SHAKEIN: SECURE USER AUTHENTICATION OF SMARTPHONES WITH SINGLE-HANDED SHAKES

D. RAJIV KUMAR[1]
[1] Pg Scholar (M.Sc)
I.KAVITHA JACKLEEN [2]
[2]Associate Professor and Head of the Department
[1] Dept of CSE, Global College Of Engineering And Technology, Kadapa
[2] 1 Dept of CSE, Global College Of Engineering And Technology, Kadapa

Abstract : Smartphones have been widely used with a vast array of sensitive and private information stored on these devices. To secure such information from being leaked, user authentication schemes are necessary. Current password/pattern-based user authentication schemes are vulnerable to shoulder surfing attacks and smudge attacks. In contrast, stroke/gait-based schemes are secure but inconvenient for users to input. In this paper, we propose ShakeIn, a handy user authentication scheme for secure unlocking of a smartphone by simply shaking the phone. With embedded motion sensors, ShakeIn can effectively capture the unique and reliable biometrical features of users about how they shake. In this way, even if an attacker sees a user shaking his/her phone, the attacker can hardly reproduce the same behaviour. Furthermore, by allowing users to customise the way how they shake the phone, ShakeIn endows users with the maximum operation flexibility. We implement ShakeIn and conduct both intensive trace-driven simulations and real experiments on 20 volunteers with about 530; 555 shaking samples collected over multiple months. The results show that ShakeIn achieves an average equal error rate of 1:2% with a small number of shakes using only 35 training samples even in the presence of shoulder-surfing attacks.

I. INTRODUCTION

Computer security (Also known as cyber security or IT Security) is information security as applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term security -- or the phrase computer security -- refers to techniques for ensuring that data stored in a computercannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system. The usage of smartphones is booming in the last decade. Thevigorous growth is due to the powerful computing capabilities,large storage capacity and personal assistance instead of justmaking telephone calls or sending message. The vastfunctionalities and the comfort smartphones provide helpedpeople access their personal information like bank accounts,sending/receiving emails, mobile payment, shopping, photos,stocks through phones.Screen locker is a cardinal utility that prevents smartphonesfrom unintentional/unauthorized operations and secures thepersonal information. The Android phones and the AppleiPhone can lock themselves automatically after being idle for ashort period. This mechanism can protect the privacy of theusers. The existing approaches are password, pattern andbiometric authorization. These approaches are not wellsupported due to deficiency of security. IPhones generally usea four digit password which can be cracked by brute forceattack. Android devices use a nine point geometric pattern.

The short password or simple patterns are easy to use but theyare vulnerable to shoulder surfing attacks. In addition shortpassword and simple patterns can be guessed by the smudgesleft on the screen. Long passwords can be adopted to preventthese attacks but it usually give the users an awful experienceevery time they unlock the phone. Biometrics like fingerprintrecognition, face recognition, voice recognition are being usedbut these unlock mechanism achieve satisfactory performance.

These unlocking mechanism frequently suffer from biometrichacking attacks.In this paper, we propose a secure smartphone authenticationscheme based on user's handshake gestures. A shake cites to a'to & fro' movement of the hand holding the smartphone andswinging/shaking it in X-axis, Y-axis and Z-axis coordinateplane of the device. Different users wave their smartphone in adifferent way. Some wave it gently while others do itdrastically. This makes the waving speed, frequency of shakes,the waving range and the direction of shakes different fromuser to user. These patterns derive the user's distinctivefeatures and styles which can hardly be reproduced by others.

II. LITERATURE SURVEY

D. Smith, J. Wetherall, S. Woodhead, and A. Adekunle [4] proposed security mechanism is essential which keeps document of node's public and private key. While a node forwards a packet to the following node inside the path it generates a random range and encrypts it with the public key of node. Once the two hops lost node obtained this packet it decrypts and send the equal random huge variety as an acknowledgement. Acknowledgement is authenticated with the aid of the node's public key and some encryption method.But the node does not obtained acknowledgment by hops left node and it indict the only hop away node as selfish.

