Orientation Based Accelerometer Analysis (OBAA) for Mobile Gestures

Memorable Authentication

Andrew Holland
Computer Science
Central Michigan University
Mount Pleasant, USA
Andrew.Holland@cmich.edu

Dr. Tony Morelli
Computer Science
Central Michigan University
Mount Pleasant, USA
Tony.Morelli@cmich.edu

Abstract— **Mobile authentication today primarily relies on Personal Identification Numbers (PINs). For PINs to be secure from the majority of malicious users, it must contain a high number of digits and be entropic. Human memory generally struggles when it attempts to recall highly entropic numeric codes. Gesture-based authentication using Quick Reference (QR) codes, and internally analyzed accelerometer data from mobile devices, allow for sustaining a more user-friendly, memorable, and low expense alternative to PINs. This paper presents a technique for users to capture movements of their mobile device by analyzing the orientation of devices and the speed at which these orientations transition via accelerometer data. These motions are described as the user's gesture. Gestures can be used to identify a user, while QR codes can be used to indicate a specific machine a user can attempt to authenticate with. A user study was performed and showed gesture-based authentication results in a more user preferred, entropic and memorable authentication system in comparison to similar applications.**

Keywords-authentication; android; mobile; accelerometer; QR; gesture; human-computer interaction

I. Introduction

User authentication has been a vital issue in verifying access since the inception of user account services. Account services offered to a specific user must have measures for preventing unauthorized access to the provided resources. Plaintext passwords could be applied to mobile devices but it is widely known that users cope to compensate for the inability to memorize alphanumeric sequences [18]. These coping strategies can leave entire sectors vulnerable [12]. Remedies of automated password hashing increase computations on already limited resources [16].

Personal Identification Numbers (PINs) are the dominant form of mobile authentication due to its ease of use and limited resource requirement to authenticate. For a PIN to be secure, it should have a long and highly entropic numeric code. Unfortunately, users also have difficulty remembering long and highly entropic PINs.

Alternatives have been developed that seek to balance the constrained resources of mobile devices while providing a more preferable and secure mode of authentication. Common implementations of these alternatives to PINs include: (a) collecting biometric data; (b) analyzing graphical input, (c) assessing orientation of the device or hand.

Although this application will collect biometric data, it will not collect biometric data that the user could view as critical or invasive such as Deoxyribonucleic Acid (DNA) or fingerprints. It will also lack the guess ability found in [3] and the threat of replication. This system will not require specialized equipment. Instead, it offers an alternative that is implemented with a common mobile operating system, and mobile device.

This paper proposes a system within the spectrum of assessing mobile device orientation using accelerometers. Accelerometers are equipped to an increasing number of mobile devices. Accelerometers are instruments that can measure the physical manipulation and orientation of a device by recording free falling gravitational forces. In this work "gestures" refer to the recordings of these physical manipulations that were created by the Orientation Based Accelerometer Analysis (OBAA).

Rather than focusing on predetermined positions to test or stratify across a single dimensional axis, this research utilizes all directional axes from the accelerometer and allow users to create completely customized gestures that are more secure and usable. Specifically, this paper focuses on the entropic opportunity of analyzed raw accelerometer data, error-rates of authentication sessions, and user preferential scores. This implementation could be used to increase the security of users' mobile devices, and decrease instances forgotten means of authentication.

II. Related Works

The majority of user authentication methods are composed of properties that users poses, e.g. fingerprints [1], palm veins [1], gait [8], [15] and macro and contextual behavioral analysis [9], [21], or what a user knows which includes passwords, or a combination of both which includes speech recognition [1], and touch analysis [2], [6]. These methods can require excessive computation to complete the authentication process which can be taxing on the limited resources of mobile devices. In contrast accelerometer-based authentication does not require extensive computation or form factorization to authenticate to the device.

DOI: 10.5176/2251-3043_5.2.369

© The Author(s) 2017. This article is published with open access by the GSTF

There have been a plethora of implementations specifically designed for improving performance, usability, and memorability in mobile authentication using accelerometers. These projects can be categorized in two distinct groups.

