

Universal Multi-Factor Authentication Using Graphical Passwords

Alireza Pirayesh Sabzevar, Angelos Stavrou
Computer Science Department,
George Mason University,
Fairfax, Virginia, 22030
{apirayes, astavrou}@gmu.edu

Abstract

In this paper, we present a series of methods to authenticate a user with a graphical password. To that end, we employ the user's personal handheld device as the password decoder and the second factor of authentication. In our methods, a service provider challenges the user with an image password. To determine the appropriate click points and their order, the user needs some hint information transmitted only to her handheld device. We show that our method can overcome threats such as key-loggers, weak password, and shoulder surfing. With the increasing popularity of handheld devices such as cell phones, our approach can be leveraged by many organizations without forcing the user to memorize different passwords or carrying around different tokens.

1. Introduction

Authentication in the computer world refers to the act of confirming the authenticity of the user's digital identity claim. Currently, popular authentication mechanisms are mainly based on the following factors: something that the user has (an object), knows (a secret), or uniquely represents him (biometric identifiers) [1]. In the simplest form, a system that requires authentication challenges the user for a secret, typically a pair of username and password. The entry of the correct pair grants access on the system's services or resources. Unfortunately, this approach is susceptible to several vulnerabilities and drawbacks. These shortcomings range from user-selected weak or easily guessable passwords to more sophisticated threats such as malware and keyboard sniffers [2]. An adversary has an abundance of opportunities to compromise the text-based password authentication mechanisms. For long time the computer industry has been in a quest for better alternatives but without popular success: most of our current systems still use the primitive text-based authentication schemes.

To amend some of the shortcomings of the textual passwords, researchers turned their attention to passwords that utilize graphical objects [3, 4, 5]. Graphical authentication has been proposed as a user-friendly alternative to password generation and authentication [6, 7]. The main difference to textual passwords is the use of a device with graphical input: the user enters the password by clicking on a set of images, specific pixels of an image, or by drawing a pattern in a pre-defined and secret order. The proposed systems claim to provide a superior space of possible password combinations compared to traditional 8-character textual passwords [4]. This property alone renders attacks including dictionary attacks and keyboard sniffers computationally hard increasing our ability to defend against brute-force attacks. Furthermore, according to Picture Superiority Effect Theory [8], concepts are more likely to be recognized and remembered if they are presented as pictures rather than as words. Thus, graphical password presumably delivers a higher usability compared to text-based password.

Another way of enhancing the security of the common text-based password is employing multi-factor authentication. In general, multi-factor authentication is a way of authentication in which two or more independent factors are used as part of the user credentials. Multi-factor authentication is usually accomplished by combining the traditional text-based authentication with another factor. These factors can include smart cards, USB tokens, handheld devices, or one-time password tokens. Having two or more factors strengthens but also complicates the authentication process. More specifically, two-factor authentication has been with us for a quite time. Popular examples of two-factor authentication systems are the ATM machines: to complete any transaction, the bank customer has to carry both a bank-issued card (credit or debit card) and her personal identification number (PIN).

We propose a system that leverages both graphical passwords and multi-factor authentication. Our approach overcomes the limitations of the traditional password (either textual or graphical) systems. To that end, we employ graphical password

combined with a handheld device to form a novel method of multi-factor authentication. As a result, we are able to provide a secure authentication via unsecure terminal.

The rest of the paper has been organized as follows: section 2 explains the background of graphical authentication, two factor authentication mechanisms, and the benefits of using handheld device as the second factor of authentication. In section 3, we define some of the main key concepts of our approach. In addition, we discuss three alternative communication methods between the authenticator and user in section 4. Section 5 provides in-depth details about our authentication model and explanation about different types of password image and their strength. The security enhancements of the proposed scheme are analyzed in section 6. In section 7, we discuss the related work and differentiate our approach from previously proposed work. In the remainder of the paper, we briefly describe our prototype implementation and our future plans.

2. Background

Text-based username and password is vulnerable to guessing, dictionary attack, key-loggers, shoulder-surfing and social engineering [9-11]. As mentioned before, to overcome the shortcomings of text-based password, techniques such as two-factor authentication and graphical password have been employed.

