Investigating the possibility to use differentiated authentication based on risk profiling to secure online banking

Martin Butler
Business School, Stellenbosch University, Stellenbosch, South Africa, and
Rika Butler
School of Accountancy, Stellenbosch University, Stellenbosch, South Africa

Received 28 November 2014
Revised 28 November 2014
Accepted 9 January 2015

Abstract

Purpose – The purpose of this paper was to determine factors that could be used to create different authentication requirements for diverse online banking customers based on their risk profile. 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 factors that could be used to create different authentication requirements for diverse online banking customers based on their risk profile.

Design/methodology/approach – A web-based survey was designed to determine online consumers' competence resecure online behaviour, and this was used to quantify the online behaviour as more or less secure. The browsers used by consumers as well as their demographical data were correlated with the security profile of respondents to test for any significant variance in practice that could inform differentiated authentication.

Findings – A statistical difference between behaviours based on some of the dependant variables was evident from the analysis. Based on the results, a case could be made to have different authentication methods for online banking customers based on both their browser selected (before individual identification) as well as demographical data (after identification) to ensure a safer online environment.

Originality/value – The research can be used by the financial services sector to improve online security, where required, without necessarily reducing usability for more "security inclined" customers.

Keywords User authentication, Online banking, Security, Access control, Differentiated authentication, Risk profiling

Paper type Research paper

1. Introduction

The phenomenal growth of online banking has transformed the way in which consumers interact with their financial services providers. Both banks and customers have recognised the benefits of this new medium, such as increased convenience and efficiency for customers and a decrease in cost and expanded customer base for banks (Moscato and Altschuller, 2012, p. 51; Ravi *et al.*, 2006, p. 62). As the use of online banking increases, security issues relating to confidentiality, integrity and privacy remain a foremost concern in the minds of online banking service providers and users.

Information & Computer Security
Vol. 23 No. 4, 2015
pp. 421-434

2056-4961
DOI 10.1108/ICS-11-2014-0074

Due to the sensitive nature of online banking information and transactions, security-related concerns are regarded as one of the major issues affecting the adoption of online banking by users (Moscato and Altschuller, 2012, p. 52). These concerns are indeed well founded.

Almost inevitably, the exponential growth in Internet banking has been paralleled with an equally swift and altogether more disturbing rise in sector fraud. As banking transactions have moved from physical bank locations, with vaults protecting their customers' assets, to the online world, so have the criminals (Rice, 2012, p. 441), who use increasingly complex methods of attacks. With the huge potential financial gain, cyber criminals are using more resources and enhanced technological capability to conduct online fraud.

2. User authentication

User identification and authentication when transacting online remain a foundation for computer security (Conklin *et al.*, 2004, p. 1). User authentication uses something a user knows, something a user has or a characteristic unique to the user (Hunton *et al.*, 2004, p. 139) to identify and authenticate the user.

In principle, there are only three authentication categories that can be used to secure the online environment, as indicated in Table I. In online banking, more often than not authentication is based on a combination of two or more of these factors.

It is well-documented that traditional personal identification methods, like passwords, have limitations and challenges and are often unable to satisfy the security requirements of the highly inter-connected information society and the diverse risks associated with the online environment. As authentication is an essential element of online banking security, new technologies for improvement are continuously evolving in an attempt to address these challenges (Usman and Shah, 2013, p. 2). As a result, user authentication methods are becoming more diversified, and a number of different technologies have been developed for online authentication.

Biometrics refers to identification based on 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 *et al.*, 2013; Tassabehji and Kamala, 2012). Keystroke dynamics, a type of biometrics which also uses a behavioural trait unique to a user, is a technology that ensures that the user, post-authentication, is indeed the user authenticated (Pisani and Lorena, 2013). The benefit of keystroke dynamics, although rather complex and

Table I.
Types of authentication

Authentication types	Validating	Examples
Proof-of-knowledge	Something the user knows	Passwords, PIN, mother's maiden name and telephone number
Proof-of-Possession	Something the user possess	Smartcards, tokens, hardware devices and digital certificates
Proof-of-Characteristics	A physical or behavioural attribute	Fingerprints, wrist vein patterns, iris/Retina scan and facial/voice recognition

processing intensive to implement, is the non-intrusive nature and continuous monitoring post-authentication.

