FingerID: A New Security Model Based on Fingerprint Recognition for Distributed Systems

Sara Jeza Alotaibi, David Argles
Learning Societies Laboratory, University of Southampton, United Kingdom
sja2g09, da{@ecs.soton.ac.uk}

Abstract

The current practice of password based security for distributed systems in general and the Internet in particular is inadequate. Besides, remembering a plethora of long passwords and pass phrases sometimes as many as 15 or 20 is cumbersome .This raises the need to introduce a better and more reliable authentication mechanism which is not dependent on a series of characters, but rather on a technology that is unique and only possessed by the individual. Similar services already exist, and they are good in some situations, but prove to be inadequate under other circumstances. Overall, three main requirements of the everyday Internet user remain unaddressed – freedom from memorizing many passwords and pass phrases; convenience and ease of use; and security. The present paper attempts to offer an answer to all these problems by just one solution, named FingerID. The contribution of this study is of considerable significance, as it would revolutionize the way Internet security is managed.

1. Introduction

The invention of the Internet is one of the most revolutionary of the 20th century [1]. The Internet has changed our lives, and continues to do so with new technologies being introduced all the time. However, it is also one of the most potent weapons in the hands of the wicked.

Terrorism, money laundering, drug trafficking and gunrunning coordinated through the Internet are just some of the malevolent manifestations. A lesser evil but more widespread is the financial frauds ingeniously orchestrated over the Internet by breaking into the security system and spiriting away the hard earned money of many innocent victims [2]. Phishing and Identity theft are some of the attacks that every online user of the 1.8 billion-population of Internet users [35] must have come across. These security threats to the personal information of Internet users raise the need for improved security measures and authentication mechanisms so that intruders can be discouraged.

Another hitch that humans have inherited from the use of the Internet is the maintenance of the great number of accounts held by the Internet users. A survey was carried out through a previous research study regarding the number of accounts held by Internet users. The sample of the survey comprised random Internet users of different age groups. The question concerning the number of accounts provided different choices: less than 5 accounts; less than 10 accounts; less than 15 accounts; 15 accounts and more. The results of the survey revealed that 44% (highest rank) of Internet users have more than 15 web accounts. Such an Internet user will face great difficulty in remembering log-in details for his web accounts, along with the personal details that are given.

A simple solution that might come to one's mind is to maintain the same username and passwords for all the web accounts maintained on the web. However, such an approach is never advised, since it increases vulnerability of information, and therefore makes it easy for the intruder to attack all web accounts [3]. A similar solution is to keep easy passwords [4], but this approach also makes intrusion more achievable for malicious users. On the other hand, long and complex passwords seem like a good solution, but it would ultimately prove to be impractical for Internet users to remember [5].

2. Proposed Solution

Extensive studies are underway in the field of computer technology with the objective to overcome the problems that have been discussed in the preceding section. Some ideas have already been implemented so as to enhance security over the Internet; some of them are IPsec Protocol [10], [11], Pretty Good Privacy (PGP) [13], Multipurpose Internet Mail Extension (MIME) [12], Secure/Multipurpose Internet Mail Extensions (S/MIME) [14], Circuit-Level Gateways [15] and Application-Level Gateways [15].

However, not much work has so far been carried out to replace the conventional form of authentication of username and password on the World Wide Web. This authentication mechanism prevailed for many years, but the needs of the current times do not coincide with its application [7]. The current times require greater convenience and enhanced security, simply because the intruder has become very smart and technologically savvy [6]. There is now the need for Internet users to break the relation between long passwords and their obligation to remember it [8]; therefore we began with the concept of a service that would maintain web accounts for the user rather than the user going through the ordeal. Similar services already exist, but each has their limitations and drawbacks.

Computer technology has improved so much that natural features are now being used for authentication. These natural characteristic are termed as 'biometric', and the systems that make use of such features in terms of providing access to respective users are known as biometric authentication systems [9]. The biometric of fingerprints has been chosen for the authentication purpose of FingerID.

Both existing, and our proposed, systems were evaluated against the criteria of Security, Accessibility and Usability. Accordingly, an idea was generated which would fundamentally alter the entire authentication mechanism; replacing memorised passwords with fingerprint data. This laid the foundation for FingerID - a service to maintain multiple web accounts with the user's fingerprint.