In most of the schemes, graphical password employs graphical presentations such as icons, human faces or custom images to create a password [3]. Graphical password techniques can be classified into two categories: recognition-based and recall-based [12].

In recognition-based systems, a series of images are presented to the user and a successful authentication requires a correct images being clicked in a right order. In recall-based systems, the user is asked to reproduce something that he or she created or selected earlier during the registration. These methods assume if the number of possible pictures is sufficiently large, the possible password space of a graphical password scheme may exceed that of text-based password and therefore it is virtually more resistance to attacks such as dictionary attacks. Also, from the usability standpoint, the graphical password claims to be superior to text-based password due to the fact that humans can remember pictures better than text. Since the graphical password is not widely deployed in real systems vulnerabilities of graphical passwords are still not fully understood. However there are a handful of research papers on this subject that we have summarized their results in Table 1 [12-14].

Table 1: Comparing the security of graphical and text-based passwords

Vulnerability/Issues	Text-Based Password	Graphical Password
Dictionary Attack	•	
Guessing	•	•
Spyware/Key-logger	•	•
Shoulder-surfing	•	•
Social Engineering	•	

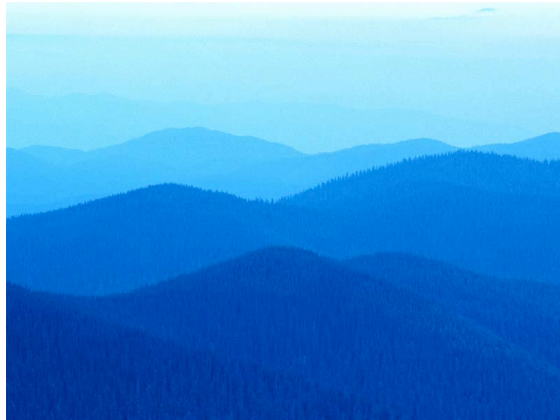
Multi-factor authentication is supposed to deliver a higher level of security assurance. For example business networks may require users to provide a password and a random number from a security token to pass the authentication. Knowing the password and having the security token at the same time provides a higher degree of confirmation about the identity of a person.

However, the two-factor authentication raises some new challenges, especially in the area of usability. One of the usability challenges is that two-factor authentication is not standardized. There are a handful of different authentication factors with various implementations. At the same time, the same authentication factor employed by different institutions is not necessarily interoperable. As the result, usually users are expected to remember dozens of unique passwords and carry multiple physical items as the second authentication factor.

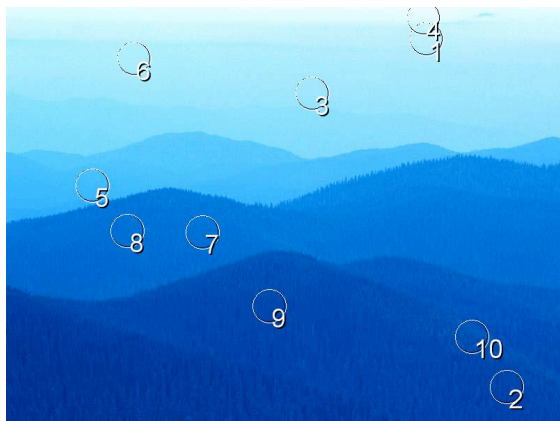
Cell phone is such a popular technology that it is safe to assume nowadays almost everybody carries a cell phone. Embedded technologies such as RFID, GPS, Bluetooth, pointing and touching sensors, digital cameras, and image and voice recognition offer new applications for cell phones to go beyond voice communication. As a result, cell phones are quickly taking over many personal computing tasks, among them authentication. As a matter of fact, an emerging authentication technologies based on cell phones are appearing which transforms the cell phone into an authentication device by using SMS messaging or an interactive telephone call [15]. Using cell phone in such a way eliminates the need for a separate hardware token which in turn positively impacts the usability of the authentication scheme.

Contrary to previous approaches, we employ a cell phone as the second factor of authentication in conjunction with graphical password. This enhances the overall scheme and strengthens the entire authentication process against known types of attacks. Our work is unique because it is the first to leverage graphical password as a second factor for authentication. In addition, our method can effectively address the guessing and shoulder-surfing issue of other image-password methods.

