Literature Review: Facial Authentication System for the Web

Ryan Collins
Supervisor: Andrei Krokhin

April 12, 2019

1 Introduction

Problem Background Currently, username and password authentication is commonplace throughout the web. However, username and password based authentication systems have a number of problems. Some common passwords can be broken using dictionary attacks, especially if they are a word, or contain a word. Furthermore, the process of shoulder surfing is possible (watching out for someone's password, and how they type it).

An easy to use system is necessary to remove the choice from the user (in terms of password), relying on the user being automatically detected, and several confirmation methods to ensure the user is indeed who they say they are (and not just someone spoofing the system).

Areas of Research One initial consideration is to detect who a specific user is. Some existing measures require further images of a user and require the training of a neural network. While this might work for a small number of faces, this isn't easily scalable.

While one could easily train a neural network to determine whether a given person is present, this isn't scalable. An alternative method would be to instead use a method involving vectorising an image of a face into the key features, and using these features [TL08] However, this could also be done with deep learning using an auto-encoder to generate a vector, that can then be used in identifying the user. [ZLZ15]. This is ideal, because one could then more easily carry out a search through a database using a much more concise vector, compared to the larger Gabor vector that might be produced, or indeed the entire image.

With the given input, how can we be sure that it is original? How can we confirm that the input isn't spoofed, and the person is in front of the camera at the correct time? The solution is to use liveness tests, to ensure that the input is of someone who is alive, and not spoofed.

On just an image, one could use a CNN along with non-linear diffusion. The non-linear diffusion reduces noise and simplifies images for further processing,

while the CNN is then used to classify whether a diffused face image is real or faked. On the NUAA dataset (a set of faked and real faces), an accuracy of 99% was achieved. The CNN used was trained with backpropagation, using the scholastic gradient method, where the pixel value was normalised between 0 and 1. The hyperbolic tangent function was used as an activation function. For classification, a softmax function was used. [AM17]

One method is to carry out pupil tracking. This triggers an LED to light up, and tracks the user's pupil and compares it to the location of the LED. [KTK17] For the web, while this method of using LEDs wouldn't necessarily match up, one could instead use visual indicators within the web browser.

Another method is to use eye blinking. The method proposed uses an ultrasonic sensor, which wouldn't be present for most devices connected to the web. However, alternative computer vision methods could be used. Furthermore, this paper uses a blink pattern as a password, with the user being detected based on the dimensions of their eyes.[Asa+15]

One newer method is known as face flashing. This method involves flashing patterns of light through the user's screen, which can then be detected using camera video. If the user is real, and therefore the video isn't being spoofed, then the light should follow expected parameters. This method has been partially designed to work with Cloud-based computing, and would work fairly well for mobile devices. [Tan+18] While this can't work for all devices (particularly IoT devices that have cameras but not screens), this is a fairly good approximation.

As part of our system, once we carry out the necessary authentication, the system itself needs to tie-in well to other existing web systems. SSO can be used, with the system acting as the single sign on manager. There are various different methods available to do this, such as SAML2, OpenID and OAuth which are the most popular used on the web. The overall goal of SSO is to remove requiring separate IDs and passwords for many systems, instead relying on one single set of credentials. The five key focuses of Identity and Access Management (and the overall goal of SSO) are:

1. Authentication services: check which user is trying to log in. However, IAM suggests multiple methods of auth (rather than just one).
2. Auth Management: what can a user access?
3. Identity Management: Managing the accounts of the users using the service (creating their account, removing their account).
4. Federated Identity: presents third parties with a token for authentication, rather than username/password. All passwords go through SSO portal.
5. Compliance Management: Monitoring and reporting for audits. Check against security standards.

