Assessing the Vulnerability of Magnetic Gestural Authentication to Video-Based Shoulder Surfing Attacks

Alireza Sahami Shirazi[✦], Peyman Moghadam[°], Hamed Ketabdar[*], Albrecht Schmidt[✦]

[✦]University of Stuttgart,
VIS
Stuttgart, Germany
{alireza.sahami, albrecht.schmidt}
@vis.uni-stuttgart.de

[°]Autonomous Systems Laboratory,
CSIRO ICT Centre
Brisbane, Australia
peyman.moghadam@csiro.au

[*]Deutsche Telekom Laboratories,
TU Berlin
Berlin, Germany
hamed.ketabdar@telekom.de

ABSTRACT

Secure user authentication on mobile phones is crucial, as they store highly sensitive information. Common approaches to authenticate a user on a mobile phone are based either on entering a PIN, a password, or drawing a pattern. However, these authentication methods are vulnerable to the shoulder surfing attack. The risk of this attack has increased since means for recording high-resolution videos are cheaply and widely accessible. If the attacker can videotape the authentication process, PINs, passwords, and patterns do not even provide the most basic level of security. In this project, we assessed the vulnerability of a magnetic gestural authentication method to the video-based shoulder surfing attack. We chose a scenario that is favourable to the attacker. In a real world environment, we videotaped the interactions of four users performing magnetic signatures on a phone, in the presence of HD cameras from four different angles. We then recruited 22 participants and asked them to watch the videos and try to forge the signatures. The results revealed that with a certain threshold, i.e, *th*=1.67, none of the forging attacks was successful, whereas at this level all eligible login attempts were successfully recognized. The qualitative feedback also indicated that users found the magnetic gestural signature authentication method to be more secure than PIN-based and 2D signature methods.

Author Keywords

Magnet; signature; mobile phone; authentication

ACM Classification Keywords

H.5.2 Information Interfaces and Presentation: User Interfaces—*Input devices and strategies*; K.6.5 Computing Milieux: Security and Protection—*Authentication*.

General Terms

Experimentation, Security, Human Factors

CHI'12, May 5–10, 2012, Austin, Texas, USA.
Copyright 2012 ACM 978-1-4503-1015-4/12/05...$10.00.

INTRODUCTION

Smart phones are being ever more widely adopted around the world. Besides telephony, many other services are used on modern smart phones, including online banking, and e-commerce. Accordingly, phones store sensitive information such as contacts, communication logs, photos, and navigation histories. Each time a user authenticates and unlocks the phone, access to this sensitive information is granted. Hence, secure user authentication is a crucial requirement. Furthermore, users regularly interact with their smart phones for various purposes such as checking calendars, making calls, etc.. Therefore, authentication mechanism must also be easy if it is to be accepted. Common approaches to authenticate a user on a mobile device include entering a Personal Identification Number (PIN) or a password by means of keypads or touch screens, or drawing a pattern on touch screens. However, these traditional authentication methods are extremely vulnerable to shoulder surfing, as the entire authentication process is visible. Unfortunately, potential solutions to shoulder surfing often decrease the usability of the system. Other options entail further hardware such as eye-trackers [11] for gaze-based authentication or security tokens.

With the wide availability of embedded and hidden video recording technologies, the risk of shoulder surfing has increased significantly. Mobile phones mostly include cameras that can be used for high-resolution video recording. Watches and sunglasses with video recording functionalities are available for less than $100. Security cameras have been mounted in many environments and access to such video feeds may be commonly available. Hence, all of these options enable attackers to videotape the interaction process of users with their phones. With accessing to these videos, the traditional authentication methods such as PINs, passwords, and patterns do not provide the basic level of security, and an attack is simple and straightforward.

In this research, we investigated the vulnerability of a magnetic-based gestural authentication scheme to video-based shoulder surfing and signature-snooping attacks through simulating realistic situations. In a recent work, Ketabdar *et al.* introduced *MagiSign* as a touchless, gesture-based authentication method based on the interaction between a magnet and a device [8]. The idea was inspired partly by the Around Device Interaction (ADI) framework [2,10], which proposes using individual space around the device for interaction with it. ADI has been investigated appropriate interaction techniques for mobile and touch devices. It extends the interaction space of devices beyond their physical boundary, allowing the effective use of 3D space around the device for interaction.

The principle underlying the magnetic gesture technique is that the magnetic field surrounding the device is monitored by a magnetometer (compass). Such sensors are embedded in current high-end mobile phones and used mainly for navigation purposes. Moving a magnet in the peripheral area of a device affects the measured magnetic field sensed by the embedded compass. Thus, the user's hand-movement patterns can be encoded into temporal changes in the magnetic field, captured by the compass sensor. By recording the momentary values of the sensor on different coordinates, a sequence of 3D vectors is obtained, which reflects the temporal pattern of the field's deformation. The sequence is then matched against templates associated with the user's signature. As the magnetic signature is performed in the air (3D), it leaves no trace and is thus highly difficult to forge.

