Improving Two-Factor Authentication Usability with Sensor-Assisted Facial Recognition

Tao Yang
Department of Computer Science,
University of Auckland
tao.yang@auckland.ac.nz

***Abstract*—Two-factor authentication is often considered by users as annoying, hard to use and time consuming due to their complexity and implementation - this often leads to users making usability-focused decisions at the expense of security. We believe the development of biometric recognition technology allows for an improvement in the way we implement two-factor authentication systems. In this paper we study the Sensor-Assisted Facial Recognition (SAFR) system and analyze its security and usability compared to current token-based two-factor authentication systems. We believe that the SAFR system can replace and improve the usability of two-factor authentication for use with low-security services while suggesting possible implementations for use in high-security applications. We also highlight key strengths and weaknesses of the SAFR system, and note the innovations SAFR brings to improving the usability of facial recognition while maintaining security. In this way we hope to break down what we believe is one of the key barriers that prevents users using two-factor authentication. We also suggest further avenues of research to improve the usability of facial recognition systems.**

I. Introduction

The usability of security systems needs to be a key focus when designing such systems. It is well known that humans are the weakest link in any system that needs itself to be secure (A key example being the compromising of RSA's master keys via a user failing to recognise a phishing email), and it is important that a user's perception of use and actual behaviour of use need to be considered when the design of security systems are concerned - To quote Avi Douglen [1]:

> "Security at the expense of usability comes at the expense of security "

As security is becoming more of a concern among the general public, there needs to be a significant attempt to make these systems usable and convenient for the user as well as maintaining security. Current forms of fingerprint recognition technology is one such example of design that focuses on usability - A survey run by Bhagavatula [2] found a significant number of respondents who used iPhones also use Apple's Touch ID fingerprint unlock, and a majority of these users using fingerprint unlock out of convenience. Although their implementation of fingerprint unlock had security flaws (a PIN is required as a backup to fingerprint authentication, which can be guessed), such a high rate of use is something that designers of biometric security systems should strive for alongside making their systems secure. One such system where this usability has been significantly more difficult to achieve is with facial recognition.

"Good" facial recognition that properly balances usability and security is difficult to achieve. Bhagavatula [2] found that users of Android face unlock listed poor reliability and the inability to use the feature in low-light situations as key downsides to using face unlock, and even survey participants who had never used face unlock were concerned about the usability of this system. Chen [3] notes that with current facial authentication technology there is a tradeoff between security and usability, and provides two examples. Android face unlock focuses on usability with low precision and complexity, presumably to allow for faster processing; This makes such a system vulnerable to photo attacks - the facial recognition version of a replay attack - where a static image or a video is used to fool Android's facial recognition. Toshiba Face Recognition Utility focuses on security, achieving high precision via a 30 second authentication process - this is significantly longer than a standard login process however, and brings into question why users would use this system over a normal password system that is significantly less complex.

One possible way to reduce reduce the complexity and issues around facial recognition systems while not significantly increasing security concerns is use in two-factor authentication (2FA) systems. 2FA is a system of authentication that relies on two of three factors (Something you know, something you have, something you are) to mitigate issues where only one of these factors are use. Most commonly, services that use 2FA require the something you know and something you have factors - for example, a password and a randomly generated token. However, depending on the implementation of 2FA, this can cause significant usability issues. Fagan [4] found that while a majority of their survey participants use 2FA to increase security, a majority also cited concerns about convenience as to why they did not use 2FA. "Convenience or more specifically the avoidance of the inconvenience of 2FA is a chief concern among those who don't use 2FA". We believe that we must look towards other methods for implementing 2FA that are significantly better in terms of usability.

In this report, we analyze the facial recognition system proposed in Chen et al (2014), and look at possible implementations of this system for the purpose of 2FA. In tests, this system performed comparably to 3D authentication and Android face unlock against various attack models, and was significantly better with respect to the false alarm rate as well as the speed of detection. We analyse and discuss the usability of this system with respect to current literature, and suggest the use of this system as a more user-friendly alternative to current token-based 2FA systems.