1) A Comparison of Perceived and Real Shoulder-surfing Risks between Alphanumeric and Graphical PasswordsAUTHORS: F. Tari, A. Ozok

Previous research has found graphical passwords to be more memorable than non-dictionary or "strong" alphanumeric passwords. Participants in a prior study expressed concerns that this increase in memorability could also lead to an increased susceptibility of graphical passwords to shoulder-surfing. This appears to be yet another example of the classic trade-off between usability and security for authentication systems. This paper explores whether graphical passwords' increased memorability necessarily leads to risks of shoulder-surfing. To date, there are no studies examining the vulnerability of graphical versus alphanumeric passwords to shoulder-surfing.This paper examines the real and perceived vulnerability to shoulder-surfing of two configurations of a graphical password, Passfaces™[30], compared to non-dictionary and dictionary passwords. A laboratory experiment with 20 participants asked them to try to shoulder surf the two configurations of Passfaces™ (mouse versus keyboard data entry) and strong and weak passwords. Data gathered included the vulnerability of the four authentication system configurations to shoulder-surfing and study participants' perceptions concerning the same vulnerability. An analysis of these data compared the relative vulnerability of each of the four configurations to shoulder-surfing and also compared study participants' real and perceived success in shoulder-surfing each of the configurations. Further analysis examined the relationship between study participants' real and perceived success in shoulder-surfing and determined whether there were significant differences in the vulnerability of the four authentication configurations to shoulder-surfing.Findings indicate that configuring data entry for Passfaces™ through a keyboard is the most effective deterrent to shoulder-surfing in a laboratory setting and the participants' perceptions were consistent with that result. While study participants believed that Passfaces™ with mouse data entry would be most vulnerable to shoulder-surfing attacks, the empirical results found that strong passwords were actually more vulnerable.

2) Password Entry Usability and Shoulder Surfing Susceptibility on Different Smartphone PlatformsAUTHORS: F. Schaub, R. Deyhle

Virtual keyboards of different Smartphone platforms seem quite similar at _rst glance, but the transformation from a physical to a virtual keyboard on a small-scale display results in user experience variations that cause significant divergences in usability as well as shoulder surfing susceptibility, i.e., the risk of a bystander observing what is being Typed. In our work, we investigate the impact of both aspects on the security of text-based password entry on mobile Devices. In a between subjects study with 80 participants, we analyzed usability and shoulder surfing susceptibility of password entry on different mobile platforms (iOS, Android, Windows Phone, Symbian, MeeGo). Our results show significant differences in the usability of password entry (required password entry time, typing accuracy) and susceptibility to shoulder surfing. Our results provide insights for security-aware design of on-screen keyboards and for password composition strategies tailored to entry on smart phones.

3) Smudge Attacks on Smartphone Touch ScreensAUTHORS: Adam J. Aviv, Katherine Gibson

Touch screens are an increasingly common feature on personal computing devices, especially smartphones,where size and user interface advantages accrue from consolidating multiple hardware components (keyboard, number pad, etc.) into a single software definable user interface. Oily residues, or smudges, on the touch screen surface, are one side effect of touches from which frequently used patterns such as a graphical password might be inferred. In this paper we examine the feasibility of such smudge attacks on touch screens for smart phones, and focus our analysis on the Android password pattern. We first investigate the conditions (e.g., lighting and camera orientation) under which smudges are easily extracted. In the vast majority of settings, partial or complete patterns are easily retrieved. We also emulate usage situations that interfere with pattern identification, and show that pattern smudges continue to be recognizable. Finally, we provide a preliminary analysis of applying the information learned in a smudge attack to guessing an Android password pattern.

4) Secure Unlocking of Mobile Touch Screen Devices by Simple Gestures: You can see it but you can not do itAUTHORS: M. Shahzad, A. X. Liu