The security of such an authentication method is of considerable importance. We assume that attackers can transparently and cheaply record high-resolution videos in the vicinity of the user, so that authenticating the user by pressing (soft) keys is not secure at all. In order to assess the security of the magnetic-based authentication method, a realistic threat model was set up and a study conducted. The work described in this paper is – to the best of the authors' knowledge – the first attempt at evaluating the resistance of a magnetic gestural authentication method to the video-based shoulder surfing attack. We hypothesize that even with access to optimal video footage of the magnetic signature interaction from various angles, it is still extremely hard to forge the signature.

RELATED WORK

Authenticating users has constituted a challenge for many years and researchers have explored and improved various methods. Current authentication methods can be divided into three main categories: (1) Token based, e.g., a security token generator (2) Biometric based, e.g., fingerprints, and (3) Knowledge based, e.g., passwords. While biometric methods provide a high level of security, they involve costly hardware. On the other hand, in a typical password authentication, because people are used to choosing easy-to-remember passwords, dictionary attacks [13] can succeed. For instance, in a case study of 14,000 UNIX passwords, searching from a "dictionary" of merely $3x10^6$ words revealed almost 25% of the passwords [9]. Preventing dictionary attacks for most techniques leads to a heavy computational load [12] or onerous user requirements that reduce acceptance. Other techniques, such as designing cognitive games [15], adopting strong password policies [4], and using graphical passwords [1,6] appear to be yet other examples of the classic trade-off between usability and security [17].

On mobile devices, user authentication is conducted by weak mechanisms, based mainly on PINs and patterns. In lieu of an alphanumeric password, researchers have examined the feasibility of other authentication schemes [14]. Authenticating a user through his typing characteristics, known as keystroke analysis, is proposed in [3]. However, this requires users to type on the device, which may still be vulnerable to shoulder surfing attacks. *Awase-E* is an authentication method uses photographic images taken by users rather than text-based passwords [16]. The trial-axial accelerometer is also used to capture gestures and authenticate users [5]. By contrast, *MagiSign* uses magnetic patterns for authentication [8]. Having a 3D gesture similar to one's signature can minimise anxiety about memorability.

3D MAGNETIC SIGNATURE

The idea behind the magnetic gesture authentication scheme is to use the embedded magnetic sensor of the mobile phone as a means of authenticating users. A typical magnetic sensor contains a 3D Hall effect sensor that registers the strength of magnetic field along different dimensions. A Hall effect sensor produces a voltage (Hall potential V_H) proportional to the magnetic flux density (B in Tesla), due to the so-called Hall effect. The output from the sensor is provided in the x, y, and z coordinates of the phone. This output can have different ranges depending on the device. For instance, in the iPhone 3GS, the value range is between ±128 μT. Sliding a magnet around the device changes the original magnetic field around the device. Therefore, the temporal pattern of a field's deformation can be obtained by capturing the sensor values on x, y, and z.

In our prototype, in order to define an authentication gesture or magnetic signature (*Sign*), the user arbitrarily moves an appropriate permanent magnet (e.g., a magnetic token/stylus or a magnet in a finger ring) around the device along 3D trajectories. The movement of the magnet produces deformation patterns in the measured magnetic field. Users indicate the beginning and end of each signature by pressing a button. The overall effect of this trajectory on the device/sensor is recorded in the form of a sequence of vectors, with each element containing an instantaneous sample of the sensors values in each coordinate. The input sequence (*Forge*) can then be matched against templates associated with the user's signature. In order to match templates, we use a template matching approach called multi-dimensional Dynamic Time Warping (DTW) [18]. DTW is suitable for measuring similarities between two signal sequences that may vary in time or speed. Popular tree-based classifiers or neural networks in this context require a considerable number of samples in order to provide acceptable resolutions. DTW measures a similarity, which is based on the distance between two sequences and can operate with a limited number of templates and still achieve very accurate results.

As when people sign the 2D signature is varied each time to some degree, in order to define a 3D magnetic signature and check the repeatability, the user is required to enter the signature templates five times ($Sign_t$, t = {1,…,5}). The average distance of all templates is then calculated and used as the main signature ($Sign_d$). If the samples are not sufficiently similar to each other, the user is asked to repeat the procedure. Once the user successfully registers its own personalized 3D signature, the system can be used. In order to login, users have three attempts ($Forge_t$, t = {1,2,3}). For each attempt $Ratio_t = Forge_t / Sign_d$ is calculated. If $Ratio_t$ is smaller than threshold (*th*) the login is successful. The first successful attempt is enough to authenticate the user.