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" (Feig, 2007, p. 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. 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 more recent applications of the OTP 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 number but rather on the actual digital certificate placed on the phone (Wolfe, 2011, p. 10).

Amid increasing pressure to protect customers online, some of the major global banks are turning towards two-factor and multi-channel authentication. However, increasing the authentication unilaterally for all users does not take cognisance of the fact that users display vastly different behaviour when interacting online.

3. The user challenge

An important departure point to improve security systems is to recognise that proper password security systems involve both human and technological aspects (Brostoff and Sasse, 2002, p. 41). Technical measures incorporated into security systems are of little value if users do not understand the measures, risks or consequences associated with improper use of these measures. Researchers (Pfleeger and Caputo, 2012; Anderson and Agarwal, 2010) suggest a greater understanding of the behaviour of users to prevent them from being the "weakest link". Conklin *et al.* (2004, p. 5) support this view by arguing that the untrained user represents one of the weakest links in a security system.

Passwords, in combination with other measures, remain critical to identify and authenticate online banking users, and even the most sophisticated security systems can become useless if computer users do not choose and manage their passwords properly (Tam *et al.*, 2010, p. 233). Nonetheless, despite issues 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 used (Furnell, 2005, pp. 9 and 11).

Furnell (2007, p. 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. However, studies by Furnell *et al.* (2007), Riley (2006), Tam *et al.* (2010) and Wessels and Steenkamp (2007, p. 11) found that when users do possess the knowledge to distinguish between secure and insure practices, their practical application thereof often lack. 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, p. 71).

An important contributor to online security is selecting "strong" passwords that are hard to guess (secure) but still memorable (convenient) (Conklin *et al.*, 2004, p. 5). However, when dealing with passwords, users are confronted with a "security-convenience trade-off" (Tam *et al.*, 2010, p. 242), which causes a conflict between the convenience of remembering and the security of passwords (Weber *et al.*, 2008, p. 46).

Depending on whether security or convenience is the foremost concern for users, the password practices that those users apply will either be secure or not.

Yan *et al.* (2004, p. 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, p. 1; Yan *et al.*, 2004, p. 25; Furnell, 2005, p. 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 *et al.*, 2007, p. 3; Furnell, 2005, p. 10; Notoatmodjo and Thomborson, 2009, p. 71).

As discussed in this section, users may differ in their password performance due to various reasons. As user behaviour concerning passwords has a direct effect on the level of security of a system, computer users remain a weak link in online security (Gehringer, 2002, p. 369). When users do not select and manage passwords with care, it may make those passwords more susceptible to potential abuse and misuse (Furnell, 2005, p. 10).

4. Differentiated authentication

Financial institutions have for some time now used segmentation or profiling of their customers for amongst other credit scoring and marketing purposes (Ravi *et al.*, 2006). This segmentation is a key method used by banks to better understand their customers to subsequently provide the services required (Durkin, 2004, p. 485).

Yet, to date, concerning user authentication, financial institutions uniformly apply the same level(s) of authentication to all users, irrespective of any knowledge known about the user and their potential online behaviour. This means that all users are required to undergo the same methods (and hence security levels) of authentication and that no attributes associated with the particular user is used to distinguish between 'more' or "less" security-proficient users to create differentiated authentication. After identification, all users, irrespective of any additional knowledge that may be known, or inferred at the point of authentication, are treated equally during the verification process and therein lies the opportunity.

The different levels of knowledge and application of online security pose an opportunity for increased online safety where it is needed most. According to Choubey and Choubey (2013), institutions have a predicament in introducing more layers of security, as it leads to more difficulty for end-users in accessing and utilising their financial information. When a complex authentication regime fitted to the "least secure" and "untrained" user is created to ensure fail-safe authentication, it raises unnecessary entrance barriers for authentication of users that behave in a secure manner. 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. Choubey and Choubey (2013, p. 202) argue that the "learning curve associated with different types of security features could become a bottleneck in market diversity in future".

