A Framework for Federated Authentication Using the Cloud

Abdulwahid Al Abdulwahid

Centre for Security, Communications and Network Research, Plymouth University

Abdulwahid.alabdulwahid@plymouth.ac.uk

SECURITY WITH PLYMOUTH UNIVERSITY

Introduction

There are 6.8 billion mobile subscribers currently in existence many of which are increasingly utilising smartphones and other devices with a wide range of capabilities. Smartphones are capable of accessing, storing and processing personal, financial, medical and business information that are often considered sensitive and confidential. Therefore, close attention has been drawn to the critical importance in securing them from any unauthorised access. Authentication is a key security control for any computing system, whether that is a PC, server, laptop, tablet or mobile phone. However, authentication is traditionally poorly served, with existing implementations falling foul of a variety of weaknesses. Research has suggested novel approaches to authentication such as transparent authentication and cooperative and distributed authentication. However, these technologies merely focus upon individual platforms rather than providing a universal and federated authentication approach that can be used across technologies and services. This poster utilises the advent of cloud computing, its universal connectivity, scalability and flexibility, which offers a new opportunity of achieving usable and convenient authentication seamlessly in a technology and service independent fashion.

Current Problems

Whilst various methods of authentication exist, they have a variety of drawbacks.

- **Knowledge-based authentication:** They are poorly selected, reused, shared, forgotten, unchanged, or even not used at all.
- **Token-based authentication:** They have higher cost, might need additional reader devices. The user is required to carry multiple tokens for accessing a variety of services.
- **Biometrics-based authentication:** There is a likely need for additional reader devices, so their performance and cost are questionable.
- **Two/Multi-factor authentication:** They combine the downsides of each used authentication method.

Whilst the abovementioned approaches increase the level of security, they degrade user convenience, and remain point-of-entry.

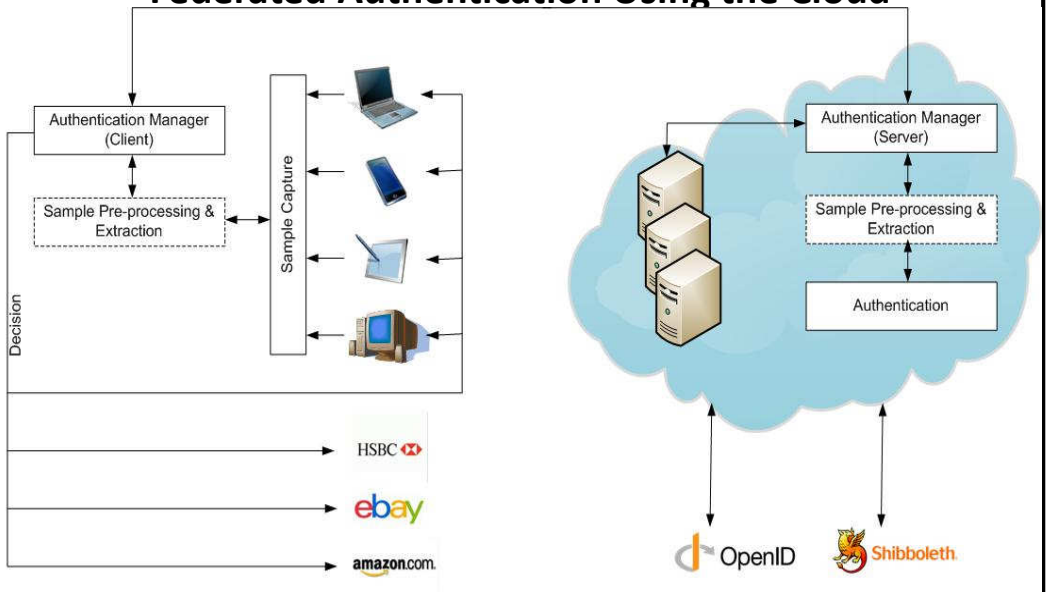
Research has proposed novel approaches, such as transparent authentication (TAS) (Clarke et al., 2011), and cooperative and distributed authentication (Aura) (Hocking et al., 2011). However, they solely focus upon individual platforms rather than providing a universal and federated authentication approach that can be used across different technologies and services.

Current Requirements

With the aforementioned evolution of authentication mechanisms and of digital devices functionality, the proposed authentication approach requires to balance the trade-off between security and convenience by being:

- Continuous
- Transparent
- Universal
- Federated that can be used across technologies and services.

Federated Authentication Using the Cloud



The concept of federated authentication is to centralise the task of authenticating an individual to a trusted third-party provider in the cloud. Through providing a device and service independent authentication approach, the centralised authority benefits from capturing different samples, thus accumulating them and removing duplication as the user no longer needs to enrol and authenticate on and to each device. Instead, the user has a single authentication profile within the cloud authentication manager, where they are able to manage and monitor their profile. Any participated device or service will merely send a request to the cloud authentication manager and be informed of its current real-time identity confidence. Accordingly, the user are allowed access to other devices and services. In this manner, individual devices themselves are relieved of a significant amount of data processing and storage, including a large volume of duplicated activities that would be occurring with TAS and Aura enabled systems.

Conclusion

Verifying the authenticity of a user to use a digital device or service has become crucial. Individuals, businesses and governments undertake an ever-growing range of activities online and via mobile. Authentication is at the vanguard of ensuring only the authorised user is given access; however, it has historically suffered from a range of issues related to the security and usability of the approaches. In order to provide them with adequate protection, innovative robust authentication mechanisms have to be utilised in a universal level, so they operate in a transparent, continuous and user-friendly fashion.

The proposal builds upon existing research on transparent and distributed authentication, with a view of capitalising upon the benefits that cloud computing provide. An authentication system built upon this would provide a more secure, user-friendly, universal and technology independent environment.

Future Work

As this proposed framework evolves, further research will be undertaken to consider human-aspects of security, including the privacy of highly sensitive biometric data and the operational factors that must be incorporated within the architecture to ensure a usable but highly secure system.

References

Clarke, N. (2011). Transparent user authentication: biometrics, RFID and behavioural profiling. Springer London.

Hocking, C. G., Furnell, S. M., Clarke, N. L., & Reynolds, P. L. (2011). Authentication Aura - A distributed approach to user authentication. Journal of Information Assurance and Security, 6(2), 149–156.

Acknowledgments

This proposed framework would not be comprehended without the generous support from my supervisor Dr. Nathan Clarke. I am grateful to be his supervisee.