2.1. FingerID

FingerID provides the user with the facility to maintain multiple web accounts from a single source without the concern of having to remember multiple credentials. It is also a common practice to give away differing information on the web and to then forget which information has been revealed to which website. This makes information vulnerable and difficult to update. FingerID solves this problem by making itself the single source where information of the user will be maintained. Any updates or deletions can be achieved effectively, and one can effectively keep track of what information is sent out on the web. Moreover, Internet users are faced with the tedious process of filling out registration forms at every new account or subscription to a service on the web. FingerID provides the service of filling out the forms by giving the respective service provider with the user's credentials.

The scope of this research is based on key principles: (1) concurrent studies in progress; (2) a live project for the development of the solution; and (3) field-testing. This is supported by hard techno-economic analysis, which ensures that the solution is commercially viable. Many solutions languish in the dark tunnels of academic history and gather dust for not being commercially viable; therefore, the present study encompasses the entire gamut of the subject surrounding the problem. These constitute a critical review of the literature, development of a solution as a live project, inclusion of the requirements of everyday Internet users, field-testing the models, and techno-economic feasibility analyses.

FingerID involves the human element from two aspects: fingerprint scans are taken from humans and the human interaction with the system to utilise the service. Therefore, an innovative HCI theory has been adapted for the research study whereby there is an amalgamation of scientific research with design research.

2.1.1. Four-Tier Architecture. FingerID has a four-tier architecture comprising the following tiers: client, interface, control and distribution. All these tiers are developed and implemented. The figure below shows the architecture that provides the framework of the system which serves as the base for the centralised access of web accounts and fingerprint authentication system.

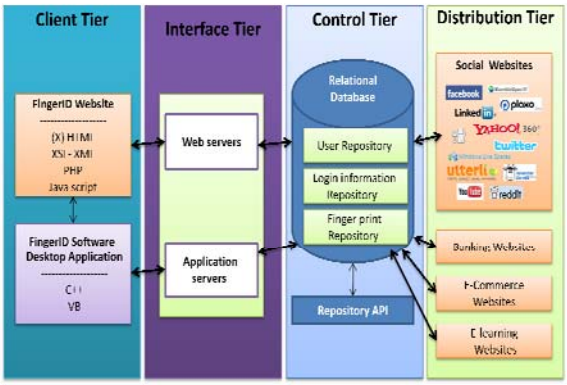

Figure 1. 4-Tier architecture of FingerID

2.1.2. FingerID Design. The FingerID system has been programmed to request the user's fingerprint scan for registration purposes when he is a new user to the system. Following the user registering to become a member, he can then gain access to multiple web accounts under one service. The registration process of the user will only take place once, and later scans will be used to verify the user to provide him access to his web accounts.

The FingerID system is composed of two main parts: website and software (browser). The hosting of the website is carried out on a dedicated web server running on Windows XP with PHP 5.3.1 and MySQL 5.1.4. Nevertheless, the software developed and tested on a computer installed with Windows XP, VB.Net 2008 and Microsoft Access. The following figures show the FingerID flowcharts as well as a screen shot of the FingerID system:

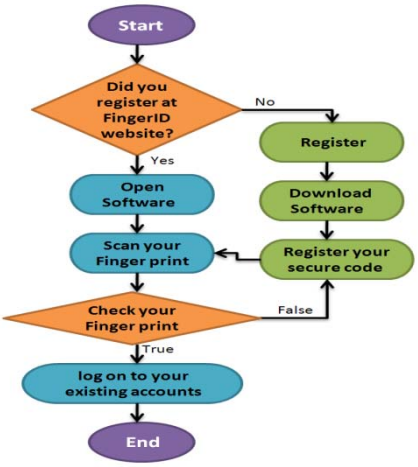

Figure 2. FingerID Flowchart

Figure 3. FingerID Browser and FingerID Website

The system is live, and a user community has been established.

3. Comparison with Similar Applications

The security of user information on the web has been an area of interest and concern for many years. The consequences of vulnerability of data are so intense that users and organisations both take extensive measures and spend a great deal of their resources making their information safe. Many applications have been developed in the past with the objective to improve the security, accessibility and usability on the Internet; some of these have been analysed here on the basis of the three chosen criterion. The idea behind isolating these criteria was to enable a robust comparison of the applications' features, benefits, advantages, and disadvantages, which would eventually lead to the framing of the research questions. These criteria are:

3.1. Security

Username and passwords are usually kept simple by Internet users so that they can be remembered easily; this makes intrusion and password cracking much simpler for the intruder. Another bad practice which has been observed is that people tend to use the same password for multiple accounts, which thereby enables the intruder to gain access to more information and utilise such data for malicious purposes.

