Literature Review: Facial Authentication System for the Web

Ryan Collins
Supervisor: Andrei Krokhin

October 9, 2018

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 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.

[**SSOOverview**]

In terms of security standards, what standards are there? https://pages.nist.gov/800-63-3/sp800-63-3.htmlapproved

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. [**SAMLFingerPrint**]

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