*Proceedings of the Eighth International Symposium on*
*Human Aspects of Information Security & Assurance (HAISA 2014)*

# Improving Internet Banking Security by using Differentiated Authentication based on Risk Profiling

M.J. Butler and R. Butler

Stellenbosch University, South Africa
email: martin.butler@usb.ac.za; rbutler@sun.ac.za

## Abstract

Online security remains a challenge to ensure safe transacting on the internet. User authentication, a human-centric process, is regarded as the basis of computer security and hence secure access to online banking services. The increased use of technology to enforce additional actions has the ability to improve the quality of authentication and hence online security, but often at the expense of usability. The objective of this study was to determine if there are factors that could be used to create different authentication requirements for different users. That is, could internet banking users, for example, be directed to different authentication regimes after classifying their potential safety profile based on the browser that they are using? A web-based survey was designed to determine online consumers' perceptions of their skills and competence in respect of passwords creation and management practices, and capture demographical data as well as choices in browsers used. After using a construct for password performance, derived from previous research on the same dataset, the browser used was compared with use of poor password practices. Based on the results a case could be made to have different authentication methods for consumers based on their browser selected to ensure a safer online environment.

## Keywords

Online banking, User authentication, Differentiated authentication, Risk profiling

## 1. Introduction

The phenomenal growth of online banking has transformed the way in which consumers interact with their financial services provider. The majority of clients' interaction with their service providers occurs online via their preferred browser and is increasingly moving towards mobile platforms. User authentication remains a foundation for computer security (Conklin, Dietrich and Walz, 2004:1) and passwords, in combination with other measures, remains critical to identify and authenticate online banking users.

Computer users remain a weak link in online security since user password practices has a direct effect on the level of security of a system (Gehringer, 2002:369). Not selecting and managing passwords with care may make those passwords more susceptible to potential abuse and misuse (Furnell, 2005:10). Accordingly, even the most sophisticated security systems are compromised if users do not select and manage their passwords properly (Tam, Glassman and Vandenwauver, 2010:233). Despite problems relating to password security remaining 'conspicuously unsolved',

passwords as a means to identify users, whether in isolation or combination, remains the most common method of authentication (Furnell, 2005:9 and 11).

Newer technology supported authentication systems like biometrics and One-time-Pin are becoming popular (Tam *et al.* 2010:233) and do contribute to a safer online environment. However, the use of these technologies is uniformly applied to all users. That is, the attributes of users are not used to create differentiated authentication. All users, irrespective of any additional knowledge that may be known, or inferred at the point of authentication, are treated equally when verified.

## 2. Online banking

As the user of online banking increases security issues relating to confidentiality, integrity, and privacy have become a progressively greater concern to both banks and customers. Banks recognise the benefits, like increased efficiency and customer convenience, of this new medium. Despite this growing ubiquity of online banking services, security and privacy concerns and fears are still foremost in the minds of users and are indeed well founded.

Almost inevitably, this exponential growth in internet banking has been paralleled with an equally swift and altogether more disturbing rise in sector fraud. With the amount of money at stake, today's so-called cyber criminals have greater resources and enhanced technological capability to conduct online fraud. As banking transactions have moved from physical bank locations with vaults protecting their clients' assets to the online world, so have the criminals (Rice, 2012:441).

User authentication, including those for online banking services, employs something a user knows, a user has, or something the user does (refer Table 1). With the increasingly diverse risks in online environments, user authentication methods are also becoming more diversified, and in online banking more often than not it is based on a combination of two or more of such factors.

## 3. The technological contributions

It is well documented that traditional personal identification methods, like passwords, suffer from a number of drawbacks and are unable to satisfy the security requirement of the highly inter-connected information society. As a result a number of different technologies have been developed and implemented in online authentication.

- Biometrics refers to identification of an individual based on his/her physiological or behavioural traits. This ranges from the use of physical features including voiceprints, fingerprints and iris recognition, to behavioural features including gait and handwriting recognition. Biometrics is inherently difficult to copy, share and distribute; difficult to forge; and importantly cannot be lost or forgotten because the individual has to be physically present (Kaman, Swetha, Akram and Varaprasad, 2013; Tassabehji and Kamala, 2012).

