A New Model for Accessing Distributed Systems by Using Fingerprint as a Password

Sara Jeza Alotaibi, Dr. Mike Wald, Dr. David Argles

Learning Societies Lab / School Of Electronics and Computer Science / University Of Southampton

Southampton / United Kingdom

sja2g09@ecs.soton.ac.uk , mw@ecs.soton.ac.uk , da@ecs.soton.ac.uk

Abstract

It is recognised that, how things stand at present, distributed systems in general and the internet specifically do not benefit from adequate security systems, with password-based methods deemed insufficient. Furthermore, with this particular approach, users are required to remember many different passwords-with individuals commonly required to have 15-20 different details to memorise. Accordingly, the need is raised as to how a more efficient and reliable method can be implemented which does not rely on a sequence of characters, but which rather on a unique technology utilised only by the individual. With this in mind, it is noteworthy to acknowledge that there are already such services in application, but which are nevertheless viewed as being inadequate under such circumstances. Essentially, it is recognised that there are three fundamental criteria needing to be fulfilled by internet users: convenience and ease of use; freedom from memorising many passwords; and security. With these in mind, this study seeks to provide a solution to these issues through the implementation of system: FingerID. Accordingly, this paper seeks to provide a significant contribution in the fact that it has the potential to transform the way in which security over the internet is achieved.

1. Introduction

Technology has undergone significant developments and changes during recent years has induced a very hi-tech era for vast populations across the globe, but has also ultimately created a number of different opportunities for crime-related behaviours to be carried out. Importantly, this has subsequently introduced the need to ensure safe, secure and sophisticated ways of ensuring the identification of users when granting access, thereby providing stronger, more robust ways of ensuring sensitive and confidential data remain protected, all of which are geared towards ensuring web communities and online users are safeguarded from malicious activities. With the aforementioned in mind, it is noted that users are commonly susceptible to various online attacks, such as identify theft and phishing, both of which the majority of online users have, at one time or another, experienced [1]. Accordingly, it is recognised that laws and regulations will need to consider providing online users with a greater degree of online protection through the facilitation and application of identity recognition systems.

Importantly, it should also be recognised that users are commonly holding more and more accounts online. This was considered during the conduction of a survey which targeted a sample of 79 internet-using individuals of different ages and both genders. The survey was made available through both online and offline portals[1], with the respondents asked how many online accounts they held; as a result, it was established that 44% of all internet users hold more than 15 online accounts. Taking this into account, it can then be seen that internet users are going to face a number of different issues when trying to remember all user details for their online accounts.

With the above discussion taken into account, the unique personal identification system has a foundation of three key factors: the introduction of one online identification program; the application of biometric identification system, namely fingerprint ID; and a unique recognition system for each online account holder, such as FingerID, which provides high levels of accessibility, security and usability.

This study is broken down into various sections: the first section provides a theoretical overview of the topic at hand; secondly, a summary of the considerations to be taken into account will be provided; thirdly, the FingerID system will be considered; and finally, the fourth section will provide a conclusion of this study, along with recommendations for future researches.

[1] It was made available from April 5, 2010 to May 5, 2010 at <http://qtrial.qualtrics.com/SE/?SID=SV_7NInQmVL928SDQM&SVID>.

2. Current Considerations

With the use of various protocol—such as Liberty Alliance, SAML, Shibboleth, and WS Federation [2]—a security assertion token to distributed systems will be provided through a Single Sign-On (SSO) system. Accordingly, this SSO software will obtain the token, carry out a verification check, and accordingly provide the user with permission to gain access to their online accounts—and all without the need to actually sign-in [2]. However, it should be noted that, thus far, very little research has been focused on this arena and the potential replacement of more traditional username/password security methods, although it has been acknowledged that password-based methods are inadequate when striving to provide online protection. In this regard, it can be stated that this commonly utilised system is out of date, and ultimately does not provide users with the required level of protection necessitated by modern-day technological developments. Importantly, malicious users, i.e. hackers and intruders, have also become more advanced and learned in their methods [3]. With this in mind, it is also important to highlight that various methods introduced with the aim of providing better accessibility, security and usability have been inadequate for one reason or another, as can be seen when considering three fundamental criterion detailed in Table 1 below:

Table 1: Summary of comparison with similar applications

Current Applications	Level of security	Level of accessibility	Level of usability
OpenID	✓ [8]	✗ [12]	✗ [13]
Shibboleth	✓ [7]	✗ [14]	✗ [14]
OAuth	✓ [2]	✗ [16]	✓ [15]
Liberty Alliance	✗ [17]	✗ [17]	✓ [18], [19]
Microsoft Passport	✗ [20], [21]	✓ [9], [10]	✓ [11]

As can be seen from the above table, it is necessary for online users to establish different behaviours, i.e. to disassociate themselves with the need to remember long passwords [4]. Furthermore, it should also be recognised that, thus far, there has been no software introduced which corresponds with the characteristics and level of originality established through the proposed FingerID system. Accordingly, in this regard, previous studies focus on the aim of ensuring log-in and maintenance processes are more accessible, secure and usable to users. With this in mind, the research question in this study is: 'What process provides online users with access to a number of different systems through one accessible, secure and usable platform?'

Importantly, the systems previously introduced and the one proposed in this paper have been reviewed and considered in mind of the criteria established thus far, i.e. accessibility, security and usability. It was with such criteria in mind—with attention to how the entire process of logging in could be achieved without needing to remember a number of different usernames and passwords—that the idea of FingerID was first born.

3. Proposed Solution: FingerID

Computer-related technologies have undergone a great deal of advances and developments during recent years, with progressions reaching the stage of more natural elements being considered for security and authentication purposes. With this in mind, it is recognised that nature provides one very important characteristic in all of its creations: individuality; this can be seen when considering a number of different features, including eye colour, DNA signature, facial image, palm print and voice, etc. [5]. With this in mind, as of early days, fingerprints have been recognised as being one of the most fundamental and valuable ways of establishing an individual's identity. Advantages include that the necessary component, i.e. the fingerprint, is convenient to use, readily available, and unique, thereby providing 'accuracy, size, cost, performance and proven track record' [6], [5]. Importantly, such features are known as biometrics, with the FingerID platform, in this regard, known as a biometric authentication system [6]. This particular solution noted in this paper recognises and discusses the advantages of this software, which is notably more secure and easily managed than other security tools.

The FingerID solution provides users with the ability to maintain a number of different online accounts without the requirement to memorise a number of different log-in details. This particular solution overcomes the common problem associated with holding numerous accounts and passwords, which is that different information may be assigned to different accounts, thereby increasing the likelihood of forgetting important data.

Accordingly, it can be seen that such information may be difficult to remember, thereby increasing the vulnerability of such accounts. However, FingerID overcomes this problem, and similarly provides the ability to update and delete data, which provides users with the ability to ensure information remains up-to-date. Furthermore, it is also recognised that users are commonly required to fill in forms and account request information, which can be both tedious and time-consuming. In this regard, FingerID also eradicates this issue by communicating the user's details to the service provider in question.

Notably, the overall research scope in this regard is centred on three different values: firstly, other on-going researches; a live project concerned with the introduction of a solution; and field-testing. With these principles in mind, this research is further supported through hard techno-economic analysis, which provides insight into the overall commercial viability of the proposed solution.

As has been discussed thus far, the concept of FingerID considers two different elements from a human standpoint: firstly, the fingerprint is scanned from the person; and secondly, the service is utilised through human interaction. Accordingly, for the purpose of the research study, a HCI theory has been amended and applied whereby a combination of design research and scientific research has been implemented [22].

3.1 Four-Tier Architecture

The FingerID solution has four different levels representing each of the fundamental stages of the identification process, namely client, interface, control and distribution. Notably, each of these levels has been both developed and adopted. With this in mind, the figure below highlights the way in which the system framework has been created, which works as the foundation for the authentication of the fingerprint system and subsequent access of online accounts.