However, research by Ciampa *et al.* (2013) indicated that "consumers are willing to take extra steps to protect their identities". More than nine out of every ten 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. Almost 75 per cent of the consumers indicated 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.

This creates on opportunity to investigate whether using risk-based authentication (RBA) could be a viable option for the authentication of South African online banking customers. RBA uses historical and contextual information associated with the user to build a risk profile for the user, which can be used during the authentication of the user (Traore *et al.*, 2014, p. 576). It can either be user-dependent (the same authentication would be used for every session initiated by the user) or transaction-dependent (different authentication levels are required of a user in different situations, based on the potential risk associated with that transaction). In addition, RBA can be applied proactively (integrated with the login process to flag users who are "risky") or reactively (to identify and revert ongoing or completed transactions regarded as "risky") (Traore *et al.*, 2014, p. 600).

Although the source IP addresses or the velocity of transactions originating from a certain IP address or by a specific account can be used for risk profiling, Traore *et al.* (2014) argue that such attributes are susceptible to fraud and may easily be spoofed and can proof not the most secure method to use for profiling. Researchers have also investigated profiling based on keystroke dynamics as well as mouse dynamics as measures to improve security (Traore *et al.*, 2014; Usman and Shah, 2013). However, Traore *et al.* (2014, p. 578) identified a deficiency in existing research on risk-based authentication in that none of the research "has taken into account the user behavioural patterns in the risk management process".

Instead of applying the same level(s) of authentication uniformly to all online banking users, this research proposes that it may be a feasible idea to differentiate between "more secure" and "less secure" users and define a differentiated authentication regime based on the risk associated with certain user characteristics. 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).

The first step (Figure 1) would be to use pre-identification information to potentially differentiate authentication "on arrival". The biggest potential in this level lies in the

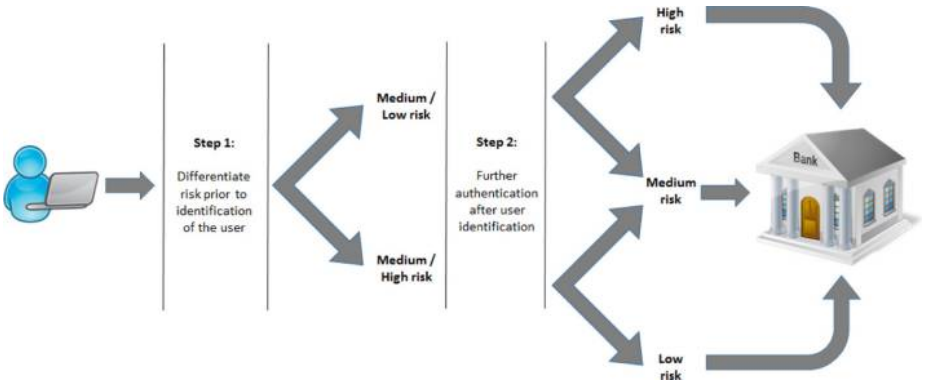

Figure 1.
Proposed authentication process

browser that the user uses as well as the IP address. It is well-documented that certain browsers, especially older versions of browsers, are more prone to malware and similarly that cyber threats originate from specific global locations that can be identified via the IP address used. Although not to be used as a security indicator in isolation, the browser used by the online banking customers may provide an indication of the type of behaviour (more or less risky) that may be associated with that customer.

The second step (Figure 1) would be to use known demographical data associated with the user post identification to further authenticate the user via a second or third level of authentication. In this instance, the institution would not infer data from the anonymous visitor but use the results of the initial authentication process to raise additional entrance barriers, where appropriate, to improve security.

In addition, and this is not shown as it fails outside the scope of the research, technologies such as keystroke dynamics could in essence be a third step in the process, as particularly risk users could be monitored beyond authentication to further improve security.