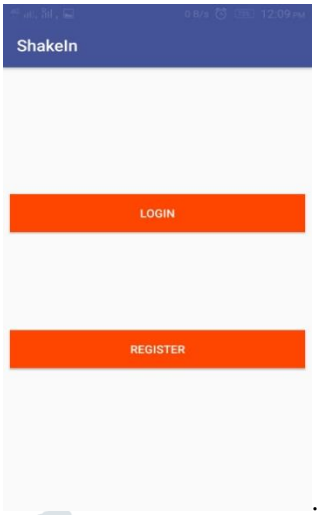
With the rich functionalities and enhanced computing capabilities available on mobile computing devices with touch screens, users not only store sensitive information (such as credit card numbers) but also use privacy sensitive applications (such as online banking) on these devices, which make them hot targets for hackers and thieves. To protect private information, such devices typically lock themselves after a few minutes of inactivity and prompt a password/PIN/pattern screen when reactivated. Passwords/PINs/patterns based schemes are inherently vulnerable to shoulder surfing attacks and smudge attacks. Furthermore, passwords/PINs/patterns are inconvenient for users to enter frequently. In this paper, we propose GEAT, a gesture based user authentication scheme for the secure unlocking of touch screen devices. Unlike existing authentication schemes for touch screen devices, which use what user inputs as the authentication secret, GEAT authenticates users mainly based on how they input, using

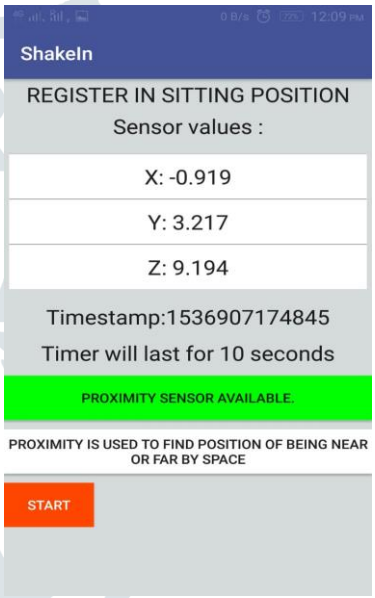
distinguishing features such as finger velocity, device acceleration, and stroke time. Even if attackers see what gesture a user performs, they cannot reproduce the behavior of the user doing gestures through shoulder surfing or smudge attacks. We implemented GEAT on Samsung Focus running Windows, collected 15009 gesture samples from 50 volunteers, and conducted real-world experiments to evaluate GEAT's performance. Experimental results show that our scheme achieves an average equal error rate of 0.5% with 3 gestures using only 25 training samples.