Before delving into more details about our systems, we introduce the terminology used for the rest of the paper.



Password Image



Key Image

Figure 1: A password image and its corresponding key image

3. Terminology

For our approach, the **user's handheld** is a computing resource that can be conveniently be carried in the user's pocket. In some of our communication scenarios, the handheld device is used to store cryptographic keys and execute encryption-related calculations. Additionally, the handheld must be capable of displaying graphical images. Although we use cell phones for our implementation, for the sake of generality, in the rest of this paper, we will refer to the term "handheld" meaning any mobile device that is equipped with a display. We will also define a **challenger** to be a typical online service provider. The challenger offers potential authentication mechanisms to the user. To be authorized and gain access to resources, the user has to successfully complete one of the presented authentication mechanisms. On the other hand, by **Terminal**, we refer to the computing resource with a graphical screen and pointing input device or touch-screen capability. This is the device that that user

uses to reach to the services provided by the Challenger. The terminal can be public or private. Using the public terminal might be riskier but the nature of threats on both public and private terminals are the same.

The authentication comes in the form of two images. The first image is the **password image** which is sent to the user's terminal as a challenge for password. The password image can be plain or encrypted. The password image is encrypted, if and only if it contains some information about click points. In this case the password image and key image are identical.

Key image is a copy of password image which is always encrypted and signed by challenger and can be validated and decrypted on user's handheld device. The key image contains enough information to show the click spots to the owner of handheld.

There are some **clickable** areas in the password image. The user's password is the **click points** and their order. The click points are clickable areas in the password image which a user can identify them by looking at the key image. The click points and their order are either highlighted in the key image or the user can determine them with some prior knowledge. To make guessing the password more difficult, the number of clickable areas in the password image might be more than the click points. Figure 1 shows an example of password images and the corresponding key images prior to encryption or after decryption.

4. Communication Alternatives

In the public terminal, the user receives and the screen displays a random password image with multiple clickable areas on terminal screen. At the same time, the key image with information about click points appear on the screen of user's handheld which is linked to the identity of the user. Therefore the user learns about the click points and their order if and only if she has access to her handheld. There are several ways to transfer the encrypted password image to the user's handheld which are explained in the followings.

4.1 Direct Communication

The challenger sends a password image to the terminal. At the same time, the challenger prepares the key image, encrypts it, digitally signs the encrypted image and emails it to the user's handheld. The user's handheld verifies the signature and decrypts the image. For every authentication, the key image changes but the password image may or may not change. Figure 2 illustrates the transactions

between challenger, terminal, handheld and the user in this method.

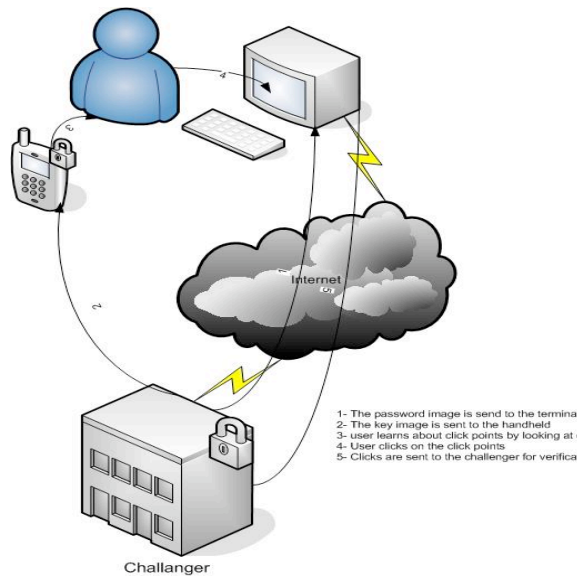


Figure 2: Challenger-Handheld Direct Communication

4.2 Photographic Communication

The challenger prepares a key image, encrypts it and sends it to the user’s terminal. Using the handheld’s camera, the user takes a photo of the encrypted key image which the handheld can decrypt it. At this point the user is able to click on the appropriate spots on the password image. The image on the screen remains unencrypted and doesn’t match what the user sees on the handheld. However what is important here is the click points and not the actual image. Figure 3 illustrates the transactions between challenger, terminal, handheld and the user in this method.