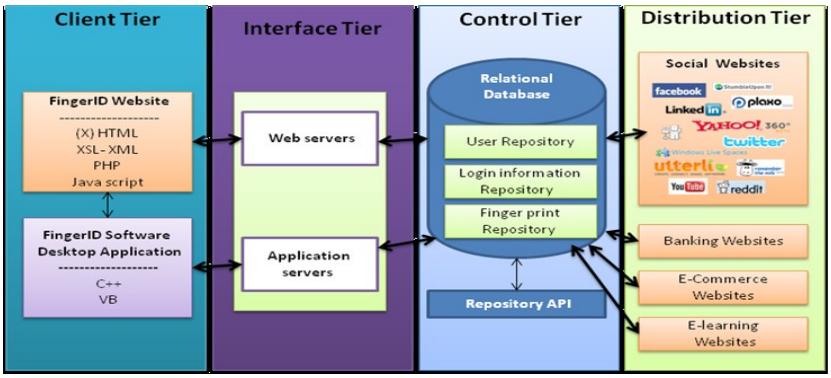

Fig.1: 4-Tier architecture of FingerID

3.2 FingerID Token Exchange Description

FingerID token exchange description diagram is given below:

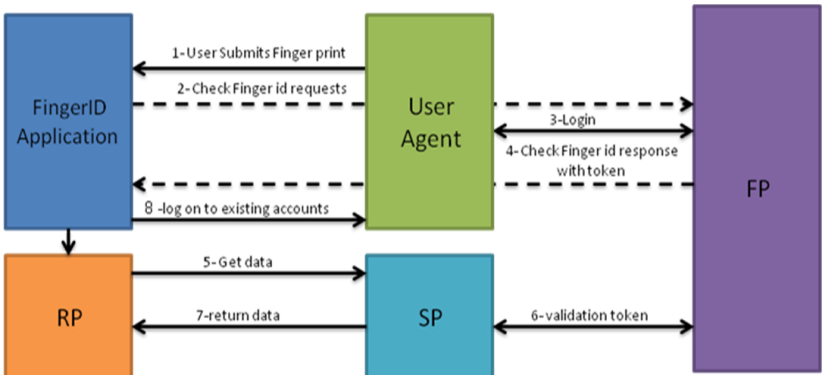

Fig.2: Token Exchange Protocol

The entities in Figure 2 have the following meanings [23]:

- **RP (Relying Party):** This entity is responsible for acquiring the identity of the user. The main objective of RP is to verify the user so that he can gain the desired access.

- **User Agent:** This is typically a web browser. The user in this component is defined as the individual who has a digital identity and who participates in the exchange of data with the aid of the client software.
- **SP (Service Provider):** SP is responsible for providing the service to the verified users. This verification is achieved with respect to a token issued by the FingerID provider (FP).
- **FingerID Provider (FP):** This serves as a FingerID authentication server that transmits confirmation to RP about the possession of the identifier by the user.

3.3 FingerID Design

The FingerID system has been created in such a way so as to require the user's fingerprint to be provided and scanned during initial use of the system, thereby facilitating system registration. Following the completion of this process, the user—who is then classified as a member—is able to gain access to the numerous accounts held, with such permission provided through the utilisation of one sole system. The system registration is a process the user only needs to go through once; subsequent scans will be carried out only for the purpose of user authentication.

Importantly, the system comprises two main components: the software (browser) and website. This website is hosted on an online server dedicated for this purpose, utilising Windows XP with MySQL 5.1.4 and PHP 5.3.1. With this in mind, the figure below highlights the flowchart of the FingerID model, and further shows a screenshot of the system during its utilisation.

