Mobile Device based Authentication

Swadhin Pradhan
CS, The University of Texas at Austin, USA

I. Introduction

Smartphones now-a-days are used mainly for surfing the web, checking social networks or playing games than making a phone call, which is only the fifth most frequent activity [5]. This means that users trust their smartphones to store and access sensitive data, ranging from contacts to financial details [3] (indeed 35% use their devices for online banking [2]). Moreover, a typical user now has around 25 accounts but only 6.5 unique [9] but not-so-strong passwords [1] to protect these accounts. At the same time, smartphones are prone to loss: a 2012 report by the Pew Internet Project estimated that nearly a third of cell phone users have had a device lost or stolen [6]. Still 35% of the users do not lock their smartphones [16] which can put all their accounts and sensitive information at risk. The main reason behind this lazy locking behavior is the need of unlocking their devices around 110 times a day [4]. However, users want to preserve their privacy from strangers or family members [3], but they also crave for fewer taps to access their desired information. This eternal trade-off between usability and security can be resolved if we have implicit authentication system powered by higher level of security. So, to solve this, different online services are using two-factor authentication to make the security tighter.

II. Related Work

For unlocking smartphones, people prefer pattern based passwords irrespective of its error rate or longer input time [16]. However, this technique is prone to touch screen based spatial feature based attack or temporal feature based attack [17]. Even oily residues, or smudges, on the touch screen surface, can also reduce the guessing space by around 50% [7]. Shoulder-surfing i.e. looking over someone's shoulder, to get passwords, PINs etc. is also a problem that has been difficult to overcome. At the same time, [12] shows that accelerometer measurements can be used to extract 6-character passwords in as few as 4.5 trials (median), which make text or PIN based passwords vulnerable. So, to counter this, researchers [8] suggested to use smartphone or web activity based questions as authentication challenges which are dynamic by nature but they suffer of false rejection rate. To increase the level of security without compromising the user experience, researchers are thinking to ever-increasing wearable technology. For example, pass-thoughts are used by reading brain signals of users via wearable EEG headsets and authors claim to get around 99% accuracy [10], [14], [15], [13]. Moreover, motion biometrics can be used, similar to vital biometrics. This would require that a smartwatch have a sophisticated motion detector like Apples M7 chip in the iPhone 5S. And to improve two factor authentication, people use the proximity of the users phone to the device being used to log in. Some researchers measure the proximity of the two devices is verified by comparing the ambient noise recorded by their microphones [11].

III. Conclusion

In this report, I discus relevant related works regarding authentication.

References

[1] 2014 splashdata password report. http://http://splashdata.com/press/worst-passwords-of-2014.htm.

[2] 51% of u.s. adults bank online. http://www.pewinternet.org/2013/08/07/51-of-u-s-adults-bank-online/.

[3] Cell phone activities 2013. http://www.pewinternet.org/2013/09/19/cell-phone-activities-2013/.

[4] How often do you check your phone? locket app data shows users unlock smartphone 110 times per day. http://www.idigitaltimes.com/how-often-do-you-check-your-phone-locket-app-data-shows-users-unlock-smartphone-110-times-day-364787.

[5] Making calls has become fifth most frequent use for a smartphone for newly-networked generation of users. http://news.o2.co.uk/?press-release=making-calls-has-become-fifth-most-frequent-use-for-a-smartphone-for-newly-networked-generation-of-users.

[6] Privacy and data management on mobile devices. http://www.pewinternet.org//www.pewinternet.org/2012/09/05/privacy-and-data-management-on-mobile-devices/.

[7] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith. Smudge attacks on smartphone touch screens. In *Proceedings of the 4th USENIX Conference on Offensive Technologies*, WOOT'10, Berkeley, CA, USA, 2010. USENIX Association.

[8] S. K. Dandapat, S. Pradhan, B. Mitra, R. R. Choudhury, and N. Ganguly. Activpass: Your daily activity is your password. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, CHI 2015, Seoul, Republic of Korea, April 18-23, 2015*, pages 2325–2334, 2015.

[9] D. Florencio and C. Herley. A large-scale study of web password habits. In *Proceedings of the 16th International Conference on World Wide Web*, WWW '07, New York, NY, USA. ACM.

[10] B. Johnson, T. Maillart, and J. Chuang. My thoughts are not your thoughts. In *Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing: Adjunct Publication*, UbiComp '14 Adjunct, New York, NY, USA, 2014. ACM.

[11] K. Nikolaos, M. Claudio, S. Claudio, and C. Srdjan. Sound-proof: Usable two-factor authentication based on ambient sound. arXiv, 2015.

[12] E. Owusu, J. Han, S. Das, A. Perrig, and J. Zhang. Accessory: Password inference using accelerometers on smartphones. In *Proceedings of the Twelfth Workshop on Mobile Computing Systems &#38; Applications*, HotMobile '12, New York, NY, USA, 2012. ACM.

[13] S. Pradhan, A. Balashankar, N. Ganguly, and B. Mitra. (stable) virtual landmarks: Spatial dropbox to enhance retail experience. In *2014 Sixth International Conference on Communication Systems and Networks (COMSNETS)*, pages 1–8, Jan 2014.

[14] S. Pradhan, S. K. Dandapat, N. Ganguly, B. Mitra, and P. De. Aggregating inter-app traffic to optimize cellular radio energy consumption on smartphones. In *2015 7th International Conference on Communication Systems and Networks (COMSNETS)*, pages 1–8, Jan 2015.

[15] S. Pradhan, S. K. Dandapat, N. Ganguly, B. Mitra, and P. De. Aggregating inter-app traffic to optimize cellular radio energy consumption on smartphones. In *2015 7th International Conference on Communication Systems and Networks (COMSNETS)*, pages 1–8, Jan 2015.

[16] D. Van Bruggen, S. Liu, M. Kajzer, A. Striegel, C. R. Crowell, and J. D'Arcy. Modifying smartphone user locking behavior. In *Proceedings of the Ninth Symposium on Usable Privacy and Security*, SOUPS '13, New York, NY, USA, 2013. ACM.

[17] E. von Zezschwitz, P. Dunphy, and A. De Luca. Patterns in the wild: A field study of the usability of pattern and pin-based authentication on mobile devices. In *Proceedings of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services*, MobileHCI '13, New York, NY, USA, 2013. ACM.