5. Research problem and objective

Proposing a differentiated authentication regime for users is dependent on the ability to differentiate between users' security practices as well as the ability to uniquely identify the user, or user group, to impose the additional measures. Raising additional entrance requirements after initial identification is not complex, as 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, whether it is possible to identify user group attributes that correlate to security practices.

The objective of this research is to:

- create a performance metric of online banking consumers' password practices to categorise users' online behaviour practices;
- correlate their practices with their browser of preference and analyse if there is any difference in performance, based on the browser of choice; and
- correlate their practices with captured demographics and analyse if there is any difference in performance, based on their demographical information.

6. Methodology

6.1 Survey

The data were 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.
- *Browser usage*: Determining the browser used by the respondents.
- *Demographical information*: Gathering demographical information that could be correlated with password performance.

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.

6.2 Sample of respondents

Out of a total of 914 attempts, 791 responses were received. As 57 respondents did not use Internet banking, it left a sample of 734 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.

6.3 Performance construct

A function for performance used by McCloy *et al.* (1994) was used as primary construct to create a measure of potential password performance. McCloy *et al.* (1994) defined performance (PC) as 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).

A 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.
- *Motivation*: 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 factors such as password length, complexity, different character sets, as well as common words. Users were also asked about the sharing of passwords and the last time that they had changed their Internet banking password to get an indication of practice, i.e. knowing about regular changes constitutes "knowledge", having changed the password in the last 12 months constitutes "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 actions, 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 to provide an indication of users' motivation.

Based on the knowledge, capability and motivation, an online security score was calculated for each respondent to be used in the analysis for potential differences in behaviour that could potentially be used to distinguish more and less secure users.

6.4 Data analysis

The only parameter used for pre-identification comparison was browser usage, as the survey was South African based, and more than 95 per cent of respondents thus originated from within South Africa. 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 primarily used.

In terms of demographics, four different dependent variables (age, gender, highest qualification and years of Internet experience) were used to determine if a difference in behaviour among users were evident (Table II). From the sample of 734 valid responses, some of the categories rendered small subsets that needed to be excluded for analysis and comparison purposes, as indicated in Table II.

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 (Table II). The test was used to decide whether the differences in the samples average scores were large enough to conclude that the groups' average scores are unequal.

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

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

In terms of normality, a visual inspection indicated sufficient normality in the data for dependent variable category. In terms of variance, the rule of thumb is that the variance of the largest sample is not larger than twice the smallest sample, and this was used to ensure that the test could be performed.

The zero hypothesis was defined as no significant variance between sample means, i.e. $H0$: $\mu_1 = \mu_2 = \mu_3 = \mu_4$ and the alternate hypothesis as a significant difference between the means, i.e. $H1$: $\mu_1 \neq \mu_2 \neq \mu_3 \neq \mu_4$. If the zero hypothesis is true, then the "between group variance" will be equal to the "within group variance".

7. Results

The results of the statistical test for variance (ANOVA) in sample means for a confidence interval of 95 per cent for the individual dependant variables are shown in Tables III-VII. In each instance, the test checked to see if $F > F$ crit to decide if the null criteria can be rejected. In instances where this was the case, the null hypothesis was rejected showing a significant variance between sample means, thus inferring potential for a differentiated level of password performance, based on the dependent variable. In instances, where the $F < F$ crit the null hypothesis could not be rejected.

Dependent variable	Categories	N	Comment
Browsers	Four different browsers	708	Blackberry, Opera and other/no idea omitted
Age	Five different brackets	734	None omitted–sufficient numbers for each category
Gender	Male/female	734	None omitted
Highest qualification	Six different levels of qualification	721	Grade 10 omitted with only 13 responses for the category
Internet experience	Three different categories	734	Users were categorised into > 10 years, 5 to 10 and <5 years of experience

Table II.
Parameters used

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 III. One-way ANOVA test for difference between browser means

ANOVA: single factor (0.05)

Summary

Groups	Count	Sum	Average	Variance
15-24	36	12.29428	0.341508	0.023979
25-34	271	101.1412	0.373215	0.025963
35-49	282	102.7689	0.364429	0.021436
50-59	103	37.39235	0.363033	0.025715
>60	43	14.98542	0.348498	0.025537