A. Gait Recognition

Gait recognition [8], [15] is the process of assessing accelerometer data and establishing behavioral thresholds which maintains a measure of "trust" to verify if a valid user has access to the device. Though this experiment uses accelerometer data to verify users; it does not extrapolate the data to X or Y axis; rather it records and analyses all axes. This application also commits to repeated single-session authentication while gait recognition as detailed in [9], [16] rely on continuous analysis.

B. Motion-Gestures

There have been two categories of motion-gesture implementations. The first category analyzes the position of the mobile device or customized equipment [4], [11], [13]. The second category analyzes the position of the users' hand [15].

In [4] and [13] accelerometer data is analyzed in short succession allowing single authenticated access. Reference [11] used customized equipment, whilst this study uses common android mobile devices. This study could successfully analyze the intended pre-developed motions. This is done through the analysis of raw accelerometer data as a set of individual positions within the stream to authenticate.

In [14] users were tested on if they could apply proprioceptive analyses on vibrational outputs from the mobile device. They found that users could accurately assess the position of their hand (and thus the device) without being able to see. Though the proprioceptive nature of motion will be relevant in this study; there is a focus on the users' ability to decide the position of the device instead of the device deciding the position of the users' hand.

It is also important to recognize implementations that were developed with the same prerogatives as Gait and Motion gestures but used graphical and physical inputs; which can be categorized in two more distinct groupings.

C. Graphical Free-Form

Graphic based mobile authentication has included graphical patterns [17, 19, 22], and PassShapes [20]. Graphical patterns display a dotted 3x3 grid in which users slide their finger across dots in a dedicated pattern to authenticate. Similarly, PassShapes analyze a predetermined pattern, but allows a blank canvass. It was found in [19] that Android graphical patterns are less secure than 3-digit PINs. In [20] PassShapes are compared with 5-digit PINs as a basis for their memorability and usability study which will be similarly applied in this study. Unlike PassShapes and Graphical patterns which analyze a two-dimensional space this system analyzes three dimensions.

D. Vibrainput

Vibration based input or "vibrainput" [5], [10] operation studies implement another form of motor memory by having the user analyze vibrations for each selected randomized character and only allowing access upon proper selection of vibration pattern pairs associated with each randomized character. Though vibrainput studies compare their authentication with PINs and rely on motor memory from users they do not access accelerometer data or user-hand positions as a basis for authentication.

III. Implementation

The Gesture-Based authentication system consists of a backend server, frontend user interfaces, and an accelerometer analysis algorithm.

A. Backend Server

The Windows Operating system, Apache HTTP server, MySQL database, and PHP server-side scripting (WAMP) web development platform has several functions: 1) hosts the developed authentication scripts, 2) maintains a master log function that tracks all actions which include authentication attempts and outcomes, time-elapsed for authentication process, duration of gesture creation period, username, and the target machine, 3) host a database table that maintains records of users and machines which are referenced to validate a user's attempted access, and unlock a machine's log-in screen upon success.

B. Frontend User Interfaces

The two primary user interfaces are composed of a user log-in screen and a mobile device application.

1) Log-in Screen

The log-in screen posted a quick reference (hereafter: QR) code and the machines names as displayed in figure 1. QR codes are two-dimensional (2-D) matrix codes that belong to a larger set of machine readable code. These types of code are generally referred to as barcodes. These barcodes can be recognized as bars, squares, or other parallelograms; and can store data statically or dynamically. This study utilized a 21x21 QR code that was statically assigned the value of the test machine's posted name; which can be captured by the mobile applications QR reader. The log-in screen was developed using Java SDK 7 within the Eclipse IDE version 4.5.2.

Figure 1. QR code statically assigned "Computer 1"

2) Mobile Application

The mobile application was provided the following functions 1) recording the users' submitted username, 2) recording the accelerometer data, 3) writing the raw accelerometer data to the phone, 4) recording the log-in screens posted QR code, 5) submitting updates to a user's

© The Author(s) 2017. This article is published with open access by the GSTF

accelerometer stream passcodes, and 6) formatting and submitting HTTP post data to the central authentication server. The mobile application was developed using Android development Studio version 1.5.1.