- Out-of-band authentication is a method of verifying a 'user's identity using a channel other than the one being used to facilitate the transaction' in order to improve online security (Feig, 2007:23). By using a second communication channel that should also be unique to the same user, the level of security is greatly improved and this is fast becoming a standard in online banking.
- Graphical passwords have been proposed as alternatives to text-based **password** authentication. Biddle, Chiasson and Van Orschot (2012) provided a comprehensive overview of published research in the area, covering both usability and security aspects as well as system evaluation.
- One-time-pin (OTP) is a system where text messages are sent to phones with one-time use codes to verify a login. This popular method is a subset of Out-of-band authentication. Some of the newer applications of the One-time PIN place a digital certificate on the user's phone to authenticate future transactions. The system does not rely at all on the mobile phone's phone number but rather on the actual digital certificate placed on the phone (Wolfe, 2011:10).
- Key stroke dynamics is a technology to ensure that the user, post-authentication, is indeed the user authenticated (Pisani and Lorena, 2013). The benefit of key stroke dynamics, although rather complex and processing intensive to implement, is the non-intrusive nature and continuous monitoring post-authentication.

Amid increasing pressure to protect customers online, some of the major global banks are turning towards two-factor and multi-channel authentication. However, to date all measures are uniformly applied to all users, irrespective of any information that may be known at instance of authentication, or even after authentication when the user and attributes associated with the user is known. An important departure point to address poor password performance is recognising that proper password security systems involve both human and technological aspects (Brostoff and Sasse, 2002:41). Technical measures incorporated into security systems are of little value if users do not understand the measures, risks or consequences associated with poor password practices.

## 4. The user challenge

Conklin *et al*. (2004:5) regards an untrained user as one of the weakest links in a security system. While certain password users may be very proficient in applying proper password practices, proper security measures and guidelines are often 'unknown, neglected, or avoided' by other computer users (Notoatmodjo and Thomborson, 2009:71). However, institutions use the same method of authentication for all users. For example, creating a complex authentication regime fitted to the 'least secure' user to ensure fail safe authentication in spite of very limited knowledge of online security, raises unnecessary entrance barriers for authentication of users that behave in a secure manner. Differentiating levels of knowledge and application among users is a concern, but also an opportunity to increase online safety were it is needed most.

In principle, there are only three authentication categories that can be used to secure the online environment as indicated in Table 1.

| Authentication Types | Validating | Examples |
|---|---|---|
| Proof-of-Knowledge | Something the user knows – tacit knowledge or knowledge shared by the service provider | Passwords, PIN, Mother's maiden name, Telephone number |
| Proof-of-Possession | Something the user possess | Smartcards, Tokens, Hardware devices, Digital certificates |
| Proof-of-Characteristics | Something physical or behavioural attribute | Fingerprints, Wrist vein patterns, Iris/ Retina scan, Facial/Voice recognition |

**Table 1: Types of Authentication**

Choubey and Choubey (2013) reviewed a number of security features used by different banks globally. The measures employed ranged from simple password only systems to rather complex structures involving an OTP generated through external hardware. Somewhere in between are systems involving additional information based of memorable words or other user information.

According to Choubey and Choubey institutions have a predicament in introducing more layers of security since it leads to more difficulty for end-users in accessing and utilising their financial information. In addition, the spread in security features leads to difficulty in the security testing of different banks as well as inconveniencing users when they move from one institution to another. They even argued that the "learning curve associated with different types of security features could become a bottleneck in market diversity in future" (Choubey and Choubey, 2013:202).

## 5. The cost, convenience and security conundrum

An important contributor to online security is selecting 'strong' passwords that are hard to guess (secure) but still memorable (convenient) (Conklin *et al*. 2004:5). However, when dealing with passwords users are confronted with a 'security-convenience trade-off' (Tam *et al*. 2010:242), which causes a conflict between the convenience of remembering and the security of passwords (Weber, Guster, Safanov and Schmidt, 2008:46). Depending on whether security or convenience is the foremost concern for users, password practices will either be secure or not.