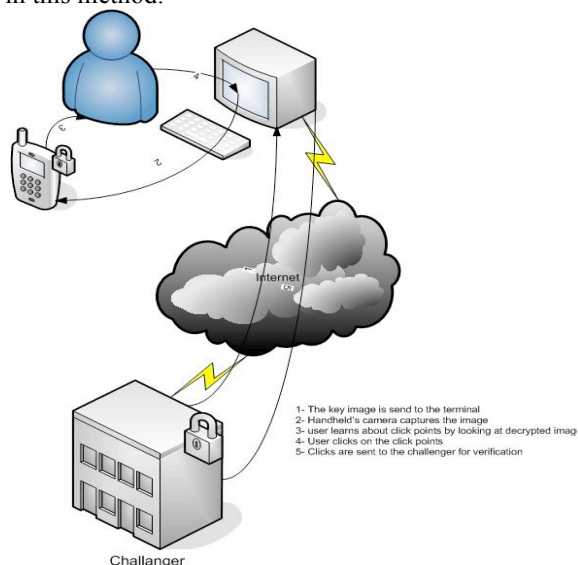


Figure 3: Challenger-Handheld Photographic Communication

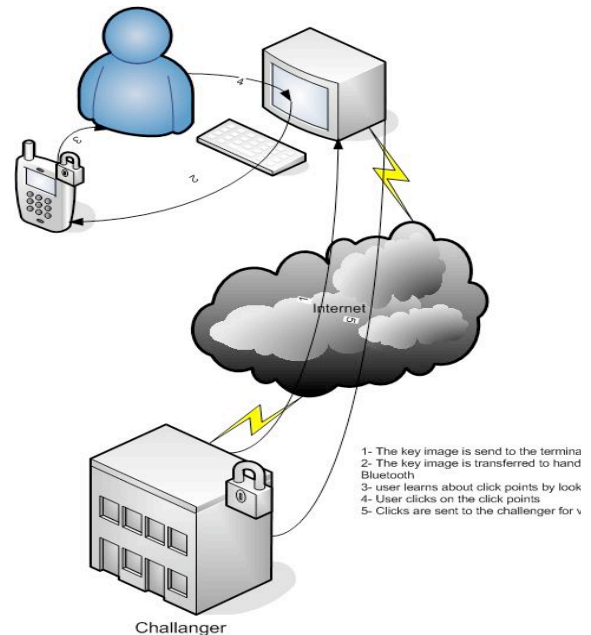


Figure 4: Challenger-Handheld Indirect Communication

4.3 Indirect Communication

Similar to method 2, the challenger prepares a key image, encrypts it and sends it to the user’s terminal. The user’s handheld and terminal are able to communicate via Bluetooth or USB and transfer a copy of the password image to the handheld and decrypt it. At this point, the user is able to click on the appropriate spots on the password image. The image on the screen remains unencrypted and doesn’t match what the user sees on the handheld. Again, what is important here is the click points and not the actual image.

Figure 4 illustrates the transactions between challenger, terminal, handheld and the user in this method.

6. Discussion

6.1 Recognition-based or recall-based?

The approach we take belongs to neither recognition nor recall-based system categories. It does borrow, however, elements from both. In the case the user selects a pin or a secret to be incorporated in the graphical password, our system can be categorized as recall-based. On the other hand, if we allow user to pick her own image, then the image can work similar to PassMark [16] (used as Anti-Phishing mechanism of Bank Of America [17]) which adds a flavor of Recognition-based systems to our proposed system.