C. OBAA Algorithm

The Accelerometer Stream is the basis of user authentication. The stream is dependent upon recorded accelerometer data from a mobile devices accelerometer. The gesture is the recorded movements, but the accelerometer streams are the algorithms interpretation of the movements. Accelerometers are devices that measures gravitational-force or proper acceleration. Accelerometers observe three directional axes of X, Y, and Z. If the phone is facing the user the X axis runs horizontally, the Y axis runs vertically to the phone, and the Z axis runs to and fro the user. There are eighteen potential positions for each entry of raw accelerometer data which include six positive and negative "basic" directional positions and twelve "cross" directional positions.

This algorithm is dependent on both time-based and orientation-based aspects to create an accelerometer stream. When a user maintains the mobile device in any of the eighteen given positions it will record said position into the accelerometer stream. During the speed in which positions are transposed can change the streams final output. If the user transitions the device from the Z to the Y position in under 0.05 seconds the analysis can record Z then Y, but if the user transitions at a slower pace than 0.50 seconds the analysis algorithm can record Z, ZY, and then Y. This time and orientation based analysis allow greater variance and security to the finalized accelerometer stream.

IV. User Evaluation

The main purpose of this study is to evaluate the usability and feasibility of Gesture-Based authentication.

A. User Study Design

To analyze the near term memorability impact of using gestures in comparison to PINs the study implemented repeated measuring of this experimental design over time. Using this approach, it would be possible to observe the long term impact of using these gestures on memory. There were two distinct groups created from randomly selected participants to compare unique combinations of *method (*user-created gesture) and *implementation* (six distinct gesture system, eighteen distinct gesture system) variables. The combinations included gesture & six-distinctions, and gesture & eighteen-distinctions. The decision to have six distinct character gesture analysis compared against an eighteen distinct character gesture analysis was made in order to have a greater understanding on potential security and usability impact of gesture analysis given more distinct possible characters on the accelerometer stream.

B. Hypotheses

With the perspectives gained on mobile authentication the hypotheses for the study focused on memory, preference, and security which included:

(H1) – Users will prefer using gestures in comparison to PINs.

(H2) – Gestures will be more memorable than PINs and PassShapes.

(H3) – Gestures will have longer accelerometer streams which will be more secure in regards to random entry/dictionary attacks in comparison to PINs.

C. Participants and Setup

For the study, 10 volunteering participants, aged between 20 and 25 (Mean=22) from the general public were randomly assigned to two experimental groups. 10 out of 10 participants stated they had daily mobile device experience.

The study was conducted in a laboratory environment. An HP laptop running Windows 10 and a customized Java log-in application was connected to a 17-inch LCD display with 1600x900 pixel resolution. The users were also provided an LG G3 mobile device with the developed Android gesture-based authentication application. Participants were not compensated monetarily for their participation in each 15-minute session.

D. Procedure

In the study, participants were directed to sit in front of the QR log-in screen and conduct an authentication process which included inputting their username, recording the posted QR code, recording their gesture and sending the data to the server. The collection of both quantitative measurements such as task completion time and qualitative feedback on the users' reactions to the gesture-based authentication system was collected.

The participants in both groups were given a uniform informational sheet that guided them through the process of creating a gesture within the developed Android application. Participants upon completion of creating their gesture, were instructed to memorize their gesture and completed an authentication session. After which they were queried on what strategies, if any; they employed to create their gesture. Afterward, all participants had to fill out a questionnaire collecting demographic data.

After collecting basic information from the participants were requested to re-authenticate with their respective gesture. This measurement was recorded for comparison between memorability after a brief thought provoking activity in attempt to erase their short term recollection of the created gestures. When a participant failed to remember their gesture it was re-displayed to them.

V. Results

Results from the user studies will be discussed within the three primary criterion of preference, memorability, and entropy.