ANOVA

Source of variation	SS	df	MS	*F*	*p*-value	*F* crit
Between groups	0.050227	4	0.012557	0.521762	0.719775	2.384132
Within groups	17.56836	730	0.024066			
Total	17.61858	734				

Table IV. One-way ANOVA test for difference between age groups means

ANOVA: single factor (0.05)

Summary

Groups	Count	Sum	Average	Variance
Female	385	135.0951	0.350896	0.021252
Male	350	133.487	0.381391	0.026612

ANOVA

Source of variation	SS	df	MS	*F*	*p*-value	*F* crit
Between groups	0.17049	1	0.17049	7.162323	0.007611	3.854176
Within groups	17.44809	733	0.023804			
Total	17.61858	734				

Table V. One-way ANOVA test for difference between gender means

Table VI.
One-way ANOVA test for difference between highest qualification means

ANOVA: single factor (0.05)						
Summary						
Groups		Count	Sum	Average	Variance	
Secondary school (Grade 12)		82	29.48339	0.359554	0.023719	
Graduated from college (diploma)		125	47.27635	0.378211	0.027872	
Graduated from university (B Degree)		163	57.39526	0.352118	0.020906	
Honours degree or post-graduate diploma		192	69.8821	0.363969	0.023401	
Masters degree		133	51.02487	0.383646	0.02456	
Doctorate		27	9.583841	0.354957	0.029044	
ANOVA						
Source of variation	SS	df	MS	*F*	*p*-value	*F* crit
Between groups	0.098738	5	0.019748	0.820581	0.53514	2.22661
Within groups	17.23081	716	0.024065			
Total	17.32955	721				

Table VII.
One-way ANOVA test for difference between experience means

ANOVA: single factor (0.05)				
Summary				
Groups	Count	Sum	Average	Variance
>10	516	196.1658	0.380166	0.024295
5-10	146	49.28081	0.33754	0.022761
<5	73	23.13552	0.316925	0.019571

ANOVA						
Source of variation	SS	df	MS	*F*	*p*-value	*F* crit
Between groups	0.397372	2	0.198686	8.44529	0.000237	3.008026
Within groups	17.22121	732	0.023526			
Total	17.61858	734				

Four different types of browsers ($n = 708$) yielded a large enough subset and acceptable criteria for the ANOVA (Table III). In this instance, the null hypothesis could be rejected indicating a statistically significant difference in population means and thus support for RBA based on browsers used.

Five different age groups ($n = 734$) yielded a large enough subset and acceptable criteria for the ANOVA (Table IV). However, the null hypothesis could not be rejected. Based on this test, there is no statistical evidence to support the proposal that users display different behaviour based on their age.

The gender samples yielded different means and variations, and this was supported by the ANOVA test (Table V). The null hypothesis could be rejected, lending support for the concept of differentiating based on gender.

It is rather important to point out that statistical evidence does not necessarily indicate good practice. It could indeed be ill conceived and not advisable for institutions

to use gender for RBA, as this may create perception problems beyond the potential value contribution.

Six different highest levels of qualifications ($n = 721$) yielded a large enough subset and acceptable criteria for the ANOVA (Table VI). Surprisingly, the null hypothesis could not be rejected, indicating no statistically significant difference in population means and thus no support for RBA based on user qualifications.

Three different Internet experience bins yielded a large enough subset and acceptable criteria for the ANOVA (Table VII), and in this instance, the null hypothesis could be rejected, indicating a statistically significant difference in population means and thus support for RBA based on years of Internet experience.

Table VIII contains a summary of the results of the tests for difference in variance. Based on the analysis, it can be inferred that there is a statistical difference in password performance for three of the five dependant variables analysed.

Firstly, the preferred browser could be an indicator of password behaviour, lending support for the potential to differentiate prior to identification based on the browser used. Secondly, gender and experience showed differences between category means, providing support for potential differential authentication based on these parameters. Interestingly enough, there was no statistical support for risk profiling based on highest level of qualification or the age of respondents.