6.2 Security Analysis and key-space

With the introduction of the notion of random click points, it is computationally harder to perform attacks that depend on exhaustive search or password eavesdropping. More precisely, brute force, dictionary attacks, shoulder-surfing, and social engineering against the proposed scheme becomes arbitrarily hard. The number of unique clickable areas in the password image and the number of minimum click points required define completely the combinatorial complexity of the authentication scheme. The size of the key space grows both with the number of clicks and with the number of clickable areas. If the image has α clickable areas and p click points, there exist α^P possible valid password combinations. Therefore, the probability of guessing a password is $1/\alpha^P$. For instance, if there are 32 areas and the password length is 6 clicks then the total number of potential combinations is:

$\alpha^P = 32^6 = 2^{30} \approx 10^{10}$ and conversely the probability of success is approximately $1/10^{10}$. The same calculation but for 64 areas and 8 password clicks produces approximately 2.8×10^{15} combinations. A possible option to make the click areas easy to identify, is to use a user-defined PIN or password. This password can be incorporated into the image key. We can then prepare password image and key image such as the one shown in Figure 5. With 94 characters valid for passwords, a 10 by 10 matrix would be more than sufficient for our purpose. We continue by examining each one of the attacks independently. Table 2 compares the vulnerabilities of our suggested method with other graphical passwords.

6.3 Shoulder surfing

When users enter their graphical passwords on a public terminal, there is always the risk of attackers stealing their password by direct observation. There has been previous research that we can apply on how to make the graphical passwords resistant against shoulder surfing [13]. In our solution, the terminal screen doesn't help the shoulder-surfer because each time the click points appear at different location of the password image. At the same time, smaller size screen of handheld device significantly diminishes the potential of shoulder surfing.

6.4 Terminal key-loggers and Malware?

Graphical password scheme appear to immediately solve the key-logger security issue by replacing the keystrokes with clicks; so does our proposed scheme. Unfortunately, graphical password schemes do remain susceptible to more sophisticated attacks such

as screen recording. Contrary to plain graphical passwords, in our scheme, the attackers cannot utilize the screen capturing technique to expose our password. They can, however, use the captured clicks to mount a single access attack. To address that, for our future work, we plan to involve the hand-held device to verify the sites where we submit our authorization credentials.

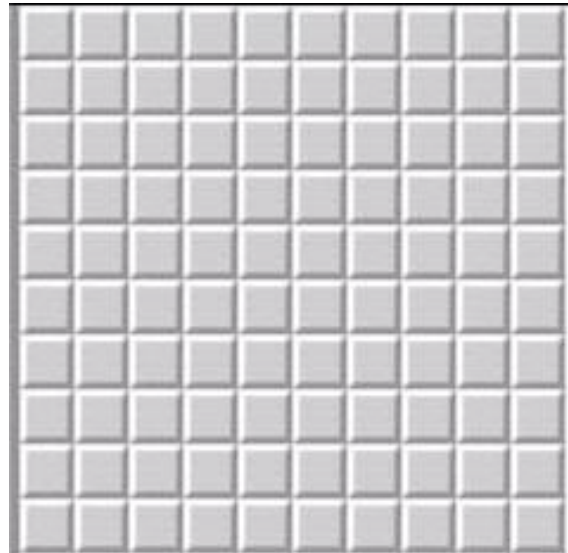


Figure 5: An Password Image and Key Image for more complicated secrets

6.5 What if the handheld gets lost or stolen?

The proposed system is resistant against physical security threats. If the click points are explicitly marked, then anybody who has access to the handheld can authenticate as the real owner of the handheld. For example, while the click points are marked in the key image, the order of clicks can be something that only the handheld owner knows. So

while having the handheld can reveal the click points, no knowledge about the click order will be provided. Figure 1 depicts an example supporting our argument: if the authentication system needs user to click on the clickable areas in just in order, then anybody who has access to the handheld can su the authentication. However, if the order is defined by a secret word (i.e. 5 digit pin) then having access to the handheld and consequently the key image is not sufficient for successful authentication.

6.6 Brute-force attacks

Previous studies have shown that many password images have popular points. These points are more likely to be chosen by users as part of their passwords. These popular spots can be guessed or can be exploited by attackers using different techniques [14, 18]. In our system the clickable areas are randomly chosen by the system. Therefore, due to no human involvement all the areas in the image have equal possibility to be part of a clickable area and guessing become completely irrelevant.

Another benefit of this system is that the terminal never learns any thing about the user password. For example, an ATM machine in the bank learns about user PIN number during the transaction. In our system, it only learns about some clickable areas which are randomly scattered on the image and will change for the next transaction.