A. Preference

The questionnaire focused on user familiarity, preference, and strategies employed by the users. All users stated that they were "very familiar" or "somewhat familiar" with mobile devices, and personal identification numbers. A total of 80% of the users stated they would prefer the gesture based system instead of personal identification numbers for authentication.

© The Author(s) 2017. This article is published with open access by the GSTF

Some unique strategies noted by users included creating gestures that were culturally relevant (such as the Konami code), or thinking of the gestures as shapes. The majority of the users (60%) stated that the system felt “simple” or “basic,” whilst others (40%) also noted that the system felt “natural” or “familiar” to them when creating and authenticating with gestures so they felt no strategy was needed. Some (20%) stated this feeling as a “muscle memory” moment.

B. *Memorability*

The authentication trial taken immediately after the gesture creation process for the eighteen-character group was 100% whilst the six-character group was 80%. The second user trial taken after the user study questionnaire was completed with the users was steady for the eighteen-character group with 100% but decreased with the second group to 40%.

C. *Entropy*

The average length of the accelerometer streams in the six-character gesture was 4 characters. The average length of the eighteen-character gesture was 6.33 characters. By observing the entropic calculation of E = R^L where E = entropy, R = the range of values, and L = the number of characters within the stream; it should be noted that the average entropy of eighteen-character streams as E_1 = 18^6 = 34,012,224 possible combinations, and the average entropy of six-character streams as E_2 = 6^4 = 1,296 possible combinations.

The average time participants used to execute their gestures for the eighteen-character group was 5.959 seconds; whilst the average time utilized by the six-character group was 5.333 seconds.

VI. Discussion

This study shows promise for hypothesis (H1). By observing the preference data, it was displayed that a large majority of users would prefer to authenticate with gestures instead of personal identifications numbers. When further discussing what strategies were employed many users stated that the natural feeling of the gesture creation process, and authentication sessions aided them in remembering their individual gesture.

At first glance, the memorability of gestures may appear to contrast with hypothesis (H2). The explanation was revealed upon observing the questionnaire and discussing strategies that users employed during the study. All users stated they were “somewhat” or “very” familiar with Personal Identification Numbers. This disparity in familiarity would negatively impact the memorability gesture performance due to low familiarity. Even with this lack of practice the eighteen-character gesture group retained 80–100% memorability of their gestures.

Initial observations on the entropy of gestures displayed the drastic difference in comparative entropy. The average PIN length used in similar studies was 5; which would mean an Entropy of E_3 = 10 ^ 5 = 1,000,000. This would mean that six-character gestures’ entropy is drastically lower than the average PIN length in comparative studies, however, the average eighteen-character gestures’ entropy is far greater than the entropy of PINs as displayed in Table I.

TABLE I. Entropy Calculation of Authentication Systems

Authentication System	Possible Characters (R)	Average Length (L)	Entropy E = R^L
6-character Gesture	6	4	1,296
PIN	10	5	1,000,000
18-character gestures	18	6	34,012,224

This confirms hypothesis (H3), however observation revealed that there was little variation in the average character length between eighteen-character gestures and six-character gestures. Eighteen-character gestures have triple the space of six-character gestures but it the average gesture length of the eighteen-character system was only 150% larger than the average six-character gestures. To understand this peculiarity one would have to observe the transitional space occupied by the two different gestures.

Early in this paper the “basic” and “cross” directional positions were explained. The transition from a “basic” position to a “cross” directional position is described as a single unit of transitional space, and a transition from one “basic” position to another unique “basic” position as a transitional space of two units.

By observing these transitional space changes it was found that eighteen-character gestures length has a 200%–300% increase in character length in comparison to the six-character gesture when their gesture lengths are equivalent. The character length had a minimum of 300% increase when the occupied space of the eighteen-character gesture is double that of a six-character gestures.

VII. Conclusion

By observing the preference of users who have participated in the study, the high levels of comparative entropy, and memorability there is potential to expand on the use of analyzing accelerometer data as another form of authentication in the form of gesture-based authentication that is both preferred by users in comparison to PINs and more entropic.