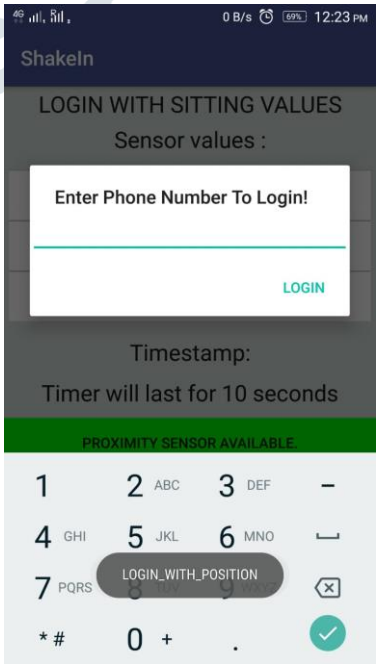
III. SYSTEM MODEL

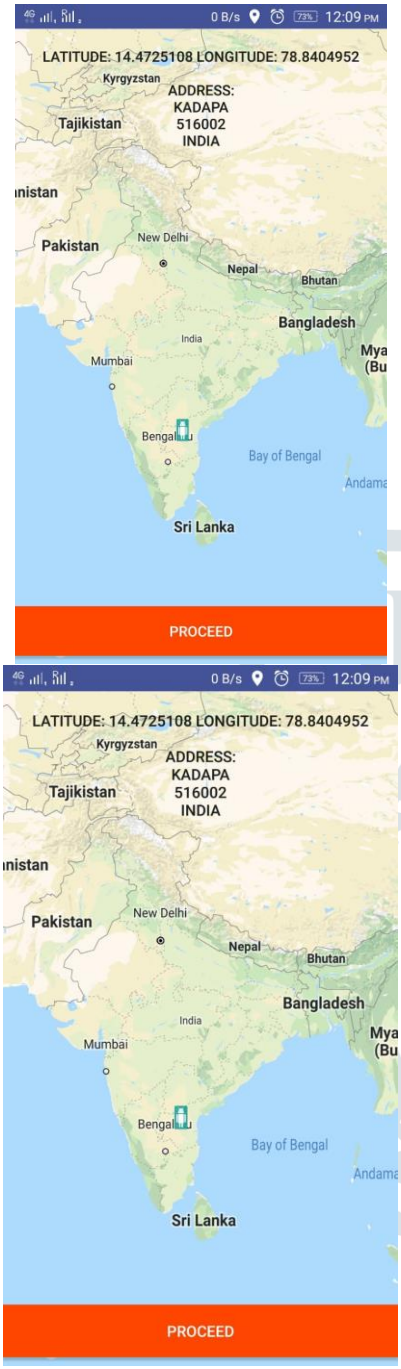
Current behavioural-characteristics-based schemes such as gait recognition, keystroke dynamics and phone usage statistics need an enormous amount of time to determine the legitimacy of a user and have low accuracy. Most recent schemes based on strokes on touch screens can achieve very high accuracy but need two-handed operations which limits its applicable scenarios. OpenSesame and uWave are the two schemes mostly related to our work. OpenSesame allows users to shake or roll their phones with no special requirements and derives four types of geometric features with threeaxis raw acceleration readings. Probability density functions (PDFs) of those feature samples are further used to train classifiers and verify a user. UWave can verify the legitimacy of a user by comparing the time series of three-axis acceleration readings of a testing gesture drawn in the air to a pre-defined template library by employing dynamic time warping (DTW). In this paper, we propose a smartphone user authentication scheme, called ShakeIn, based on customized single handed shakes. A shake refers to a to-and-fro movement with one hand holding a smartphone and swinging the x-, y- and z- axis coordinate plane of the phone around the elbow in the air. In essence, ShakeIn adopts a machine learning methodology, consisting of a training phase and an authentication phase. More specifically, in the training phase, ShakeIn first asks a legitimate user to choose his/her preferred shaking styles and collects a small number of shakes.The key insight behind ShakeIn is that people have consistent and distinguishing physiological characteristics (e.g., the physical structure of the arm) and behavioural characteristics (e.g., shaking behaviour patterns) while doing shakes.

IV. RESULTS&DISCUSSIONS









REFERENCES

[1] European Union Agency for Network and InformationSecurity, "Top Ten Smartphone Risks,"https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks.

[2] F. Tari, A. Ozok, and S. H. Holden, "A Comparison of Perceivedand Real Shoulder-surfing Risks between Alphanumeric andGraphical Passwords," in Proceedings of the second ACM Symposiumon Usable privacy and security, 2006, pp. 56–66.

[3] F. Schaub, R. Deyhle, and M. Weber, "Password Entry Usabilityand Shoulder Surfing Susceptibility on Different Smartphone Platforms,"in Proceedings of the 11th ACM International Conference onMobile and Ubiquitous Multimedia, 2012.

[4] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith,"Smudge Attacks on Smartphone Touch Screens," WOOT, vol. 10,pp. 1–7, 2010.

[5] The Apple Inc., "About Touch ID Security on iPhone and iPad,"https://support.apple.com/en-us/HT204587.

[6] M. Shahzad, A. X. Liu, and A. Samuel, "Secure Unlocking ofMobile Touch Screen Devices by Simple Gestures: You can seeit but you can not do it," in Proceedings of ACM MobiCom, 2013.

[7] J. R. Kwapisz, G. M. Weiss, S. Moore et al., "Cell Phone-basedBiometric Identification," in Proceedings of IEEE Biometrics Compendium,2010.

[8] D. Gafurov, K. Helkala, and T. Søndrol, "Biometric Gait AuthenticationUsing Accelerometer Sensor," Journal of Computers, vol. 1,no. 7, pp. 51–59, 2006.

[9] C. Yuan, X. Sun, and R. Lv, "Fingerprint Liveness Detection Basedon Multi-Scale LPQ and PCA," China Communications, vol. 13,no. 7, pp. 60–65, 2016.

[10] F. Monrose, M. K. Reiter, and S. Wetzel, "Password HardeningBased on Keystroke Dynamics," International Journal of InformationSecurity, vol. 1, no. 2, pp. 69–83, 2002.