Table 2: Comparing security of our graphical password with other solutions

Vulnerability/Issues	Graphical Password	Our Suggested method
Dictionary Attack		
Guessing	•	
Spyware/Key-logger	•	
Shoulder-surfing	•	
Social Engineering		

7. Related Work

On of the seminal papers on the topic of graphical password goes back to 1996 which has been patented under United States Patent 5,559,961 [3]. The patent explains an authentication system that displays pieces of graphical image in a mosaic work fashion. Rather than entering a textual password, to successfully authenticate, the user must click on predetermined areas of an image in a correct sequence. User selects the click points and their order during the enrollment and they get stored in the system as the user's password. Since then, many other graphical password schemes have been proposed [12].

Déjà Vu [5] is a famous one form University of California at Berkeley which authenticates a user through her ability to recognize previously seen images. In Déjà Vu, images are randomly generated using a hash visualization technique. The enrolment contains password selection and a training phase to improve the user's recognition. In contrast, our proposed solution is more of a recall-based scheme. We don't need to train our users because the users learn about the click points by looking at the decrypted key image on her handheld device. While we randomly choose our image from a limited set of images, with a little bit change and add an image generator subsystem, we can mount machine-generated images.

PassPoint is another famous graphical password scheme [7] which allows arbitrary images to be used. As a result, a user can click on any place on an image to create a password. A picture contains hundreds to thousands of memorable points, so the possible password space is quite large. Our idea is very close to PassPoint except the click points are picked by the system not user.

Passfaces [19] is a commercial authentication product based on the graphical password. Users are given a random set of faces (typically 3 to 7) to serve as their secret authentication code. They are then taken through a "familiarization process". During the authentication process, users should pick out their assigned faces, one at a time, from successive groups of nine faces.

There are some security concerns about graphical passwords. For example, in recall-based schemes such as PassPoint there are some areas in the image which are more likely to be selected by the users, known as hotspots [14]. Our proposed scheme is not vulnerable to hotspots because the click points are randomly selected.

In addition, the graphical passwords are resistant against traditional key-loggers because the keystrokes have been replaced with clicks. However, more sophisticated spywares capable of screen recording [20] still can capture the user password. Our solution is resistant to this type of attack because we have separated the password entry from the password itself.

The idea of using the handheld device as the second factor of authentication is not new either. There are some commercial products [15] [21] as well as many published paper such as [22]. Our work is different than any previous work as we are expanding the idea of graphical password into the two-factor authentication area. To our knowledge, this is something that hasn't been done in any other previous work.

Some studies [23, 24] assume the user's handheld is a trusted device and they secure user's session on public terminals using the trusted handheld. While we agree that the personal handheld device might be

more secure and private than a public terminal, however we believe neither device is trustworthy enough to reveal the password to. We believe the physical security of the handheld devices is the greatest concern and any solution based on handheld devices should factor this risk.

8. Implementation

As a proof of concept, we developed a web-based authentication system based on Microsoft .Net technology. We implemented three different types of password images:

- 1) Random images with random clickable areas.
- 2) User picked image with random clickable areas.
- 3) A grid of clickable squares.

The clickable areas are implemented using widely deployable browser-independent server-side HTML Image Maps with circular or rectangular hot spots. Every clickable area is associated with a random code which is meaningful only for the authentication server. This code will be sent to the authentication server when a clickable area is clicked.

For the communications, we implemented a prototype of the direct communication (section 4.1) and the other methods are left for future developments. When the key image is displayed on the user handheld, it indicates to the user the clickable areas.

9. Conclusion

In this paper, we propose a new authentication scheme based on graphical password and multi-factor authentication. Our approach can be effectively and securely used as user-friendly authentication mechanism for public and un-trusted terminals. Our proposed solution is unique in many ways:

1. It is the first graphical password solution that employs two-factor authentication.
2. We never assume the handheld device is trusted.
3. Our solution resists screen recording attacks.
4. Our method doesn't need a "familiarization" or a lengthy "password setup" process.
5. Lost or stolen handheld doesn't expose a security risk.