VIDEO-BASED SHOULDER SURFING ATTACK

In general, the degree of shoulder surfing threat depends on the situation. Keypads or touch screens in alphanumeric or graphical passwords are particularly vulnerable, since an adversary can easily obtain a direct view of the interface. For a signature-based authentication method, initial discussions and observations showed that people find it extremely hard to imitate a signature based on a single observation. Hence, in our threat model we have assumed that the user's magnetic signature is videotaped with HD cameras from different angles and the adversary has full access to these videos.In order to compensate the loss of 3D information in 2D videos and also provide more information to attackers, the signing action is videotaped from four different angles: front, rear, left, and right. We used 2D cameras instead of 3D sensors (e.g., Kinect) as 2D cameras are widely available to attackers. To assess the vulnerability of the method to the shoulder surfing attack, the videos are then provided to adversaries to forge the targeted signatures. In addition to the shape of the signature itself, the dynamics embedded implicitly in the temporal samples of the templates establish characterizing properties. It is anticipated that these complications prevent the adversary from forging the signature.

It should be mention that other potential attacks, e.g., 3D path construction or a robot arm for forging the signature might be possible. But it requires great effort and serious engineering. Besides, if an attacker has free access to the phone (e.g., when it is stolen) he has potentially an unlimited number of attempts. To ensure practical security, one would only allow a certain number of tries and/or alternative login mechanisms after certain unsuccessful attempts.

EXPERIMENT

In order to evaluate the security of the technique against video-based shoulder surfing, we implemented a prototype and conducted a lab study. We recruited 22 right-handed participants (50% male) with an average age of 29.3 years (SD = 6.6) from Craigslist. The participants include students, self-employed, or employees.

Apparatus

The prototype consists of a mobile phone with a magnetometer and a PC that runs the authentication software. The magnetic sensor on the iPhone 3GS has a low sample rate and is often saturated. Hence, to obtain more precise information, we used a higher quality external sensor attached to the phone. The SHAKE SK6 [7] sensor senses magnetic fields and transmits data to a PC over a Bluetooth connection. The authentication software on the PC captures the signals and matches them with the signature templates to authorize the user.

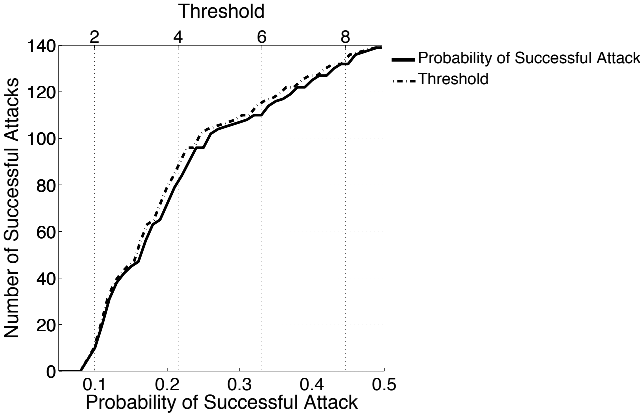

Figure 1: With *th*=1.67 the number of successful attacks is zero and its probability is 0.08 (FP=0, FN=0).

Shoulder surfing video footage

To record the video footage of the magnetic-based authentication, we additionally recruited four users (2 male and 2 female; all right handed with ages between 24 and 45 (SD = 9)). They were asked to define a magnetic signature using the prototype. There was no limitation on the shape or length of the signature, as far as the magnetometer being able to detect the interaction. The interactions were videotaped from the four angles. We also asked the participants to enter their defined magnetic signatures five times. They could practice as many times desired before defining a signature. The average distance between the five samples ($Sign_d$) was used as the target template for the attack. All users used the same magnet to define the signatures.

Procedure

After giving the participants an introduction to the study, we asked them to complete a questionnaire about their demographics and behavior with respect to the use of PINs. We then explained and presented the shoulder surfing attack to the participants. We provide them a short training and all relevant hints for forging, e.g., the phone position/orientation, how the magnet was held, and hands positions. Afterwards, we conducted the experiment. The four videos were shown to each participant who was then asked to forge the targeted signatures. There was no limitation on the study duration and they could watch the videos as many times as desired before trying to forge the signature. They could slow down the videos, too. The order of the videos was counterbalanced. The users used the same magnet as the one used in the video. As the attacks were processed offline, all participants were asked to try all three attempts per each signature, resulted in total 264 attacks. At the end, participants completed the second questionnaire that provided some qualitative feedback about the authentication method, using 5-point Likert scales. The study took approximately 60 minutes per participant and each was paid €20.