II. Sensor-Assisted Facial Recognition

Chen [3] proposes a sensor-assisted facial recognition (hereafter referred to as SAFR) system for smartphones that attempts to solve security concerns in current smartphone facial recognition systems as well as attempting to maintain a high usability for such a system. SAFR uses a combination of standard smartphone sensors to achieve this - a front-facing video camera, an accelerometer, and an ambient light sensor.

During the authentication process for SAFR, a user picks up their phone and moves it horizontally for a short distance in front of their face. The front-facing camera is immediately used to detect and record a video of the user's face. The accelerometer is used to establish that the user is properly moving the phone, as well as tracking movement of the phone to establish movement relative to the video recorded. Finally, the ambient light sensor is used to ensure that light conditions for face capture are sufficient. This system enables analysis of a 3D environment involving the user that wishes to be authenticated, and defends against photo attacks (An attacker showing a photo of the victim to the facial recognition system) which only target the 2D facial recognition capabilities of these systems. The use of an accelerometer in conjunction with video input allows SAFR to track movement of the device relative to the user, and defends against simple video attacks (An attacker shows a video of the victim, an attack which accounts for systems that specifically checks for photo attacks) as movement within the video now needs a corresponding movement of the phone. A extension of the video attack can involve directly streaming video to the device, making the authentication system believe that the video is being captured in real time. This attack is also foiled by the motion sensor part of this system.

SAFR was implemented and tested on a Samsung Galaxy Nexus, which released in October 2011 - it is of note that most users of smartphones nowadays will likely have significantly better phones than this, and this establishes that the system can be used with a wide range of software. With this hardware, detection rates ranged from around 85% at the lowest to 97% at the highest, and a false alarm rate of up to 10%. The best of these detection rates (97% detection rate at 3% false alarm rate) was chosen for further analysis of attack models. The system was tested against photo attacks (pictures printed on paper) and video attacks (videos played from another device), and were compared with results from attacks on Toshiba 3D authentication as well as Android face unlock. These results found SAFR performing less accurately than 3D authentication, but better than Android face unlock against both photo and video attacks. However, SAFR also has a significantly lower false alarm rate, and detection time is significantly faster.

We feel it is necessary to mention here that while the ambient light sensor is used with screen brightness to improve lighting conditions for facial recognition, there is no mention of the testing of SAFR in low light environments or complete darkness. This is a known and key issue with facial recognition systems and was a key concern from participants in [2] when discussing Android face unlock. This is a niche in the consumer facial recognition market most prominently demonstrated by the Windows Hello feature in Windows 10, which uses infrared for light-agnostic facial recognition [5]. Unfortunately, current smartphones do not yet have the infrared sensors required for this style of recognition.

Chen [3] does not suggest any use cases for SAFR, however their system is designed to reduce the tradeoff between security and usability, and demonstrates as such. The restricted hardware requirements of needing input from a video camera as well as an accelerometer, limits the use of such a system to devices such as smartphones that are actually able to make use of these sensors.

III. Concerns with current two-factor authentication systems

Krol [6] presents a comprehensive view of how 2FA is perceived in an online banking environment that requires the use of 2FA tokens across various implementations. The key findings are that user satisfaction significantly decreased as the complexity of a 2FA system increased. User satisfaction concerns around 2FA tokens involved not knowing/understanding the purpose behind hardware tokens, not knowing/understanding how 2FA token systems worked, and a feeling of insecurity despite needing hardware tokens. Some users even specifically avoided using banks that used hardware tokens to avoid associated inconveniences. Similarly, Fagan [4] showed that for three of their four advice topics (Updates, 2FA and Password Resetting), the majority of users that followed this advice did so for the purpose of security, while users mostly chose not to follow this advice more so due to concerns about usability and convenience than concerns about security.