We can apply our system to more than just authentication mechanisms: our system is applicable anywhere that there is a need to enter sensitive or private data. For instance, Social Security Number

can be entered via our system without leaking or revealing any directly usable information to the terminal or even the handheld device.

9. References

- [1] "Authentication," in *Wikipedia, the free encyclopedia* <http://en.wikipedia.org/wiki/Authentication>.
- [2] "Amecisco Inc.," <http://www.keylogger.com>.
- [3] G. E. Blonder, "Graphical passwords," US Patent 5,559,961, 1996.
- [4] N. J. D. Kirovski, and P. Roberts, "Click Passwords," in *IFIP International Information Security Conference*, 2006.
- [5] R. Dhamija and A. Perrig, "Déjà Vu: a user study using images for authentication," USENIX Association Berkeley, CA, USA, 2000, pp. 4-4.
- [6] T. Pering, M. Sundar, J. Light, and R. Want, "Photographic authentication through untrusted terminals," *Pervasive Computing, IEEE*, vol. 2, pp. 30-36, 2003.
- [7] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical password system," *International Journal of Human-Computer Studies*, vol. 63, pp. 102-127, 2005.
- [8] D. L. Nelson, Reed, U. S., & Walling, J. R. , "Pictorial superiority effect," *Journal of Experimental Psychology: Human Learning & Memory*, vol. 2, pp. 523-528, 1976.
- [9] D. V. Klein, "Foiling the Cracker: A Survey of, and Improvements to, Password Security," *Proceedings of the USENIX UNIX Security Workshop, (Portland)*, pp. 5-14, 1990.
- [10] V. Roth, K. Richter, and R. Freidinger, "A PIN-entry method resilient against shoulder surfing," *Proceedings of the 11th ACM conference on Computer and communications security*, pp. 236-245, 2004.
- [11] M. Kumar, T. Garfinkel, D. Boneh, and T. Winograd, "Reducing shoulder-surfing by using gaze-based password entry," *Proceedings of the 3rd symposium on Usable privacy and security*, pp. 13-19, 2007.
- [12] X. Suo, Y. Zhu, and G. S. Owen, "Graphical Passwords: A Survey," IEEE Computer Society Washington, DC, USA, 2005, pp. 463-472.
- [13] S. Wiedenbeck, J. Waters, L. Sobrado, and J. C. Birget, "Design and evaluation of a shoulder-surfing resistant graphical password scheme," in *Proceedings of the working conference on Advanced visual interfaces*, Venezia, Italy, 2006, pp. 177-184.
- [14] J. Thorpe and P. C. van Oorschot, "Human-Seeded Attacks and Exploiting Hot-Spots in Graphical Passwords," in *Proceedings of the 16th Annual Usenix Security Symposium*, 2007.
- [15] "Positive Networks, the company, PhoneFactor," <http://www.phonefactor.com>.
- [16] D. Geer, "Security technologies go phishing," *Computer*, vol. 38, pp. 18-21, 2005.

- [17] "SiteKey at Bank of America," in <http://www.bankofamerica.com/privacy/sitekey/>.
- [18] S. Chiasson, R. Biddle, and P. C. van Oorschot, "A second look at the usability of click-based graphical passwords," in *Proceedings of the 3rd symposium on Usable privacy and security* Pittsburgh, Pennsylvania 2007, pp. 1-12.
- [19] "Passfaces, the company," <http://www.passfaces.com/>.
- [20] "e-surveiller," in <http://e-surveiller.com/>: SurveillanceTech LLC
- [21] "RSA, the company, RSA mobile," in http://www.rsa.com/press_release.aspx?id=1506.
- [22] S. G. M Wu, R Miller "Secure Web Authentication with Mobile Phones," in *DIMACS Workshop on Usable Privacy and Security Software*, 2004.
- [23] R. Sharp, J. Scott, and A. Beresford, "Secure mobile computing via public terminals," in *Proceedings of the International Conference on Pervasive*, Dublin, Ireland, 2006.
- [24] M. Mannan and P. C. van Oorschot, "Using a Personal Device to Strengthen Password Authentication from an Untrusted Computer," *Financial Cryptography and Data Security (FC'07)*, 2007.