Whilst other work has implemented authentication systems that rely on biometric or accelerometer data this work contributes an alternative authentication system that can allow account level authentication without recording pervasive data, or require sensitive sensory recognition.

Whilst this study focused on user preference it was limited to a laboratory setting. To gather a more reliable representation of how users would react to the presented authentication system a “in the wild” study should be conducted with a larger sample pool size that includes a larger age range.

This study focused on comparing PINs with gestures, as a potential alternative authentication system a comparative study should be conducted between user created passwords and gestures.

The gesture creation process was also left entirely to the user’s preference. This revealed inconsistencies in the length of gestures. The implementation of standards such as a minimum

© The Author(s) 2017. This article is published with open access by the GSTF

transitional space, or gesture time should be implemented for more consistent results.

Despite these limitations gesture-based authentication provides an opportunity to authenticate with desktops, provide account level authentication with a virtual reality environment, or even provide a more mobility-minded form of authentication for individuals with physical disabilities.

REFERENCES

[1] M. Boatwright and X. Luo, “What do we know about biometrics authentication?” in Proceedings of the 4th Annual Conference on Information Security Curriculum Development, ser. InfoSecCD ’07. New York, NY, USA: ACM, 2007, pp. 31:1–31:5.

[2] W. F. Bond and E. A. Awad, “Touch-based static authentication using a virtual grid,” in Proceedings of the 3rd ACM Workshop on Information Hiding and Multimedia Security, ser. IH&MMSec ’15. New York, NY, USA: ACM, 2015, pp. 129–134.

[3] S. Chowdhury, R. Poet, and L. Mackenzie, “Exploring the guessability of image passwords,” in Proceedings of the 7th International Conference on Security of Information and Networks, ser. SIN ’14. New York, NY, USA: ACM, 2014, pp. 264:264–264:271.

[4] R. D. Findling, M. Muaaz, D. Hintze, and R. Mayrhofer, “Shakeunlock: Securely unlock mobile devices by shaking them together,” in Proceedings of the 12th International Conference on Advances in Mobile Computing and Multimedia, ser. MoMM ’14. New York, NY, USA: ACM, 2014, pp. 165–174.

[5] R. D. Findling and R. Mayrhofer, “Towards device-to-user authentication: Protecting against phishing hardware by ensuring mobile device authenticity using vibration patterns,” in Proceedings of the 14th International Conference on Mobile and Ubiquitous Multimedia, ser. MUM ’15. New York, NY, USA: ACM, 2015, pp. 131–135.

[6] N. Z. Gong, M. Payer, R. Moazzezi, and M. Frank, “Forgery-resistant touch-based authentication on mobile devices,” in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security, ser. ASIA CCS ’16. New York, NY, USA: ACM, 2016, pp. 499–510.

[7] J. Gurary, Y. Zhu, G. Corser, J. Oluoch, N. Alnahash, and H. Fu, “Maps: A multi-dimensional password scheme for mobile authentication,” in Proceedings of the 2015 International Conference on Interactive Tabletops & Surfaces, ser. ITS ’15. New York, NY, USA: ACM, 2015, pp. 409–412.

[8] C. C. Ho, C. Eswaran, K.-W. Ng, and J.-Y. Leow, “An unobtrusive android person verification using accelerometer based gait,” in Proceedings of the 10th International Conference on Advances in Mobile Computing &; Multimedia, ser. MoMM ’12. New York, NY, USA: ACM, 2012, pp. 271–274.

[9] S. Kentros, Y. Albayram, and A. Bamis, “Towards macroscopic human behavior based authentication for mobile transactions,” in Proceedings of the 2012 ACM Conference on Ubiquitous Computing, ser. UbiComp ’12. New York, NY, USA: ACM, 2012, pp. 641–642.

[10] T. Kuribara, B. Shizuki, and J. Tanaka, “Vibrainput: Two-step pin entry system based on vibration and visual information,” in CHI ’14 Extended Abstracts on Human Factors in Computing Systems, ser. CHI EA ’14. New York, NY, USA: ACM, 2014, pp. 2473–2478.