Both Krol [6] and Fagan [4] demonstrate that users will make tradeoffs between usability and convenience where possible regardless of whether the use is compulsory or optional. Facilitating ease of use will help users in compulsory-use situations to more easily access services, and better convince users in optional-use situations to use these systems. Users from Krol [6] gave suggestions as to what their ideal authentication systems should involve - Biometrics (for simplicity, compared to username, password and token based authentication), reduced cognitive and physical effort, a faster and simpler process, and authentication portability (the participants gave the example of a single sign-on system for their computer that involved personal accounts such as their bank accounts). While portability may be difficult to achieve (considering competing services may not wish to cooperate), we believe this presents an opportunity to replace existing token 2FA systems for logging into online services.

IV. Improving current two-factor authentication systems

Google [7] currently has a new form of 2FA called Google Prompt, designed to improve the speed at which users are able to log into their services. Previously, users of Google 2FA were required to input a token code generated on their mobile device as part of the login process, which significantly increased time taken to log in. This new new token-less implementation simply has the user verify on their mobile device whether they intend to log in or not.

We believe a similar process can be used for biometric authentication. Following a user's input of login details into an online service, a mobile device registered to the user can prompt the user to record biometric data, initiating the authentication process outlined in SAFR. In this process, we can actually satisfy all three factors for authentication, and in a way that still takes significantly less time to authenticate than traditional 2FA token authentication. Depending on the security requirements of the application a user wishes to use, we may only need to satisfy two factors for authentication. For example, logging into a low-risk environment such as a user's social network account may only need the "Something you have "and "Something you are "factors - A user would only need to use their registered device to authenticate via SAFR.

As discussed previously in [4], many non-users of 2FA find 2FA systems less convenient (presumably against password input). Fagan and Khan note that participants in their survey were considering a security/convenience trade-off when looking at using 2FA. Similarly, participants in interviews done by Krol [6] wish for faster, easier and simpler procedures of authentication as their ideal procedure - one such suggestion by a participant is the use of biometrics. We believe that in this situation, SAFR is an ideal system for this. SAFR is reasonably fast and accurate considering the hardware used, allowing for its use across a wide range of devices. The speed of SAFR's face recognition is a significant benefit if it is to be used as a part of 2FA - One participant in Krol et al (2015) said they would like a system that takes at most 10 seconds for recognition. The process outlined above would take at most 3 seconds, limited only by the processing speed of SAFR. There is also a possibility for faster processing when higher resolution/frame rate cameras are available, as well as better internal hardware, further reducing this figure. This improvement in the simplicity and speed of this approach will likely motivate more users to pick up 2FA when they feel the convenience/security trade-off is significantly more worthwhile.

V. Discussion and Conclusion

This paper discussed the Sensor-Assisted Facial Recognition system developed by Chen [3] and proposed possible use cases for this technology to replace current forms of two-factor authentication. We believe an opportunity exists to replace some uses of current token-based 2FA forms with the use of SAFR on a registered mobile device, thus reducing the complexity and time cost of using 2FA systems, thus motivating more users to use these systems. When 2FA systems are implemented poorly, complexity of use and time costs are the key reasons why users dislike and/or reject the use of these 2FA systems, as shown in the surveys done by Krol [6] and Fagan [4]. We believe that SAFR can reduce the complexity and time cost compared to current 2FA token systems, and that this can motivate users to make better use of 2FA systems where possible.

Unfortunately, a significant limitation of the SAFR system is how it would be involved when accessing services not on mobile. As SAFR requires a portable camera equipped with an accelerometer, we can not use inbuilt cameras on a laptop or webcams at a PC, as these devices will more likely than not lack the necessary sensors for SAFR. Depending on the security requirements of the service, organizations may also feel that SAFR is not secure enough by itself (whether due to not being an established system, or risk of vulnerabilities in SAFR or the Android platform), and will still require use of a password when logging into services. In situations where use of 2FA is optional, this may still cause perceived inconvenience to the user. While the use of biometrics may allow easier understanding of the purpose of having multiple factors in authentication, users may still feel inconvenienced by needing a second factor, and will refrain from use. This is directly supported by data from Krol et al (2015) which found a negative correlation between the number of credentials required for authentication and the satisfaction with such systems.