8. Limitations of the research and recommendations

The following three limitations of the recommendations and hence the research have 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 by users, 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 privacy for online users.

The research does not aim to make a business case for different authentication based on risk profiling but rather provides statistically proof that it should at least be considered as a potential option to improve online security.

Test parameter	F	p-value	F crit	Interpretation
Browsers	7.9582	3.18 E-05	2.6175	Reject null hypothesis
Age	0.5218	0.71978	2.3841	Cannot reject null hypothesis
Gender	7.1623	0.00761	3.8542	Reject null hypothesis
Qualification	0.8206	0.53515	2.2266	Cannot reject null hypothesis
Internet experience	8.4452	0.00023	3.0080	Reject null hypothesis

Table VIII. Combined results of ANOVA test for all dependent variables

9. 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 while 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 *et al.*, 2013; Wahlberg *et al.*, 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 associated with Internet banking have always been a concern to the service providers and users. In studying factors that lead to the adoption of online banking, Yap *et al.* (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 such as a factor.

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. In addition, once authenticated the institutions may be in possession of demographical data about the user that could be useful to better understand the user and their risk profile. There clearly exists an opportunity for financial services institutions to create differentiated authentication based on the risk profile of their Internet banking customers.

References

Anderson, C.L. and R. Agarwal, R. (2010), "Practising safe computing: a multimethod empirical examination of home computer user security behavioral intentions", *MIS Quarterly*, Vol. 34 No. 3, pp. 613-643.

Brostoff, S. and Sasse, M.A. (2002), "Safe and sound: a safety-critical approach to security", *Proceedings of the New Security Paradigm Workshop 2001*, available at: 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, pp. 2-8.

Chiasson, S. and Biddle, R. (2007), "Issues in user authentication", CHI Workshop: Security User Studies: Methodology and Best Practices, 28 April-3 May, San Jose, CA.

Choubey, J. and Choubey, B. (2013), "Secure user authentication in Internet Banking: a qualitative survey", *International Journal of Innovation, Management and Technology*, Vol. 4 No. 2, pp. 198-203.

Ciampa, M., Mark, R. and Enamait, J. (2013), "A comparison of user preferences for browser password managers", *Journal of Applied Security Research*, Vol. 8 No. 4, pp. 455-466.

Conklin, A., Dietrich, G. and Walz, D. (2004), "Password-based authentication: a system perspective", *Proceedings of the 37th Annual Hawaii International Conference on System Sciences*, *IEEE Computer Society Washington, DC*, pp. 1-10.

Durkin, M. (2004), "In search of the internet-banking customer – exploring the use of decision styles", *The International Journal of Bank Marketing*, Vol. 22 No. 7, pp. 484-503.

Feig, N. (2007), "Authentication goes mobile: banks look to out-of-band authentication as customers seek enhanced online banking security", *Bank Systems + Technology*, Vol. 23, p. 23.

Furnell, S.M. (2005), "Authenticating ourselves: will we ever escape the password?", *Network Security*, Vol. 2005 No. 3, pp. 8-13.

Furnell, S.M. (2007), "An assessment of website password practices", *Computers and Security*, Vol. 26 Nos 7/8, pp. 445-451.

Furnell, S.M., Bryant, P. and Phippen, A.D. (2007), "Assessing the security perceptions of personal Internet users", *Computers and Security*, Vol. 26 No. 5, pp. 410-417.

Gaur, M.S., Patel, D. and Saini, A. (2013), "Insecurities within browser: issues and challenges", in *Proceedings of the 6th International Conference on Security of Information and Networks (SIN '13)*, *ACM*, *New York, NY*, pp. 458-458.

Gehringer, E.F. (2002), "Choosing passwords: security and human factors", *Technology and Society*, pp. 369-373.

Hunton, J.E., Bryant, S.M. and Bagranoff, N.A. (2004), *Core Concepts of Information Technology Auditing*, John Wiley & Sons, Inc., Hoboken, NJ.