Yan, Blackwell, Anderson and Grant (2004:25) determined that users rarely choose passwords that are both hard to guess and easy to remember. Factors that contribute to this 'password overload' are the increasing number of password-protected systems, enforced password lifetime and composition rules and human memory limitations (Chiasson and Biddle, 2007:1; Yan *et al*. 2004:25; Furnell, 2005:10). This results in users developing their own methods to remember their passwords. When the security motivation is secondary to convenience it leads to weak password practices, which include using short and weak passwords that are easy to remember, sharing passwords, writing down passwords, re-using passwords and not changing

passwords regularly (Campbell, Kleeman and Ma, 2007:3; Furnell, 2005:10; Notoatmodjo and Thomborson, 2009:71).

Unfortunately the usability of security technologies is often neglected by designers (Brostoff and Sasse, 2002:41). Furnell, Bryant and Phippen (2007:416) recommend improving the usability of security features as users often don't apply these features because they have problems to find, understand and use these security features. Inglesant and Sasse (2010) advise greater emphasis on human computer interface (HCI) principles to increase password security.

## 6. Differentiated authentication

Furnell (2007:445) remarks that one of the reasons why many computer users do not apply safe password practices is because 'they may not know any better' due to a lack of appropriate knowledge, guidance and support. To date all instances of authentication are uniformly applied to users. Irrespective of any knowledge known about the user and their potential online behaviour, the same methods (and hence security levels) of authentication is required for all users.

According to Ciampa, Mark and Enamait (2013) research indicated that 'consumers are willing to take extra steps to protect their identities, but they do not necessarily want to pay extra for these services'. The proposition of this paper is then that due to the different strengths in passwords selected, and the different measures taken to keep passwords secure, it may perhaps be a better idea to rather differentiate between 'more secure' and 'less secure' users and define a differentiated authentication regime. Such a differentiated authentication regime would take cognisance of all known information (inferred at the point of authentication) or associated with the user immediately after 'First level authentication' (refer to Figure 1).

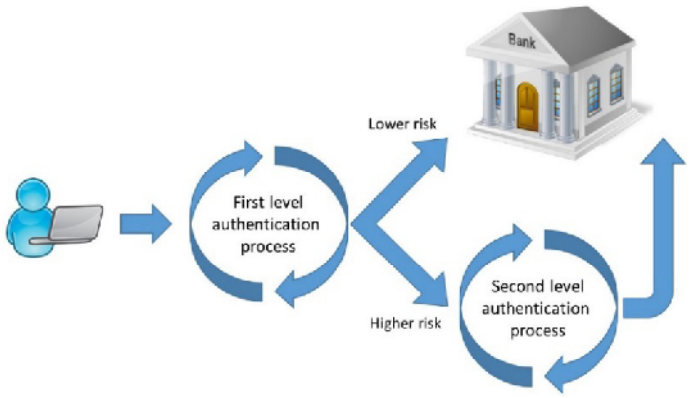


**Figure 1: Proposed authentication process**

More than nine out of every 10 people surveyed by Ciampa *et al*. (2013) indicated their willingness to deal with more than just the usual user name/password

authentication if it meant stronger security. Consumers indicated a high degree of acceptance of 'risk-based' authentication, with 73% indicating a positive inclination towards an institutional-side assessment of the user's identity based on such things as log-on location, IP address, and transaction behaviour.

## 7. Research problem and objective

Proposing a differentiated authentication regime is dependent on (1) the ability to actually differentiate between users security practices and (2) being able to uniquely identify the user, or use group, to impose the additional measures. Raising additional entrance requirements after initial identification is not complex since the identification action provides user specific attributes that could be used to infer a potential risk profile. More interesting is the use of information known at, or even before, authentication. That is, if it is possible to identify user group attributes that correlate to security practices. This lead to questioning if browser preference could potentially indicate an underlying disposition towards online security, or not.

