Topic 22: User identification

George Markham
Reg 100130020
george.markham@uea.ac.uk

October 30, 2018

Abstract

Contents

1 Introduction **2**
1.1 Background and Key Issues 2
1.2 Aim and Objectives 3
1.3 Study Plan 3

2 Literature review **4**

3 Methods **4**
3.1 Usernames & Passwords 4
3.2 Biometrics 4
3.3 Behavioural Biometrics 4
3.4 Alternative Methods 4

4 Analysis and Discussion **4**
4.1 Comparison and Contrast 4
4.2 Evaluation 4

5 Summary **4**

1 Introduction

User identification has become increasingly important with the advent of the internet. Businesses, governments, and the general public are sharing personal, sometimes very sensitive information with trusted parties. The key issue being that word *'trusted'*. How does one prove one's identity to another user or system across the globe?

There are seemingly constantly news stories relating to data theft, last year's Equifax (credit reporting agency) hack could have potentially leaked nearly half the population of the United State's extremely sensitive data (Ng & MUSIL 2017). The amount and the sensitivity of the data held on most of the general population of the world can be incredibly damaging if leaked, it can potentially lead to serious fraud that can have very damaging consequences for people. This data theft can be hindered by using secure ways of identifying and authenticating users. Some of those methods will be discussed in section 3. If implemented correctly they can potentially mitigate the risk of data theft. Some methods of more secure identification are already being implemented, for example companies such as Google, Facebook and PayPal allow the use of Two Factor authentication, where a user augments the security of their username and password by entering a separate code sent to their device (usually a mobile phone). The code adds extra security as a potential attacker is unable to access a user's account and data unless they also have access to the user's phone. These codes are also resistant to brute force attacks as they are only valid for a short amount of time.

For many years we have relied on passwords to authenticate and identify ourselves but passwords are consistently proven to be insecure and unreliable forms of identification. There are, however, alternatives to the username and password method. Smartphones are including biometric identification methods such as using fingerprints sensors and facial analysis. Other methods for identification can also be considered, for example typing habits, mouse use and speaker recognition can all potentially be used to uniquely identify a person.

1.1 Background and Key Issues

The main issue with non-biometric based identification methods is that they are easily forgeable. Take the example of a fingerprint, even amongst identical twins you are still able to be identified with no significant decrease in accuracy (Han et al. 2004). Compare that with the assumption that a password can be known to many different people (either legitimately or illegitimately) then it is clear that biometric identification methods could be superior to traditional username and password methods.

Biometric methods encompass many different ways to identify a user. Sections 3.2 and 3.3 will cover the various methods of using both biometric (fingerprints, iris scanning etc...) and behavioural biometric techniques (typing habits, mouse habits etc...) to identify a user. The usefulness of these techniques varies with the use case, for example it is illogical to attempt to use typing habits to identify a user on a telephone call, equally it is not always feasible to use voice identification when authenticating a user for a website.

Alternative methods will also be discussed including the possibility of identifying a user with real-world documents such as a passport, drivers license or ID card. These systems are already secured against fraud so may be a great candidate for use with computer systems.

In addition to the methods mentioned above there are also public-key encryption algorithms already developed and in use that, although developed for sending encrypted messages, can also potentially be considered forms of identification.

1.2 Aim and Objectives

This study aims to provide evidence that biometric, behavioural biometric and alternative forms of user identification are superior to a traditional username and password based method. To do this the various methods of identification outlined in section 3 will be evaluated using evidence gathered from previous studies to determine their usefulness compared with each other and username and password identification.

1.3 Study Plan

As part of this study the various methods of identification will be compared and contrasted in order to outline their respective strengths and weaknesses. These comparisons will be based on data from past work external to this study. Each technique will be compared to other, similar, techniques and their various merits and weaknesses will be discussed in section 4.

2 Literature review

3 Methods

3.1 Usernames & Passwords

3.2 Biometrics

3.3 Behavioural Biometrics

3.4 Alternative Methods

4 Analysis and Discussion

4.1 Comparison and Contrast

4.2 Evaluation

5 Summary

References

Banerjee, S. P. & Woodard, D. L. (2012), 'Biometric authentication and identification using keystroke dynamics: A survey', *Journal of Pattern Recognition Research* **7**(1), 116–139.

Cazier, J. A. & Medlin, B. D. (2006), 'How secure is your password? an analysis of e-commerce passwords and their crack times', *Journal of Information System Security* **2**(3), 69–82.

Eisen, O. (2017), 'Systems and methods for user identification using graphical barcode and payment card authentication read data'. US Patent App. 15/473,026.

Han, Y., Ryu, C., Moon, J., Kim, H. & Choi, H. (2004), A study on evaluating the uniqueness of fingerprints using statistical analysis, *in* 'International Conference on Information Security and Cryptology', Springer, pp. 467–477.

Lanitis, A. (2009), 'A survey of the effects of aging on biometric identity verification', *International Journal of Biometrics* **2**(1), 34–52.

Morris, R. & Thompson, K. (1979), 'Password security: A case history', *Communications of the ACM* **22**(11), 594–597.

Ng, A. & MUSIL, S. (2017), 'Equifax data leak may affect nearly half the us population'. **URL:** *https://www.cnet.com/news/equifax-data-leak-hits-nearly-half-of-the-us-population/*

Notoatmodjo, G. (2007), Exploring the'weakest link': A study of personal password security, PhD thesis, Citeseer.

O'Gorman, L. (2003), 'Comparing passwords, tokens, and biometrics for user authentication', *Proceedings of the IEEE* **91**(12), 2021–2040.

Yampolskiy, R. V. & Govindaraju, V. (2008), 'Behavioural biometrics: a survey and classification', *International Journal of Biometrics* **1**(1), 81–113.