RESULTS

We determined the corresponding *Ratio* for all trials. As its histogram shape was close to the gamma distribution, which is the maximum entropy probability, the data was fitted into the gamma distribution ($p < .05$). The number of successful attacks and its probability were calculated by sweeping the threshold (*th*) from 1.22 to 9.02, as shown in Figure 1. The results revealed that, with $th = 1.67$ the number of successful attacks is zero (false positive and false negative rates are also zero) and its probability is 0.08. To evaluate accuracy of authenticating eligible users, we validated all five samples of each defined signature ($Sign_t$) using a 5-fold cross-validation technique. With the same threshold ($th = 1.67$), the results yielded all eligible login attempts were successfully recognized (100% accuracy). It should be noticed that this accuracy is calculated based on a small sample set (4 users each 5 signature templates).

Based on the qualitative feedback, all the participants felt comfortable during the study and found the technique easy to use. 63% of the participants mentioned that it was (very) hard to follow the hand movements of the person in videos. 81% confirmed that it was (very) hard to forge the signature. 78% also believed that the magnetic signature method is a (very) secure method, in comparison to paper signatures and PIN codes.

DISCUSSION & CONCLUSION

The risk of shoulder surfing attacks has increased, as means of recording high-resolution videos are cheaply and widely accessible. If the attacker can videotape the authentication process, PINs, passwords, and patterns do not even provide a basic level of security. Hence, a new and truly secure authentication method is crucial. The reported experiment revealed that even with access to the video footage of magnetic gestural authentications from the different angles, it is still very hard to forge magnetic signatures. Additionally, the system is accurate and very easy to use. The 3D space allows more flexibility in choosing a unique signature than regular 2D signatures. The qualitative feedback revealed that users do not consider PIN-based and 2D signature (paper-based signature) authentications to be sufficiently secure. This technique does not require any change to the physical characteristics or design of mobile devices, relying only on a magnet and an internally embedded sensor.

ACKNOWLEDGMENT

This project is partially supported by the German Research Foundation (DFG) in the Cluster of Excellence in Simulation Technology (EXC 310/1) at the University of Stuttgart.

REFERENCES

1. Biddle, R., Chiasson, S., van Oorschot, P.C. Graphical Passwords: Learning from the First Twelve Years. *ACM Computing Surveys 2011*
2. Butler, A., Izadi, S., Hodges, S. SideSight: multi-“touch” interaction around small devices. *Proc. of UIST’08*, 201–204.
3. Clarke, N.L. Furnell, S.M. Authenticating mobile phone users using keystroke analysis. *Int. J. Inf. Security’06.*
4. DoD. *Department of Defense Password Management Guideline*. Washington, DC: National Computer Security Center, CSC-STD-002-85, 1985.
5. Farella, E., O’Modhrain, S., *et. al*. Gesture Signature for Ambient Intelligence Applications: A Feasibility Study. *Proc. Of Pervasive Computing’06*, 2006, 288–304.
6. Forget, A., Chiasson, S., and Biddle, R. Shoulder-surfing resistance with eye-gaze entry in cued-recall graphical passwords. *Proc. Of CHI’10*, 1107–1110.
7. Hughes S. and O'Modhrain S.. SHAKE – Sensor Hardware Accessory for Kinesthetic Expression. *Proc. of Enactive’06*, pages 155.
8. Ketabdar, H., Yüksel, K.A., Jahnbekam, A., Roshandel, M., and Skripko, D. MagiSign: User Identification/Authentication. *Proc. Of UBICOMM’10.*
9. Klein, D.V. Foiling the cracker: A survey of, and improvements to, password security. *Proc. of the 2nd USENIX Security Workshop*, (1990), 5–14.
10. Kratz, S. ,Rohs, M. HoverFlow: expanding the design space of around-device interaction. *Proc. Of MobileHCI’09*, 4:1–4:8.
11. Kumar, M., Garfinkel, T., Boneh, D., and Winograd, T. Reducing shoulder-surfing by using gaze-based password entry. *Proc. of SOUPS’07*, 13–19.
12. Lin, C.L., Sun, H.M., and Hwang, T. Attacks and solutions on strong-password authentication. IEICE Transactions on Communications, 2001, 2622–2627.
13. Morris, R. and Thompson, K. Password security: a case history. *Commun. ACM 22*, 11 (1979), 594–597.
14. Qibin Sun, Zhi Li, Xudong Jiang, and Kot, A. An interactive and secure user authentication scheme for mobile devices. *ISCAS’08*, 2973–2976.
15. Roth, V., Richter, K., Freidinger, R. A PIN-entry method resilient against shoulder surfing. *Proc.CCS’04*, 236.
16. Takada, T. and Koike, H. Awase-E: Image-based authentication for mobile phones using user’s favorite images. *Proc. Of MobileHCI’03*, 347–351.
17. Tari, F., Ozok, A.A., and Holden, S.H. A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords. *Proc. SOUPS’06.*
18. Ten Holt, G., *et al.*.Multi-dimensional dynamic time warping for gesture recognition. *Proc. of ASCI 2007.*