[SSD15]

In terms of security standards, a system for the web needs to follow the required standards to ensure it's fairly secure, especially for the level of data

that's required to be secured. For Identity Proofing (user provides evidence that they are indeed who they say they are), there are three levels: IAL1 doesn't require any link to their real life identity, IAL2 has evidence that a real world identity exists and verifies that the link to this real world identity actually exists, and IAL3 which requires a physical presence for identity proofing. For the authentication process, there are three levels: AAL1 requires either single or multi-factor authentication, and successful auth requires the user to prove possession and control of the authenticator; AAL2 requires two methods of authentication (two factor); AAL3 requires the use of hardware authentication and two distinct methods of authentication. [PF17]

SAML2 has also been researched into using a biometric system before - using fingerprints. This system overcomes the initial security concerns with passwords, by using fingerprints (which can't be as easily guessed or stolen). It was also found however that the client-side nature of such a system also lends itself well to further attacks, due to the necessary transmission of raw biometric data between client and server. [KSR17]

2 Definitions

3 Important Issues of Identified Themes

4 Proposed Direction of Project

Therefore, there is a need for a system that encorporates facial liveness, facial recognition and various other extra security measures together, in a system that is secure for web-based authentication. By creating a service accessible via an API, these system can be used both for web, as well as for IoT devices, which don't necessarily require all the security measures of our system, but they're certainly welcome.

5 Conclusion

References

[TL08] Siu-Hong Tse and K. Lam. "Efficient face recognition with a large database". In: *2008 10th International Conference on Control, Automation, Robotics and Vision*. Dec. 2008, pp. 944–949. DOI: 10.1109/ICARCV.2008.4795645.

[Asa+15] A. Asaduzzaman et al. "Improving facial recognition accuracy by applying liveness monitoring technique". In: *2015 International Conference on Advances in Electrical Engineering (ICAEE)*. Dec. 2015, pp. 133–136. DOI: 10.1109/ICAEE.2015.7506814.

[SSD15] A. Sharma, S. Sharma, and M. Dave. "Identity and access management-a comprehensive study". In: *2015 International Conference on Green Computing and Internet of Things (ICGCIoT)*. Oct. 2015, pp. 1481–1485. DOI: 10.1109/ICGCIoT.2015.7380701.

[ZLZ15] Z. Zhang, J. Li, and R. Zhu. "Deep neural network for face recognition based on sparse autoencoder". In: *2015 8th International Congress on Image and Signal Processing (CISP)*. Oct. 2015, pp. 594–598. DOI: 10.1109/CISP.2015.7407948.

[AM17] Aziz Alotaibi and Ausif Mahmood. "Deep face liveness detection based on nonlinear diffusion using convolution neural network". In: *Signal, Image and Video Processing* 11.4 (May 2017), pp. 713–720. ISSN: 1863-1711. DOI: 10.1007/s11760-016-1014-2. URL: https://doi.org/10.1007/s11760-016-1014-2.

[KSR17] M. Y. Khodabacchus, K. M. S. Soyjaudah, and G. Ramsawock. "Secured SAML cloud authentication using fingerprint". In: *2017 1st International Conference on Next Generation Computing Applications (NextComp)*. July 2017, pp. 151–156. DOI: 10.1109/NEXTCOMP.2017.8016191.

[KTK17] M. Killioğlu, M. Taşkiran, and N. Kahraman. "Anti-spoofing in face recognition with liveness detection using pupil tracking". In: *2017 IEEE 15th International Symposium on Applied Machine Intelligence and Informatics (SAMI)*. Jan. 2017, pp. 000087–000092. DOI: 10.1109/SAMI.2017.7880281.

[PF17] M. E. Garcia P. A. Grassi and J. L. Fenton. *NIST Special Publication 800-63-3 Digital Identity Guidelines*. June 2017.

[Tan+18] Di Tang et al. "Face Flashing: a Secure Liveness Detection Protocol based on Light Reflections". In: *25th Annual Network and Distributed System Security Symposium, NDSS 2018, San Diego, California, USA, February 18-21, 2018*. 2018. URL: http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/02/ndss2018%5C_03B-5%5C_Tang%5C_paper.pdf.