It may be possible that the accuracy and precision of SAFR is still not high enough for some organisations' needs. Both Bhagavatula [2] and Krol [6] note that users perceive biometrics to be more secure than standard password authentication, however in practice this is often not the case - Bhagavatula [2] states that "current implementations of biometric authentication cannot be more secure than a PIN because a PIN can always be used as a fallback mechanism". A possible reason for this inclusion is due to a lack of confidence that a facial recognition system can achieve the accuracy and precision required for these fallback mechanisms to not be required; Alternatively, in low-light situations where the device does not recognise its own inability to recognise a user's face properly the user may need to manually override the authentication process. Also note that the tests used in SAFR for comparisons rely on the best case scenario - at worst, SAFR had lower detection rates and had false alarm rates on par with Android Face Unlock. This suggests that more research may be needed to further improve detection rates, and consistently reduce the false alarm rates of detection.

Other issues not directly related to usability or security should also be considered. Bhagavatula [2] noted that their survey participants felt Android face unlock was uncool, draws too much attention, did not want to look like they were taking a selfie, and so on. This is a problem that will not likely have a proper solution, however these downsides can possibly be mitigated by increasing the speed of recognition, or the development of facial recognition techniques that have greater allowances - for example, recognition with a partially obscured face. A increase in prevalence of use of facial recognition systems in the future may also improve social perception of the use of these systems.

We believe that the dated hardware in the original implementation of SAFR allows for further research on improved hardware that may allow for an improvement in the precision of authentication while maintaining a high speed. Alternate avenues of research may also involve looking at a varying level of recognition accuracy and precision depending on how long the system is allowed to process for, or vice versa. If the SAFR system is improved to a level of performance that organizations will be comfortable with using without requiring other credentials, this will be significantly beneficial for organizations and users alike.

REFERENCES

[1] A. Douglen. (2011, August) Xkcd #936: Short complex password, or long dictionary passphrase? [Online]. Available: http://security.stackexchange.com/questions/6095/xkcd-936-short-complex-password-or-long-dictionary-passphrase/6116#6116

[2] C. Bhagavatula, B. Ur, K. Iacovino, S. M. Kywe, L. F. Cranor, and M. Savvides, "Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption," *Proc. USEC*, 2015.

[3] S. Chen, A. Pande, and P. Mohapatra, "Sensor-assisted facial recognition: An enhanced biometric authentication system for smartphones," in *Proceedings of the 12th Annual International Conference on Mobile Systems, Applications, and Services*, ser. MobiSys '14. New York, NY, USA: ACM, 2014, pp. 109–122. [Online]. Available: http://doi.acm.org/10.1145/2594368.2594373

[4] M. Fagan and M. M. H. Khan, "Why do they do what they do?: A study of what motivates users to (not) follow computer security advice," in *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*. Denver, CO: USENIX Association, Jun. 2016, pp. 59–75. [Online]. Available: https://www.usenix.org/conference/soups2016/technical-sessions/presentation/fagan

[5] G. Fritsche, "Understanding windows 10," in *Proceedings of the 2015 ACM Annual Conference on SIGUCCS*, ser. SIGUCCS '15. New York, NY, USA: ACM, 2015, pp. 75–78. [Online]. Available: http://doi.acm.org/10.1145/2815546.2815577

[6] K. Krol, E. Philippou, E. D. Cristofaro, and M. A. Sasse, ""they brought in the horrible key ring thing!" analysing the usability of two-factor authentication in UK online banking," *CoRR*, vol. abs/1501.04434, 2015. [Online]. Available: http://arxiv.org/abs/1501.04434

[7] Google. Sign in faster with 2-step verification phone prompts. [Online]. Available: https://support.google.com/accounts/answer/7026266