Kaman, S., Swetha, K., Akram, S. and Varaprasad, G. (2013), "Remote user authentication using a voice authentication system", *Information Security Journal: A Global Perspective*, Vol. 22 No. 3, pp. 117-125.

McCloy, R.A., Campbell, J.P. and Cudeck, R. (1994), "A confirmatory test of a model of performance determinants", *Journal of Applied Psychology*, Vol. 79 No. 4, pp. 493-505.

Moscato, D.R. and Altschuller, S. (2012), "International perceptions of online banking security concerns", *Communications of the IIMA*, Vol. 12 No. 3, pp. 51-64.

Notoatmodjo, G. and Thomborson, C. (2009), "Passwords and Perceptions", *Proceedings of the Australasian Information Security Conference (AISC2009), Wellington, New Zealand*, *Conferences in Research and Practice in Information Technology*, Vol. 98, pp. 71-78.

Pfleeger, S.L. and D. D. Caputo, D.D. (2012), "Leveraging behavioral science to mitigate cyber security risk", *Computers & Security*, Vol. 31 No. 4, pp. 597-611.

Pisani, P.H. and Lorena, A.C. (2013), "A systematic review on keystroke dynamics", *Journal of the Brazilian Computer Society*, Vol. 19 No. 4, pp. 573-587.

Ravi, V., Carr, M. and Sagar, N.V. (2006), "Profiling of internet banking users in India using intelligent techniques", *Journal of Services Research*, Vol. 6 No. 2, pp. 61-73.

Rice, P. (2012), "Civil liability theories for insufficient security authentication in online banking", *DePaul Business & Commercial Law Journal*, Vol. 10 No. 3, pp. 439-460.

Riley, S. (2006), "Password security: what users know and what they actually do", *Usability News*, Vol. 8 No. 1, available at: http://psychology.wichita.edu/surl/usabilitynews/81/Passwords.asp (accessed 19 March 2013).

Tam, L., Glassman, M. and Vandenwauver, M. (2010), "The psychology of password management: a tradeoff between security and convenience", *Behaviour and Information Technology*, Vol. 29 No. 3, pp. 233-244.

Tassabehji, R. and Kamala, M.A. (2012), "Evaluating biometrics for online banking: the case for usability", *International Journal of Information Management*, Vol. 32 No. 5, pp. 489-494.

Traore, I., Woungang, I., Obaidat, M.S., Nakkabi, Y. and Lai, I. (2014), "Online risk-based authentication using behavioural biometrics", *Journal of Multimedia Tools and Applications*, Springer, pp. 575-602.

Usman, A.K. and Shah, M.H. (2013), "Strengthening e-banking security using keystroke dynamics", *Journal of Internet Banking and Commerce*, Vol. 18 No. 3, pp. 1-11.

Wahlberg, T., Paakkola, P., Wieser, C., Laakso, M. and Roning, J. (2013), "Kepler – raising browser security awareness", *Software Testing, Verification and Validation Workshops (ICSTW), 2013 IEEE Sixth International Conference on, 18-22 March*, pp. 435-440.

Weber, J.E., Guster, D., Safanov, P. and Schmidt, M.B. (2008), "Weak password security: an empirical study", *Information Security Journal: A Global Perspective*, Vol. 17 No. 1, pp. 45-54.

Wessels, P.L. and Steenkamp, L. (2007), "Assessment of current practices in creating and using passwords as a control mechanism for information access", *South African Journal of Information Management*, Vol. 9 No. 2.

Wolfe, D. (2011), "Bank sharpens authentication", *American Banker*, Vol. 10 No. 22.

Yan, J., Blackwell, A., Anderson, R. and Grant, A. (2004), "Password memorability and security: empirical results", *Security and Privacy, IEEE*, Vol. 2 No. 5, pp. 25-31.

Yap, K.B., Wong, D.H., Loh, C. and Bak, R. (2010), "Offline and online banking – where to draw the line when building trust in e-banking?", *International Journal of Bank Marketing*, Vol. 28 No. 1, pp. 27-46.

Corresponding author
Martin Butler can be contacted at: martin.butler@usb.ac.za