The objective of this study was to:

- Create a performance metric of online banking consumers' password practices.
- Correlate their practices with their browser of preference and analyse if there are any difference in performance, based on the browser of choice.

If there are a difference in behaviour, it provides an opportunity to raise different authentication regimes based on the risk profiling associated with the browser used.

## 8. Methodology

### 8.1. Survey

The data was gathered by the distribution of an online survey. The instrument was designed and refined via two iterations of pilot testing. The survey contained questions to determine:

- Password performance: By testing the respondents' knowledge, capability and motivation a measure of potential performance could be constructed.
- Demographic information: Gathering demographic information that could be correlated with password performance.
- Browser usage: Determining the browser used by the respondents.

The survey was distributed via email to a database of online South African users from the authors' tertiary institution and also via snowball method by the researchers.

### 8.2. Sample of respondents

Out of a total of 914 attempts 791 responses were received. A further 54 respondents did not use internet banking which left a sample of 737 valid responses. Demographical information was analysed to determine a potential bias within the sample and it was determined that there was an acceptable alignment between the known South African online consumer demographics and the sample demographics.

### 8.3. Performance construct

A function for performance used by McCloy, Campbell and Cudeck (1994) was used as primary construct to create a measure of potential performance. McCloy *et al.* (1994) defined performance (PC) is a function of the declarative knowledge (DK), relating to a task, the user's capability to perform the task (PKS) and motivation (M): PC = f (DK, PKS, M). The computer user's password performance was thus defined as a function of the following three components:

- Knowledge : the user's knowledge, education, skills and competencies relating to password practices;
- Capability: the user's aptitude to apply password-related knowledge properly when creating and managing passwords; and
- Motivation (M): the underlying desire behind the user's password behaviour.

The respondents' **knowledge** was tested in the questionnaire by means of a set of questions that tested their knowledge about strong and secure passwords as well as good practice in terms of safekeeping and not sharing passwords.

The respondents' **capability** was tested by asking them to rank different combinations of passwords from the most to the least secure. In ranking the passwords they needed to display their ability to understand the factors such as password length, complexity, different character sets, as well as common words. Although the sets of five different passwords were selected by the researchers to have different levels of security, it was also verified by different password strength meters. Users were also asked about the sharing of passwords and the last time that they changed their internet banking password to get an indication of practice, i.e. knowing about regular changes constitute knowledge, having changed the password in the last 12 months constitute capability.

In terms of **motivation** respondents were tested about prioritising security using the security-convenience trade-off. It was decided that security as a top priority is an acceptable predictor of motivation to behave securely. A second set of questions prompted users about factors that will lead to a change in password practices. In this instance the construct defined different prompts and used action, based on the event as an indicator of motivation. Finally, the desire to use additional knowledge, such as getting access to information from the survey and guidelines for online security, was used as an element of motivation.

### 8.4. Data analysis

Users' perceptions about their password performance was analysed based on the perceptions and practices applied and a metric calculated for each respondents' Knowledge, Capability and Motivation. It was decided to not infer the browser use from that of the respondents' choice to complete the survey, but rather to ask which browser they mostly used. Figure 2 shows the frequency distribution for the performance by preferred browser.

