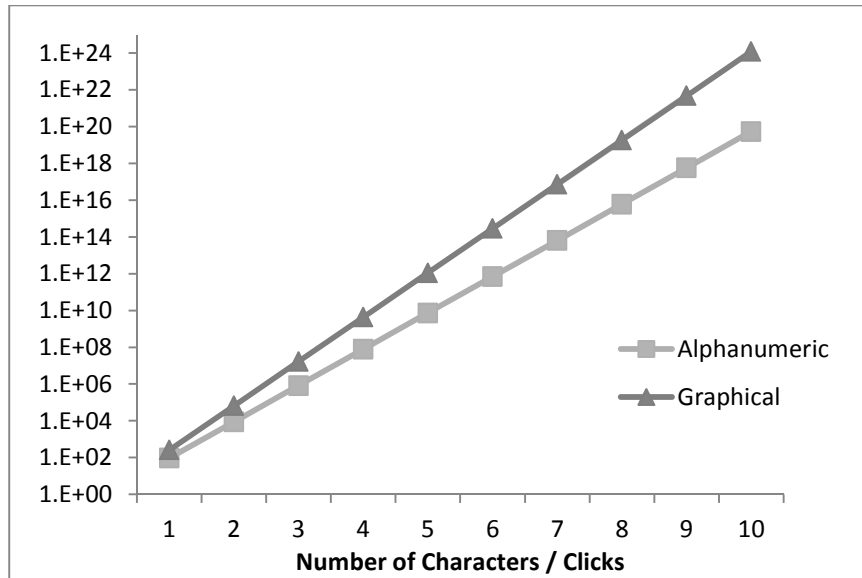


Figure 3. Key space for alphanumeric and CCP graphical passwords.

A factor that is not considered in this analysis is that while each graphical password image has 256 possible grid locations to select from, not all of the grid locations contain something of interest to encourage people to click it. For example, from Figure 1, it would be unlikely for a user to click in a grid location in the ocean, as there would be no reference to guide successive clicks. A complete analysis of this approach should consider the percentage of grid locations considered sufficiently interesting to click on.

### User Analysis

Over 50 users used our graphical password system and provided feedback on its usability and memorability. Figure 4 shows the results of a survey asking participants how easy the system was to use. The average rating was 3.8 on a scale of 1 to 5. Individual comments included the fact that it took longer to click a sequence of grid locations than simply typing a password, and that the image size should be adjustable to allow for easier navigation when clicking.

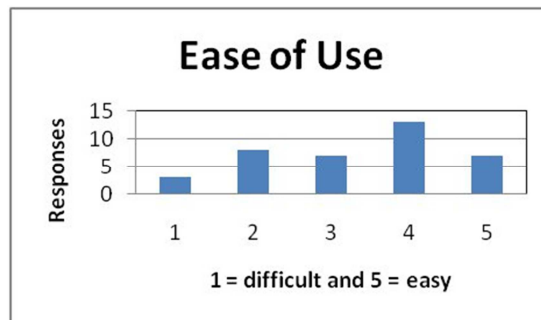


Figure 4. User survey on system's ease of use.

In terms of memorability, 60% of the users rated the system as easier to remember than alphanumeric, while 40% said it was more difficult. One suggestion for improving usability was to allow the user to go back one level to change the sequence versus having to reset and start from the beginning.

## System Limitations

Although the implemented system is only a prototype, there are some known issues if this scheme were to be used in a production system. By definition, the user needs to be online to access Google maps. Such a system may be useful for applications such as entering passwords to access an online resource or when online access is constantly available. However, when online access is limited or unavailable, some type of fallback system would be necessary. Similarly, if the Google map server is down, the approach will not be able to load successive images. An ideal system would recognize when such limitations exist and go into some type of alternative mode. The approach, as described, also does not address the problem of shoulder surfing. If an attacker sees the end location of successive zooms, they can replicate the sequence.

## CONCLUSIONS

User feedback of this approach is that it is easy to use. However, the fact that 40% indicated it was harder to remember than alphanumeric indicates that it is not, in its current form, ready to replace traditional authentication techniques. A larger user study is necessary to exercise the system and collect quantifiable information on the effect of different levels, and ways to improve the user interface.

## Appropriateness as a class project

This project met the goals for the research project in the Information Warfare class. It was an original area of research providing an opportunity to explore a security topic in greater depth. It contained an implementation and experimentation phase with an opportunity to perform analysis on collected data. Students learned about different graphical password approaches, key space calculation, creating a prototype system for testing, designing a user study, and interpreting results. In addition, by using Processing and Google Maps as the programming environment, the prototype of the tool could be quickly created and used to gather user data. The implementation did not get in the way of focusing on the problem and security concepts being explored. The students, as a result of this project, have a better understanding of graphical passwords and an appreciation of conducting a user study to determine the effectiveness of a proposed system.

## REFERENCES

- [1] Biddle, R., Chiasson, S., Van Oorschot, P. C., Graphical password authentication using cued click points, *12<sup>th</sup> European Symposium on Research in Computer Security (ESORICS)*, Dresden Germany, 2007.
- [2] Birget, J., Brodskiy, A., Memon, N., Waters, J., Wiedenbeck, S., Authentication using graphical passwords: basic results", *ACM International Conference Proceeding Series*, Vol. 93, 2005.
- [3] Birget, J., Brodskiy, A., Memon, N., Waters, J., Wiedenbeck, S., Authentication using graphical passwords: effects of tolerance and image choice", *Symposium On Usable Privacy and Security (SOUPS)*, 2005.
- [4] Birget, J., and Sobrado, L., Graphical passwords, *The Rutgers Scholar: Undergraduate Research*, Department of Computer Science, Rutgers University, Camden New Jersey, 2002.
- [5] Ian, J., Mayer, A., Monrose, F., Reiter, M. K., and Rubin, A. D., The design and analysis of graphical passwords" *Proceedings of the Eighth USENIX Security Symposium*, 1999.
- [6] Owen, G. S., Suo, X., and Zhu, Y., Graphical passwords: a survey, *Proceedings of the 21<sup>st</sup> Annual Computer Security Applications*, IEEE, 463-472, 2005.
- [7] Renaud, K., On user involvement in production of images used in visual authentication, *Elsevier Journal of Visual Languages and Computing*, 2008.
- [8] Schweitzer, D., Boleng, J., Hadfield, S., Providing an undergraduate research experience in a senior level security course, *Proceedings of the 13th Colloquium for Information Systems Security Education*, 2009.