[11] [11] J. Liu, L. Zhong, J. Wickramasuriya, and V. Vasudevan, “User evaluation of lightweight user authentication with a single tri-axis accelerometer,” in Proceedings of the 11th International Conference on Human-Computer Interaction with Mobile Devices and Services, ser. MobileHCI ’09. New York, NY, USA: ACM, 2009, pp. 15:1–15:10.

[12] M. L. Mazurek, S. Komanduri, T. Vidas, L. Bauer, N. Christin, L. F. Cranor, P. G. Kelley, R. Shay, and B. Ur, “Measuring password guessability for an entire university,” in Proceedings of the 2013 ACM SIGSAC Conference on Computer &; Communications Security, ser. CCS ’13. New York, NY, USA: ACM, 2013, pp. 173–186.

[13] F. Hong, M. Wei, S. You, Y. Feng, and Z. Guo, “Waving authentication: Your smartphone authenticate you on motion gesture,” in Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems, ser. CHI EA ’15. New York, NY, USA: ACM, 2015, pp. 263–266.

[14] T. Morelli and E. Folmer. Twuist: A discrete tactile-proprioceptive display for eye and ear free output on mobile devices. In Proceedings of Haptics Symposium 2012 (HAPTICS’12), pages 443–450, Vancouver, Canada, 2012.

[15] M. Muaaz and R. Mayrhofer, “An analysis of different approaches to gait recognition using cell phone based accelerometers,” in Proceedings of International Conference on Advances in Mobile Computing &; Multimedia, ser. MoMM ’13. New York, NY, USA: ACM, 2013, pp. 293:293–293:300.

[16] D. Schmidt and T. Jaeger, “Pitfalls in the automated strengthening of passwords,” in Proceedings of the 29th Annual Computer Security Applications Conference, ser. ACSAC ’13. New York, NY, USA: ACM, 2013, pp. 129–138.

[17] M. Sherman, G. Clark, Y. Yang, S. Sugrim, A. Modig, J. Lindqvist, A. Oulasvirta, and T. Roos, “User-generated free-form gestures for authentication: Security and memorability,” in Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services, ser. MobiSys ’14. New York, NY, USA: ACM, 2014, pp. 176–189.

[18] E. Stobert, “The agony of passwords: Can we learn from user coping strategies?” in CHI ’14 Extended Abstracts on Human Factors in Computing Systems, ser. CHI EA ’14. New York, NY, USA: ACM, 2014, pp. 975–980.

[19] S. Uellenbeck, M. D¨urmuth, C. Wolf, and T. Holz, “Quantifying the security of graphical passwords: The case of android unlock patterns,” in Proceedings of the 2013 ACM SIGSAC Conference on Computer &; Communications Security, ser. CCS ’13. New York, NY, USA: ACM, 2013, pp. 161–172.

[20] R. Weiss and A. De Luca, “Passshapes: Utilizing stroke based authentication to increase password memorability,” in Proceedings of the 5th Nordic Conference on Human-computer Interaction: Building Bridges, ser. NordiCHI ’08. New York, NY, USA: ACM, 2008, pp. 383– 392.

[21] A. W´ojtowicz and K. Joachimiak, “Model for adaptable context-based biometric authentication for mobile devices,” Personal Ubiquitous Comput., vol. 20, no. 2, pp. 195–207, Apr. 2016.

[22] Y. Yang, G. D. Clark, J. Lindqvist, and A. Oulasvirta, “Free-form gesture authentication in the wild,” in Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, ser. CHI ’16. New York, NY, USA: ACM, 2016, pp. 3722–3735.

Authors' Profile

Andrew Holland is an undergraduate Ronald E. McNair scholar currently studying computer science within the computer science department at Central Michigan University, Mount Pleasant.
His research interest are in User Anonymity and Privacy, Cryptographic Ciphers and Network Analysis.

Tony Morelli is an Associate Professor of Computer Science at Central Michigan University. His research areas include gaming and accessibility.

© The Author(s) 2017. This article is published with open access by the GSTF