There are a lot of applications and systems that tried to solve these issues. One of the most significant applications is OpenID; that is a fast and convenient way of accessing multiple web accounts and to avoid the tedious task of remembering information for all accounts separately [21]. The user registers at OpenID with a username and password, and their credentials will then be used by OpenID to provide access to the desired web accounts. The username and password is knowledge-based, and only known to the user. The same information will be maintained in all of the web accounts, which also enhances the security of information [17]. Additionally, the Shibboleth system is high secure application, but it focused on the access and identity management of an organisational set-up, rather than random Internet users. It is a standards-based system which provides single sign-in on the Internet for access to organisational data or licensed resources. It implements the aspect of security by commonly found federated identity standards. The standard—which is followed the most by them—is OASIS' Security Assertion Markup Language (SAML). This provides further privacy to access on the web by giving the power to the browser user and the home web page so as to control the flow of information sent out to each application [16]. Moreover, there are some secure services revolve around the distributed sharing of data, and do not provide any log-in facilities for any website or web account such as Open authorisation (OAuth); which is a platform through which users can share their private data (pictures, videos, bank accounts, etc.) with users on other websites without revealing their usernames and passwords to anyone [22]. The authentication mechanism of the owner of the account is based on the username and password, and therefore it is knowledge-based as OpenID. The visitors who view the permitted data cannot view any other data, and access to the owner's private data does not require the owner to reveal his credentials therefore security level is good [44].

However, some existing systems are not highly secure; even though they comprise extremely important and private data relating to the individual. One of these applications is liberty alliance; that it focused and concerned with establishing a global network where customers, vendors and governments can perform online transactions whilst ensuring privacy and security [28]. The level of security is not very good in the case of Liberty alliance. The nature of the information—i.e. credit card details—is far too important to be shared with so many websites. Essentially, the user will be connected with a liberty alliance associated website even if he doesn't realise this is the case. Ultimately, the sharing of

information, to a great extent, increases the chances of its misuse [29]. Other application is Microsoft Passport that advertises the fact that business owners can enhance their business by incorporating Windows Live ID service on their websites; in this way, the users will be able to log-in automatically at the business owner's website and will thus increase their traffic [32]. Through the Internet there is a hacking tool available for Microsoft Passport which poses a threat to its security. This indicates that strong security measures have not been implemented. If a user logs-in at Hotmail to check email, he might not realise but he has provided access to his Passport wallet for the next 15 minutes without the need for any verifications. An intruder might subsequently use this time to gain access to any of his MSN accounts without his knowledge [33], [34].

All these security issues raise the need to introduce a high secure authentication mechanism that is FingerID. The access to the web accounts which is given after the fingerprint scan matches with the registered print in the database. All the fingerprint scans are saved at a centralised point and is not accessible to any application other than FingerID. Fingerprints are an individual's unique characteristic, which therefore cannot be possessed by anyone else. Additionally, FingerID uses various types of security tools that are Secure Web Services, TimeStamp and SSL Certificate. Data and fingerprint templates are encrypted to enhance the security of the system.

3.2. Accessibility

Several problems have been identified through research over the years regarding the accessibility. Later, some tools and methods were stated and have been proposed by different organizations to make the websites and software applications more accessible. However, the level of accessibility for a lot of systems is not commendable. For example, the users at OpenID have complained about the frequency of visual images and graphics used to verify whether a human is making the entry [23]. Such graphical content proves to be difficult for disabled individuals. Besides, disabled people will experience difficulty in utilising the features on the Open authorisation (OAuth) website and authenticating themselves to gain access owing to the username and password authentication mechanism [27].

Nevertheless, No evidence has so far been established that would indicate that Liberty Alliance and the Shibboleth system have taken measures to provide accessibility to their users. Therefore, it cannot be stated that they are accessible to less able users [25].

On the other hand, Microsoft Passport has made provisions which enable disabled people to use websites without difficulty [18]. Microsoft Shared Computer Toolkit has great features to facilitate accessible navigation and log-in process for a windows user. This toolkit has been integrated with Microsoft Passport, thereby provides accessibility to the disabled user [19]. However, this service is only limited for the websites where Windows Live ID service is incorporated. Notably, this is a significant limitation, since not all websites are equipped with this service. Microsoft Passport has incorporated commercial benefits within its service; on the other hand, FingerID does not offer any commercial benefits so far, since the product is very new. Besides, FingerID requires no entry of password at log-in; therefore, it would be very useful for disabled people. Fingerprint scanners are widely available nowadays, and even present in laptops; therefore, users will have no problem in utilising the services offered by FingerID.