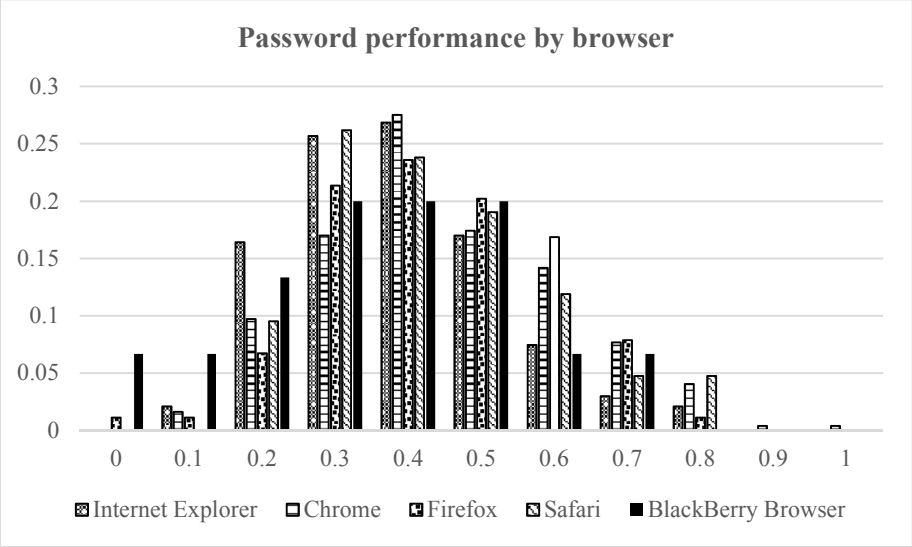


**Figure 2: Password performance by survey results**

From the sample of 737 valid responses the following were excluded as being too small a sample to infer any usable results, BlackBerry Browser (15), Opera (5), Other / No idea (4) which left a total sample of 708 responses. The mean level of Password Performance measured for Internet Explorer (0.336) is lower than that of either Chrome (0.394), Firefox (0.391) or Safari (0.381). But are these differences statistically significant?

## 9. Password performance and browser selection

A one-way Analysis of Variance (ANOVA) was used to examine differences between two or more groups created from a single independent variable, in this instance password performance, on a single dependent variable, in this instance, browser used. The test is used to decide whether the differences in the samples average scores are large enough to conclude that the groups' average scores are unequal.

The ANOVA is proven to be reliable under the following assumptions:

- the values in each of the groups (as a whole) follow the normal curve,
- with possibly different population averages
- equal population standard deviations.

In terms of normality, Figure 2 indicates sufficient normality in the data for each browser to conduct the test. In terms of variance, the rule of thumb is that the largest sample (Internet Explorer) is not larger than twice the smallest sample (Opera), which is indeed the case as indicated in Table 2.

The zero hypothesis was defined as no significant variance between sample means, i.e. $H_0$: $\mu_1 = \mu_2 = \mu_3 = \mu_4$ and the alternate hypothesis as a significant difference between the means, i.e. $H_1$: $\mu_1 \neq \mu_2 \neq \mu_3 \neq \mu_4$. If the zero hypothesis is true, then the 'between group variance' will be equal to the 'within group variance.' Table 2 shows the results of the statistical test for variance in sample means for a confidence interval of 95%.

**Anova: Single Factor (0.05)**

SUMMARY

| *Groups* | *Count* | *Sum* | *Average* | *Variance* |
|---|---|---|---|---|
| Internet Explorer | 335 | 112.6109 | 0.336152 | 0.020634 |
| Chrome | 247 | 97.33837 | 0.394082 | 0.027622 |
| Firefox | 88 | 34.41523 | 0.391082 | 0.021622 |
| Safari | 42 | 15.98869 | 0.380683 | 0.023587 |

ANOVA

| *Source of Variation* | *SS* | *df* | *MS* | *F* | *P-value* | *F crit* |
|---|---|---|---|---|---|---|
| Between Groups | 0.55758 | 3 | 0.18586 | 7.958215 | 3.1803E-05 | **2.61748** |
| Within Groups | 16.53497 | 708 | 0.023354 | | | |
| Total | 17.09255 | 711 | | | | |

**Table 2: One-way ANOVA test for difference between sample means**

Because F (7.96) > F crit (2.62) the null hypothesis was rejected showing a significant variance between sample means and thus inferring a differentiated level of password performance based on users' browser most often used. By merely

inferring which browser an online banking consumer is using, it is thus conceivable to perform risk-based authentication as suggested by Ciampa *et al*. (2013).