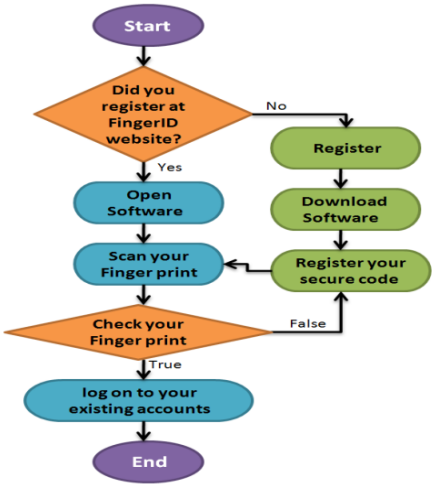

Fig.3: FingerID Flowchart

Fig.4: FingerID Browser and FingerID Website

When the system is live and running, a user community has been determined[2]. This situation has been tested through various means: accessibility, usability and security were established through lab testing; and user

[2] Details can be found at <www.fingerid.me>.

satisfaction was also determined. In order to carry out such testing, a model of an empirical operational nature was created, the results of which were reviewed and analysed through the utilisation of appropriate statistical tools. These tools—in addition to the results achieved through such—will be further considered in future studies.

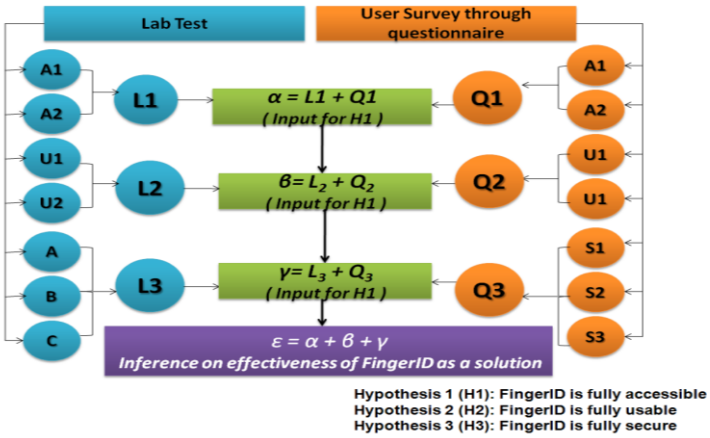

Fig.5: Operational Model for research

4. Conclusion and Suggested Future Work

Internet users usually opt for fairly simple username and password combinations owing to the large number of accounts held online; however, such an approach means that their accounts are vulnerable to attacks, hacking and intrusion. Moreover, it has also been noted that users commonly utilise the same usernames and passwords for a multitude of account, which also enables intruders to gain wide-ranging access to a number of accounts, with the information held in such potentially utilised for malicious reasons. However, the proposed FingerID solution is recognised as heightening security owing to access being granted on the unique fingerprint of the user. Such a security measure means that access is much more difficult to gain without authorisation, particularly when compared to standard username and password methods.

With the aforementioned in mind, FingerID seeks to prove internet users with a greater level of protection and convenience owing to the fact that there will no longer be the need to memorise a number of different usernames and passwords for various accounts. Furthermore, the FingerID solution has been created with the overall aim of increasing levels of security for online users.

There are a number of different recommended strategies which can be adopted by websites in order to improve the overall accessibility, security and usability of the internet for users; however, it should be acknowledged that very few websites adhere to such. With this in mind, however, FingerID seeks to overcome this problem and provide users with the ability to make use of an application which provides all the necessary accessibility, security and usability measures. In this regard, FingerID has tested all of these individuals elements through the conduction of a number of different activities.

Importantly, this solution is able to provide users with an accessible and secure way of utilising online accounts. With this in mind, it is clear that this study has succeeding in providing a revolutionary means of online authentication. Importantly, this solution provides the user with the ability to gain access through fingerprint scans; notably, additional biometric measures—such as face gestures and palm prints—may be an aim for future development.

References

[1] Miniwatts Marketing Group, “Internet World Statistics”, *World Internet Users and Population Stats*, 2009.