3.3. Usability

Usability is a very important factor that measures the quality of a user's experience when interacting with websites or systems. Even though a lot of organizations proposed usability principles, there are a lot of systems and applications not meet the usability demands of the current times. For instance, the usability level of OpenID still requires further enhancement, since users face major issues and confusion when performing desired functions [24]. Notably, user experiences have been studied and indicate that Shibboleth lacks usability since usability is limited to organisational use and cannot be used for general Internet users since they will need to get organisational credentials to get access [25].

On the other hand, evidence shows that OAuth has a good level of usability concerning its features and pages. Users navigate with convenience and perform the required functions without any problems [26]. Moreover, Liberty Alliance offers great usability to its users [31]. Liberty Alliance is known to bridge fixed and mobile networks as well as provide great usability to its users [30]. Furthermore, Microsoft Passport has taken steps to ensure that their website possesses a commendable level of usability. One such example is that of a standard followed by them whereby 'all Passport enabled sites should possess sign-out buttons'. This sign-out button should enable the user to sign out of not only that specific site but all other associated Passport-enabled sites to which a user is currently logged in. Another one of their standards is that the colour of the buttons on the site should be such that they are easily visible [20]. Furthermore, our proposed system, that is FingerID, offers great usability to its users since it enables them to avoid the redundant entry of password and usernames at every log-in.

Once the user has logged in FingerID, he can easily access all the web accounts in one place.

4. Summary and Results

The extensive study of the existing applications and relevant literature enabled understanding of the requirements of accessing web accounts with security, accessibility and usability. These three criteria were determined as the areas in which the hypotheses were tested, and thus results were concluded. The research question that had been framed to accumulate the purpose and direction of the research study is as follows:

'What is the procedure to enable web users to access distributed systems on one accessible, usable and secure platform?'

This is the question which directed the project towards achieving a certain aim and objective. An effective research question ensures the researcher remains focused on the path rather than exploring new dimensions for research on diverse topics. Three research questions were formulated and three hypotheses were developed based on the criteria of accessibility, usability and security. These hypotheses were field-tested by two means: (1) lab testing to test accessibility, usability and security; and (2) user satisfaction. For this purpose, an empirical operational model was developed and the results were analysed with the use of suitable statistical instruments.

The table below shows a critical review of an extensive evaluation of similar software applications in the market denote that FingerID is coupled with security, usability and accessibility. No software or application has so far been established which matches the features and innovation that can be witnessed by the usage of FingerID.

Table 1. Summary of Comparison with Similar Applications

Current Applications	Level of security	Level of accessibility	Level of usability
OpenID	✓ [17]	✗ [23]	✗ [24]
Shibboleth	✓ [16]	✗ [25]	✗ [25]
OAuth	✓ [44]	✗ [27]	✓ [26]
Liberty Alliance	✗ [29]	✗	✓ [30], [31]
Microsoft Passport	✗ [34], [33]	✓ [18], [19]	✓ [20]
FingerID	✓	✓	✓

FingerID is an efficient and reliable alternate to the conventional authentication mechanism of username and password. FingerID aims to promote the convenience for the Internet user since he will not have to remember multiple passwords for a multiple number of accounts. FingerID has been developed with the objective of improving the process of log-in in the user's web accounts. The biometric that has been selected is fingerprint in order to enable greater convenience for everyone.

5. Conclusion and Future Work

The username and password authentication mechanism no longer serves the current times of increasing identity thefts and intrusion activities. The authentication mechanism which can serve the need of the existing times is to have a mechanism that relies upon unique characteristics that cannot be stolen. Fingerprints seem to be the most applicable solution to the above mentioned concern of security breach.

There are many guidelines available for ensuring usability, accessibility and security on the web; however, it is noteworthy to state that not many websites abide by such guidelines. FingerID aims to change this and to provide its users with an application that caters to all of these required areas. Accessibility, usability and security guidelines have been tested on the FingerID website and browser by means of numerous activities. Such activities have been discussed in detail in the future papers.

The username/password authentication mechanism is no longer fit for purpose. In this paper, we propose a cost effective, convenient and secure authentication-solution to the everyday users throughout the world for undertaking secure dealings over the Internet. The study envisions of worldwide application of the solution. It visualizes seeing Internet users happily authenticating their identity in a hassle free manner and going about doing their activities in a secure environment without the fear or trepidation of loss of identity and money.

FingerID will authenticate the user on the basis of his fingerprint scans. Other biometric authentication methods—for example, palm prints and face gestures—will be taken as a goal for the future. Another aim of the project is to encourage further research and development on the subject.

