Authentication through Smartwatch and Smartphone

Swadhin Pradhan, Lili Qiu
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 [13] 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 explicit 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 [13]. However, this technique is prone to touch screen based spatial feature based attack or temporal feature based attack [14]. 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]. 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

This is the conclusion.

REFERENCES