[2] Z. A. Khattak, S. Sulaiman, L. A. Manan, “A Study on Threat Model for Federated Identities in Federated Identity Management System”, *Information Technology (ITSim), 2010 International Symposium,* IEEE, Kuala Lumpur, 2010.

[3] Science News, "Smart Methods for Detecting Computer Network Intruders”, *Science Daily,* 2002.

[4] J. M. Williams, “New security paradigms”, *Proceedings of the 2002 Workshop on New Security Paradigms*, Virginia Beach, Virginia, 2002, pp. 97-107.

[5] Z. Riha and V. Matyas, “Biometric authentication systems”, *FI MU. Report Series, FIMU-RS-2000-08*, 2000.
[6] M. McGinity, “Staying connected: Let your fingers do the talking”, *Communications of the ACM*, vol. 48, no. 1, 2005, pp 21-23.
[7] R. L. Morgan, S. Cantor, S. Carmody, W. Hoehn, K. Klingenstein, “Federated Security: The Shibboleth Approach”, *Educause Quarterly*, vol. 27, no. 4, 2004, , pp. 12-17.
[8] T. DiVito, “OpenID: A Potential Authentication Technology”, *Decision Line,* School of Business-Camden, Rutgers University, Newark, USA, 2008.
[9] S. Baklanov, “Security models in ASP.NET. Authentication”, *XLineSoft*, 2005.
[10] D. Shinder, “How to Use Microsoft’s Shared Computer Toolkit”, *Window Security,* TechGenix Ltd, 2005.
[11] R. Oppliger, “Microsoft .NET Passport: A Security Analysis”, *IEEE Computer Society Press*, Vol. 36, Issue 7, Los Alamitos, CA, USA, 2003, pp. 29-35.
[12] B. Ferg et al., *“*OpenID Authentication 2.0—Final”, *OpenID Community*, Dec. 2007; http://openid.net/specsopenid-authentication-2_0.html . [Accessed the 15th of January 2010, 11:15]
[13] J. Zhou, “OpenID usability is not an oxymoron”, *FactoryCity*, 2008.
[14] C. Joie, “Understanding Shibboleth- SLO Issues”, *Internet2,* 2010.
[15] M. Engel, “MySpaceID Usability Testing”, *Slide Share.net*, MySpace, 2009.
[16] “Accessibility issues of social Web”, *W3C*, 2010; http://www.w3.org/WAI/PF/wiki/Social_Web#OAuth_Accessibility_Issues. [Accessed the 15th of January 2010, 11:15]
[17] P. Judge, S. Shankland, “Liberty - is usability compatible with security?”, *ZDnet US*, July 2002; http://www.zdnet.co.uk/news/servers/2002/07/16/liberty-is-usability-compatible-with-security-2119220/ . [Accessed the 15th of January 2010, 11:15]
[18] T. Skytta, “Liberty Alliance Completes Two Projects Based on their ID-WSF”, *Sun Security,* vol. 73, issue 5, 2004.
[19] H. Mikkonen, M. Silander, "Federated Identity Management for Grids," *icns, International conference on Networking and Services (ICNS'06),* USA, 2006, pp.69.
[20] W. Redmond, “Microsoft Passport: Streamlining Commerce and Communication on the Web”, *Microsoft News Center*, 1999.
[21] K. Choo, “Issue report on business adoption of Microsoft Passport”, *Information Management & Computer Security*, Emerald Group Publishing Limited, vol. 14, issue 3, 2006, pp. 218-234.
[22] W. E. Mackay, A. L. Fayard, “HCI, Natural Science and Design: A Framework for Triangulation across Disciplines”, *DIS'97: Designing Interactive Systems* (August 18-20) ACM: Amsterdam, pp. 223-234, 1997.
[23] L. Kolas, A. Staupe, “A personalized E-learning Interface”, *In: EUROCON 2007 The International Conference on “Computer as a Tool”,* IEEE Xplore, 2007, Warsaw , pp. 2670—2675.