6. References

[1] B. Starr, Helium, "Groundbreaking inventions of the 20th century", *Helium*, 2010.

[2] Z. Tian, N. Xu, W. Peng, "E-Commerce Security: A Technical Survey," iita, vol. 2, *Second International Symposium on Intelligent Information Technology Application,* IEEE Xplore, China, 2008, pp.956-960.

[3] D. Argles, A. Pease and R. J. Walters, “An Improved Approach to Secure Authentication and Signing”, *Advanced Information Networking and Applications Workshops, AINAW '07, 21st International Conference*, IEEE Xplore, Niagara Falls, Canada, 2007, pp. 119-123.

[4] D. Denning, "Protecting Public Keys and Signature Keys," *IEEE Compute Society,* IEEE Xplore, vol. 16, USA, 2006, pp. 27-35.

[5] V. Gligor, “A guide to understanding covert channel analysis of trusted systems”, *Technical Report NCSC-TG-030, National Computer Security Center*, USA, 1993.

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

[7] Z. Riha and V. Matyas, “Biometric authentication systems”, *FI MU. Report Series, FIMU-RS-2000-08*, 2000.

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

[9] M. McGinity, “Staying connected: Let your fingers do the talking”, *Communications of the ACM*, vol. 48, no. 1, 2005, pp 21-23.

[10] InterPeak AB, “IPsec- Internet Protocol Security”, *InterPeak AB, Version 1.22-r,* 2005.

[11] TimeStep Corporation, “Understanding the IPSec protocol suite”, *IPSec2.0*, 1998.

[12] N. Borenstein, N. Freed, “MIME (Multipurpose Internet Mail Extensions): Mechanisms for Specifying and Describing the Format of Internet Message Bodies”, *Network Working Group*, 1993.

[13] The Corporation for Research and Educational Networking (CREN)**,** “PGP: Pretty Good Privacy”, *Cren.net*, 2001.

[14] Javvin Technologies Inc., “MIME and SMIME: Multipurpose Internet Mail Extensions and Secure MIME”, *Jaavin.com*, 2010.

[15] AT&T and Lumeta Corporation, “Firewall Gateways”, *AT&T and Lumeta Corporation*, 1994.

[16] 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**.**

[17] T. DiVito, “OpenID: A Potential Authentication Technology”, *Decision Line,* School of Business-Camden, Rutgers University, Newark, USA, 2008.

[18] S. Baklanov, “Security models in ASP.NET. Authentication**”,** *XLineSoft***,** 2005.

[19] D. Shinder, “How to Use Microsoft’s Shared Computer Toolkit”, *Window Security,* TechGenix Ltd, 2005.

[20] R. Oppliger, “Microsoft .NET Passport: A Security Analysis**”,** *IEEE Computer Society Press*, Vol. 36, Issue 7, Los Alamitos, CA, USA, 2003, pp. 29-35.

[21] E. Bond, “Securing the Blogosphere through OpenID: Relying Parties, Unite”, *AOL Developer Network*, 2007.

[22] J. Jackson, “OAuth 2.0 security used by Facebook, others called weak”, *Computerworld Security newsletter*, IDG.net, 2010.

[23] B. Ferg et al., *“*OpenID Authentication 2.0—Final”, *OpenID Community*, Dec. 2007.

[24] J. Zhou, “OpenID usability is not an oxymoron”, *FactoryCity*, 2008.

[25] C. Joie, “Understanding Shibboleth- SLO Issues”, *Internet2,* 2010.

[26] M. Engel, “MySpaceID Usability Testing”, *Slide Share.net*, MySpace, 2009.

[27] “Accessibility issues of social Web”, *W3C*, 2010.

[28] A. Nghiem, *IT Web services: a roadmap for the enterprise*, Prentice Hall PTR, USA, 2003.

[29] P. Judge, S. Shankland, “Liberty - is usability compatible with security?”, *ZDnet US*, July 2002.

[30] T. Skytta, “Liberty Alliance Completes Two Projects Based on their ID-WSF”, *Sun Security,* vol. 73, issue 5, 2004.

[31] H. Mikkonen, M. Silander, "Federated Identity Management for Grids," *icns, International conference on Networking and Services (ICNS'06),* USA, 2006, pp.69.

[32] “Use Windows Live ID for Your Web Site”, *Windows Live ID*, 2006.

[33] W. Redmond, “Microsoft Passport: Streamlining Commerce and Communication on the Web”, *Microsoft News Center*, 1999.

[34] 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.

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