## 10. A differentiated model of user interaction

While some computer users may apply poor password practices due to ignorance, studies by Furnell *et al.* (2007), Riley (2006) and Tam *et al*. (2010) found that although users do possess the knowledge to distinguish between secure and insure practices, their practical application thereof often lacks. There exists an opportunity for financial services institutions to create differentiated authentication based on the risk profile of the client. Although the test performed here was for a single factor known at the point of authentication, it is conceivable to extend this beyond the initial authentication (see Figure 1) and also differentiate after identification by using factors that could be inferred from demographical information known by the financial services institution.

A common remedy to improve password performance is security education, training and awareness programs (Riley, 2006; Furnell *et al*. 2007:417). To date this education could be voluntary for all users, or ideally, targeted at the necessary users. It is further conceivable, in fact highly desirable, that this 'targeted training' could also be directed at users that are in 'critical need' for education. Rather than a blanket one size fits all training, it is possible to direct a user to a 'how to create a strong password' session only when the password is deemed to be 'weak'.

A final recommendation considers the uniform warnings often present on Internet banking sites. Even after authentication, users are uniformly warned about the latest online scam as part of their education. It is possible to, for example, infer how the user accessed the URL and warn about clicking on links rather than typing in the URL. By tailoring the communications with the user through the use of risk profiling not only are the message more appropriate, but conceivably the attention of the consumer that notices a tailored message.

## 11. Limitations of the research and recommendations

The following two limitations of the recommendations and hence research has been noted:

- Differentiated authentication and subsequent communication could be construed as discrimination. The concept of risk profiling is not new, but is mostly not as "in your face" as what could be experienced by users if applied during and immediately after online authentication.
- In spite of the observed difference in security practices it has not been proven in this research to be material in nature. Further research is required to establish the extent and impact of the difference.
- A negative effect on online privacy for online users.

## 12. Conclusion

Continued technological innovation and competition among existing banks and new market entrants has led to a growing array of banking products and services. These include traditional activities such as accessing financial information, obtaining loans and opening deposit accounts, as well as relatively new products and services such as electronic account payment services, personalised financial 'portals', account aggregation and business-to-business market exchanges. The dependence on technology for the provision of these services ensuring the necessary security present additional risks for banks and new challenges for banking regulators.

The online world is the embodiment of paradoxes where great effort goes into firewalls, security audits and virus checkers, and yet at the same time, the access given to a web browser often makes these defences futile. Multiple authors (Gaur, Patel and Saini, 2013; Wahlberg, Paakkola, Wieser, Laakso and Roning, 2013) have investigated the inherent security issues within browsers that could be exploited technically and have indicated the difference in vulnerability when using a particular browser. This research, however, uses the browser selection choice as a user attribute and does not seek to identify browser issues, but rather attempt to understand the user behaviour by using the browser selected as an user attribute. The security risks of Internet banking have always been a concern to the service providers and users. In studying factors that lead to adoption of online banking, Yap, Wong, Loh and Bak (2010) determined that 'web site features that give customers confidence are significant situation normality cues'. It is reasonable to infer that differentiated authentication could be construed as such a factor.

Passwords will remain the most common authentication method used by computer systems and the human factor remains an important consideration to ensure security. This research suggests that using 'risk-profiling' to create a system of differentiated authentication of users, using a relative unassuming attribute such as the browser used could improve online security.

## 13. References

Biddle, R., Chiasson, S. and Van Orschot, P.C. (2012), "Graphical Passwords: Learning from the First Twelve Years", *ACM Computing Surveys,* Vol. 44, No. 4, pp1-19.

Brostoff, S. and Sasse, M.A. (2002), "Safe and Sound: a Safety-critical approach to security", Proceedings of the New Security Paradigm Workshop 2001, http://hornbeam.cs.ucl.ac.uk/hcs/people/documents/Angela%20Publications/unsorted/p41-brostoff.pdf, (Accessed 10 April 2014).

Campbell, J., Kleeman, D. and Ma, W. (2007), "The good and not so good of enforcing passwords composition rules", *Information Systems Security*, Vol. 16, No. 1, pp2-8.

Chiasson, S. and Biddle, R. (2007), "Issues in User Authentication", CHI Workshop: Security User Studies: methodology and best practices, April.